



LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Toimitilaturvallisuuden toteuttamismallin luominen

Syri, Minna

2016 Laurea



Laurea-ammattikorkeakoulu

Toimitilaturvallisuuden toteuttamismallin luominen

Minna Syri
Turvallisuusosaamisen
koulutusohjelma
Opinnäytetyö
Marraskuu, 2016

Syri Minna

Toimitilaturvallisuuden toteuttamismallin luominen

Vuosi 2016 Sivumäärä 82

Organisaatioturvallisuudella on tärkeä osuus organisaation toimintaedellytysten ja kilpailukyvyn ylläpitämisessä. Organisaation turvallisuudentilan ylläpitäminen ja kehittäminen ovat kuitenkin jatkuvien haasteiden kohteena: muun muassa turvallisuutta uhkaavien riskien monimuotoistuminen sekä tiukentuneet kansainväliset ja kansalliset turvallisuusvaatimukset vaativat organisaatioiden riskienhallintaprosessien jatkuvaa kehittämistä.

Monien muiden organisaatioiden tapaan myös tämän opinnäytetyön kohdeorganisaatiossa Tullissa on toiminnan turvallisuuden tason merkitys organisaation toimintakyvylle yhä merkittävämmässä roolissa. Kohdeorganisaation turvallisuutta koskevien vaatimusten lisääntyminen on tuonut mukanaan haasteita organisaatioturvallisuuden toteuttamiselle turvallisuuden eri osaluilla. Turvallisuusvaatimuksia on asetettu esimerkiksi valtioneuvoston asetuksessa tietoturvallisuudesta valtioneuvoston hallinnossa, jossa säädetään valtioneuvoston viranomaisten asiakirjojen luokittelusta, sekä luokiteltujen asiakirjojen tietoturvallisuusvaatimuksista muun muassa tilaturvallisuutensa osalta.

Opinnäytetyön tavoitteena on ollut kehittää kohdeorganisaation käyttöön toimitilaturvallisuuden toteuttamismalli, jonka tarkoituksena on auttaa määrittämään ja toteuttamaan toimitilojen tarpeenmukaisen turvallisuustason saavuttamiseksi tarvittavat toimenpiteet. Toimitilaturvallisuuden toteuttamismallin vaatimukset pohjautuvat pitkälti valtioneuvoston asetukseen tietoturvallisuudesta valtioneuvoston hallinnossa, jonka lisäksi vaatimusmäärittelyssä on riskiperusteisesti huomioitu kohdeorganisaation toimintaan ja tiloihin liittyviä erityispiirteitä ja -tarpeita. Riskianalyysin suorittamiseksi ja organisaation sisäisten tilaturvallisuusvaatimusten määrittämiseksi on suoritettu organisaation toimitilojen turvallisuudentilan nykytilakartoitus käyttäen pääasiallisena tutkimusmenetelmänä kyselytutkimusta.

Toimitilaturvallisuuden nykytilakartoituksen perusteella toimitilojen turvallisuudentason yhtenäistämisen apuvälineenä hyödynnettävälle toteuttamismallille on tarvetta. Toteuttamismallia on tarkoitus hyödyntää paitsi olemassa olevien tilojen turvallisuuden tilan kehittämisessä, mutta ennen kaikkea myös uusien toimitilojen ja muutosten kohteena olevien tilojen rakentamis- ja turvallisuussuunnittelussa. Tarve toimitilaturvallisuuden toteuttamismallille oli selkeästi työelämälähtöinen, jota kautta myös työn toteuttamismalli, tutkimuskysymykset ja sisältö pitkälti määräytyivät.

Asiasanat: Toimitilaturvallisuus, fyysinen turvallisuus, riskienarviointi, tietoturvallisuusasetus, tietoturvallisuus

Ohjaaja: Seppo Leminen, Laurea

Syri Minna

Developing a tool for improving an organization's premises security

Year	2016	Pages	82
------	------	-------	----

Corporate security has an important role in maintaining an organization's capacity and competitiveness. Maintaining and developing the organization's security and safety is challenging: the increasing diversity and increasing of the security risks and also tighter international and national security requirements requires continuous development of the organization's risk management processes.

Corporate security is a more and more relevant actor in organizations' operations quality and continuity. Successful security risk management is essential for the organization's performance, but increasing security requirements cause challenges for implementing demanded security actions in different sectors of safety and security. The Government Decree on information security in central government contains provisions on the general information security requirements. The requirements include regulations for classifying documents in central government and regulations for the information security requirements corresponding to the classification and applicable to the handling of documents. Also the target organization of this thesis must accomplish the requirements of the Government Decree on information security.

The aim of the thesis is to develop a planning and implementation tool to help improve the target organization's premises security. It is important to be able to define the necessary requirements and actions needed to accomplish and maintain the required security level. The requirements of the planning and implementation tool are based mainly on the Government's Decree on information security in central government. Internal security requirements of the target organization are taken into account based on internal risk assessments and needs. Performing the security risk assessment includes mapping the present state of premises security. The mapping of the present state was made by using questionnaire as a research method.

The result of the mapping of the present state was that there is an obvious need to standardize the processes of developing and maintaining the realization of the organization's premises security. The planning and implementation tool of premises security will be utilized to raise the level of premises security in the target organization. The tool will also be used when developing new premises and planning premises security. The need for the tool is based on needs of the target organization, which also directed the realization and content of the development project.

Key words: Premises security, physical security, risk assessment, information security

Supervisor: Seppo Leminen, Laurea

Executive Summary

Organisaatioiden turvallisuuden tilan ylläpitäminen ja kehittäminen ovat jatkuvien haasteiden kohteena. Toimijoiden turvallisuutta uhkaavien riskien monimuotoistuminen sekä organisaatioiden tukitoimintojen ulkoistamisen myötä lisääntynyt sidosryhmäyhteistyö vaativat toimijoiden riskienhallintaprosesseilta jatkuvaa kehittämistä ja kehittymistä. Lisäksi kansalliset, kansainväliset ja sidosryhmien edellyttämät tiukentuneet turvallisuusvaatimukset tuovat omat lisähaasteensa riskienhallintatyön toteuttamiselle.

Ei myöskään riitä, että organisaatio kykenee tunnistamaan toimintaansa kohdistuvat riskit, vaan oleellista on kyetä huolehtimaan riskienhallintatoimenpiteiden jalkauttamisesta käytäntöön. Riskien ja kehittämiskohteiden tunnistamiseksi ja tarpeenmukaisten toimenpiteiden suunnittelemiseksi organisaation voi olla tarpeen kehittää käyttöönsä erilaisia turvallisuusriskienhallintatyökaluja. Turvallisuustoimenpiteiden mitoittaminen mahdollisimman kustannustehokkaalle tasolle on tärkeää, jotta mahdollistetaan riittävän turvallisuustason toteuttaminen, huolimatta toimijoihin mahdollisesti kohdistuvista kustannussäästötarpeista.

Opinnäytetyön kehittämiskohteena oli luoda työn kohdeorganisaationa toimivan Tullin käyttöön *toimitilaturvallisuuden toteuttamismalli*, jonka avulla voidaan varmistua Tullin toimitilojen täyttävän tarpeenmukaiset tilaturvallisuusvaatimukset. Toteuttamismallin tilaturvavaatimukset perustuvat pitkälti valtioneuvoston asetukseen tietoturvallisuudesta valtionhallinnossa (681/2010). Lisäksi vaatimusmäärittelyssä on huomioitu Tullin sisäiset turvallisuusvaatimukset sekä osana opinnäytetyötä tehdyn toimitilojen nykytilakartoituksen perusteella tunnistetut tilaturvallisuuden kehittämistarpeet.

Organisaation tilaturvallisuuden nykytilakartoitus

Tullin toimitilaturvallisuuden nykytilan ja kehittämistarpeiden määrittämiseksi suoritettiin toimipaikoille kyselytutkimus. Kysely kohdistui yli sataan Tullin käytössä olevaan toimitilaan, ja tarkoituksena oli saada kartoitettua toimitilojen tilaturvallisuusvyöhykejaottelu sekä tilojen turvallisuusjärjestelmät. Tutkimuksen kyselylomakkeet lähetettiin hallintopalvelupäälliköiden kautta toimitilaryhmän paikallisille vastuuhenkilöille, jotka täyttivät tilojen pohjakuviin vaaditut tiedot turvallisuusvyöhykkeistä ja turvallisuustekniikkaa koskien.

Kyselylomakkeen lisäksi toimipaikoille annettiin ohjeita tilojen turvallisuusvyöhykeluokittelun suorittamiseksi ja turvallisuustekniikan kartoittamiseksi myös puhelimitse ja sähköpostitse. Näin pyrittiin varmistamaan tutkimuksen avulla saatujen nykytilatietojen oikeellisuus ja kattavuus. Tilojen turvallisuutta koskevien pohjatietojen paikkansapitävyys oli tärkeää, koska

nykytilatietojen perusteella tunnistettiin tilakohtaisesti tarvittavat kehitystoimenpiteet vaaditun tilaturvallisuuden tason saavuttamiseksi.

Kartoituksen suorittamisessa haasteelliseksi osoittautui etenkin tilakohtaisen turvallisuusvyöhykejaottelun suorittaminen, jota koskevia periaatteita ei organisaatiossa riittävällä tarkkuudella tunnettu. Tullin turvallisuusvyöhykejaottelun periaatteena on, että valtioneuvoston tietoturvallisuusasetuksen mukaisesti tilat jaetaan turvallisuusvyöhykkeisiin tiloissa käsiteltävän ja säilytettävän tiedon suojaustasoluokituksen perusteella. Tilojen sisällä on lisäksi mahdollista suorittaa toimintokohtaista tasoluokittelua, jonka avulla varmistutaan tiedonsaanti-tarpeen periaatteen toteutuvan, eli että tiedot ovat pelkästään niiden henkilöiden saatavilla, joilla on tarve kyseisiä tietoja käsitellä.

Huomionarvoista kartoituksen avulla saaduissa tuloksissa oli, että tilaturvallisuuden tasossa on havaittavissa huomattavia eroja toimipaikkojen välillä. Valtakunnallisesti esiintyi hyvin eritasoisia ratkaisuja turvallisuusvyöhykeluokittelun osalta, jonka lisäksi ilmeni tilojen turvallisuusteknisten ratkaisujen olevan osin puutteellisia ja vailla yhtenäistä linjaa. Tulosten perusteella voitiin todeta selkeä tarve tilaturvallisuuden tason ja sen toteutusmallien yhdenmukais-tamiselle.

Organisaation tilaturvallisuuden tason kehittäminen

Nykytilakartoituksen tulosten perusteella tunnistettiin ja kuvattiin tarpeenmukaisen turvallisuustason saavuttamiseksi vaadittavat tilaturvallisuuden kehittämistarpeet. Kehittämistarpeet kerättiin taulukkoon toimitilakohtaisesti hyvin yksityiskohtaisella tasolla, mikä mahdollisti taulukon hyödyntämisen turvallisuushankintojen suunnittelun apuna.

Yksityiskohtaisten tilaturvallisuuspuutteiden lisäksi opinnäytetyössä pyrittiin tunnistamaan organisaation tilaturvallisuuden tasoon vaikuttavia yleisiä tekijöitä. Työssä kuvatut tilaturvallisuuden parantamiseen tähtäävät yleisen tason toimenpiteet perustuvat organisaatioturvallisuuden yleisiin teorioihin, eivätkä ne näin ollen ole kohdeorganisaation virallisia kehittämis-kohteita. Opinnäytetyön tutkimustulosten ja taustateorian perusteella tunnistettuja tilaturvallisuuden kehittämishaasteita ovat turvallisuusratkaisuiden etukäteissuunnittelun ja turvallisuusjärjestelyjen yhdenmukaisuuden parantaminen sekä turvallisuustietoisuuden lisääminen.

Organisaation ennakoivan turvallisuussuunnittelun tavoitteena on huomioida tilaturvallisuudelle asetetut vaatimukset jo tilasuunnitteluvaiheessa. Toimintojen sijoittamista koskevat suunnitelmat ja tilan turvallisuusratkaisut tulisi kyetä linjaamaan riittävän yksityiskohtaisella tasolla jo tilahankkeen alkuvaiheessa. Koska tilojen toiminnalliset, rakenteelliset ja tekniset turvallisuusratkaisut ovat toisistaan riippuvaisia, on tilaturvallisuussuunnittelua tärkeä edistää

kokonaisuutena. Ennakkoon suunniteltujen ratkaisujen avulla pyritään saavuttamaan kustannustehokkaasti tarpeenmukainen tilaturvallisuustaso.

Toisena yleisen tason haasteena työssä nähtiin tarve tilaturvallisuuden toteuttamisen yhdenmukaistamiselle. Puutteellinen turvallisuussuunnitteluprosessi johtaa helposti myös siihen, että toimipaikkojen turvallisuusratkaisuille ei kyetä muodostamaan yhdenmukaista toteutusmallia. Tällöin organisaation tilaturvallisuuden taso vaihtelee alueittain ja toimipaikoittain, mikä hankaloittaa organisaatitasoisen tilaturvallisuusmallin ylläpitämistä ja kehittämistä. Myös henkilöstön toiminnan kannalta on haasteellista, että toimipaikkojen välillä on merkittäviä eroja tilaturvallisuusratkaisuissa ja muissa turvallisuuskäytännöissä.

Kuitenkin vaikka tiloihin kyettäisiin suunnittelemaan ja toteuttamaan tarkoituksenmukaiset tilaturvallisuusratkaisut, on tilaturvallisuuden tason ylläpitäminen viimekädessä riippuvaista henkilöstön asenteesta ja toiminnasta. Edistyneimmätkin turvatekniset järjestelyt eivät ole riittäviä, mikäli henkilöstö ei ole tietoinen turvallisuustoimien toteuttamiseen liittyvistä ohjeista. Organisaation johdon vastuulla on määrittää paitsi osata määrittää ja toteuttaa turvallisuuden tavoitela, mutta myös pystyä kouluttamaan ja sitouttamaan henkilökunta noudattamaan haluttuja turvallisuuskäytäntöjä. Organisaation puutteellinen turvallisuuskulttuuri voi vaarantaa tehokkaatkin turvatekniset tilaturvallisuusratkaisut.

Toimitilaturvallisuuden toteuttamismalli

Tullitoimipaikoille suoritettujen nykytilakartoituksen tuloksia sekä tulosten perusteella tehtyjä johtopäätöksiä hyödynnettiin luotaessa Tullin tilaturvallisuuden kehittämiseen tähtäävä toimitilaturvallisuuden toteuttamismalli. Vaikka toteuttamismalli pohjautuu pääasiallisesti valtioneuvoston tietoturvallisuusasetukseen, pystyttiin toimipaikkojen tilaturvallisuuskartoituksen tulosten avulla varmistamaan toteuttamismallin vaatimusten olevan suhteutettu kohdeorganisaation tarpeiden ja vaatimusten mukaisiksi. Näin vaatimukset saatiin kohdistettua koskemaan nimenomaan Tullin toimintaan ja toimitiloihin liittyviä turvallisuusriskejä.

Toteuttamismallin sisältämien organisaation sisäisten turvallisuusvaatimusten määrittely perustuu nykytilakartoituksen avulla saatujen tulosten lisäksi myös organisaation toimintoihin ja toimipaikkoihin liittyvien turvallisuusriskien analysointiin. Riskikartoituksen osalta on huomionarvoista muun muassa tilojen sijainti ja toimintaympäristö; muita vaikuttavia tekijöitä voivat olla esimerkiksi yhteiskäyttöisten tilojen muut toimijat, ympäröivien tilojen ulkopuoliset toimijat sekä tiloissa tapahtuvan toiminnan laatu ja laajuus.

Toimitilaturvallisuuden toteuttamismallia käytetään työkaluna Tullin toimitilojen turvallisuussuunnittelussa

Työn kehittämiskohteena olleelle toimitilaturvallisuuden toteuttamismallille oli selkeät työelämälähtöiset tarpeet, jotka auttoivat määrittämään toteuttamismallin sisältöä. Tullissa on meneillään ja tulossa suuri määrä toimitilahankkeita, joiden turvallisuussuunnittelua ja turvallisuusratkaisuiden toteuttamista toimitilaturvallisuuden toteuttamismallin on tarkoitus auttaa tehostamaan ja yhdenmukaistamaan. Tilan käyttömukavuus ja turvallisuus eivät saisi olla toisiaan pois sulkevia ominaisuuksia, vaan tilat tulisi yhteistyössä kyetä suunnittelemaan sekä toimiviksi että turvallisiksi. Ennakoiva turvallisuussuunnittelu ja suunnittelua ohjaavat työkalut ovat oleellisen tärkeässä asemassa yhteistyön onnistumisen varmistamisessa ja halutun lopputuloksen saavuttamisessa.

Tulevaisuudessa mallia on tarkoitus hyödyntää myös auditointityökaluna olemassa olevien tilojen turvallisuuden tilan kehittämisessä tarpeenmukaiselle tasolle. Toteuttamismallin laajempi käyttö sekä uusien että olemassa olevien tilojen turvallisuussuunnittelussa auttaa parantamaan tilaturvallisuuden toteuttamisen yleisiä haasteita, eli turvallisuussuunnittelun ennakointikykyä, turvallisuusratkaisujen yhdenmukaisuutta sekä organisaation turvallisuustietoisuutta. Toteuttamismallin käyttöönoton myötä se väistämättä lisää organisaation tietoisuutta tilaturvallisuutta koskien, ja auttaa näin turvallisuustoimenpiteiden viemisessä käytäntöön.

Tulevaisuuden kehittämistarpeet

Jatkossa toteuttamismallia on tarpeen kehittää siten, että sitä voidaan hyödyntää myös käsiteltäessä Tullin toimitilaturvallisuusvaatimuksia ulkopuolisten toimijoiden kanssa. Mallia tulee kyetä käyttämään tehtäessä tila- ja turvallisuussuunnittelua esimerkiksi tilojen omistajien, vuokranantajien, urakoitsijoiden ja muiden mahdollisten sidosryhmien kanssa. Mallista on tarpeen tehdä supistettu versio ulkoisten sidosryhmien hyödynnettäväksi, jotta Tullin toimitilaturvallisuusvaatimukset saadaan soveltuvin osin vietyä heidän tietoisuuteensa, ja näin toteutettua vaaditut toimenpiteet käytännössä.

Toinen toteuttamismalliin liittyvä kehittämistarve liittyy Tullin uudistuviin työskentelyympäristöihin. Valtion toimitilastrategia kannustaa toimitilojen muuntojoustavuuteen muun muassa monitoimityötilojen, nimeämättömien työpisteiden ja etätöiden avulla. Uusien työskentelyympäristöjen käyttöönotto vaatii uudistumista myös tilojen turvallisuusratkaisuilta, jotta tarkoituksenmukaisesta tilaturvallisuuden tasosta voidaan varmistua myös uudentyyppisten tilojen ja työskentelytapojen osalta. Toimitilaturvallisuuden toteuttamismallia tulee tulevaisuudessa kyetä laajentamaan siten, että myös nämä uudenlaiset työskentelytilat ja -tavat pystytään toteuttamaan siten, että ne näyttävät tarpeelliset turvallisuusvaatimukset.

Sisällys

1	Johdanto	11
1.1	Työn tausta	11
1.2	Työn tavoite ja tutkimuskysymykset	12
1.3	Työn rajaus	14
1.4	Työn rakenne ja eteneminen	14
2	Organisaatioturvallisuus	16
2.1	Organisaatioturvallisuuden toteuttamisen yleisiä tavoitteita	17
2.2	Organisaatioturvallisuuden nykytilanne Suomessa	17
2.3	Organisaatioturvallisuuden toteuttamisen haasteita	19
2.4	Turvallisuuden johtaminen	21
2.5	Turvallisuuden riskienhallintaprosessi	23
3	Toimitilaturvallisuus	25
3.1	Toimitilaturvallisuuden rooli tietoturvallisuuden toteuttamisessa	25
3.2	Toimitilaturvallisuuden kehittäminen	27
3.3	Toimitilaturvallisuuden toteuttamiseen vaikuttavia organisaatioturvallisuuden muita osa-alueita	31
3.3.1	Tietoturvallisuus	31
3.3.2	Henkilöstöturvallisuus	32
3.3.3	Sidosryhmäturvallisuus	33
4	Tullin toimitilaturvallisuuden nykytilanne	34
4.1	Toiminta ja toimitilat	34
4.2	Tilojen turvallisuusvyöhykejaottelu	35
4.3	Turvallisuusvyöhykkeiden tilaturvallisuusvaatimukset	37
4.4	Asiakirjojen suojaustasoluokittelu	38
4.5	Valtion toimitilastrategia	41
5	Keskeiset asetukset ja standardit	41
5.1	Laki viranomaisten toiminnan julkisuudesta	42
5.2	Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa	42
5.3	Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta	43
5.4	Toimitilojen tietoturvaohje	43
5.5	Kansallinen turvallisuusauditointikriteeristö	44
5.6	Finanssialan keskusliiton standardit ja ohjeet	44
6	Kehittämistyön toteuttaminen	45
6.1	Tutkimuksellinen kehittäminen	45
6.2	Tutkimusaineiston valinta ja keräämisen aikataulu	46
6.3	Tiedonhankinnan menetelmät	48

	6.3.1 Kyselytutkimus.....	49
	6.3.2 Havainnointi.....	51
7	Tutkimustulokset.....	52
	7.1 Tutkimustulosten yhteenveto.....	52
	7.2 Tullitoimipaikkojen toimitilaturvallisuuden nykytila.....	54
	7.3 Toimitilaturvallisuuden todetut puutteet ja kehityskohteet.....	56
	7.4 Todettujen puutteiden kehittämistoimenpiteet.....	57
	7.4.1 Ennakoiva turvallisuussuunnittelu.....	57
	7.4.2 Turvallisuusjärjestelyjen yhdenmukaisuus.....	58
	7.4.3 Turvallisuustietoisuuden lisääminen.....	59
	7.5 Toimitilaturvallisuuden toteuttamismalli.....	61
	7.5.1 Toteuttamismallin taustat.....	62
	7.5.2 Toteuttamismallin turvallisuusvyöhykejaottelu.....	66
8	Päätelmät.....	67
	8.1 Johtopäätökset.....	67
	8.2 Tutkimuksen luotettavuus ja arviointi.....	71
	8.3 Jatkotutkimusmahdollisuudet.....	72
	Painetut lähteet.....	74
	Sähköiset lähteet.....	76
	Kuviot.....	78
	Liitteet.....	80

1 Johdanto

Luvussa on kuvattu opinnäytetyön aiheen taustaa sekä työn tavoitteita. Lisäksi luvussa on kuvattu yksityiskohtaiset tutkimuskysymykset, johon työssä on haettu vastauksia työn kehittämiskohteen tarkoituksenmukaisen lopputuloksen saavuttamiseksi.

1.1 Työn tausta

Organisaatioiden turvallisuuden tason ylläpitäminen ja kehittäminen kohtaavat nykyaikana jatkuvia haasteita. Turvallisuutta uhkaavien riskien monimuotoistuminen, toimijoilta vaaditut kustannussäästöt sekä organisaatioiden tukitoimintojen ulkoistamisen myötä lisääntynyt sidosryhmäyhteistyö vaativat organisaatioiden riskienhallintaprosesseilta ja -toiminnoilta jatkuvaa kehittämistä ja kehittymistä. Lisäksi kansalliset, kansainväliset ja sidosryhmien edellyttämät tiukentuneet turvallisuusvaatimukset tuovat lisäpainetta riskienhallintatyön toteuttamiselle.

Ei myöskään riitä, että organisaatio kykenee tunnistamaan sen toimintaan kohdistuvat riskit, vaan oleellista on kyetä huolehtimaan myös riskienhallintatoimenpiteiden jalkauttamisesta käytäntöön. Riskien ja kehittämiskohteiden tunnistamiseksi ja tarpeenmukaisten toimenpiteiden suunnittelemiseksi organisaatioiden voi olla tarpeen kehittää käyttöönsä erilaisia turvallisuusriskienhallintatyökaluja.

Organisaatioturvallisuus on tärkeä osa-alue organisaation toimintaedellytysten ja kilpailukyyn ylläpitämisessä. Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI:n mukaan organisaation turvallisuuden tasolla voidaan nähdä olevan suora vaikutus organisaation toimintakykyyn, palveluiden kehittämiseen ja tuottamiseen, toiminnan jatkuvuuden varmistamiseen sekä laadunhallintaan (Toimitilojen tietoturvaohje 2013).

Monien muiden organisaatioiden tapaan myös tämän opinnäytetyön kohdeorganisaatiossa Tulissa on toiminnan turvallisuuden tason merkitys organisaation toimintakyvyn ylläpitämiselle yhä merkittävämmässä roolissa. Organisaation toimintojen sähköistyminen ja turvallisuutta uhkaavan riskikentän laajentuminen aiemmasta ovat tuoneet mukanaan haasteita turvallisuuden toteuttamiselle. Etenkin tietoturvallisuuden osa-alueelle kohdistuu haasteita yhä useammasta suunnasta, kun toiminnan jatkuvuuden varmistamiseksi on tarpeenmukaisten tietojen saatavuudesta ja eheydestä huolehdittava, ja toisaalta taas organisaation suojattavien tietojen päätyminen ulkopuolisen haltuun voisi olla hyvin haitallista koko organisaatiolle ja sen sidosryhmille.

Apuna valtionhallinnon toimijoiden turvallisuuden tilan kehittämisessä ja ylläpitämisessä toimii valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010). Asetuksessa

säädetään valtionhallinnon viranomaisten asiakirjojen luokittelusta, sekä luokiteltujen asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista. Tietoturvallisuusasetuksen mukaisesti valtionhallinnon toimijoiden on tietoturvallisuutensa riittävän tason varmistamiseksi huolehdittava siitä, että luokiteltujen asiakirjojen käsittely- ja säilytystilojen valvonta ja suojaus ovat riittävällä tasolla.

1.2 Työn tavoite ja tutkimuskysymykset

Opinnäytetyön kehittämiskohteen tehtävänasettelu, tutkimuskysymykset ja tavoitteet määrytyivät hyvin pitkälti työelämälähtöisen tarpeen perusteella. Työn lähtökohtina toimivat kohdeorganisaation tilaturvallisuuden nykytila sekä organisaation toimitilaturvallisuuden tasolle asetetut vaatimukset, jotka vaikuttivat omalta osaltaan myös työn tutkimusstrategian ja -menetelmien valintaan. Työn varsinainen teoriapohja ja tutkimuskysymykset perustuvat pitkälti valtioneuvoston asetukseen tietoturvallisuudesta valtionhallinnossa, kohdeorganisaation nykytilakartoituksen avulla saatuihin tietoihin sekä organisaatioturvallisuuden yleisiin teorioihin. Opinnäytetyön teoreettinen viitekehys siis pohjautuu pääasiallisesti valtioneuvoston tietoturvallisuusasetukseen, mutta teoriapohja kokonaisuudessaan muodostuu kaikkien edellä mainittujen taustatekijöiden summana.

Opinnäytetyön vahvasti työelämälähtöisenä *tavoitteena oli luoda kohdeorganisaation käytöön toimitilaturvallisuuden toteuttamismalli*. Toteuttamismallin tarve ja sisältö pohjautuvat jo aiemmin mainittuun valtioneuvoston tietoturvallisuusasetukseen sekä Tullin sisäisen riskianalyysin ja tarpeiden perusteella laadittuihin vaatimusmäärittelyihin eri toimintoja ja tiloja koskien. Tietoturvallisuusasetuksen ja sen toteuttamista ohjaavan toimitilojen tietoturvaohjeen (Toimitilojen tietoturvaohje 2/2013) lisäksi toteuttamismallin tilaturvallisuusvaatimusten määrittelyssä oli tarpeen huomioida kohdeorganisaation toimintaan liittyviä erityispiirteitä ja -tarpeita. Kohdeorganisaation tilaturvallisuutta koskevan riskienarvioinnin suorittamiseksi ja organisaation sisäisten turvallisuusvaatimusten määrittelemiseksi suoritettiin toimitilojen nykytilakartoitus, jonka tuloksia peilattiin tiloihin kohdistuviin turvallisuusvaatimuksiin ja organisaatioturvallisuuden toteuttamisen yleisiin taustateorioihin.

Organisaation sisäisten riskiarviointien perusteella on valtioneuvoston tietoturvallisuusasetuksen yleisiin vaatimuksiin tehty organisaation sisäisiä tarpeita vastaavia tila- ja toimintokohtaisia tarkennuksia. Nämä sisäiset toimitilaturvallisuusvaatimukset kuvataan kehittämistehtävän tuloksena syntyvässä toimitilaturvallisuuden toteuttamismallissa, jonka yksityiskohtaista sisältöä ei kuitenkaan ole tarkoituksenmukaista esitellä tämän opinnäytetyön yhteydessä. Opinnäytetyön tarkoituksena on esitellä prosessi, taustat, nykytilakartoitus sekä teoriapohja, joiden perusteella toteuttamismallin sisältö on muotoutunut.

Taulukossa 1 on kuvattu yksityiskohtaiset tutkimuskysymykset, joihin opinnäytetyössä on haettu vastauksia.

Tutkimuskysymys	Toimenpiteet ja tavoite
Mikä on Tullin toimipaikkojen toimitilaturvallisuuden nykytila? (luku 7.2.)	<ul style="list-style-type: none"> • Nykytilakartoituksen tavoitteena on selvittää tiedot toimipaikkojen turvallisuusvyöhykejaottelusta sekä yksityiskohtaiset tiedot tilojen turvallisuusjärjestelyistä • Tutkimusmenetelmänä käytetään kyselytutkimusta, tarpeen mukaan tarkennetaan kyselytutkimuksen vastauksia haastattelun ja havainnoinnin keinoin
<p>Mitkä ovat Tullin toimitilaturvallisuuden puutteet ja kehittämiskohteet? (luku 7.3.)</p> <p>Mitkä ovat todettuja puutteita selittäviä taustatekijöitä? (luku 7.4.)</p>	<ul style="list-style-type: none"> • Nykytilakartoituksen tulosten perusteella kuvataan puutteet ja kehittämiskohteet Tullin toimitilaturvallisuuden nykytilassa • Tilaturvallisuuden tavoitetilana toimivat valtioneuvoston asetus tietoturvallisuudesta valtioneuvoston asetus -mukaiset vaatimukset sekä Tullin sisäiset tilaturvallisuusvaatimukset • Pyritään tunnistamaan ja kuvaamaan puutteisiin johtaneita taustatekijöitä, perustaen pohdinta organisaatioturvallisuuden yleisiin teorioihin
Millainen toimitilaturvallisuuden toteuttamismalli auttaa saavuttamaan tiloille asetettujen turvallisuusvaatimusten mukaisen lopputuloksen? (luku 7.5.)	<ul style="list-style-type: none"> • Kehitetään toimitilaturvallisuuden toteuttamismalli, jonka avulla pyritään jo tilaturvallisuussuunnitteluvaiheessa tunnistamaan ja mittaamaan tarvittavat tilaturvallisuusratkaisut • Tilaturvallisuuden tavoitetilana toimivat valtioneuvoston asetus tietoturvallisuudesta valtioneuvoston asetus -mukaiset vaatimukset sekä Tullin sisäiset toimitilaturvallisuusvaatimukset

Taulukko 1: Työn tutkimuskysymykset

Työn varsinaisena kehittämiskohteena olevan toimitilaturvallisuuden toteuttamismallin tavoitteena on suhteuttaa valtioneuvoston tietoturvallisuusasetuksen vaatimukset kohdeorganisaation omien vaatimusten ja toimintojen asettamien tarpeiden mukaisiksi. Luotava toteuttamismalli ei siis ole täysin yhteneväinen tietoturvallisuusasetuksen vaatimusten kanssa, vaan vaatimukset räätälöidään riskiperusteisesti vastaamaan kohdeorganisaation tarpeita siten,

että organisaation toimintoihin liittyvät erityispiirteet tulevat huomioiduksi riittävällä tarkkuudella.

1.3 Työn rajaus

Opinnäytetyön sisältö keskittyy toimitilaturvallisuuden osa-alueeseen. Toimitilojen fyysiseen turvaamiseen kuuluvien toimenpiteiden avulla pyritään varmistamaan, että kohdeorganisaation tilaturvallisuus on tarpeenmukaisella tasolla. Kohdeorganisaation toimitilaturvallisuuden tavoitetilaksi on tässä työssä asetettu valtioneuvoston asetuksen tietoturvallisuudesta valtiollahinnossa vaatimukset, joita täydennetään asetuksen täytäntöönpanon tueksi annetussa toimitilojen tietoturvaohjeessa, sekä organisaation sisäisen riskianalyysin perusteella organisaation toimitilaturvallisuudelle asetetut vaatimukset.

Opinnäytetyössä organisaation turvallisuutta käsitellään toimitilaturvallisuuden näkökulmasta. Fyysisen toimitilaturvallisuuden tavoitteena on suojata organisaation suojattavat arvot. Esimerkiksi tietoturvallisuuden osalta pyritään tällöin varmistamaan organisaation käsittelemien tietojen ja tietojärjestelmien vaatiman käyttöympäristön turvallisuus toimitilojen turvallisuusjärjestelyjen keinoin. Organisaation toimitilaturvallisuutta pyritään toteuttamaan pääasiassa erilaisista rakenteellisten ja teknisten suojauskeinojen avulla.

Organisaatioturvallisuuden osa-alueista opinnäytetyössä keskitytään käsittelemään pelkästään toimitilaturvallisuuden osa-alueita ja siihen liittyviä vaatimuksia. Työhön sisältyvässä toimitilojen turvallisuudentilan nykytilakartoituksessa ja työn tuloksena syntyvässä toimitilaturvallisuuden toteuttamismallissa ei myöskään huomioida muita organisaatioturvallisuuden osa-alueita. Organisaatioturvallisuuden eri osa-alueilla toteutettavia toimenpiteitä on lyhyesti sivuttu ainoastaan siltä osin, kuin niillä on liittymäpintaa toimitilaturvallisuuden toteuttamiseen tai kehittämiseen.

Työssä käsiteltävät toimitilaturvallisuuden vaatimukset pohjautuvat pitkälti valtioneuvoston asetuksen tietoturvallisuudesta valtiorahinnossa mukaisiin toimitilaturvallisuusvaatimuksiin sovellettuna Tullin sisäisillä turvallisuusvaatimuksilla, eikä rakenteellisia tai muita fyysiseen toimitilaturvallisuuteen liittyviä vaatimuksia ole huomioitu asetuksen ulkopuolisin osin. Muun muassa rakentamiseen, työturvallisuuteen sekä tilojen palo- ja pelastusturvallisuuteen liittyvät vaatimukset on lähtökohtaisesti rajattu kehittämistyön ulkopuolelle, vaikka niillä käytännön elämässä onkin oleellisen tärkeitä yhtymäkohtia tilaturvallisuuden toteuttamiseen.

1.4 Työn rakenne ja eteneminen

Opinnäytetyön johdantoluvussa kuvataan organisaatioturvallisuuden nykytilaa Suomessa, sekä käydään yleisellä tasolla läpi organisaation turvallisuuden tilan kehittämiseen tähtäviä toi-

mia. Lisäksi luvussa yksilöidään toimitilojen fyysisen turvallisuuden merkitystä organisaation tietoturvallisuuden toteuttamisen ja kehittämisen osalta.

Ensimmäisessä luvussa on kirjattu opinnäytetyön yleiset tavoitteet sekä tutkimukselliselta kannalta että työelämän tarpeiden osalta. Tutkimusongelmat, joihin työssä on tarkoitus hakea vastauksia, kuvataan yksityiskohtaisella tasolla. Myös työn aiheen rajausta on kuvattu ja perusteltu ensimmäisessä luvussa.

Työn toisessa ja kolmannessa luvussa esitellään työn aihealueeseen liittyvää teoriakehystä. Tutkimuksen aihepiiriin sisältyy organisaatioturvallisuuden toteuttaminen, sekä erityisesti toimitilaturvallisuus ja sen tila kehittäminen ja ylläpitäminen. Teoriaosuudessa kuvataan turvallisuuden johtamista osana toimitilaturvallisuuden toteuttamista ja turvallisuusriskienhallinnan prosessia. Toimitilaturvallisuuden kehittämisen taustoja ja toimenpiteitä esitellään edellisiä yksityiskohtaisemmalla tasolla.

Neljännessä luvussa pyritään kuvaamaan kohdeorganisaation tilaturvallisuuden toteuttamisen nykytilaa, sekä aiheeseen vaikuttavia taustatekijöitä. Luvussa kuvatut toimintamallit, tavoitteet ja taustavaikuttajat ovat niitä tekijöitä, joiden perusteella organisaation toimitilaturvallisuuden nykytilan voi katsoa muodostuneen.

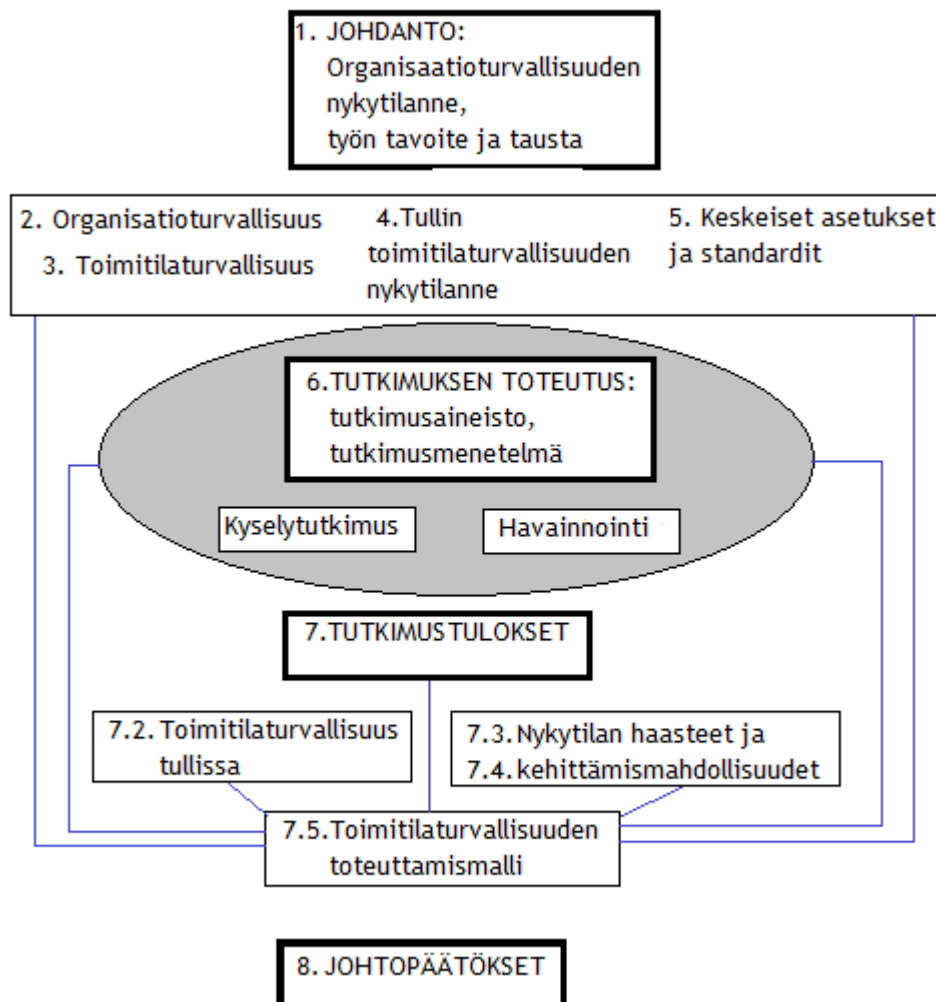
Toimitilaturvallisuuden toteuttamista ohjaavat paitsi organisaatioiden omat sisäiset linjaukset ja tarpeet, mutta lisäksi sitä säädetään myös erilaisten asetusten ja standardien kautta. Viidennessä luvussa esitellään yleisellä tasolla oleellimmat toimitilaturvallisuuden toteuttamiseen liittyvät asetukset ja standardit, joita on soveltuvin osin huomioitu työn kehittämiskohdeena olevaa toimitilaturvallisuuden toteuttamismallia laadittaessa.

Kuudennessa luvussa kuvataan työn empiirisen osuuden toteutus ja esitellään käytetyt tutkimusmenetelmät. Luvussa on avattu kohdeorganisaation toimitilojen turvallisuuden nykytilan selvittämiseksi käytettyä tutkimusta, joka suoritettiin pääosin kyselytutkimuksen keinoin.

Vastaukset työn tutkimuskysymyksiin kuvataan luvussa seitsemän. Työn tutkimuskysymykset liittyvät tiiviisti toisiinsa, mutta tulososion selkeyden takaamiseksi vastaukset esitellään omista kappaleistaan.

Johtopäätökset on kuvattu kahdeksannessa luvussa, jossa käydään läpi suoritettujen tutkimusten suoritusvaiheita. Lisäksi johtopäätöksiin sisältyy arviointi käytettyjen tutkimusmenetelmien soveltuvuudesta ja käyttökelpoisuudesta kyseisessä tutkimuksessa, ja tutkimuksen luotettavuuden arviointi. Luvussa kuvataan myös tunnistamaan työn kehittämiskohteeseen liittyviä

jatkotutkimusmahdollisuuksia. Työn rakenne kokonaisuudessaan esitellään kuvamuodossa kuviossa 1.



Kuvio 1: Opinnäytetyön rakenne kuvamuodossa

2 Organisaatioturvallisuus

Tässä luvussa kuvataan organisaatioturvallisuuden yleisiä tavoitteita ja periaatteita. Organisaatioturvallisuuteen liittyvien tutkimusten tulosten valossa käydään läpi organisaatioturvallisuuden nykytilaa Suomessa. Organisaatioturvallisuuden onnistuneen toteuttamisen lähtökohtia ovat tehokas turvallisuusjohtaminen ja toimiva riskienhallintaprosessi, joihin liittyviä tavoitteita luvussa yleisellä tasolla kuvataan.

2.1 Organisaatioturvallisuuden toteuttamisen yleisiä tavoitteita

Organisaatioturvallisuus on tärkeässä roolissa organisaation toiminnan laadun ja jatkuvuuden varmistamisessa: turvallisuuden on tarkoitus toimia tukiprosessina, joka auttaa organisaation varsinaisten ydinprosessien ja toimintojen toteuttamisessa. Perinteisen yritysturvallisuusjohtamisen kentän laajentuminen koskemaan myös julkisia toimijoita on edellyttänyt yritysturvallisuuskäsitteen ulottamista varsinaisesta yritystoiminnasta myös muihin organisaatiomuotoihin. (Leppänen 2006, 24, 59, 204.) Tässä työssä yritysturvallisuuden käsite on korvattu termillä organisaatioturvallisuus.

Yksinkertaisimmillaan määritettynä organisaation turvallisuusjärjestelyillä on tarkoitus toteuttaa paitsi lainsäädännön asettamat velvoitteet, mutta myös organisaation omat ja sopimuskumppaneiden edellyttämät turvallisuustoimenpiteet. Organisaation turvallisuusriskienhallintaprosessin yleisenä tavoitteena on mitoitaa tarpeellisiksi määritellyt riskienhallintatoimenpiteet siten, että turvallisuusriskit saadaan hyväksytylle ja hallittavalle tasolle, ilman että organisaation toiminta, tuotanto tai kilpailukyky häiriintyvät liiaksi. Riskienhallintatoimenpiteiden avulla pyritään vaikuttamaan tarpeenmukaisella tasolla riskien toteutumisen todennäköisyyteen ja toteutuneiden riskien seurausten vakavuuteen. (Yritysturvallisuus 2016.)

Organisaation riskienhallintatoimenpiteillä suojattavia arvoja voivat olla organisaatiosta riippuen esimerkiksi omaisuus, tieto, maine, henkilöstö, asiakkaat ja ympäristö. Suojattavien arvojen ja niihin kohdistuvien riskien hallintatoimenpiteiden määrittämisessä on tärkeää huomioida organisaation erityispiirteet, jotta suojautumiskeinot saadaan mitoitettua oikeassa suhteessa organisaatioon ja sen toimintaan nähden. Huomioitavia asioita voivat olla esimerkiksi organisaation koko, rooli, sisäinen ja ulkoinen toimintaympäristö sekä organisaation sidosryhmät ja niiden esittämät tarpeet. (Heljaste ym. 2008, 14-17.)

Organisaatioturvallisuuden kokonaisuus koostuu turvallisuuden eri osa-alueilla toteutettavista riskienhallintatoimenpiteistä, joiden avulla yrityksen tai organisaation tunnistettuja turvallisuusriskejä pyritään hallitsemaan. Elinkeinoelämän Keskusliiton (Yritysturvallisuus 2016) mukaisessa jaottelussa yritysturvallisuuden osa-alueita ovat työturvallisuus, palo- ja pelastusturvallisuus, tietoturvallisuus, henkilöstöturvallisuus, tuotannon ja toiminnan turvallisuus, ympäristöturvallisuus, poikkeamahallinta, varautuminen sekä kiinteistö- ja toimitilaturvallisuus. Organisaatioturvallisuuden osa-alueet on esitelty kuvamuodossa kuviossa 5 työn sivulla 31.

2.2 Organisaatioturvallisuuden nykytilanne Suomessa

Organisaation turvallisuuden tilan ylläpitämiseksi ja kehittämiseksi asetetaan useat eri tekijät. Organisaatioiden toimintaan kohdistuvat riskit ovat nykyään yhä moninaisempia ja vaikeammin hallittavia, mutta hyvin useissa organisaatioissa turvallisuustyöhön osoitetut re-

surssit toimivat riskienhallintatoimenpiteiden toteuttamista säätelevänä ja rajoittavana tekijänä. Vaikka turvallisuustoimenpiteiden tavoitteena on parantaa organisaation toimintakykyä, on turvallisuus kuitenkin usein ensimmäisiä kustannussäästöjen kohteeksi joutuvia tukitoimintoja. Tämän vuoksi organisaatioiden on tärkeää kyetä tunnistamaan toimintansa kannalta oleelliset turvallisuusriskit ja priorisoida tarpeenmukaiset riskienhallintatoimenpiteet riskien hallitsemiseksi. (ASIS Crime/Loss Prevention Council 2010, 29.)

Apuna tarvittavien riskienhallintatoimenpiteiden tunnistamisessa ja priorisoinnissa hyödynnetään organisaatioiden sisäisiä riskienarviointiprosesseja, mutta lisäksi toimijoiden on tärkeää huomioida toimintaansa ja toimintaympäristöönsä liittyvät ajankohtaiset turvallisuudentilan muutokset. Keskuskauppakamari ja Helsingin seudun kauppakamari ovat kartoittaneet Suomen yritysturvallisuuden tilaa tutkimuksessa, joka perustui 1681 suomalaisjohtajan antamiin tietoihin yrityksiin kohdistuneista rikos- ja väärinkäytösuhkista sekä organisaation käyttämistä suojautumis- ja varautumiskeinoista. Tutkimuksen tulosten osalta oleellista oli, että yritysjohdajista jopa kolmas arvioi yrityksen tietoturvallisuuden kohdistuvien riskien lisääntyneen kolmen viimeisen vuoden aikana. (Yritysten rikosturvallisuus 2012, 23, 25.)

Edellä mainittu Kauppakamarin tutkimus on tehty ja julkaistu jo vuonna 2012, mutta samansuuntaisia huomioita tehty myös muissa viimeaikaisissa aihepiiriä käsittelevissä tutkimuksissa ja tilannekuvissa. Keskusrikospoliisi laatii vuosittain yhteistyössä eri toimijoista koostuvan asiantuntijaverkoston kanssa yrityksiin kohdistuvan rikollisuuden tilannekuvan. Keväällä 2014 julkaistun tilannekuvan mukaan on tietotekniikan ja tietoverkkojen käytön lisääntyminen lisännyt huomattavasti myös niiden käyttöä rikollisen toiminnan välineenä. Organisaatioiden tietojen ja palveluiden sähköistyminen mobiiliverkkoihin ja internetiin kasvattaa väistämättä toimijoiden tietoturvallisuuden kohdistuvien riskien todennäköisyyttä ja monimuotoisuutta. (Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekatsaus nro 15 2014.)

Turvallisuusriskien toteutumisen seuraukset organisaation toiminnalle ovat moninaisia. Valtionhallinnon tietoturvan johtoryhmän antamassa suosituksessa todetaan, että tietovuodot ja muut erilaiset tietoturvallisuuden häiriötekijät vievät organisaatioilta uskottavuutta, ja myös kansalaisten luottamus hallintoon voi kärsiä toistuvien tietoturvaongelmien myötä (Tietoturvallisuus ja tulosoheutus 2004). Maineongelmien lisäksi toteutuneet turvallisuusriskit voivat aiheuttaa haasteita voi myös sopimusturvallisuuden osa-alueella. Organisaatiot ovat yleistyneen sidosryhmäyhteistyön ja toimintojen ulkoistamisen vuoksi yhä enemmän vastuussa myös alihankkijoidensa toimintojen turvallisuudesta, joten ongelmat toiminnan turvallisuuden tason ylläpitämisessä voivat näin ollen johtaa jopa juridisiin vastuisiin. (Sidosryhmäyhteistyön riskit.)

Edellä mainittujen tutkimusten ja tietojen valossa nousee tietoturvallisuuden osa-alue yhdeksi organisaatioturvallisuuden kehittämisen ajankohtaisimmista ja samalla myös haasteellisimmista osa-alueista. Kuitenkin organisaatioturvallisuuden kaikki osa-alueet ovat ainakin jossain määrin riippuvaisia toisistaan, ja organisaation toiminnan jatkuvuuden kannalta tärkeiksi luokiteltujen arvojen suojaamiseksi tarvitaan turvallisuusratkaisuja organisaatioturvallisuuden eri sektoreilla. Koska organisaation turvallisuuden tilan voi katsoa muodostuvan kaikkien turvallisuuden osa-alueiden summasta, on organisaation tarpeen kehittää ja ylläpitää toimenpiteitä kattavasti kaikilla organisaation toimintaan liittyvillä turvallisuuden osa-alueilla. (Leppänen 2006, 203.)

2.3 Organisaatioturvallisuuden toteuttamisen haasteita

Organisaatioiden turvallisuustoiminnot ovat aina olleet siinä mielessä hankalassa asemassa, että organisaation taloudellisen tilanteen ollessa tiukka, on turvallisuus usein ensimmäisiä budjettileikkausten kohteeksi joutuvia toimintoja. Organisaatioturvallisuuden tason kehittämiseksi ja ylläpitämiseksi organisaatiot joutuvat käyttämään resursseja varmistaakseen paitsi vaadittujen turvallisuusratkaisuiden olemassa olon, mutta myös varmistumaan riittävästä riskienhallinnan ja turvallisuuden hallinnan osaamistasosta.

Yksi keskeisimpiä tekijöitä organisaatioturvallisuuden tason ylläpitämisessä ja kehittämisessä onkin turvallisuusjohdon kyky saattaa turvallisuustoimintoihin sijoittamisen edut organisaation johdon tietoisuuteen. Turvallisuustoimintoihin panostaminen tulisi menoerän sijasta kyetä näkemään pikemminkin pitkän aikavälin sijoituksena, sillä onhan turvallisuuden tilan parantamisen perimmäisenä päämääränä lisätä organisaation toimintakykyä, toiminnan laatua sekä tuloksellisuutta. (ASIS Crime/Loss Prevention Council 2010, 29.)

Kuten aiemmassa luvussa esitellyn Kauppakamarin yritysturvallisuuden tilaa käsittelevän tutkimuksen tuloksista kävi ilmi, luo turvallisuutta uhkaavien riskien monimuotoistuminen haasteita organisaatioiden riskienhallintaprosessille ja riskienhallintatoimenpiteiden toteuttamiselle. Organisaatioiden käytettävissä olevat rajalliset taloudelliset resurssit luovat väistämättä tarpeen priorisoida turvallisuuden kehittämiskohteita. Kauppakamarin tutkimuksen mukaan vuonna 2012 yritysten tärkein turvallisuuden kehittämiskohde kaikissa yritysluokissa ja kaikilla toimialoilla oli tietoturvallisuus. Lähes kaksi kolmesta tutkimukseen vastanneesta yrityksestä aikoi jatkossa panostaa tietoturvallisuuteen aiempaa enemmän, mikä kuvastaa selkeästi tietoturvallisuuden merkittävyyttä toimijoiden riskienhallintaprosessissa. (Yritysten rikosturvallisuus 2012.)

Tietoturvariskien hallitseminen on sikäli jatkuvasti ajankohtainen aihe, että pääsääntöisesti kaikilla yrityksillä ja organisaatioilla on hallussaan sellaista tietoa, jonka menetys ulkopuolisille tahoille saattaa aiheuttaa toimijalle vahinkoa muodossa tai toisessa (Yritysten rikosturvalli-

suus 2012, 23). Tietoverkkorikollisuuden lisääntyminen ja monipuolistuminen luo haasteita organisaatioiden turvallisuusriskienhallinnalle (Strauchs 2010b, 81). Lisäksi yhä suurempi osa organisaatioiden tarvitsemista ICT-palveluista hankitaan nykyään ulkoistettujen palveluntarjoajien kautta, ja vaikka palvelujen tuottajien tietoturvallisuuden taso olisikin lähtökohtaisesti korkea, on asiakasyrityksen haasteellista kyetä arvioimaan palveluntuottajansa turvallisuusratkaisuja ja suorittaa näin tarpeenmukaista tietoturvariskienarviointia (Liiketoimintaa turvallisesti. Kansallinen strategia yritystoiminnan turvallisuuden parantamiseksi 2012).

Lisääntynyt sidosryhmäyhteistyö luo haasteita organisaatioiden riskienhallintatyölle myös turvallisuuden muilla osa-alueilla. Organisaatioiden ulkoistaessaan toimintojaan, perustuu toiminta yhä enemmän yhteistyöhön alihankkijoiden ja muiden sidosryhmien kanssa, mikä vaatii panostamista sopimusriskien arviointiin ja hallintaan. Toimintojen jakautuessa useiden erillisten toimijoiden välille, voi olla hankalaa määrittää taho, joka viime kädessä kantaa vastuun toiminnan riskeistä. Usein yksi toimintojen ulkoistamisen tavoitteista on pyrkiä ulkoistamaan myös kyseisiin toimintoihin liittyvät riskit, jonka vuoksi ulkoistamisen yhteydessä on tärkeää laatia riittävän yksityiskohtaiset sopimukset, joissa on määritetty toimijoiden vastuut ja velvollisuudet. (Leppänen 2006, 169-170.)

Leppäsen (2006, 102-103) mukaan nykyaikana yleistyneissä yhteishankkeissa ongelmaksi muodostuukin usein juuri sopimuskokonaisuuden puutteellisuus turvallisuusvaatimusten osalta, jolloin vastuu toimintojen turvallisuudesta uhkaa jäädä toimijoille epäselväksi. Lisäksi toimintojen ja sopimuskumppaneiden kansainvälistyminen tuo haasteita sopimusehtojen asettamiselle ja niiden toteutumisen valvonnalle, kun sopimuskumppani saattaa suorittaa toimintonsa eri maassa tai maanosassa.

Sidosryhmäyhteistyön lisääntyminen paitsi hankaloittaa riskienhallintavastuun määrittämistä, mutta saattaa myös kasvattaa organisaation maineriskien todennäköisyyttä ja seurauksia. Lisäksi organisaatioiden maineriskiä lisäävät uudet viestintätavat, kuten esimerkiksi sosiaalisen median kanavat, ja niiden myötä tehostunut tiedonkulku. Maineen arvoa organisaatiolle on hankala määrittää, ja myös sen menettämisen aiheuttamien vahinkojen seurausten määrittely on vaikeaa. Lisäksi Bergin (2012, 12) mukaan Neufeld (2007) toteaa, että yrityksen maine voi olla uhattuna, vaikka sidosryhmien käsitykset eivät perustuisikaan todellisuuteen. Mikään konkreettinen uhka ei siis välttämättä edes toteudu, mutta maineen menettämiseen johtavan niin sanotun läheltä piti -tilanteen seuraukset voivat siitä huolimatta olla organisaation toiminnan jatkuvuuden kannalta kohtalokkaita.

Organisaation omien sisäisten turvallisuusvaatimusten ohella lisähaasteita organisaation turvallisuustyölle tuovat ulkopuolisten tahojen asettamat turvallisuusvaatimukset. Kansalliset vaatimukset tiedon luokittelua ja turvallisuusluokitellun tiedon käsittelyä koskien sekä lisään-

tyvä kansainvälinen yhteistoiminta luovat omat haasteensa, jotka toimijoiden on kyettävä huomioimaan turvallisuusratkaisuissaan. Suomessa valtionhallinnon toimijoille esitetään kansallisia turvallisuusvaatimuksia esimerkiksi valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010), jossa säädetään asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä turvallisuusluokiteltujen asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista.

Kansainvälisten yhteistyökumppaneiden turvallisuusluokitellun tiedon käsittelylle puolestaan asettaa vaatimuksia laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), jossa edellytetään, että toimijat toteuttavat laissa vaadittuja turvallisuusvelvoitteita käsitellessään erityissuojattavaksi luokiteltavaa tietoaineistoa. Erityissuojattava materiaalilla laissa tarkoitetaan sellaisia salassa pidettäviä asiakirjoja, jotka on turvallisuusluokiteltu kansainvälisen tietoturvallisuusvelvoitteen mukaisesti.

Edellä on kuvattu organisaatioiden turvallisuuden tilan kehittämisen yleisiä haasteita turvallisuuden eri osa-alueilla, mutta organisaation turvallisuuden varmistamiseksi oleellista on onnistua viemään tarpeellisiksi todetut turvallisuustoimenpiteet käytäntöön. Toimenpiteiden toteuttaminen on yksi haastavimmista kokonaisuuksista organisaation turvallisuustyössä: turvallisuusorganisaation suorittaman riskienarviointiprosessin perusteella tunnistetaan ja suunnitellaan tarpeenmukaiset riskienhallintamenetelmät, mutta niiden jalkauttaminen käytäntöön vaatii turvallisuustietoisuutta koko organisaatiolta. Toimivan turvallisuuskulttuurin luominen organisaatioon vaatii paitsi turvallisuusjohdon, mutta ehdottomasti myös muun johdon sitoutumista, jotta on mahdollista saada koko henkilöstö osallistettua turvallisuustyöhön aidosti ja tehokkaasti. (Sennewald 2011, 235-236.)

Sennewaldin (2011) mukaan kehittyneimmätään turvallisuustekniikan ratkaisut eivät riitä takaamaan riskienhallintamenetelmien tehokkuutta, mikäli henkilöstö ei ole sitoutunut turvallisiin toimintamalleihin, eikä tue organisaation turvallisuusratkaisuja toiminnallaan. Henkilöstön turvallisuuskoulutuksen avulla on tarkoitus varmistaa, että henkilöstö tietää mitä heiltä odotetaan, ja minkä vuoksi. Ilman tätä tietoisuutta jää organisaation turvallisuuskulttuuri väistämättä liian heikoksi, ja turvallisuustoimenpiteiden ja -vaatimusten toteutuminen näin ollen puutteelliseksi.

2.4 Turvallisuuden johtaminen

Kuten jo aiemmassa mainittiin, voi organisaatioturvallisuuden toteutumisen perustana pitää turvallisuusjohtamisen keinoin ylläpidettävää turvallisuuskulttuuria, joka määrittelee ja ohjaa henkilöstön toimintamalleja organisaatiossa (Tietoturvallisuus ja tulosohejaus 2004, 15). Turvallisuuskulttuuria kehitetään ja ylläpidetään turvallisuusjohtamisen keinoin, joka taas on osa organisaation muuta johtamisjärjestelmää. Turvallisuusjohtamisen avulla pyritään varmista-

maan yrityksen toiminnan jatkuvuus, turvallisuus ja vaatimustenmukaisuus kaikissa yrityksen toiminnoissa. Kyseessä ei siis ole erillinen turvallisuuden tai johtamisen osa-alue, vaan tavoitteena on integroida turvallisuusjohtaminen kiinteäksi osaksi muuta johtamisjärjestelmää, ja auttaa näin parantamaan toiminnan tehokkuutta ja tuottavuutta. (Yritysturvallisuus 2016.)

Turvallisuusjohtamisen tavoitteena on tunnistaa organisaation turvallisuusriskit ja suunnitella tarpeenmukaiset toimenpiteet riskien hallitsemiseksi. Turvallisuusjohtamisen keinoin myös jalkautetaan tarpeenmukaisesti toimenpiteet turvallisuuden eri osa-alueilla. Turvallisuusasioiden jalkauttamiseksi tulee organisaation johto ja henkilöstö saada sitoutettua turvallisuustyöhön. Sitouttaminen tapahtuu määrittämällä riittävän yksityiskohtaisesti turvallisuustyön tavoitteet, sekä varmistamalla turvallisuuskoulutuksen, vastuunjaon ja tiedonkulun toimivuus. (Heljaste ym. 2008, 12-13.)

Organisaation turvallisuuskulttuurin kehittäminen vaatii turvallisuusjohtamiselta tehokkuutta ja vaikuttavuutta. Jotta organisaation turvallisuuskulttuurin perusedellytykset toteutuvat, on oleellista varmistaa riittävä tiedonkulku sekä henkilöstön tietoisuus turvallisuusasioista - turvallisuusjohdon ja esimiesten vastuulla on perehdyttää työntekijät turvallisuustoiminnan perusteisiin ja tavoitteisiin. Organisaation johtamisjärjestelmän tulee olla riittävän selkeä, jotta kaikki tietävät omat roolinsa ja vastuunsa organisaatiossa, joka taas mahdollistaa turvallisuuden perusedellytysten toteutumisen. (Leppänen 2006, 194-195.)

Johdolla on merkittävä asema myös toimiessaan organisaation henkilöstölle esikuvana sekä turvallisuusajattelun että turvallisten käyttäytymismallien suhteen. Lähtökohtaisesti turvallisuuden johtamisessa on oleellista se, ettei asioita tehtäisi toisen puolesta, vaan että ihmiset oppisivat toimimaan itsenäisesti ja tuntemaan toimintansa tarkoituksen (Lämsä & Päivike 2013, 206). Esimerkin voima onkin yksi johdon tärkeimmistä työkaluista turvallisuuskulttuurin ja -ajattelun kehittämisessä ja jalkauttamisessa.

Organisaation turvallisuusjohtamisen tärkeimpiä tavoitteita on luoda organisaatioon toimiva turvallisuuskulttuuri. Vahvan turvallisuuskulttuurin luominen ei onnistu hetkessä - eikä riittävän osaamisen puuttuessa pitkälläkään aikavälillä. Ainakaan se ei onnistu perinteisiä käskyjohtamisen periaatteita toteuttamalla, vaan vaatii tuekseen poikkitieteellistä ajattelukykyä ja riittäviä sosiaalisia taitoja. Perusvaatimuksena vahvan turvallisuuskulttuurin syntymiselle on se, että ihmiset tietävät mitä heiltä odotetaan ja minkä vuoksi. Jos nämä asiat eivät ole tiedossa, jää turvallisuusvaatimusten toteuttaminen pintapuoliseksi suorittamiseksi (Sennwald 2011, 235-236).

Turvallisuuskulttuurin kehittämisessä ja kehittämisessä on oleellista, että se vaikuttaa kahteen suuntaan. Ensinnäkin työntekijöiden turvalliset toimintamallit tukevat organisaation tur-

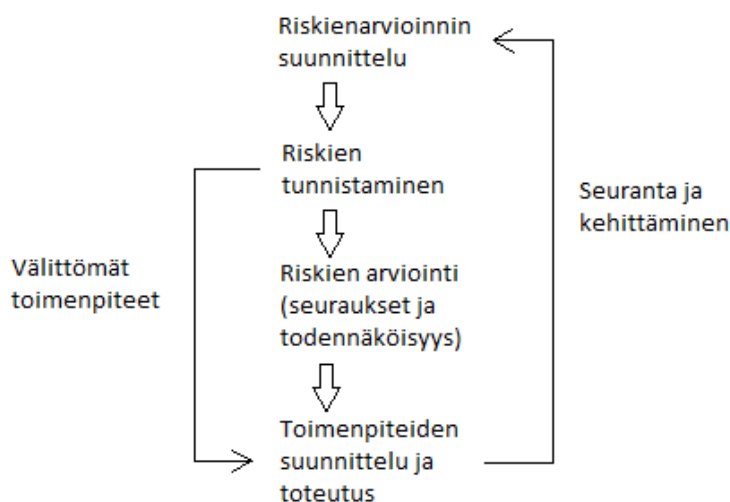
vallisuuskulttuurin kehittymistä. Toisaalta taas muuttamalla organisaatioturvallisuutta tukevia toimintamalleja, voidaan pyrkiä vaikuttamaan työntekijöiden arvoihin ja uskomuksiin ja sitä kautta myös toimintaan. Suurimmassa roolissa kehitystyössä on organisaation johto. Pystyäkseen sitouttamaan työntekijät turvallisuusvaatimusten noudattamiseen, ja varmistuakseen toimintamallien pysyvyydestä, vaaditaan johdolta ja esimiehiltä riittävää tietämystä oppimisen mekanismeista (Puhakainen & Siponen 2010, 762).

Kuten jo edellä mainittiin, on johdon tärkeää kyetä näyttämään esimerkkiä, jotta se voi odottaa myös työntekijätholta tietynlaista suoritusta. Vaikka kyse on hyvin yksinkertaisesta ja helposti ymmärrettävästä asiasta, voi sen toteuttaminen siitä huolimatta olla haastavaa. Esimerkkejä fyysisen turvallisuuden varmistamiseksi suoritettavista toimenpiteistä, jotka helposti jäävät viemättä käytäntöön, löytyy useista organisaatioista. Tietokoneet jäävät lukitsematta työpisteeltä poistuttaessa, tai dokumentteja ei käsitellä ja säilytetä niiden suojausluokitus- tasojen vaatimusten mukaisesti. Tärkeää on myös ohjeistaa henkilökunta turvallisuusratkaisuiden ja turvallisuustekniikan käytön osalta. Vaikka kyse tuntuu päällisin puolin olevan pienistä asioista, voivat ne toteutumatta jäädessään johtaa yrityksen kannalta hyvinkin haitalliseen lopputulokseen. (Reid 2004, 266-267.)

Organisaation henkilöstön asenteiden ja toimintamallien muuttaminen turvallisempaan suuntaan on haasteellista. Sen vuoksi kokonaisen ryhmän toiminnan muutokseen tähtäävä asenteiden muutos on aloitettava yksilötasolla, pyrkimällä muuttamaan yksittäisten ihmisten asenteita. Tässä yhteydessä on hyvä tiedostaa johdon esimerkin vaikutukset henkilöstön turvallisuusasenteisiin. Asenteet tuovat pysyvyyttä, ja ympäristössä, jossa tapahtumia on helppo ennakoida, on hyvä toimia. Näin ollen samanlaiset turvalliset toimintamallit ja niiden täsmällinen noudattaminen ylimmästä johdosta aina työntekijäportaaseen tukevat ryhmän yhteisen turvallisuuskulttuurin kehittymistä ja ylläpitämistä. (Aaltonen, Pitkänen & Ristikangas 2008, 183.)

2.5 Turvallisuuden riskienhallintaprosessi

Organisaation turvallisuusriskien hallintaprosessissa arvioidaan riskien toteutumisen todennäköisyyttä, ja toteutuneiden riskien seurausten vaikutuksia sekä suunnitellaan tarvittavat toimenpiteet riskien hallitsemiseksi. Riskienarvioinnin päävaiheet ovat uhkien ja riskien tunnistaminen ja toteutuneiden tapahtumien seurausten arvioiminen. Edellä mainittujen tietojen perusteella suunnitellaan ja toteutetaan riskien torjumiseksi tarvittavat toimenpiteet. Riskienhallintaprosessi on esitetty kuvamuodossa kuviossa 2. Toteutuneiden riskien seurausten pienentämiseksi organisaatiossa on oltava suunnitelma, kuinka vahingon sattuessa toimitaan, ja miten vahingosta tehokkaimmin toivutaan. (Valtionhallinnon tietoturvallisuuden johtoryhmä 2003, 15.)



Kuvio 2: Organisaation riskienhallintaprosessi

Riskikartoituksen tekeminen on tarpeen turvallisuustoimenpiteiden suunnittelemiseksi ja toteuttamiseksi. Tunnistettujen ja arvioitujen riskien perusteella määritellään tarvittavat toimenpiteet, niiden toteuttamisen vastuuhenkilöt sekä päätetään riskienhallintatoimenpiteiden seurannasta ja raportoinnista (Heljaste ym. 2008, 16-17). Turvallisuuden johtamisjärjestelmän on tärkeää olla yhteneväinen koko turvallisuusriskienhallintaprosessin osalta, joten tässä luvussa käsitellään organisaation turvallisuuden johtamisen roolia organisaation riskienhallintaprosessissa yleisellä tasolla, vaikka opinnäytetyön tutkimuskysymykset kohdistuvat pääasiallisesti toimitilaturvallisuuden osa-alueelle.

Toimiva riskienhallintaprosessi on tärkeä tekijä organisaation toimitila- ja tietoturvallisuuden riittävän tason saavuttamisessa ja ylläpitämisessä. Turvallisuusjohtaminen sekä organisaation riskien hallitseminen liittyvät kiinteästi toisiinsa, sillä riskienhallinta on osa yrityksen johtamista, sekä myös strategisten tavoitteiden saavuttamista (Ilmonen, Kallio, Koskinen & Rajamäki 2010, 7). Ilman toimivaa turvallisuusjohtamista ei voi olla toimivaa riskienhallintaa, ja toisaalta sama vaatimus toteutuu myös toiseen suuntaan: toimiva riskienhallintajärjestelmä on turvallisuusjohtamisen tärkeä työkalu.

Yksinkertaisimmillaan määriteltynä organisaation riskienhallintaprosessin tavoitteena voisi kuvata olevan organisaation turvallisuuden tason parantaminen. Kerkon (2001, 57) mukaan riskienarviointiprosessin tulosten perusteella tehdään linjauksia turvallisuutta koskevaan päätöksentekoon ja turvallisuuden johtamiseen liittyen. Toisin sanoen riskienhallintaprosessin perusteella tarpeelliseksi todetut kehittämistoimenpiteet pyritään viemään käytäntöön turvallisuusjohtamisen keinoin.

SFS-ISO 31000 -standardin määritelmän mukaan riskienhallinnan onnistuminen riippuu sen perustana olevien johtamisrakenteiden vaikuttavuudesta, sekä myös järjestelyistä, joiden avulla riskienhallinta sisällytetään organisaation eri tasojen toimintaan. Prosessin toimivuuden kannalta on siis tärkeää varmistaa, että riskienhallintaprosessista saatu tieto riskeistä raportoidaan oikealla tavalla oikealle taholle, ja että tietoa hyödynnetään päätöksenteon ja vastuiden perustana organisaation kaikilla tasoilla. Riskienhallinnan puitteiden tarkoituksena ei siis ole määrätä johtamisjärjestelmän rakennetta, vaan pikemminkin auttaa organisaatiota sisällyttämään riskienhallinta sen yleiseen johtamisjärjestelmään. Turvallisuuden johtamisjärjestelmän puolestaan voi määrittellä olevan tärkeä tekijä riskienhallinnan puitteiden suunnittelussa. (SFS-ISO 31000.)

Riskienarviointityö on oleellisessa roolissa organisaation toiminnan laadun ja turvallisuuden kehittämisessä. Toimiva riskienarviointi tarjoaa pohjan organisaation turvallisuuden eri osa-alueisiin liittyvälle päätöksenteolle. Turvallisuusjohtaja hyödyntää riskienarvioinnin tuloksia linjatessaan ja perustellessaan toiminnan turvallisuuteen tähtäävien toimintamallien viemistä käytäntöön - toimiva riskienarviointiprosessi on siis keino turvallisuusjohdon tavoitteiden saavuttamiseksi. (Kerko 2001, 57.) Riskienarviointiprosessin toteuttamisen tukena turvallisuusjohto usein käyttää erilaisia riskienhallintatyökaluja, mutta myös riskienhallintatoimenpiteiden suunnittelussa ja toteuttamisessa olisi yleensä hyödyllistä pystyä hyödyntämään tarkoituksenmukaisia turvallisuussuunnittelun apuvälineitä.

3 Toimitilaturvallisuus

Luvussa kuvataan organisaation toimitilaturvallisuuden kehittämiseen ja ylläpitämiseen liittyviä vaatimuksia ja tavoitteita. Toimitilaturvallisuuden toteuttamiskäytäntöjä on kuvattu paitsi riskienhallintaprosessin ja kustannustehokkuuden näkökulmasta, mutta myös pyritty löytämään tilaturvallisuuden toteuttamisen yhtymäkohtia turvallisuuden eri osa-alueisiin liittyen. Osa-alueista etenkin organisaatioiden tietoturvallisuuden tasolla on havaittavissa selkeä riippuvuussuhde toimitilaturvallisuuden osa-alueen kanssa.

3.1 Toimitilaturvallisuuden rooli tietoturvallisuuden toteuttamisessa

Yksi fyysisen toimitilaturvallisuuden tärkeimmistä tavoitteista on suojata organisaatiossa käsiteltävien tietojen ja tietojärjestelmien käyttöympäristön turvallisuus toimitilojen turvallisuusjärjestelyjen keinoin (Reid 2004, 19-20). Tässä työssä organisaatioturvallisuutta, organisaation tietoturvallisuutta ja niiden toteuttamistoimenpiteitä käsitellään toimitilaturvallisuuden näkökulmasta. Toimitilaturvallisuuden ratkaisuille pyritään siis varmistamaan muiden suojattavien arvojen ohella organisaation toiminnan kannalta oleellisten tietojen luottamuksellisuus, eheys ja saatavuus.

Työn edellisissä luvuissa käsiteltiin organisaatioturvallisuuden nykytilaa ja haasteita, sekä esiteltiin tutkimustuloksia, joiden mukaan etenkin organisaatioiden tietoturvallisuuden osa-alue on nykypäivänä erityisten haasteiden kohteena. Koska organisaatioturvallisuuden osa-alueet ovat kuitenkin vahvasti riippuvaisia toisistaan, tarvitaan organisaation turvallisuuden tilan ylläpitämiseksi tehokkaita riskienhallintatoimenpiteitä useilla turvallisuuden osa-alueilla. Esimerkiksi organisaation tietoturvallisuuden tason nostaminen halutulle tasolle edellyttää toimenpiteitä paitsi tietoturvallisuuteen kuuluvissa tietoliikenne-, laitteisto- ja ohjelmistoturvallisuuden osioissa, mutta myös henkilöstöturvallisuuden ja toimitilaturvallisuuden osa-alueilla. (Tietoturvallisuus ja tulosohjaus 2004, 15-16.)

Tietoturvallisuus voidaan jakaa eri osa-alueisiin hallinnollisesta tietoturvallisuudesta ja henkilöstöturvallisuudesta aina tekniseen tietoturvallisuuteen ja toiminnan jatkuvuuden varmistamiseen saakka (Tietoturvallisuus 2016). Organisaation tietoturvallisuusriskejä puolestaan voidaan jakaa esimerkiksi johtamiseen, toimitiloihin, tietojärjestelmiin, liikekumppaneihin sekä henkilöstöön ja sen toimintaan liittyviin riskeihin. Useiden tietoturvallisuusriskien hallinnassa toimitilaturvallisuuden toimenpiteet ovat tärkeässä asemassa, ja tilojen fyysinen turvallisuus onkin yksi oleellisimmista keinoista varmistaa tietoturvallisuuden toteutuminen organisaatiossa. (Leppänen 2006, 103-104).

Koska organisaatioiden tietoturvallisuuden toteuttaminen ja fyysisen toimitilaturvallisuuden varmistaminen noudattavat pitkälti yhteneväisiä toteuttamismalleja, ei näiden osa-alueiden ylläpitoa ole tarkoituksenmukaista tai edes mahdollista erottaa täysin erillisiksi toiminnoiksi. Esimerkiksi toimitilojen murtosuojauksesta, turvallisuusvalvonnasta ja paloturvallisuudesta huolehtiminen on oleellisen tärkeää tietojen luotettavuuden ja saatavuuden varmistamiseksi. Sama riippuvuussuhde toteutuu luonnollisesti myös toisinpäin: jotta turvallisuusvalvontajärjestelmät voidaan toteuttaa ja ylläpitää turvallisesti, tulee tietoverkkojen ja -järjestelmien turvallisuuden olla riittävällä tasolla. (ASIS Crime/Loss prevention Council 2010, 26.)

Tutkimustulokset osoittavat, että organisaation turvallisuusosaston ja IT-osaston välisessä yhteistyössä ilmenevät puutteet voivat aiheuttaa haasteita turvallisuustyön toteuttamisessa. Pohjois-Amerikassa vuonna 2009 tehdyssä tutkimuksessa selvitettiin sadan suuren organisaation sisäisen yhteistyön tasoa organisaatioiden turvallisuusosastojen sekä IT-osastojen käyttämiin järjestelmiin liittyen. Huomionarvoista tutkimuksen tuloksissa oli, että useissa tutkimuksen organisaatioissa turvallisuusjärjestelmien ja -ohjelmistojen turvallisuuden tason havaittiin olevan alhainen verrattuna organisaation muihin järjestelmiin. (Strauchs 2010a, 39-51.)

Tutkimuksen tuloksista ilmeni, että esimerkiksi kameravalvontajärjestelmän ja muiden turvallisuusvalvontajärjestelmien osalta ei välttämättä ole huolehdittu tiedon luottamuksellisuuden tai saatavuuden turvaamisesta samalla tasolla kuin muiden organisaation käyttämien järjes-

telmien tietoturvaluisuus oli toteutettu. Pääsyyinä tähän nähtiin organisaatioiden turvallisuus- ja IT-osastojen välisen yhteistyön liian vähäinen määrä. Koska organisaatioturvallisuuden tila koostuu kaikkien turvallisuuden osa-alueiden summasta, tarvitaan organisaatioiden toimintaan kohdistuvien riskien monipuolistuessa yhä tehokkaampaa yhteistyötä eri osastojen välillä. (Strauchs 2010a, 39-51.)

Tilaturvallisuuden varmistamiseksi toteutettavat suojausmenetelmät ovat useimmiten erilaisia rakenteellisia ja teknisiä ratkaisuja. Suoritettaessa riskienhallintaa ja määriteltäessä tarvittavia suojaustoimenpiteitä on kuitenkin oleellista tiedostaa, että pelkät tekniset tai fyysiset suojauskeinot eivät yksinään ole riittäviä toimenpiteitä organisaation toiminnan kannalta tärkeän tiedon suojaamiseksi. Kuten muidenkin turvallisuusriskien, niin myös tietoturvariskien toteutumisessa ja torjunnassa, on ihmisen toiminta tärkeässä roolissa. Henkilöstön riittävän turvallisuustietoisuuden keinoin voidaan pyrkiä vaikuttamaan siihen, ettei organisaation suojattavaa tietoa päätyisi ulkopuolisten tietoon tai haltuun. Henkilöstö, joka ei ole tietoinen turvallisuusriskeistä, eikä osaa toteuttaa riskien torjumiseksi suunniteltuja toimenpiteitä käytännössä, voi olla todellinen uhkatekijä organisaation toiminnan turvallisuudelle. (Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekatsaus nro 15 2014, 2.)

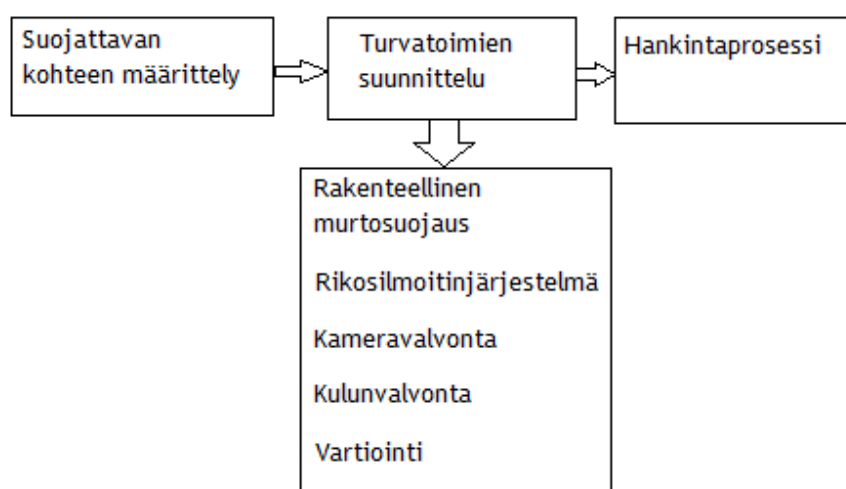
3.2 Toimitilaturvallisuuden kehittäminen

Turvallisuuden eri osa-alueiden turvallisuustoimenpiteiden tavoitteena on turvata organisaation suojattavat arvot. Osa-alueiden välillä on paljon riippuvuussuhteita ja päällekkäisyyksiä, mutta organisaation turvallisuuden tila kokonaisuudessaan on kuitenkin riippuvainen kaikkien organisaation toiminnan kannalta oleellisten osa-alueiden yhteisvaikutuksesta. Organisaation turvallisuuden tason kehittämiseksi vaadittavat toimenpiteet tunnistetaan riskienhallintaprosessin avulla, ja tarvittavat toimenpiteet puolestaan toteutetaan ja viedään käytäntöön turvallisuusjohtamisen keinoin. Turvallisuusriskienhallinta ja turvallisuusjohtaminen siis ohjaavat organisaatioturvallisuuden eri osa-alueilla toteutettavia toimenpiteitä. (Leppänen 2006, 176, 203-204.)

Valtionhallinnon tietoturvaluisuuden johtoryhmän tietoturvaluisuutta koskevassa ohjeistuksessa todetaan, että organisaation toimitilaturvaluusuriskejä voidaan arvioida muun muassa kiinteistön ja toimitilojen turvallisuusjärjestelyihin, tietojen ja järjestelmien käyttöperiaatteisiin sekä varavojärjestelmiin liittyen. Tyypillisiä tietojen ja tilojen fyysiseen turvallisuuteen liittyviä uhkia ovat turvallisuusvalvonnan puutteellisuus, tekniset viat sekä erilaiset poikkeustilanteet. Myös puutteelliset toimintatavat esimerkiksi turvallisuusohjeistuksen, käytönvalvonnan sekä sääntöjen ja koulutuksen osalta ovat selkeitä uhkatekijöitä. Toiminnasta johtuvat uhat voidaan jakaa tahattomiin, kuten esimerkiksi kaapelointiin, laitteisiin tai sähkökatkoihin liittyviin vikoihin, sekä tahallisiin tekoihin, kuten murtoihin, varkauksiin ja ilkivaltaan. (Ohje riskien arvioinnista tietoturvaluisuuden edistämiseksi valtionhallinnossa 2003, 32-33.)

Organisaation turvallisuutta uhkaavien riskien hallitsemiseksi on olemassa kaksi strategiaa: pienentää ei-toivotun tapahtuman toteutumisen todennäköisyyttä tai pienentää toteutuneen riskin seurauksia (Halibozek & Kovacich 2009, 40). Riskienarviointia voidaan pääsääntöisesti suorittaa esimerkiksi muutaman kerran vuodessa, mutta toteutuneiden riskien ja tapahtuneiden läheltä piti -tilanteiden osalta on tärkeää, että riskin toteutumiseen johtaneet syyt tunnistetaan ja käsitellään mahdollisimman reaaliaikaisesti. Toteutuneiden riskien ja läheltä piti -tilanteiden käsitteleminen auttaa tunnistamaan vastaavan kaltaiset skenaariot tulevissa riskienarvioinneissa, ja luomaan kyseisten tapahtumien varalle tarpeenmukaiset varautumistoimenpiteet. (Leppänen 2006, 165.)

Toimitilaturvallisuuden toteuttamisen toimenpiteet voidaan jakaa karkealla jaolla tilojen rakenteelliseen suojaukseen sekä teknisiin turvallisuusjärjestelyihin. Tilaturvallisuuden kehittämiseen tähtäävät toimintamallit on esitelty kuviossa 3. Tilojen rakenteellisen murtosuojauksen tarkoituksena on vaikeuttaa ja hidastaa luvaton tunkeutumista tiloihin. Rakenteellisen suojauksen lisäksi tilaturvallisuutta toteutetaan erilaisten teknisten valvontajärjestelmien avulla, kuten kulunvalvonta-, rikosilmoitin- ja kameravalvontajärjestelmillä. (Halibozek & Kovacich 2009, 185.)



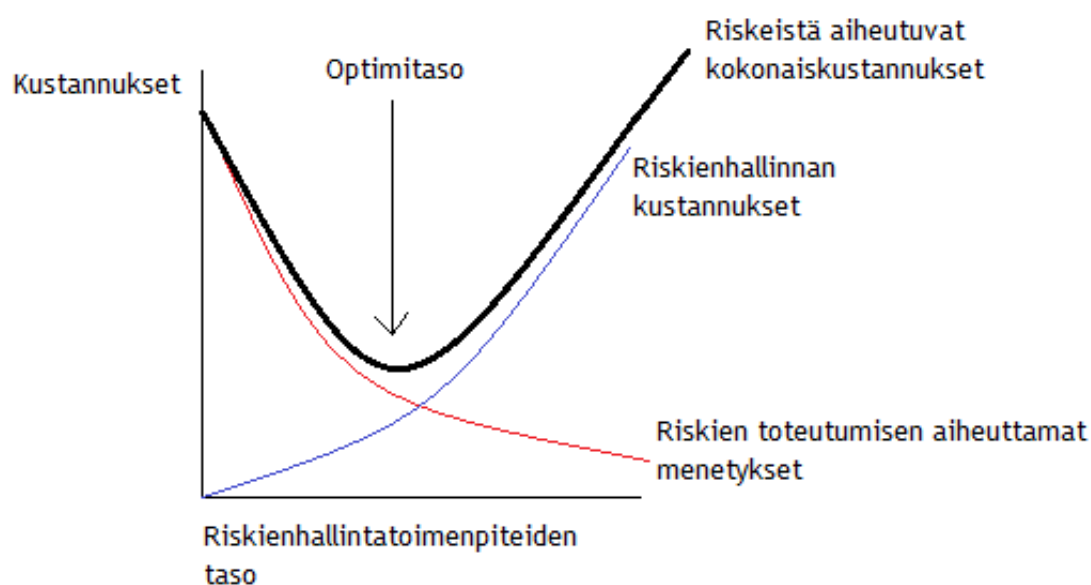
Kuvio 3: Tilaturvallisuustoimenpiteiden toteuttamismalli (mukailtu Koskenranta 2007)

Sähköinen kulunvalvontajärjestelmä toimii mekaanisen lukituksen apuna, ja sen tarkoituksena on auttaa rajaamaan henkilöiden kulkuoikeuksia tiloihin ajallisesti ja paikallisesti sekä tarvittaessa mahdollistaa tapahtuneiden kulkujen jälkikäteinen todentaminen. *Rikosilmoitinjärjestelmän* ilmaisimet reagoivat tiloissa liikkumiseen, jolloin järjestelmä siirtää tiedon hälytyksestä ennalta sovittuun kohteeseen, ja tila voidaan tarkastaa sovitun prosessin mukaisesti. *Kameravalvontajärjestelmän* avulla voidaan joko seurata tapahtumia reaaliaikaisesti tai to-

dentaa jälkikäteisesti tapahtumia tai tiloissa liikkuneita henkilöitä. Valvontajärjestelmien olemassa olo auttaa paitsi tapahtumien jälkikäteisessä selvittämisessä, mutta toimii usein myös tehokkaana ennaltaehkäisijänä tiloihin tunkeutumisen tai muiden väärinkäytösten osalta. (Fennelly 2013, 87.)

Teknisten valvontajärjestelmien suhteen on tärkeää huomioida, että ne toimivat tehokkaina tilaturvallisuuden tason korottajina vain oikein suunniteltuina ja toteutettuina. Oleellista on myös järjestelmien oikeaoppinen käyttö, joten organisaation henkilökunnalla on oltava riittävä tietoisuus järjestelmien käyttötarkoituksesta ja käytöstä. Esimerkiksi tekniset kulunvalvontaratkaisut toimivat tarkoituksenmukaisesti ainoastaan silloin, kun hallinnollisen turvallisuuden toimenpiteet toteutuvat: kehittyneimmätään kulunvalvonta- ja rikosilmoitinjärjestelmät eivät kykene suojaamaan tilaa ulkopuoliselta pääsylvä, mikäli henkilöstö ei ole sitoutunut noudattamaan organisaation vierailijakäytäntöjä tai ohjeita turvallisuusjärjestelmien käyttöä koskien. Näin ollen teknisten järjestelyjen ohella tarvitaan siis ohjeistusta ja toimivaa turvallisuuskulttuuria, jotta toimenpiteiden toteutumisesta voidaan varmistua. (Leppänen 2006, 49.)

Toimitilaturvallisuuden ratkaisujen suunnittelussa ja toteuttamisessa on huomioitava suojausmenetelmien tarkoituksenmukainen mitoittaminen tilaturvallisuudelta vaaditun tason mukaisesti. Riskienhallinnan kustannusten ja toimenpiteiden suhdetta on kuvattu kuviossa 4. Liian matalatasoinen suojaus aiheuttaa sen, että fyysiseen tilaturvallisuuteen kohdistuvat riskit jäävät korkealle tasolle. Toisaalta taas ylimitoitettut suojausmenetelmät eivät ole kustannustehokkuudeltaan tarkoituksenmukainen ratkaisu, vaan kustannukset ylittävät toteutuksesta saatavan hyödyn. Suojausmenetelmiltä vaadittavan tason määrittäminen perustuu suojattavien arvojen määrittämiseen, arvoihin kohdistuvien riskien tunnistamiseen sekä tunnistettujen riskien arvioimiseen. (Halibozek & Kovacich 2009, 205.)



Kuvio 4: Riskienhallinnan kustannusten ja toimenpiteiden suhde (mukailtu Leppänen 2006, 164)

Toimitilaturvallisuuden ratkaisujen mitoittamista tilojen suojaustarpeen mukaisesti helpottaa tilojen jaottelu turvallisuusvyöhykkeisiin tilan käyttötarkoituksen ja tilassa käsiteltävän tiedon suojaustasoluokituksen mukaisesti. Valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa on määritelty, että luokiteltujen asiakirjojen säilyttämiseen tai käsittelyyn tarkoitettujen tilojen on oltava tarpeenmukaisella tasolla suojattu luvattomalta pääsylvä. (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 14 §).

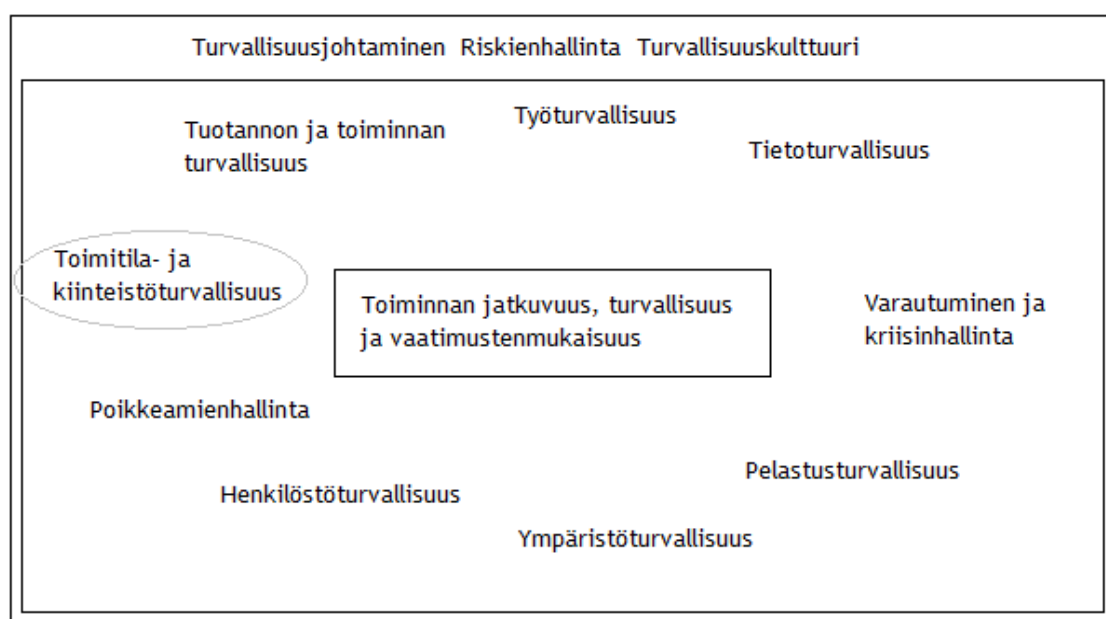
Asetuksen täytäntöönpanoa tukemaan luotu ohje tietoturvallisuudesta valtionhallinnossa puolestaan ohjeistaa yksityiskohtaisemmin eri tietoturvallisuustasojille asetetut tekniset ja hallinnolliset vaatimukset (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 14). Asetuksessa ja sen toimeenpano-ohjeessa tietojenkäsittely-ympäristöt ja tietojen hallitseminen luokitellaan kolmeen tasoon: tietoturvallisuuden perustaso, korotettu taso sekä korkea taso.

Organisaation on oleellista kyetä luokittelemaan asiakirjansa asiakirjojen luokittelusta annettujen ohjeiden mukaisesti. Tällöin välttyään yli- tai alimitoittamasta asiakirjojen luokitteluun perustuvien turvallisuusvyöhykkeiden suojaamiseksi toteutettavia toimenpiteitä toimitilaturvallisuuden tai turvallisuuden muiden osa-alueiden saralla. Asiakirjojen luokittelu ja turvallisuusvyöhykkeiden määrittäminen auttaa suunnittelemaan ja mitoittamaan tarpeenmukaiset turvallisuustoimet kustannustehokkaalle tasolle.

Toimitilaturvallisuuden toimenpiteet liittyvät olennaisesti muihin organisaatioturvallisuuden osa-alueisiin, joten huomiota on kiinnitettävä toimenpiteiden kokonaisuuden hallintaan. Turvallisuuden osa-alueiden turvallisuustoimenpiteiden on tärkeää tukea toisiaan mahdollisimman tehokkaasti, mutta toisaalta on myös vältettävä päällekkäisiä tai keskenään ristiriitaisia toteutuksia. Toimenpiteet on suunniteltava siten, että ne tukevat yhteistä päämäärää. (Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva 2012, 10.)

3.3 Toimitilaturvallisuuden toteuttamiseen vaikuttavia organisaatioturvallisuuden muita osa-alueita

Turvallisuuden eri osa-alueilla toteutettavilla turvallisuustoimenpiteillä on vaikutusta organisaation yleiseen turvallisuustasoon ja toisiin turvallisuuden osa-alueisiin. Toimivassa organisaatioturvallisuuden toteuttamismallissa toimenpiteet on suunniteltu ja mitoitettu siten, että ne tukevat toisiaan. Seuraavassa on lyhyesti käyty läpi organisaatioturvallisuuden osa-alueiden yhtymäkohdat toimitilaturvallisuuden toteuttamiseen. Elinkeinoelämän keskusliiton mukainen turvallisuuden osa-alueiden jaottelu on esitelty kuviossa 5.



Kuvio 5: Organisaatioturvallisuuden osa-alueet (mukailtu Yritysturvallisuus 2016)

3.3.1 Tietoturvallisuus

Tietopääoma on yksi organisaatioiden tärkeimmistä suojattavista arvoista, ja sen merkitys organisaatioiden toiminnalle ja toiminnan jatkuvuudelle on yhä merkittävämmässä roolissa (Halibozek & Kovacich 2009, 205). Niin valtionhallinnossa kuin muissakin organisaatioissa tie-

toturvallisuuden pääasiallisena tavoitteena on turvata organisaation toiminnan kannalta oleellisten tietojen luottamuksellisuus, eheys ja saatavuus, ja näin varmistaa toiminnan häiriötön jatkuvuus (Valtionhallinnon tietoturvallisuuden johtoryhmä 2003).

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI jaottelee organisaation tietoturvallisuuden kahdeksaan erilliseen osa-alueeseen:

- "fyysinen turvallisuus
- hallinnollinen tietoturvallisuus
- henkilöstöturvallisuus
- käyttöturvallisuus
- laitteistoturvallisuus
- ohjelmistoturvallisuus
- tietoaineistoturvallisuus
- tietoliikenneturvallisuus"

(Tietoturvallisuuden arviointi valtionhallinnossa 2006, 47.)

Tietoturvallisuuden osa-alueisiin kuuluva fyysinen tietoturvallisuus käsittää toimitilaturvallisuuden ylläpitämiseksi toteutettavia toimenpiteitä. Organisaation toimitilojen fyysisellä suojaamisella pyritään rakenteellisiin ja turvateknisiin järjestelyin estämään organisaation toiminnan kannalta tärkeiden tietojen tuhoutuminen, vahingoittuminen tai joutuminen väriin käsiin. (Tietoturvallisuuden arviointi valtionhallinnossa 2006, 50.)

Toisaalta osa-alueiden riippuvuussuhde on havaittavissa myös toisinpäin: organisaation tietoturvallisuuden tason voidaan nähdä olevan tärkeä tekijä toimitilaturvallisuuden toteuttamisessa. Tilaturvallisuuden teknisten valvontajärjestelmien toteuttaminen ja ylläpito vaatii turvallisia tietoteknisiä ratkaisuja esimerkiksi tietoliikenne- ja laitteistoturvallisuuden osalta. (Fennelly 2013, 322.)

3.3.2 Henkilöstöturvallisuus

Organisaation henkilöstöturvallisuuden tavoitteena on suojata organisaation suojattavia arvoja ja toimintoja henkilöstön aiheuttamilta riskeiltä, jotka voivat olla joko tahattomia tai tahallisia. Henkilöstöriskettä hallitaan työsuhteen koko elinkaaren aikana aina rekrytoinnista työsuhteen päättämiseen. Työsuhteen aikana toimiva henkilöstöhallinto sekä turvallisuuskulttuurin ja turvallisuustietoisuuden jalkauttaminen auttavat hallitsemaan henkilöstön aiheuttamia riskejä. (Leppänen 2006, 285-286.)

Henkilöstöturvallisuuden toimenpiteet tukevat toimitilaturvallisuuden toteuttamista. Jotta toimitilaturvallisuus toteutuu käytännössä, tulee henkilöstöllä olla tietoisuus siitä, kuinka ja

minkä vuoksi heidän tulee turvallisuustoimia toteuttaa. Usein henkilöstöturvallisuuden riskienhallintatoimenpiteiden suunnitteluvaihetta haastavampaa on toimenpiteiden jalkauttaminen käytäntöön. Toimivan turvallisuuskulttuurin luominen organisaatioon vaatii turvallisuusjohdon ja muun johdon sitoutumista, jotta myös henkilöstö saadaan osallistettua riittävän tehokkaasti. Jos henkilöstö kokee turvallisuustoimenpiteiden olevan työntekoa ja toimintaa hankaloittavia tekijöitä, on riskinä että toimenpiteet jäävät toteuttamatta. (Reid 2004, 250.)

Kehittyneimmätkään turvallisuustekniikan ratkaisut eivät riitä takaamaan turvallisuustoimenpiteiden tehokkuutta, mikäli henkilöstö ei ole sitoutunut turvallisiin toimintamalleihin, eikä tue turvallisuusratkaisuja toiminnallaan. Henkilöstön turvallisuuskoulutuksen avulla varmistetaan, että he tietävät kuinka heidän tulee tilaturvallisuuden toimenpiteitä toteuttaa. Muutoin organisaation turvallisuuskulttuuri voi jäädä heikoksi, ja turvallisuusvaatimusten toteuttaminen väistämättä puutteelliseksi. Turvallisuuden on tärkeää olla osa henkilöstön työtehtäviä, jotta se ei jää organisaation toiminnasta irralliseksi osa-alueeksi. Toimitilaturvallisuuden ratkaisut tulisivat kyetä huomioimaan ihmisten jokapäiväisessä toiminnassa, jotta niiden tehokkuudesta voidaan varmistua. (Sennewald 2011, 235-236.)

3.3.3 Sidosryhmäturvallisuus

Organisaatioiden sidosryhmätyön laajuuden ja monipuolisuuden vuoksi on sidosryhmiin liittyvien riskien hallitseminen haastava osa-alue. Nykyään organisaatioiden toiminta ja palveluiden tuottaminen on yhä riippuvaisempaa organisaation sidosryhmistä. Sidosryhmien merkitys toimintojen toteuttamiselle ja jatkuvuudelle on huomioitava turvallisuusriskienhallinnan keinoin, ja sidosryhmät tulee sisällyttää myös jatkuvuussuunnitteluun. Toimiva tiedonvaihto sidosryhmien välillä mahdollistaa sen, että tiedot organisaatioiden esittämistä vaatimuksista ja niiden toteuttamisessa mahdollisesti esiintyvistä ongelmista tulevat ajoissa ja riittävässä laajuudessa muiden toimijoiden tietoisuuteen. (Toiminnan jatkuvuuden hallinta 2016, 28.)

Sidosryhmäriskeihin pyritään varautumaan laatimalla sopimuskumppanien kanssa riittävän yksityiskohtaiset kirjalliset sopimukset, joissa kuvataan toimintaan liittyvät vastuut ja velvollisuudet. Useat organisaatiot ulkoistavat sidosryhmille toimitilaturvallisuuden toteuttamiseen liittyviä toimintoja, kuten esimerkiksi turvallisuusjärjestelmien huollon ja ylläpidon tai vartiointin. Tällöin on erityisen tärkeää, että ulkoistettujen palveluntarjoajien kanssa on huolehdittu tarpeenmukaisista sopimusehdoista, ja että ehtojen toteutumista myös valvotaan ja toimintojen laatua seurataan systemaattisesti. (Halibozek & Kovacich 2009, 224-225.)

Sidosryhmäturvallisuuteen liittyen on huomioitava paitsi suoraan sopimussuhteiset palveluntarjoajat, mutta myös organisaation tiloissa liikkuvat ja organisaation tietoa käsittelevät ulkopuoliset toimijat. Heidän osaltaan on sovittava sopimusteitse tarpeenmukaisista turvallisuuskäytännöistä ja toimintamallit on ohjeistettava henkilöstölle. Lisäksi on huolehdittava

palveluntarjoajien taustaselvityksistä ja muista luotettavuusmenettelyistä. (Halibozek & Kovacich 2009, 218.)

Toisaalta vaatimukset on luonnollisesti huomioitava myös toiseen suuntaan, sillä tavallista on, että myös sidosryhmät asettavat organisaatiolle vaatimuksia. Sidosryhmäyhteistyön sujuvuuden kannalta on tärkeää, että organisaatio ja sidosryhmät pystyvät tarvittaessa osoittamaan oman turvallisuutensa tilan sopimuskumppanilleen. Sopimuskumppanit voivat vaatia näyttöä, että organisaation turvallisuusasiat ovat hallinnassa ja toiminta on häiriötöntä, ennen kuin yhteistyöhön on mahdollista ryhtyä. Sidosryhmien turvallisuuden auditoinneissa on järkevää hyödyntää tarpeenmukaisia auditointityökaluja ja standardeja. (Yritysten rikosturvallisuus 2012.)

4 Tullin toimitilaturvallisuuden nykytilanne

Tullin toimitilaturvallisuutta käsittelevässä luvussa kuvataan organisaation toimitilaturvallisuuden liittyviä vaatimuksia, taustatekijöitä sekä haasteita. Asiat on pyritty kirjaamaan hyvin yleisellä tasolla, mutta kuitenkin kuvatut vaatimukset ja haasteet ovat tunnistettavissa pitkälti samoiksi kuin monia muitakin julkishallinnon toimijoita koskevat taustatekijät.

4.1 Toiminta ja toimitilat

Työn kohdeorganisaationa toimiva Tulli on valtakunnan laajuinen palvelu- ja lainvalvontaorganisaatio. Tullin päätehtäviin kuuluu tavarakaupan sujuvuuden edistäminen ja oikeellisuuden varmistaminen sekä tavaroiden valmistukseen ja ulkomaankauppaan liittyvien verojen, tullien ja maksujen kantaminen. Suomen ja EU:n taloudellisiin etuihin kohdistuvien uhkien ja tullirikollisuutta torjunnan lisäksi Tulli hoitaa yhteiskunnan, ympäristön ja kansalaisten suojaamiseen liittyviä tehtäviä torjumalla erilaisia terveyteen ja turvallisuuteen kohdistuvia uhkia. (Suomen tullin palvelu- ja lainvalvontaorganisaatio 2009.)

Päätehtäviensä suorittamista varten Tullin toiminnot jakautuvat ulkomaankauppa- ja verotusosastoon, valvontaosastoon, hallinto-osastoon sekä toimipaikkaosastoon. Tulliin kuuluu yhdeksän itsenäisesti toimivaa tullia, joita ovat Helsingin tullin, Lentotulli, Kotka, Vaalimaa, Nuijamaa, Imatra, Turku, Tornio ja Maarianhamina. (Tulli tutuksi 2016.)

Tullin käytössä on valtakunnallisesti yhteensä yli sata toimitilaa, joissa Tulli toimii joko omistajan, vuokralaisen tai alivuokralaisen roolissa. Osa tiloista on yhteiskäyttöisiä muiden viranomaisten tai toimijoiden kanssa ja osa tiloista puolestaan toimii niin sanottuina kylmätiloina, varastoina tai autotalleina, joissa on miehitystä paikalla ainoastaan tarpeen vaatiessa. Koska Tullin toimitilojen sijainti, koko, käyttötarkoitus ja käyttöaste vaihtelevat laajasti, tulee tilojen turvallisuusvaatimuksia määrittäessä kyetä huomioimaan edellä mainittujen lisäksi myös

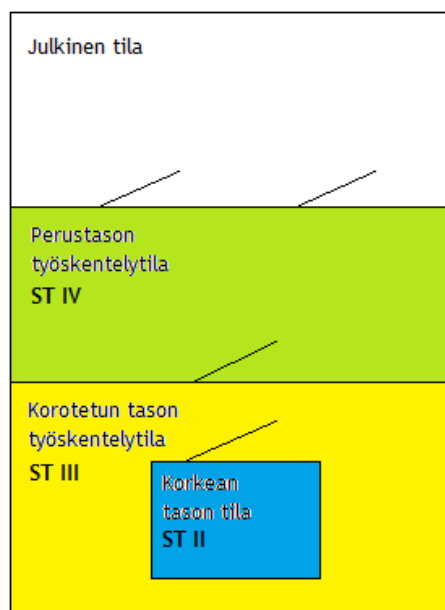
monia muita eri tekijöitä, jotta pystytään saavuttamaan kullekin tilalle tarkoituksenmukaiset turvallisuusjärjestelyt ja turvallisuustaso.

Tullin toimitilaturvallisuuden toteuttaminen perustuu vahvasti aihealuetta sääteleviin asetuksiin, ohjeisiin ja linjauksiin. Toimitilaturvallisuuden kehittäminen Tullissa on pitkälti samojen haasteiden edessä kuin työn toisessa ja kolmannessa luvussa yleisellä tasolla kuvatut organisaatioturvallisuuden nykytila ja sen haasteet. Organisaation kustannussäästötarpeet rajoittavat väistämättä myös Tullin turvallisuusratkaisujen toteuttamista, vaikka turvallisuuden tilan parantamisen perimmäisenä tarkoituksena olisikin lisätä organisaation toimintakykyä sekä toiminnan laatua ja tuloksellisuutta (Future of Corporate Security 2010, 29.).

4.2 Tilojen turvallisuusvyöhykejaottelu

Valtionhallinnon toimitilojen tietoturvaohjeen (VAHTI 2/2013) mukaan viranomaisten tilojen turvallisuusvyöhykkeet ovat rajattuja alueita, joiden ulkokuoriin ja kuorien aukkojen turvallisuuden kohdistuu erityisiä ohjeessa kuvattuja turvallisuusvaatimuksia. Lisäksi viranomaisten käytössä oleviin toimitiloihin voi sisältyä myös niin kutsuttuja julkisia tiloja, kuten esimerkiksi aula- ja yleisöpalvelutiloja, joissa ei säilytetä luokiteltua tietoa, eikä näille tiloille ole tietoturvallisuusasetuksessa määritetty erityisiä toimitilaturvallisuusvaatimuksia.

Tulli noudattaa tilojen turvallisuusvyöhykejaossa Valtionhallinnon toimitilojen tietoturvaohjeen mukaista jaottelua. Kuviossa 6 on kuvamuodossa yleistasoinen esimerkki tilojen turvallisuusvyöhykeluokittelusta. Toimitilat on luokiteltu neljään erilliseen turvallisuusvyöhykkeeseen. Lisäksi tilojen sisällä voidaan suorittaa tullitoimintokohtaista tasoluokittelua, jonka avulla varmistutaan siitä, että tiedonsaantitarpeen periaate toteutuu, eli että tiedot ovat pelkästään niiden henkilöiden saatavilla, joilla on tarve kyseisiä tietoja käsitellä. Tarvittaessa henkilöstön kulkuoikeuksia vyöhykkeiden välillä voidaan rajata esimerkiksi kulunvalvonnallisesti.



Kuvio 6: Tilojen turvallisuusvyöhykeluokittelu (mukailtu Toimitilojen tietoturvaohje 2013, 20)

Suunnitteilla ja tulossa olevien toimitilojen osalta on tavoitteena pystyä jakamaan tilat turvallisuusvyöhykkeisiin jo tilasuunnitteluvaiheessa, jolloin tiloja koskevat rakenteellisten ratkaisuiden voidaan todeta olevan sopivia riittävän hyvissä ajoin. Tällöin myös teknisten suojausmenettelyiden etukäteissuunnittelu mahdollistuu, joka taas mahdollistaa turvallisuusjärjestelyjen toteuttamisen paitsi vaatimusten mukaisella tasolla mutta myös kustannustehokkaasti. Tähän mennessä organisaation haasteena on ollut se, että tilaturvallisuusvaatimuserittelyä ei välttämättä ole osattu tehdä riittävän aikaisessa vaiheessa ja riittävän yksityiskohtaisella tasolla, jolloin turvallisuussuunnittelun ja -toteutuksen osalta ei ole päästy parhaaseen mahdolliseen lopputulokseen.

Organisaation turvallisuusvyöhykemäärittelyyn vaikuttavat oleellisesti paitsi salassa pidettävän tiedon suojaustaso, niin myös tilakohtaisen riskianalyysin pohjalta tehdyt uhka-arviot. Tilan riskianalyysi tulisi pyrkiä tekemään toiminto- ja toimipaikkakohtaisesti, jotta kyetään huomioimaan toimipaikkakohtaiset erot muun muassa toimintaympäristön osalta. Lisäksi on huomioitava käytännön toimintojen osalta esimerkiksi tiedon käsittelytapa, eli käsitelläänkö tilassa tietoa sähköisesti, manuaalisesti vai suullisesti, sekä jätetäänkö tieto tilaan säilytykseen vai ei (Toimitilojen tietoturvaohje 2013).

Tullin toimitilojen luokittelu turvallisuusvyöhykkeisiin on hoidettu edellä mainittujen vaatimusten mukaisesti. Paitsi että turvallisuusvyöhykejako suoritetaan suojaustasoluokittelun tiedon mukaisesti, niin organisaation tulee analysoida toimintaympäristönsä ja tiloihinsa koh-

distuvia riskejä, ja huomioida riskianalyysin tulokset soveltuvin osin tilojen turvallisuusvyöhykkeitä määritettäessä ja toteutettaessa (Toimitilojen tietoturvaohje 2013, 19).

4.3 Turvallisuusvyöhykkeiden tilaturvallisuusvaatimukset

Tullin käytössä on valtakunnallisesti yhteensä noin sata toimitilaa, joiden sijainti, toimintaympäristö, koko, käyttötarkoitus ja käyttöaste vaihtelevat laajasti. Kaikki edellä mainitut tekijät tulee kyetä huomioimaan suoritettaessa tilaturvallisuutta koskevaa riskianalyysia ja määritettäessä tiloja koskevia organisaation sisäisiä turvallisuusvaatimuksia.

Edellisessä kohdassa kuvatut salassa pidettävien tietojen suojaustasoluokat määrittävät sen, millaisia käsittelyvaatimuksia tietojen osalta on noudatettava. Valtioneuvoston tietoturvallisuusasetuksessa edellytetään, että jo perustasolla (asiakirjojen suojataso IV) asiakirjojen käsittely- ja säilytystilat ovat riittävästi suojatut ja valvotut. Perustasoa korkeammilla tasoilla (asiakirjojen suojaustasot I-III) edellytetään perustasoa huomattavasti tiukempia tilaturvallisuusjärjestelyitä.

Tullin toimitilojen tilaturvallisuusvaatimukset pohjautuvat valtioneuvoston tietoturvallisuusasetuksen täytäntöönpanon tueksi laadittuun Toimitilojen tietoturvaohjeeseen. Ohjeessa on annettu suuntaviivat toimitilojen rakentamissuunnittelulle sekä toimitilojen turvallisuutta parantaville rakenteellisille ja teknisille ratkaisuille. Ohje auttaa huomioimaan kansalliset lakisääteiset sekä kansainvälisten turvallisuussäännösten toimitilaturvallisuuden vaatimukset, ja antaa perusteet virastokohtaisen toimitilaturvallisuuden soveltamisohjeen laatimiselle (Toimitilojen tietoturvaohje 2/2013).

Tulli on laatinut toimitilojen tietoturvaohjeeseen perustuvan Tullin toimitilaturvallisuuden toteuttamisohjeen, jossa ohjeen vaatimuksia on pyritty kirjaamaan organisaation omat tarpeet huomioivalle tasolle. Tullin ohje sisältää vaatimukset eri turvallisuusvyöhykkeen tiloille, mutta ohjeessa ei ole niin yksityiskohtaisella tasolla huomioitu esimerkiksi erilaisten erityistilojen vaatimuksia, että ohjetta voisi suoraan hyödyntää tila- tai turvasuunnittelun apuvälineenä. Organisaatiolla on siis ollut selkeä tarve saada käyttöönsä yksityiskohtaisemmat tilaturvallisuusvaatimukset sisältävä työkalu, jossa on laajemmin huomioitu erityyppisiä tilaratkaisuja.

Valtionhallinnon säästötoimenpiteiden seurauksena Tulli, kuten myös monet muut valtionhallinnon toimijat, on aiempaa enemmän siirtynyt ja siirtymässä monitoimityötilojen toteuttamiseen, joka mahdollistaa tilojen kustannustehokkaan hyödyntämisen. Toimitilojen tietoturvaohjeen (VAHTI 2/2013) mukaisesti perustason ja korotetun tason vyöhykkeillä on mahdollista hyödyntää avo- tai monitoimityötilatoteutusta. Kuitenkin pääsy perustasoa korkeamman turvallisuustason vyöhykkeelle tulee olla vain niillä henkilöillä, joiden työtehtävät tätä edellyt-

tävät. Monitoimityötilat ja nimeämättömiin työpisteisiin siirtyminen vaativat siis yksityiskohtaista ja ennakoivaa etukäteissuunnittelua, jotta tarpeenmukaiset turvallisuusratkaisut ja henkilöiden kulkuoikeusrajaukset tilojen välillä on mahdollista toteuttaa.

4.4 Asiakirjojen suojaustasoluokittelu

Salassa pidettävällä asiakirjalla tarkoitetaan kaikkia niitä asiakirjoja, jotka on lainsäädännössä määritelty pidettäväksi salassa. Laki viranomaisten toiminnan julkisuudesta määrittelee 5§ toisessa momentissa viranomaisen asiakirjan seuraavasti:

”Viranomaisen asiakirjalla tarkoitetaan viranomaisen hallussa olevaa asiakirjaa, jonka viranomainen tai sen palveluksessa oleva on laatinut taikka joka on toimitettu viranomaiselle asian käsittelyä varten tai muuten sen toimialaan tai tehtäviin kuuluvassa asiassa. Viranomaisen laatimana pidetään myös asiakirjaa, joka on laadittu viranomaisen antaman toimeksiannon johdosta, ja viranomaiselle toimitettuna asiakirjana asiakirjaa, joka on annettu viranomaisen toimeksiannosta tai muuten sen lukuun toimivalle toimeksiantotehtävän suorittamista varten.”

Julkisuuslain 24 §:ssä on lueteltu yksityiskohtaisesti, mitkä viranomaisen asiakirjat ovat salassa pidettäviä.

Tietoturvallisuusasetuksen 8 §:ssä säädetään salassa pidettävien asiakirjojen ja tietojen luokituksen perusteista. Asetuksen mukaan salassa pidettävät asiakirjat ja niihin sisältyvät tiedot luokitellaan perustuen niiden käsittelyssä vaadittaviin tietoturvallisuusvaatimuksiin. Luokittelu on mahdollista suorittaa myös siten, että tietoturvallisuusvaatimukset kohdistuvat ennenkaikkea niihin asiakirjoihin tai asiakirjan käsittelyvaiheisiin, joissa tietoturvallisuustoimenpiteet ovat suojattavan edun vuoksi tarpeen. Luokittelu on kuitenkin mahdollista tehdä vain niille asiakirjoille, suojattavan edun vuoksi käsittelyvaatimusten noudattamisen on tarpeenmukaista.

Salassa pidettävien asiakirjojen luokittelussa myös Tullissa käytetään valtionhallinnossa seuraavia käsittelyvaatimuksia osoittavia suojaustasoja valtioneuvoston tietoturvallisuusasetuksen (681/2010) 9§ mukaisesti:

”*Suojaustaso I*, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitettulle yleiselle edulle.

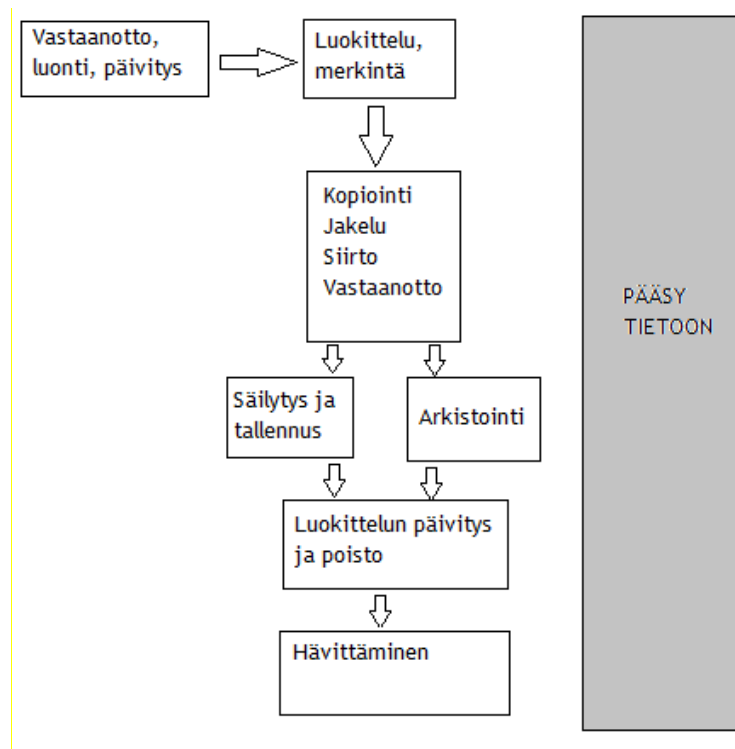
Suojaustaso II, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitettulle yleiselle edulle.

Suojaustaso III, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitettulle yleiselle tai yksityiselle edulle.

Suojaustaso IV, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitettulle yleiselle tai yksityiselle edulle.”

Edellä mainitun suojaustasojaottelun lisäksi kansainvälisten aineistojen luokittelun ja käsittelyn osalta on huomioitava kansainväliset tietoturvelvoitteet, joista säädetään laissa kansainvälisistä tietoturvaluokittelusta (588/2004). Kansainväliset tietoturvelvoitteet ohjaavat viranomaisen toimenpiteitä erityissuojattavan tietoaineiston säilytystilojen turvallisuusvaatimusten sekä tietoaineiston käsittelyn aikaisen suojaamiseen liittyvien vaatimusten toteuttamiseksi.

Organisaation tietosuojalle asetettujen vaatimusten on tärkeää toteutua tietojen käsittelyn kaikissa vaiheissa tiedon luomisesta tai vastaanottamisesta sen hävittämiseen saakka. Tiedon käsittelyn vaiheet valtioneuvoston ohjeistuksen perusteella on kuvattu kuviossa 7. Koska Tulli pyrkii täyttämään tietosuojalle ja sitä myötä myös tilaturvallisuudelle asetetut vaatimukset tiedon käsittelyn kaikissa vaiheissa, on koko tiedonkäsittelyketjun oltava tiedossa, jotta kaikkien vaiheiden varalle voidaan suunnitella tarpeenmukaiset suojaustoimenpiteet. Myös henkilöstön on tunnettava tietojenkäsittelyä koskevat vaatimukset kaikissa tiedonkäsittelyn vaiheissa.



Kuvio 7: Tiedon käsittelyn vaiheet (mukailtu Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2013)

Tietoturvallisuusasetuksen osalta oleellista on tietojen luokittelun todenmukaisuus, koska väärällä tasolla tehty luokitus voi johtaa joko lisäkustannuksiin tai liian alhaiseen turvallisuustasoon (Toimitilaturvallisuuden toteuttamishoje 2010, 13). Asiakirjan suojaustaso määräytyy sen sisältämien tietojen ylimmän suojaustason mukaisesti (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 68). Toisaalta täytyy myös huomioida tietoturvallisuusasetuksen vaatimus, jonka mukaisesti asiakirjoja ei saa luokitella, mikäli se suojattavan edun vuoksi ei ole tarpeellista (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 8 §).

Haasteena myös kohdeorganisaatiossa on suojaustasoluokittelun oikeellinen suorittaminen, koska tulojen turvallisuusvyöhykeluokittelu tehdään pääsääntöisesti tiloissa käsiteltävän tiedon suojaustasoluokittukseen perustuen. Henkilöstön on tärkeää tuntea ja hallita tietojen luokittelua koskevat ohjeet sekä tiedon käsittelyssä tarvittavien työvälineiden turvallisuusmenettelyt. Henkilöstölle tulee antaa säännöllisesti tarvittavaa koulutusta, jotta tietojen luokittelu tapahtuu todellisen tarpeen mukaisesti, eikä tiedon luottamuksellisuus vaarannu väärän tai kokonaan tekemättä jääneen luokittelun vuoksi. (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 37.)

4.5 Valtion toimitilastrategia

Muiden valtionhallinnon toimijoiden tavoin myös Tullin toimitilaturvallisuuden toteuttamista ohjaa vahvasti paitsi jo aiemmin mainittu valtioneuvoston tietoturvallisuusasetus, mutta merkittävä rooli on myös valtioneuvoston periaatepäätöksellä valtion uudesta toimitilastrategiasta, joka hyväksyttiin vuoden 2014 lopussa. Valtion toimitilastrategia korostaa tilojen muuntojoustavuutta, tilatehokkuuden parantamista sekä uusien työnteon tapojen, kuten esimerkiksi etätyön, tukemista (Valtioneuvoston periaatepäätös valtion toimitilastrategiaksi 2014).

Strategiassa tilaturvallisuusnäkökulmaa on sivuttu tilaratkaisujen tavoitetilakuvauksessa, jossa tavoitetilaksi on määritelty tilojen terveellisyys ja turvallisuus sekä valtion kokonaisedun ja yhteiskuntavastuullisuuden varmistaminen. Tilojen turvallisuuteen liittyvät kysymykset ja vastuut on nähty tärkeäksi määritellä tilojen vuokrauksen yhteydessä, varsinkin silloin, kun tilojen saattamiseksi tarpeenmukaiselle tasolle vaaditaan perusparannuksia tai suurempia korjauksia. Koska tilan käyttäjän turvallisuusvaatimukset kasvattavat rakennushankkeiden kustannuksia, tulee niiden olla tarkoituksenmukaisella tasolla toteutettu.

Tilatoteutuksilta vaaditut kustannussäästöt aiheuttavat sen, että myös tilaturvallisuusratkaisuissa tulee kyetä löytämään kustannustehokkain ratkaisu riittävän turvallisuuden tason takaamiseksi, ja ylimitoitettuja ratkaisuja tulee kyetä välttämään. Huomionarvoinen strateginen linjaus myös Tullin tilahankkeisiin liittyen koskee turvallisuussopimusten yhdenmukaistamista. Yhdenmukaiset sopimusmallit auttavat yhtenäistämään palveluntuottajille asetettavia turvallisuusvaatimuksia sekä tarvittaessa edistävät tilojen yhteiskäyttöä muiden valtionhallinnon toimijoiden kanssa.

Valtion toimitilastrategian linjausten mukaiset vaatimukset tilojen muuntojoustavuuden, etätyön lisääntymisen ja kustannussäästöjen osalta luovat omat haasteensa Tullin toimitilaturvallisuuden toteuttamiselle. Toimitilojen turvallisuusvyöhykkeet vaativat eritasoisia rakenteellisia ja teknisiä turvallisuusratkaisuja, jotka on tärkeää huomioida myös tilojen muutostilanteissa. Lisäksi tilojen muuntojoustavuus tarkoittaa sitä, että myös tilojen turvallisuusratkaisuiden tulisi tarvittaessa kyetä joustamaan tiloissa tapahtuvien muutosten myötä. Muuntojoustavuuden vaatimus aiheuttaa paineita tilojen turvallisuussuunnittelulle, ja saattaa vaatia myös uudenlaisia toteutusmalleja vanhoihin ratkaisuihin verrattuna. Myös etätyön tuomat haasteet vaativat organisaatiolta kokonaan uusia tietoturvallisuusratkaisuita ja tietoturvallisuuden toteuttamismalleja.

5 Keskeiset asetukset ja standardit

Seuraavassa luvussa on soveltuvin osin kuvattu kohdeorganisaation tilaturvallisuuden toteuttamista säätelevät ja ohjaavat lait, asetukset ja standardit.

5.1 Laki viranomaisten toiminnan julkisuudesta

Laissa viranomaisten toiminnan julkisuudesta säädetään viranomaisia koskevasta vaitiolovelvollisuudesta, asiakirjojen salassapitovelvoitteesta sekä eräistä muista tietojen saantia koskevista rajoituksista, joiden tarkoituksena on yleisen ja yksityisen edun suojaaminen. Laissa säädetään yksityiskohtaisesti viranomaisten velvollisuuksista lain tarkoituksen toteuttamiseksi erilaisten asiakirjojen ja tietojen osalta.

Julkisuuslain mukaan viranomaisten on huolehdittava siitä, että heidän asiakirjojensa ja tietojärjestelmiensä tietosuojaa, eheys ja laatu turvataan asianmukaisin menettelytavoittein, joita määritettäessä huomioidaan tietojen merkitys ja käyttötarkoitus. Tietojen suojaamiseen tähtäävien toimenpiteiden tavoitteena on henkilötietoja käsiteltäessä varmistua yksityiselämän suojan ja muiden yksityisyyden suojaa turvaavien perusoikeuksien toteutumisesta. Laissa määritellään myös, että toimenpiteillä pyritään lisäksi edistämään hyvää tietojenkäsittelytappaa. (Laki viranomaisten toiminnan julkisuudesta 621/1999.) Laissa on selkeitä vaatimuksia organisaation tietoturvallisuuden ja asiakirjojen käsittelyn osalta.

5.2 Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa

Valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010) säädetään valtionhallinnon viranomaisten asiakirjojen luokittelua ja käsittelyä koskevista tietoturvallisuusvelvoitteista. Asetus perustuu viranomaisten toiminnan julkisuutta koskevaan Julkisuuslakiin (621/1999), jossa määritetään viranomaisten asiakirjojen julkisuutta ja salassapitoa koskevat velvoitteet.

Tietoturvallisuusasetuksessa edellytetään, että valtionhallinnon toimijoiden tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja. Asetuksessa on määritetty toimitilaturvallisuusvaatimukset eri suojaustasojen tiedon käsittely-ympäristöille. Asetuksen 14 §:ssä on kuvattu yksityiskohtaisesti luokiteltujen asiakirjojen käsittely- ja säilytystiloja koskevat turvallisuusvaatimukset. Vaatimukset edellyttävät, että joiden mukaan valtionhallinnon viranomaisen on toiminassaan toteutettava seuraavia toimenpiteitä:

- 1) "tilat, joissa säilytetään tai muutoin käsitellään luokiteltuja asiakirjoja, suojataan asianmukaisesti lukituksella, kulunvalvonnalla ja muilla toimenpiteillä luvattoman pääsyn estämiseksi tiloihin ja siellä oleviin asiakirjoihin;
- 2) henkilöt, joille annetaan pääsy tiloihin, joissa säilytetään tai muutoin käsitellään suojaustasoon I tai II kuuluvia asiakirjoja, ovat tunnistettavissa;

- 3) suojaustasoon I ja II kuuluvat asiakirjat säilytetään sellaisessa kassakaapissa tai muussa lukittavassa kaapissa, holvissa tai tilassa, joka estää luvattoman pääsyn asiakirjaan sisältyviin tietoihin;
- 4) henkilöt, joille annetaan pääsy arkistoon taikka tietokonekeskukseen tai muihin tietojärjestelmien ylläpidon tai tietoliikenteen toimivuuden kannalta merkityksellisiin tiloihin, joissa säilytetään tai käsitellään suojaustasoon III kuuluvia asiakirjoja taikka suojaustasoon IV kuuluvia valtakunnalliseen henkilörekisteriin talletettuja asiakirjoja, ovat tunnistettavissa.”

(Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 14§.)

Lisäksi asetuksessa säädetään, että mikäli asiakirjan tai siihen sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi mahdollisesti aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle julkisuuslain 24 §:n 1 momentin 2 ja 7-10 kohdassa tarkoitetulla tavalla, tulee asiakirjat suojaustasomerkinnän lisäksi tai sen sijasta luokitella erityisellä turvallisuusluokitusmerkinnällä (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010).

5.3 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (2/2010) on laadittu tukemaan valtioneuvoston tietoturvallisuusasetuksen toimeenpanoa. Ohje linjaa valtionhallinnon toimijoiden toimitilaturvallisuuden perusteita. Ohjeessa myös määritellään yksityiskohtaiset tietoturvallisuusvaatimukset perustason, korotetun tason ja korkean tason tilojen osalta.

Ohjeessa tilaturvallisuudella käsitetään erilaiset rakenteelliset ja valvonnalliset turvallisuusjärjestelyt, joiden avulla on tarkoitus varmistaa tilojen ja niissä käsiteltävien ja säilytettävien tietojen pysyminen vain oikeutettujen tahojen hallinnassa ja käytössä. Viranomaisen on määriteltävä vastuullaan olevien tilojen turvallisuusratkaisut, joiden tulee käsittää rakenteelliset ratkaisut, valvontajärjestelmät sekä tarpeenmukaiset tilojen käyttöoikeuksiin liittyvät vaatimukset. (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2/2010.)

5.4 Toimitilojen tietoturvaohje

Valtionhallinnon toimitilojen tietoturvaohje (VAHTI 2/2013) ohjaa tietoturvallisuusasetuksen (681/2010) toimeenpanoa. Ohjeen tarkoitus on auttaa valtionhallinnon toimijoita suunnittelemaan ja toteuttamaan toimitilaturvallisuuteen liittyviä toimenpiteitä, joiden tavoitteena on

varmistua salassa pidettävien tietojen luottamuksellisuudesta. Ohje antaa suuntaviivat rakentamissuunnittelulle sekä olemassa olevien toimitilojen turvallisuussuunnittelulle, sekä auttaa luomaan menettelytavat lakisääteisten velvoitteiden ja kansallisten ja kansainvälisten toimitilaturvallisuusvaatimusten toteuttamiseksi.

Toimitilojen tietoturvaohjeeseen on sisällytetty VAHTI:n vuonna 2012 julkaisema ohje ICT-varautumisen vaatimuksista, joten sitä suositellaan hyödynnettävän myös suunniteltaessa ja toteutettaessa uusia tietoteknisiä laiteiloja. Lisäksi ohjeessa on soveltuvin osin huomioitu kansallisen turvallisuusauditointikriteeristö Katakriin toimitilaturvallisuusveloitteet.

5.5 Kansallinen turvallisuusauditointikriteeristö

Katakri (2015) on viranomaisten käyttöön tarkoitettu auditointityökalu, jota käytetään arvioitaessa sidosryhmien kykyä suojata viranomaisen salassa pidettävää tietoa. Katakria hyödynnetään auditointityökaluna arvioitaessa kohdeyrityksen turvallisuusjärjestelyjen tasoa yritysturvallisuusselvityksessä tai viranomaisten tietojärjestelmien turvallisuusarvioinnissa. Lisäksi Katakria voidaan käyttää työkaluna organisaatioiden turvallisuustyössä ja sen kehittämisessä.

Katakri käsittää sekä kansallisiin säädöksiin että kansainvälisiin veloitteisiin pohjautuvat vähimmäisvaatimukset. Vaatimukset perustuvat voimassa olevaan lainsäädäntöön sekä Suomea sitoviin kansainvälisiin tietoturvallisuusveloitteisiin. Katakriin vaatimukset ovat pääosin yhteneväiset valtioneuvoston tietoturvallisuusasetuksen vaatimusten ja niiden toteuttamista ohjaavien ohjeiden kanssa, osin Katakri menee yksityiskohtaisemmalle tasolle.

5.6 Finanssialan keskusliiton standardit ja ohjeet

Valtionhallinnon toimitilojen tietoturvaohje (2/2013) sisältää suoria viittauksia seuraaviin Finanssialan keskusliiton standardeihin. Ohjeiden sisältöä on hyödynnetty myös laadittaessa Tullin sisäisiä ohjeita ja malleja toimitilaturvallisuuden toteuttamiseksi.

- Rakenteellinen murtosuojeluohje I-III
- Murtohälytysjärjestelmät ja -palvelut ohje 2008
- Rakenteellisen murtosuojauksen tuotteet
- Standardi SFS-EN 1627: Ristikot, kalterit ja murransuojaovet
- Standardi SFS-EN 356: Murransuojalasit ja kalvot
- Standardi SFS-EN 1627 (-1630): Murransuojaseinät (tai Pohjoismaisen normin SSF 1047 mukaisen testauksen ja sertifiointin mukaan)

FK:n ohjeet on laadittu Finanssialan keskusliiton Vakuutuslainsäädäntö ja turvallisuus -yksikössä. Ohjeet on suunnattu vakuutusyhtiöille vakuutusehtojen laadinnan tueksi, sekä toi-

mijoille suojattavan kohteen turvallisuusratkaisuiden, -järjestelmien ja -palveluiden valinnan ja suunnittelun apuvälineeksi. (Murtohälytysjärjestelmät ja -palvelut ohje 2008.) Kohdeorganisaatio hyödyntää tarpeen mukaisissa hankinnoissaan ohjeiden sisältämiä tietoja tuotteista ja niiden luokista.

6 Kehittämistyön toteuttaminen

Luvussa on kuvattu opinnäytetyön tutkimuksen ja kehittämisosion etenemistä. Luku sisältää kuvauksen tutkimuksen lähtökohdista aina tutkimusotteesta tutkimusstrategiaan. Lisäksi kuvataan käytetyt tutkimusaineiston tiedonkeruumenetelmät sekä aikataulut.

6.1 Tutkimuksellinen kehittäminen

Tutkittavan ilmiön ja siihen liittyvän taustateorian perusteella on työn tutkimusotteeksi valikoitunut kvalitatiivinen tutkimusote (Heinonen, Keinänen, Paasonen 2013, 33). Metsämuurosen (2011) mukaan laadullinen tutkimusote soveltuu tutkimuksiin, joissa tarkastellaan tapahtumien yksityiskohtaisia rakenteita ja tutkitaan tilanteita, joissa kaikkia vaikuttavia tekijöitä ei voida kontrolloida. Jotta työn tavoitteeksi asetetun lopputuloksen tarkoituksenmukaisuudesta voidaan varmistua, ohjautuu tutkimus siis selkeästi laadullisen tutkimuksen suuntaan.

Kirjosen (2007, 117-118) mukaan yksi tutkimuksen teon tavoitteista voi olla kehittäminen avulla muuttaa organisaation tiettyä toimintoa aikaisempaa parempaan tai tehokkaampaan suuntaan. Tämän opinnäytetyön tutkimuksellisen osion tarkoituksena oli auttaa kehittämään työkalu, jonka avulla kohdeorganisaation tilaturvallisuuden tasoa voidaan pyrkiä nostamaan tarpeenmukaiselle tasolle.

Tutkimusstrategian valintaa ohjaa tutkimuksen tarkoitus tai tehtävä (Hirsjärvi, Remes, Sajavaara 2012, 137). Laadulliselle tutkimukselle on ominaista, että tutkimusongelma täsmentyy tutkimuksen aikana: johtoajatus on selvillä tutkimusta suunniteltaessa, mutta tutkimusprosessin aikana tutkimukseen liittyvät ratkaisut saattavat saada uusia muotoja ja suuntia (Aaltola, Valli 2001, 69-70). Myös tämän tutkimuksen tutkimusongelmia tuli tutkimuksen edetessä kyetä muokkaamaan tarpeenmukaiseen suuntaan.

Tieteellisen tutkimuksen tekemisessä on oleellista tutkimuskysymyksen tai -tehtävän onnistunut muotoileminen ja asettaminen. Jotta opinnäytetyön kehittämiskohteena olevan organisaation toimitilaturvallisuuden taso saataisiin nostettua halutulle tasolle, tuli jo työn alkuvaiheessa kyetä määrittelemään kehitystyön kohteena oleva ongelma tai kysymys. Koska kyseessä on kvalitatiivinen tutkimus, on tutkimuksen teon teorioita kuitenkin mahdollista ja myös tarpeellista muuttaa tämän järjestyksen osalta (Hirsjärvi ym. 2012, 125). Tämän opinnäyte-

työn osalta tämä tarkoitti sitä, että vasta tavoitteenasettelun jälkeen linjattiin tarkemmin käytettävät tutkimusmenetelmät.

6.2 Tutkimusaineiston valinta ja keräämisen aikataulu

Laadulliselle tutkimukselle on ominaista, että tutkimuksen kohde voi olla hyvinkin moniulotteinen. Tutkittavan kohteen eri osa-alueet muovaavat ja vaikuttavat toisiinsa samanaikaisesti, josta syystä tutkimuskohdetta on pyrittävä käsittelemään mahdollisimman kokonaisvaltaisesti näkökulmasta. (Hirsjärvi ym. 2012, 161.) Yhtenä suurimpana haasteena, joka on seurausta tutkimuskohteen käsittelyn laajasta näkökulmasta, voi pitää tutkimusasetelman tarkoituksenmukaista rajaamista. Tutkimusasetelman rajaaminen on välttämätöntä mielekkään ja ehyen ongelmanasettelun löytämiseksi. Tutkimuksessa saatu aineisto kasvaa helposti liian laajaksi, joten varsinaisen tutkimusasetelman ulkopuolinen aineisto on kyettävä rajaamaan lopullisen tutkimuksen ulkopuolelle. (Aaltola & Valli 2001, 71.)

Koska aineiston rajaaminen tapahtuu viime kädessä tutkimuksen tekijän toimesta, on siinä väistämättä ainakin osin kyse tulkinnallisesta rajauksesta. Laadullinen aineisto ei siis sellaiseenaan kuvaa todellisuutta, vaan tutkijan omat tarkastelunäkökulmat ja rajaukset vaikuttavat kerättävän aineiston luonteeseen. Tämä on huomioitava jo tutkimustehtävän rajausvaiheessa, jotta tutkimusaineiston ydinsanoma on tunnistettavissa ja hyödynnettävissä myöhemmissä vaiheissa. (Aaltola & Valli 2001, 71-72.) Opinnäytetyön tutkimuskysymysten ratkaisemiseksi suoritettuna tutkimuksessa ei aineiston rajauksen kanssa tullut ongelmia, koska tutkimuksen lopputuloksena tarvittavan aineiston määrä ja laatu oli määritelty etukäteen riittävän yksityiskohtaisella tasolla. Ongelmia oli pikemminkin siinä, ettei valitun tutkimusmenetelmän avulla saatu riittävän yksityiskohtaisia vastauksia esitettyihin kysymyksiin.

Kvalitatiivisessa tutkimuksessa on tavoitteena tulkita ja ymmärtää tutkittavaa asiaa, ja tutkimusaineiston keräämiseen käytetäänkin useimmiten avoimia kysymyksiä (Heinonen ym. 2013, 35). Myös tässä tutkimuksessa tarvittavien taustatietojen keräämiseen käytettiin pääsääntöisesti avoimia kirjallisia kysymyksiä, joihin saatuja vastauksia tarkennettiin tarpeen mukaan suullisten kysymysten avulla. Vastauksia selvityksen aiheena oleviin kysymyksiin haettiin myös havainnoinnin menetelmin, silloin kun kirjalliset ja suulliset kysymykset eivät tuottaneet riittävän yksityiskohtaista tietoa.

Toimitilaturvallisuuden nykytilakartoituksessa selvitettiin Tullin toimitilojen yleistasoiset tiedot tiloissa sijaitsevista turvallisuusvyöhykkeistä sekä tilojen turvallisuusjärjestelyistä. Kartoituksessa toimipaikoille lähetettiin kysely, jossa toimipaikkojen tuli kuvata mitä turvallisuusvyöhykkeitä toimipaikalla on, ja mitä turvallisuusjärjestelmiä tiloissa on käytössä.

Kartoitus kohdistui yhteensä 110 toimipaikkaan. Luku käsittää kaikki kiinteistöt, jotka ovat Tullin omistuksessa, joissa Tulli on vuokralaisena tai jossa Tullilla muutoin on toimintaa. Tullin toimipaikkojen pääpiirteittäinen maantieteellinen sijoittautuminen käy ilmi kuviosta 8. Kartoituksen ulkopuolelle jätettiin sellaiset Tullin käytössä olevat tilat, joissa ei säilytetä suojaustasoluokiteltua tietoa ja joissa ei ole Tullin kiinteitä tietoliikenneyhteyksiä. Tällaisia tiloja ovat monet niin sanotut kylmäasemat, joissa Tullin henkilökunta käy ainoastaan tarpeen vaatiessa suorittamassa esimerkiksi asiakaspalvelua. Nämä tilat edellyttävät erilaisia turvallisuusratkaisuja kuin miehitettyjen tilojen turvallisuustoimenpiteet, eikä niitä näin ollen ollut tässä tutkimuksessa tarvetta huomioida.

Alueittaiset lukumäärätiedot kartoitukseen sisällytetyistä toimitiloista ovat seuraavat:

Eteläinen alue 39

Itäinen 28

Läntinen 22

Pohjoinen 21



Kuvio 8: Tullin toimipaikat vuonna 2015 (Tullitoimipaikat kartalla)

6.3 Tiedonhankinnan menetelmät

Tutkimusmenetelmillä tarkoitetaan sitä, miten käsiteltävänä olevaan ilmiöön suhtaudutaan. Tutkimusaineiston keräämiseksi on käytettävissä useita erilaisia tiedonkeruutapoja eli tutkimusmenetelmiä. Tutkittavan kohteen perusteella tehdään valinta käytettävistä tutkimusmenetelmistä. Yksityiskohtaista tarkastelua vaativaa aihe tarvitsee hitaan ja yksityiskohtaisen tutkimusmenetelmän ja päinvastoin. (Heinonen ym. 2013, 35.)

Hirsjärven ym. (2013, 187-188) mukaan tutkimusaineiston keräämismenetelmiä on olemassa neljää tyyppiä: kysely, haastattelu, havainnointi ja dokumenttien käyttö. Tässä työssä käytettiin menetelminä kyselytutkimusta, jonka avulla saatuja tietoja tarkennettiin tarvittaessa

tarkentavin kysymyksiin, sekä havainnointia. Tutkimuksessa syynä usean menetelmän käytölle oli ennen kaikkea se, että kerätyn tiedon haluttiin olevan mahdollisimman kattavaa ja oikeellista, ja Metsämuurosen (2001, 64) mukaan menetelmätriangulaation eli usean tutkimusmenetelmän avulla saatua tietoa voidaan pitää varmempana kuin pelkästään yhdellä menetelmällä kerättyä tietoa.

6.3.1 Kyselytutkimus

Tutkimuksessa käytetyt tutkimusmenetelmät valinnassa oleellista oli, että kerätty tutkimusaineisto on riittävän yksityiskohtaista, jotta voidaan varmistua aineiston hyödynnettävyydestä tutkimuksessa. Kartoitettavien toimitilojen suuren lukumäärän vuoksi ei ollut mahdollista tutustua jokaiseen tilaan empiirisesti, joten pääasiallisesti tutkimusmenetelmäksi toimitilojen nykytilan määrittämiseksi valikoitui kyselytutkimus.

Kyselytutkimus on käyttökelpoinen menetelmä, kun tarkoituksena on suorittaa laajoja yleiskartoituksia tai tehdä esitutkimusta tarkemmille tutkimuksille (Heinonen ym. 213, 38). Näin ollen kyselytutkimus oli looginen valinta tutkimusmenetelmäksi selvitetessä Tullin toimipaikkojen turvallisuuden tilaa. Tarvittavien tietojen saamiseksi toteutettiin kyselytutkimus Tullin toimipaikoille. Tutkimuksen kyselylomake on nähtävillä liitteessä 1.

Kyselytutkimus oli tarkoitus suorittaa aikavälillä huhtikuu-kesäkuu 2015. Todellisuudessa kyselyn vastauksia ei saatu kerättyä suunnitellulla aikataululla, vaan lopulliset täydelliset vastaukset saatiin kokoon vasta syyskuussa 2015. Suoritetun kyselytutkimuksen tarkempi toteutusai-kataulu on nähtävillä kuviosta 9.

4/2015	6/2015	6-8/2015	10/2015
Nykytilakartoituksen kyselytutkimuksen aloitus	Kyselyn vastausten pyydetty toimitusaika	Vastausten tarkentavien tietojen kerääminen -havainnoinnit -tarkentavat kysymykset	Nykytilakartoituksen tulokset valmiit ja dokumentoitu

Kuvio 9: Kyselytutkimuksen suorittamisen aikataulu

Suoritettaessa kyselytutkimusta on kyselylomake olennainen tutkimusväline, joten lomakkeen suunnitteluvaiheessa tulisi tutkimuksen kohteena oleva tutkimusongelma olla riittävän yksityiskohtaisella tasolla kuvattuna (Heinonen ym. 2013, 40). Toimipaikoille lähetetyssä kyselylomakkeessa pyrittiin saamaan selville toimipaikkojen turvallisuusvyöhykejaottelu sekä tiedot turvallisuusjärjestelmien toteutuksesta. Koska aihealueen oletettiin olen vieras ainakin osalle

kyselyyn vastaavista tahoista, toimitettiin varsinaisen kyselyn liitteenä tarkentavaa materiaalia, jonka oli tarkoitus ohjata kyselyn vastaajia toimittamaan tarvittavat tiedot mahdollisimman yksityiskohtaisella ja todenmukaisella tasolla.

Pelkän kyselytutkimuksen avulla ei kuitenkaan onnistuttu keräämään tarvittavan yksityiskohtaisia tietoja, joten tarkentavia kysymyksiä jouduttiin tekemään haastattelumenetelmin puhelimitse ja sähköpostilla. Muutaman suuren ja haastavan toimitilan osalta tutkimusaineistoa kerättiin kyselyn ohella myös empiirisesti havainnoimalla tilojen turvallisuusratkaisuja tilaturva-auditointien avulla.

Aikataulu kyselytutkimuksen suorittamiseksi oli hyvin tiukka. Toimipaikoille annettiin tarkka päivämäärä, johon mennessä toimitilaturvallisuuskartoitukseen tuli vastata. Vastausten saamisen jälkeen toteutettiin tarvittavat toimenpiteet puuttuvien tietojen selvittämiseksi. Käytännössä jouduttiin kysymään lisätietoja ja tarkennuksia valtaosasta saatuja vastaksia. Lisäksi vieraillemalla paikan päällä saatiin riittävän tarkat tiedot, mikäli esimerkiksi toimitilojen turvallisuusvyöhykkeiden tunnistaminen riittävällä tasolla osoittautuu liian haasteelliseksi toteuttaa toimipaikkojen toimesta.

Toimipaikoille lähetetty toimitilaturvallisuuskartoitus päädyttiin lähettämään alueellisten hallintopalvelupäälliköiden kautta, joita pyydettiin ohjaamaan kartoitukset toimipaikkojen vastuushenkilöille. Toimipaikoilla on nimetyt paikalliset toimitilaryhmän edustajat, joilla on pääsyoikeudet kiinteistönhallinnan Optimaze-järjestelmään, josta on saatavilla toimitilojen ajantasaiset pohjakuvat. Vastuushenkilöiden vastuulla oli täyttää tilojen pohjakuviin tiedot tilojen turvallisuusvyöhykejaottelusta sekä turvallisuusteknisistä ratkaisuista.

Ennen kyselyn vastausajankohdan umpeutumista hallintopalvelupäälliköille lähetettiin kyselystä muistutus, jossa tarkennettiin vastausten sisällön vaatimuksia. Suuressa osassa vastauksista on merkattu pohjakuviin ainoastaan turvallisuusvyöhykkeet, mutta turvallisuusjärjestelmistä ei vastauksissa ollut riittävän yksityiskohtaista tietoa. Pohjakuviin pyydettiin merkinnät tilojen valvontakameroista, rikosilmoitinjärjestelmän ilmaisimista sekä kulunvalvonnan alaisuudessa olevista ovista.

Tutkimuksen yhteydessä suoritettussa kyselytutkimuksessa kaikilta kyselyyn vastaajilta kysyttiin samoja asioita toimipaikan koosta ja toiminnoista riippumatta. Kaikkien toimipaikkojen myös odotettiin vastaavan kyselyyn: mikäli vastausta ei saatu määräaikaan mennessä, pyydettiin tietoja uudelleen tai toisen vastuushenkilön kautta. Mikäli vastausta ei saatu, selvitettiin kartoituksen vaatimat tiedot puhelimitse haastatteleamalla.

Kyselylomakkeen avulla kerättiin tiedot toimipaikkojen tilaturvallisuuden nykytilasta. Toimipaikkoja koskevat taustatiedot, kuten esimerkiksi kiinteistön osoite, koko ja muut tilaa koskevat perustiedot, olivat saatavilla keskitetysti, eikä niitä ollut tarvetta kyselylomakkeella selvittää. Kyselyt lähetettiin alueellisille (etelä, länsi, itä ja pohjoinen) hallintopalvelupäälliköille, jotka sitten osoittivat kyselyt edelleen paikallisille toimipaikkojen toimitiloista vastaaville henkilöille.

Kyselyssä toimipaikkojen odotettiin täyttävän tilojen pohjapiirroksiin tiedot turvallisuusvyöhykkeistä sekä yksityiskohdat tilojen turvallisuusjärjestelmien sijainnista. Käytetty kyselylomake ei ollut muodoltaan varsinainen lomake, johon vastaajat olisivat voineet suoraan tarvittavat tiedot täyttää. Koska tavoitteena oli saada toimipaikkojen tilaturvallisuusjärjestelyt liitettyä tilojen pohjakuviin, toimi lomake pikemminkin ohjeistuksena, jonka mukaisesti vastaajat täydensivät tarvittavat tiedot tilojen pohjakuviin.

Lisäksi kyselyn mukana liitteenä toimitettiin tarvittavat ohjeet koskien muun muassa tilojen turvallisuusvyöhykejaottelun suorittamista. Vastaajien pyytäessä lisäohjeistusta, annettiin heille puhelimitse sekä sähköpostitse yksityiskohtaisia neuvoja luokittelun suorittamiseksi ja tarvittavien tietojen toimittamiseksi. Lisätarkennuksia jouduttiin tekemään valtaosaan saaduista vastauksista.

Tiedusteltaessa jälkikäteen kyselyyn vastaajilta syytä saatujen vastausten vaillinaisuuteen, oli osasyynä kyselylomakkeen liian yleistasoisen ohjeistus, ja toisaalta taas vastaajien puutteelliset teoriatiedot koskien teknisiä turvallisuusjärjestelmiä ja tilojen turvallisuusvyöhykeluokittelua. Kyselylomakkeen laadinnassa haasteellista oli se, että kyselyä laadittaessa ei ollut yksityiskohtaista tietoa siitä, mikä taho vastaukset kyselyyn tulee kunkin toimipaikan osalta antaa. Lisäksi kyseessä on sen verran laaja ja monimutkainen aihealue, että riittävän yksityiskohtaisen ohjeistuksen antaminen pelkästään kyselyn saatekirjeessä osoittautui hankalaksi.

Toimipaikoille suoritetun kyselytutkimuksen avulla ei saatu kerättyä tietoa riittävän laajasti ja yksityiskohtaisesti, vaan saatuja vastauksia jouduttiin tarkentamaan puhelimitse ja sähköpostitse tehtävillä tarkentavilla kysymyksillä. Puhelimitse ja sähköpostitse tehtävien tarkentavien kysymysten tarkoituksena oli varmistaa kartoitusten tulosten yhdenmukaisuus sekä luotettavuus. Vallitsevan tilanteen kartoittamisen oli tärkeää tarpeen onnistua luotettavasti ja yhdenmukaisesti, jotta tulosten perusteella voitiin tehdä riittävät päätelmät nykytilanteesta.

6.3.2 Havainnointi

Tieteellisellä havainnoinnilla tarkoitetaan tutkimusaineiston keräämistä, jossa tarvittava tieto kootaan systemaattisesti. Koottavan tiedon tulee olla riittävän tarkkaa sekä ehdottoman luot-

tettavaa, joten onnistunut havainnoinnin suorittaminen edellyttää aina ennakkosuunnittelua. Ennen havainnoinnin suorittamista on siis päätettävä mitä, miten ja milloin tutkitaan. (Heinonen ym. 2013, 35-36.)

Vaikka tutkimuksen pääasiallisena tutkimusmenetelmänä käytettiin kyselytutkimusta, ei kaikkia tarvittavia tietoja ollut mahdollista kerätä kyselytutkimuksen avulla. Näin ollen osassa toimipaikkoja suoritettiin havainnointia paikan päällä joko ennen kyselylomakkeen lähettämistä tai sen lähettämisen jälkeen, jotta tarvittavat tiedot saatiin kerättyä tarpeenmukaisella tarkkuudella kaikista toimipaikoista. Havainnoinnin avulla saatiin kerättyä toimipaikkojen tiedot riittävän yksityiskohtaisella tasolla, ja lisäksi voitiin varmistua saatujen tietojen paikkansapitävyydestä.

Toimipaikkojen turvallisuusjärjestelyjen tilan havainnointi tapahtui turvallisuusauditoinnin keinoin. Auditoidtavat toimipaikat valikoituivat joko laajuutensa tai niissä suoritettavien toimintojen perusteella. Myös kyselytutkimukseen vastaamisessa ilmenevät haasteet antoivat aiheita auditointikäyntien suorittamiselle. Osa auditoinneista liittyi meneillään oleviin tai suunnittelun asteella oleviin toimitilojen muutoshankkeisiin, eikä pelkästään toimitilojen turvallisuuden tilan kartoittamiseen. Kuitenkin näiden auditointien yhteydessä saadut tiedot olivat käyttökelpoisia myös kartoituksen tulosten käsittelyssä.

Kaikkien tilojen havainnointi, eli paikan päällä suoritettavat tilaturva-auditoinnit, olisivat oletettavasti taanneet kyselytutkimuksen tuloksia tarkemmat ja oikeellisemmat tiedot selvityksen kohteena olleista asioista. Aikataulujen ja resurssien puolesta sadan tilan havainnointi olisi kuitenkin ollut mahdoton tehtävä, joten havainnointia päädyttiin suorittamaan vain muutama tutkimuskohteeseen.

7 Tutkimustulokset

Luvussa esitellään työn tutkimuskysymysten tulokset. Ensin käsitellään tutkimustulosten yhteenvetoa kokonaisuutena, jonka jälkeen käydään yksilöllisesti läpi tulokset tutkimuskysymyksittäin.

7.1 Tutkimustulosten yhteenveto

Tutkimuksessa pyrittiin hakemaan vastauksia kolmeen erilliseen tutkimuskysymykseen. Ensimmäiseen tutkimuskysymykseen haettiin vastauksia kyselytutkimuksen avulla. Toisen tutkimuskysymyksen vastaukset perustuvat osin ensimmäiseen tutkimuskysymyksen tuloksiin, jonka lisäksi vastauksia ja tausta-aineistoa on haettu organisaatioturvallisuuden yleisistä teorioista. Kolmannen tutkimuskysymyksen vastaukset ovat muotoutuneet kahden muun tutkimuskysymyksen perusteella, jonka lisäksi kyseisen tutkimuskysymyksen teoreettinen viitekehys poh-

jautuu valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa -mukaisiin tilaturvallisuusvaatimuksiin.

Työn tutkimuskysymykset ja keskeisimmät vastaukset on esitetty taulukossa 2.

Tutkimuskysymys	Keskeisimmät vastaukset
Mikä on Tullin toimipaikkojen toimitilaturvallisuuden nykytila? (luku 7.2.)	<ul style="list-style-type: none"> • Tutkimuksen tuloksena saatiin tiedot kaikkien toimipaikkojen turvallisuusvyöhykejaottelusta sekä tilaturvallisuusratkaisuista • Yleisiä huomioita Tullin toimitilaturvallisuuden nykytilasta: <ul style="list-style-type: none"> ○ Toimitilaturvallisuusratkaisuissa on puutteita tilaturvallisuudelle asetettuihin vaatimuksiin nähden ○ Toimipaikkojen välillä on suuria eroja tilaturvallisuuden tasossa
<p>Mitkä ovat Tullin toimitilaturvallisuuden puutteet ja kehittämiskohteet? (luku 7.3.)</p> <p>Mitkä ovat puutteita selittäviä taustatekijöitä? (luku 7.4.)</p>	<ul style="list-style-type: none"> • Puutteiden ja kehittämiskohteiden esittämismalli on kuvattu kuviossa 11 työn sivulla 56. Taulukon sisältö on salassa pidettävää tietoa, eikä tietoja ole mahdollista esittää opinnäytetyön julkisuuden vuoksi. • Puutteita selittäviä tekijöitä pohjautuen organisaatioturvallisuuden yleisiin oppeihin voivat olla: <ul style="list-style-type: none"> ○ Turvallisuussuunnittelun ennakoimattomuus (luku 7.4.1.) ○ Epätietoisuus vaaditusta turvallisuustasosta (luku 7.4.2.) ○ Yleisen turvallisuustietoisuuden puutteet (luku 7.4.3.)
Millainen toimitilaturvallisuuden toteuttamismalli auttaa saavuttamaan tiloille asetettujen turvallisuusvaatimusten mukaisen lopputuloksen? (luku 7.5.)	<ul style="list-style-type: none"> • Toteuttamismallin avulla on kyettävä jo tilaturvallisuussuunnitteluvaiheessa tunnistamaan tarvittavat tilaturvallisuusratkaisut • Toteuttamismallin sisältämien tilaturvallisuusvaatimusten pohjana toimivat: <ul style="list-style-type: none"> ○ Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa ○ Tullin sisäiset toimitilaturvallisuusvaatimukset

	<ul style="list-style-type: none"> ○ Toimitilaturvallisuuden nykytilakartoituksen (tutkimuskysymys 1) perusteella huomioidut puutteet (tutkimuskysymys 2) • Mallin tavoitteena on, että sen avulla saataisiin myös laajemmin kehitettyä organisaation tilaturvallisuuspuutteisiin johtaneita tekijöitä (luvat 7.4.1.-7.4.3.)
--	--

Taulukko 2: Työn tutkimuskysymykset ja -vastaukset

7.2 Tullitoimipaikkojen toimitilaturvallisuuden nykytila

Projekti tarvitsi käyttöönsä toimipaikkakohtaiset tiedot toimitilojen turvallisuudentasosta, jotta tarpeenmukaiset turvallisuuden tilan parantamistarpeet voitaisiin tunnistaa ja kuvata. Kyselytutkimusten vastausten perusteella saatiin kartoitettua tiedot toimipaikkojen turvallisuusvyöhykejaottelusta sekä tilojen turvallisuustekniikan yksityiskohdista. Esimerkki saadusta tilaturvallisuuskuvauksesta on nähtävillä kuviossa 10.



Kuvio 10: Esimerkki kyselytutkimuksen vastauksena saadusta tilaturvallisuuskuvauksesta

Ensimmäisen tutkimuskysymyksen tuloksena saatiin määritettyä kaikkien Tullin toimitilojen toimintokohtaiset turvallisuusvyöhykkeet ja tilojen yksityiskohtaiset turvallisuusjärjestelyt. Lopputuloksena tilojen eriytyminen eri suojaluokkiin on dokumentoitu, eli vastaukset koostuvat siis 110 tilan pohjakuvasta, joihin on merkitty tilojen turvallisuusvyöhykkeet sekä turvallisuustekniikan ratkaisut. Vastausten ulkoinen laatu vaihtelee, sillä osa vastauksista toimitettiin sähköisesti ja osa manuaalisesti. Kuitenkin kyselylomaketta tarkentavien kysymysten sekä tilojen havainnoinnin avulla pystyttiin varmistamaan, että saadut vastaukset vastaavat todellisuutta. Ensimmäisen tutkimuskysymyksen vastausten oikeellisuus on oleellisen tärkeässä roolissa, koska niiden avulla lähdettiin selvittämään vastausta toiseen ja kolmanteen tutkimuskysymykseen.

7.3 Toimitilaturvallisuuden todetut puutteet ja kehityskohteet

Ensimmäisen tutkimuskysymyksen avulla selvitettyjen toimitilojen nykytilatietojen avulla päästiin selvittämään toimitilojen turvallisuudessa esiintyviä puutteita. Toiseen tutkimuskysymykseen liittyen kuvattiin turvallisuusvyöhykekohtaiset toimitilaturvallisuusratkaisujen kehittämiskohteet kaikille kartoitetuille tiloille. Peilaamalla toimitilojen turvallisuuskartoituksen avulla saatuja tietoja toimipaikkojen tilaturvallisuudesta valtionhallinnon asetuksessa tietoturvallisuudesta säädettyihin vaatimuksiin sekä organisaation sisäisiin vaatimuksiin, voitiin tunnistaa toimitilojen turvallisuusjärjestelyissä ilmenevät puutteet ja kehitysalueet.

Kehittämiskohteiden jatkokäsittelyn helpottamiseksi taulukoitiin kaikki toimitilat taulukkoon, johon merkittiin toimitilojen eri turvallisuusvyöhykkeillä esiintyneet tilaturvallisuusratkaisuiden puutteet. Esimerkki puutteiden ja kehystoimenpiteiden taulukoinnista on nähtävissä kuviossa 11. Tietojen luottamuksellisuuden varmistamiseksi on kuvion toimipaikkasarakkeesta poistettu toimipaikan nimi ja sijainti. Kuvion taulukon sisältöä on myös muokattu siten, että tiedot eivät käsittele todellisten toimipaikkojen tilannetta.

Toimipaikka	Havaitut puutteet: Perustaso	Havaitut puutteet: Korotettu taso	Ehdotetut toimenpiteet	Vaihtoehtoisesti	Muuta
A					
Tiloihin rikosilmoitinjärj.	Tilassa ei rikosilmoitinjärjestelmää.		Liikeläimäisimet kattamaan tilaan johtavat aukot.		Ei tietoliikenneyhteyksiä
Tiloihin rikosilmoitinjärj. KV-lisäystarve 5kpl		4. krs: korotettu+ -tason huoneissa ei kv-lukitusta. 1. krs: Perustason tiloissa sijaitsevilla korotetun tason huoneissa ei kv-lukitusta.	4. krs: Kv-lukitus korotettu+ -tason tiloihin (3 kpl). Ja valvontakamera tilan ovelelle. 1. krs: korotetun tason huoneisiin kv-lukitus (2 kpl) Liikeläimäisimet kattamaan kaikki Tullin tiloihin johtavat aukot.	Kv-lukituksen sijasta vaihtoehtoisesti tilaan johtavat ovet katetaan kameravalvonnalla ja tilat liikeläimäisimillä.	
Kiinteistön kv. Takavarikkotilan oveen mek. turvalukko?		1. krs: Huone 145 mekaanisesti lukittu. 2. krs: Laitetilat 221 ja 227 mek. luk.	1. krs: Kv-lukitus (1 kpl) huoneeseen 145. 2. krs: Kv-lukitus (2 kpl) laitetiloihin (221 ja 227).		
		1. krs: Huone 157 mek. lukittu. Korotetun tason huoneet (1C07.1 ja 1C07) mek. luk.	Kv-lukitus huoneeseen 157. Kv-lukitus huoneisiin (1C07.1 ja 1C07)		
E					
F	Tiloissa mekaaninen lukitus	Laitetilan ovi mek. lukittu.	Kv-lukitus tilaan kohtaviin oviin (3 kpl). Kv-lukitus laitetilan oveen (1kpl).		

Kuvio 11: Tilaturvallisuuden kehittämistarpeet taulukoituna toimipaikoittain

Tilaturvallisuuden tunnistetut muutostarpeet on tärkeää kyetä suhteuttamaan toimitilojen odotetun elinkaaren mukaisiksi, eli toimipaikkojen tilaturvallisuuskartoituksen avulla saatujen tietojen lisäksi oli tärkeää saada riittävän tarkat tiedot toimipaikkojen suunnitellusta jatkos-

ta. Mikäli toimipaikka on lakkautuksen tai suurien muutosten alla muutaman vuoden sisällä, oli asia oleellista huomioida suunniteltaessa ja toteutettaessa kohteen turvallisuusjärjestelyjä. Toimipaikkojen tulossa olevista muutoksista huolimatta kartoitukseen haluttiin sisällyttää kaikki kartoitushetkellä käytössä olevat tilat, mutta tilojen suunniteltu elinkaari huomioitiin toimenpiteiden suunnittelu- ja toteutusvaiheessa.

7.4 Todettujen puutteiden kehittämistoimenpiteet

Toiseen tutkimuskysymykseen liittyvien havaittujen puutteiden ja kehittämiskohteiden osalta oli tärkeää pyrkiä selvittämään taustoja ja tekijöitä, jotka auttavat selittämään toimitilaturvallisuuden osa-alueella esiintyviä turvallisuuspuutteita. Puutteiden korjaamiseksi vaadittavien kehittämistoimenpiteiden määrittäminen onnistuu helpommin, kun puutteiden syntyyn vaikuttaneet tekijät tunnetaan. Nykytilan ja tavoitetilan väliseen eroon johtaneita tekijöitä pyritään löytämään ja selittämään hyödyntämällä työssä aiemmin käsiteltyjä organisaatioturvallisuuden teorioita. Pääsääntöisesti kaikki tulososiossa kuvatut haasteet ja kehittämiskohdet pohjautuvat organisaatioturvallisuutta ja toimitilaturvallisuutta koskevaan taustateoriaan, eivätkä ne täten kuvaa kohdeorganisaation toiminnan virallisia kehittämistarpeita, vaan pikemminkin organisaatioturvallisuuden toteuttamisen haasteita yleisellä tasolla.

7.4.1 Ennakoiva turvallisuussuunnittelu

Kohdeorganisaation tilaturvallisuuden puutteiden voi pitkälti katsoa johtuvan riittämättömästä turvallisuussuunnittelun ennakoinnista. Ennakoivan turvallisuussuunnittelun avulla voidaan todennäköisemmin saavuttaa haluttu tilaturvallisuudentaso, kuin jos suunnittelua ei suoriteta riittävän ajoissa tai yksityiskohtaisesti. Puutteellinen turvallisuussuunnittelu johtaa helposti myös siihen, että tilojen turvallisuusjärjestelyjen yhdenmukaisuus kärsii.

Toimitilojen turvallisuudelle asetetut vaatimukset on huomioitava jo suunniteltaessa toimintojen sijoittamista ja laadittaessa kohteen turvallisuusratkaisuja rakennus- tai tilahankkeen alkuvaiheessa. Vaihtoehtoisten tilaratkaisujen välillä voi olla suuria eroja turvatekniikan kehittämistarpeessa, joten tilaratkaisut on huomioitava kohteiden turvallisuusriskejä arvioitaessa. Rakenteelliset ja tekniset turvallisuusratkaisut ovat osin toisiaan tukevia, joten tilaturvallisuutta on käsiteltävä kokonaisuutena, ja oikeiden rakenteellisten ratkaisujen avulla on mahdollista vaikuttaa tarpeeseen investoida tekniseen valvontaan. Rakenteellisten ja teknisten turvallisuusratkaisuiden ohella huomionarvoisia ovat tilojen toiminnalliseen suunnitteluun liittyvät asiat, kuten toimintojen sijoittaminen tiloissa, tilojen erottaminen toisistaan, kulunvalvonta, avainturvallisuus, kiinteistönhuolto ja vartiointi. (Leppänen 2006, 103, 347.)

Tullin toimitilaturvallisuuden turvallisuusjärjestelyt mitoitetaan ja toteutetaan riskiperusteisesti, huomioiden organisaatiota koskevat lakisääteiset vaatimukset. Varsinaisen toimintota-

solla tapahtuvan riskienarviointityön lisäksi Tullin tilaturvallisuutta auditoidaan toimipaikka-kohtaisesti keskittyen lähinnä toimitila-, tieto- ja henkilöturvallisuusasioihin. Tilaturvallisuuden auditointikäytännöt elävät kuitenkin tapauskohtaisten vaatimusten mukaisesti, eikä auditointiprosessia tai -vaatimuksia ole kuvattu yksityiskohtaisesti. Täten myöskään auditointien tuloksia ei välttämättä laajassa mittakaavassa huomioida riskienhallinnan apuvälineenä, eikä näin ollen hyödynnetä mahdollisuutta käyttää auditointien tuloksia ennakoivan varautumisen kehittämiseen.

Kustannustehokkuuden varmistamiseksi olisi tarkoituksenmukaista kehittää Tullin turvallisuus-suunnitteluprosessia aiempaa ennakoivampaan suuntaan. Näin voitaisiin varmistua siitä, että tilaturvallisuusratkaisut pystytään mitoittamaan tilan ja turvallisuusvyöhykkeen vaatimusten mukaiseksi. Ennakoinnilla voidaan säästää resursseja, ja saavutetaan todennäköisemmin tilaturvallisuudelta vaadittu lopputulos.

7.4.2 Turvallisuusjärjestelyjen yhdenmukaisuus

Tullin toimitilaturvallisuuden nykytilan suurimpia haasteita on tilaturvallisuuden yhtenäisen toteuttamismallin puuttuminen. Syitä mallin puuttumiseen ovat haasteet turvallisuusratkaisuiden suunnittelussa ja hankinnassa, joka puolestaan johtuu osin tietämyksen puutteesta, organisaation taloudellisesta tilanteesta sekä tilahankkeiden puutteellisesta suunnittelusta. Lisäksi useimmilla toimipaikoilla Tulli toimii vuokralaisen roolissa, eikä vuokranantajalla välttämättä ole tarvetta tai halua panostaa kiinteistön turvallisuusratkaisuihin ja turvallisuusjärjestelmiin. Näin ollen vuokralainen joutuu joko neuvottelemaan turvallisuusvaatimusten toteuttamisesta vuokranantajan kanssa tai huolehtimaan niiden toteuttamisesta itsenäisesti.

Toimitilojen turvallisuusauditointeja suoritetaan tarpeenmukaisesti eri laajuuksilla ja tarkkuuksilla, eikä auditointien suorittamisen voi katsoa olevan täysin suunnitelmallista tai järjestelmällistä. Varsinaiseksi haasteeksi on kuitenkin noussut auditoinneilla havaittujen kehitystoimenpiteiden jatkokäsittely ja käytäntöön vieminen. Monesti auditointien tulokset uhkaavat jäädä hallinnollisten prosessien jalkoihin, eikä tarpeellisiksi havaittuja kehitystoimenpiteitä välttämättä ole mahdollista toteuttaa käytännössä.

Vastakkainasettelu turvallisuuden tilan parantamisen ja organisaation taloudellisesti tiukan tilanteen välillä on tällä hetkellä vallitseva tilanne monissa muissakin organisaatioissa. Olisi tärkeää pyrkiä pääsemään yhteisymmärrykseen siitä, mitkä todetuista kehittämistoimista kulloinkin ovat etusijalla, ja mistä on mahdollista tinkiä. Vaatimusten mukainen turvallisuuden tila tulisi kyetä takaamaan kaikissa toimipaikoissa ympäri maan, mutta suoritettun tilaturvallisuuskartoituksen sekä tiloihin suoritettujen turvallisuusauditointien vastausten perusteella kohdeorganisaation toimipaikkojen tilaturvallisuuden tasossa on paikoin merkittäväkin vaihtelua eri toimipaikkojen välillä.

Tullin toimipaikkojen turvallisuuskäytänteiden ja -vaatimusten yhdenmukaistamista työsteetään kuitenkin jatkuvasti eteenpäin. Tavoitteena on pyrkiä toteuttamaan malliesimerkkinä toimivan, tietoturvallisuusasetuksen tilaturvavaatimukset täyttävän, Tullin toimipisteen turvallisuusjärjestelyjä ja -käytäntöjä soveltuvien osin myös muissa tullitoimipaikoissa valtakunnan laajuisesti. Virallisesti kyseessä ei ole benchmarking-menettely, mutta käytännössä vertailu ja kokemusten hyödyntäminen tapahtuu juurikin benchmarkingin oppien mukaisesti.

Ongelma ei sinällään olekaan se, etteikö tiedettäisi miten tilaturvallisuutta toteutetaan, vaan ongelmana ovat lähinnä taloudellisesti rajalliset resurssit toimenpiteiden toteuttamiseksi. Toimitilaturvallisuuden toteuttamismallin tavoitteena on tarjota selkeä näkemys siitä, mitkä auditoinneilla ja riskienarvioinneissa tarpeellisiksi todetuista kehitystoimenpiteistä olisi priorisoitava ennen muita, koska toimenpiteitä joudutaan väistämättä toteuttamaan niiden kriittisyyden sekä tilojen ja toimintojen riskiarvion perusteella.

7.4.3 Turvallisuustietoisuuden lisääminen

Syynä kahdessa edellisessä luvussa käsiteltyyn turvallisuussuunnittelun toimimattomuuteen voi ainakin osin nähdä turvallisuustietoisuuden puutteellisuuden. Puutteet turvallisuusosaamisessa poikivat myös muita ongelmia, jos henkilöstö ei osaa toiminnallaan tukea organisaation tietoturvallisuuden ratkaisuja.

Tarvetta kehittää turvallisuusohjeistusta ja lisätä turvallisuustietoisuutta sivuttiin jo aiemmin turvallisuusjohtamisen teorioiden yhteydessä. Periaatteessa kohdeorganisaatiossa on olemassa laaja-alaisesti turvallisuusohjeita turvallisuuden eri osa-alueilta. Kuitenkin turvallisuusohjeet ja turvalliset toimintamallit tulisi kyetä kohdentamaan henkilöstölle työtehtävien asettamien tarpeiden mukaisesti, jotta ne olisi mahdollista soveltuvien osin viedä henkilöstön tietoisuuteen ja sitä myötä käytäntöön.

Toimitilaturvallisuuden tavoitetilan mukaisten toteutusten käytäntöön vieminen on riippuvaisista henkilöstön asenteesta ja toiminnasta. Edistyneimmistäkin turvateknisistä järjestelyistä ei ole apua, mikäli henkilöstö ei ole sitoutunut turvallisuuskäytäntöjen toteuttamiseen. Organisaation turvallisuus- ja tietoturvallisuuspolitiikoissa kuvatut toimet on onnistuttava sisällyttämään käytännön toimintoihin. Sennewaldin (2011, 235-236) mukaan on johdon vastuulla määrittää paitsi turvallisuuden tavoitetila, mutta myös kuinka asiat viedään käytäntöön ja henkilökunnan tietoisuuteen riittävän tehokkaasti.

Kohdeorganisaation toimitilaturvallisuuden toteuttamiseen liittyvät ohjeet käsittävät pääosin tietoturvallisuuteen sekä palo- ja pelastusturvallisuuteen liittyvät toimintamallit. Lisäksi ohjeiden tulee sisältää tiedot toiminnasta sekä normaali- että poikkeustilanteissa. Poikkeusti-

lanteita koskevat ohjeet on kuvattu lähinnä kiinteistöjen pelastussuunnitelmissa, jotka eivät kuitenkaan välttämättä ole ajan tasalla tai henkilöstön saatavilla. Henkilöstön tietoisuuteen olisi myös tärkeää saattaa ohjeiden taustalla olevat tekijät, eli miksi kyseiset toimintamallit on nähty tarpeellisiksi.

Usein uudenlaisiin turvallisuuden tilan parantamiseen tähtääviin toimintamalleihin on päädytty riskienarvioinnin perusteella, joten niiden toteuttamiselle on olemassa selkeät tarpeet ja perusteet, mutta tämä tieto olisi saatettava soveltuvassa laajuudessa myös henkilöstön tietoisuuteen. Onnistunut viestintä on tärkeä tekijä toteutuneen riskin seurausten hallitsemisessa ja seurauksista toipumisessa. Tiloissa tehtyjen turvallisuusriskienarviointien tulokset olisi tärkeää käsitellä soveltuvalla laajuudella, jotta niiden perusteella tehdyt turvallisuuden kehittämistoimenpiteet saisivat tuekseen konkretiaa, ja ne olisi näin helpompi jalkauttaa käyttöön ja perustella henkilöstölle.

Organisaatiossa on tärkeää hyödyntää riskienarviointityössä saatuja tuloksia havaituista riskeistä ja uhista, ja näiden perusteella linjata tarpeenmukaisia koulutusten aihepiirejä ja sisältöjä. Monet riskeistä olisivat hallittavissa toimintamalleja muutamalla - läheskään aina ei edes ole tarvetta tehdä taloudellisia resursseja vaativia hankintoja. Parhaatkaan elektroniset lukitusjärjestelmät eivät ole turvallisia, mikäli henkilöstöä ei osaa hallita avaimia oikein, koska heitä ei ole ohjeistettu turvallisesta avainten hallinnasta ja toimintamalleista avainten kaatoamistilanteessa. Esimerkiksi myös liian joustavat vierailijakäytännöt saattavat vesittää hyvin suunnitellun ja toteutetun kulunvalvonnan ja lukituksen merkityksen.

Yleisellä tasolla organisaatioiden turvallisuusjohtamisen tavoitteena on organisaation turvallisuuspolitiikan mukaisesti luoda toimiva turvallisuuskulttuuri ja toteuttaa sen vaatimat toimenpiteet myös käytännössä. Vahvan turvallisuuskulttuurin luominen ei onnistu hetkessä, eikä myöskään perinteisiä käskyjohtamisen periaatteita toteuttamalla, vaan vaatii tuekseen poikkitieteellistä ajattelukykyä ja riittäviä sosiaalisia taitoja: Sennewaldin (2011, 235-236) mukaan lähtökohtana toimivan turvallisuuskulttuurin syntymiselle on se, että ihmiset tietävät mitä heiltä odotetaan ja minkä vuoksi, ennen kuin he voivat käytännössä toteuttaa tarvittavia toimintamalleja.

Turvallisuusjohtamisen käytäntöjen kehittämisessä ja kehittämisessä on oleellista huomioida, että turvallisuusjohtaminen vaikuttaa kahteen suuntaan. Ensinnäkin työntekijöiden turvalliset toimintamallit tukevat organisaatiokulttuurin kehittymistä, toisaalta taas muuttamalla organisaatioturvallisuutta tukevia toimintamalleja, voidaan kyetä vaikuttamaan työntekijöiden arvoihin ja uskomuksiin. Motivoinnin avulla voidaan tehostaa esimerkiksi organisaation turvallisuusohjeiden käytäntöön viemistä ja varmistaa työntekijöiden sitoutuminen. Näin henkilöstöl-

lä on mahdollisuus oppia toimimaan itsenäisesti ja tiedostamaan turvallisen toiminnan tarkoitus. (Lämsä & Päivike 2013, 206.)

7.5 Toimitilaturvallisuuden toteuttamismalli

Opinnäytetyön kolmannen ja keskeisimmän tutkimuskysymyksen tuloksena syntyi toimitilaturvallisuuden toteuttamismalli, jonka viitekehystenä toimivat valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa sekä Tullin sisäiset toimitilaturvallisuusvaatimukset. Tarve toteuttamismallille on lähtöisin kohdeorganisaation turvallisuusorganisaatiosta, ja mallin on tarkoitus toimia apuvälineenä organisaation toimitilaturvallisuuden toteuttamisessa ja kehittämisessä. Toteuttamismallin kehittämisen tavoitteena oli, että sen avulla saataisiin kehitettyä aiemmassa kuvattuja kohdeorganisaation kolmea kehittämiskohdetta: turvallisuussuunnitelun suunnitelmallisuutta, turvallisuusratkaisuiden yhdenmukaisuutta sekä henkilöstön turvallisuustietoisuutta.

Toteuttamismallin sisällössä on valtioneuvoston tietoturvallisuusasetuksen ja siihen perustuvan toimitilojen tietoturvaohjeen lisäksi huomioitu organisaation toimintaan liittyviä erityispiirteitä ja -tarpeita. Toimitilojen turvallisuusvaatimuksia määritettäessä tulee huomioida monia eri tekijöitä niin organisaation sisä- kuin ulkopuoleltakin, joita myös kohdeorganisaation toimitilojen osalta on soveltuvin osin pyritty kartoittamaan. Leppäsen (2006, 333) mukaan toimitilaturvallisuuden toteuttamiseen vaikuttavia tilojen toimintaympäristöön liittyviä tekijöitä ovat muun muassa toimipaikan sijainti, alueen kaavoitus, ympäröivät rakennushankkeet sekä lähiympäristön tiet ja pysäköintialueet sekä mahdolliset lastaus- ja purkausalueet. Lisäksi vaadittua turvallisuustasoa kohottavasti tai madaltavasti voivat vaikuttaa organisaation toimiminen erityisalueilla, kuten esimerkiksi satamissa, lentokentillä tai muissa yhteiskäyttöisissä tiloissa.

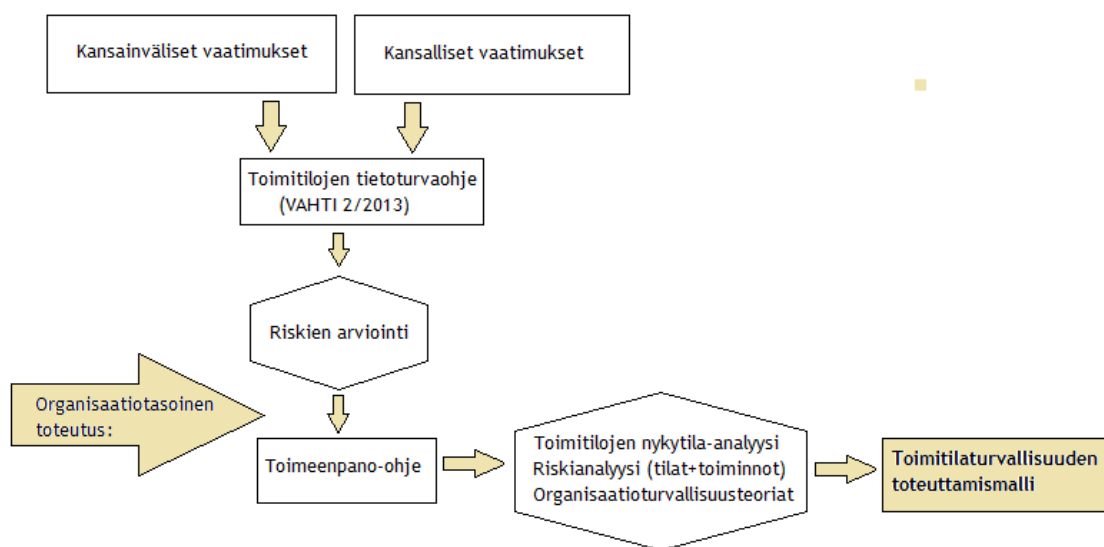
Organisaation sisäisiä toimitilaturvallisuuden vaatimuskriteereitä laadittaessa tuli huomioida myös monia ulkoisia ja taloudellisia tekijöitä, kuten tilojen elinkaari, käyttötarkoitus, toimintaympäristö, erilaiset suoritettavat riskiarviot, kustannusarviot sekä ennen kaikkea myös valtioneuvoston asetuksen tietoturvallisuudesta valtionhallinnossa aiheuttamat vaatimukset. Organisaation sisäisten riskiarviointien perusteella on tietoturvallisuusasetuksen mukaisiin yleisiin vaatimuksiin tehty tarvittavia tila- ja toimintokohtaisia tarkennuksia ja muokkauksia.

Näitä organisaatiotasojen riskiarvioiden perusteella tehtyjä tarkennuksia ja muutoksia toteutettavien turvallisuustoimenpiteiden osalta ei ole salassapitovelvoitteiden vuoksi mahdollista käydä läpi yksityiskohtaisella tasolla tässä työssä. Organisaation tarpeiden mukaan mitoitettujen turvallisuusvaatimusten perusteella on rakennettu Tullin toimitilaturvallisuuden toteuttamismalli, ja opinnäytetyön tarkoituksena on esitellä prosessia, taustatekijöitä ja teoria-tietoa, joiden perusteella toteuttamismallin sisältö on syntynyt.

Toteuttamismallin avulla voidaan varmistaa Tullin toimitilojen turvallisuusjärjestelyjen täytävän viranomaisen toiminnalle asetetut tilaturvallisuusvaatimukset sekä Tullin omaan riskianalyysiin perustuvat turvallisuusvaatimukset. Toimitilaturvallisuuden toteuttamismallia on tarpeen hyödyntää toimitilahankkeissa, jotta voidaan varmistua tilaturvallisuusvaatimusten tulevan huomioiduksi riittävän aikaisessa vaiheessa suunnitteluprosessia. Toteuttamismallia voidaan siis hyödyntää turvallisuussuunnittelun apuvälineenä, ja samalla sen vaatimuksiin tutustuminen lisää organisaation sisäistä tietoisuutta tilaturvallisuusasioista. Toteuttamismalli tarjoaa osaltaan ratkaisun kaikkiin kolmeen kehityskohteeseen, joiden toimitilojen nykytilakartoituksen perusteella todettiin vaativan kehittämistoimenpiteitä (luvut 7.4.1.-7.4.3.).

7.5.1 Toteuttamismallin taustat

Tullissa toimitilaturvallisuuden toteuttamista on tähän mennessä ohjannut Tullin toimitilaturvallisuuden toimeenpano-ohje. Toimeenpano-ohjeessa perustuu suurelta osin valtioneuvoston tietoturvallisuusasetukseen ja sen toteuttamista ohjaavaan tietoturvaohjeeseen. Tullin toimitilaturvallisuuden toimeenpano-ohjeen sovellusperiaate ja ohjeen syntyä ja sisältöä määrittävät asetukset on kuvattu kuviossa 12. Kuviossa näkyy myös toimeenpano-ohjeen ja sen taustalla olevien asetusten ja ohjeiden liittymäpinta luotuun toimitilaturvallisuuden toteuttamismalliin.



Kuvio 2: Tullin toimitilaturvallisuuden toimeenpano-ohjeen sekä toteuttamismallin sovellusperiaate (mukaillen Toimitilojen tietoturvaohje 2013, 14)

Tullin toimitilaturvallisuuden toimeenpano-ohjeessa on kuvattu suojaustasokohtaiset toimitilaturvallisuusvaatimukset, joita Tullin tiloissa pyritään toteuttamaan. Kuitenkin toimeenpano-ohjeen hyödyntäminen on Tullin tilojen turvallisuusjärjestelyjä sekä kokonaan uusia tiloja

suunniteltaessa todettu hankalaksi, koska ohjeessa ei ole riittävän riskiperusteisesti huomioitu toimintojen ja tilatoteutusten erityisvaatimuksia. Tilaturvallisuuden toteuttamista käsittelevät ohjeet ovat hyvin yleisellä tasolla, eikä niissä ole huomioitu toiminto- tai toimintaympäristökohtaisia erityispiirteitä. Toimeenpano-ohjeen rinnalle on siis kaivattu yksityiskohtaisempaa työkalua toimitilaturvallisuuden toteuttamiseksi, jotta voidaan varmistua toimitilaturvallisuusvaatimusten toteutumisesta riittävällä tasolla, kuitenkin ylimitoittamatta turvallisuusjärjestelyjä.

Jotta Tullin toimitilaturvallisuuden ratkaisut saataisiin suunniteltua ja toteutettua todellisen tilanteen vaatimalla tasolla, näki Tullin organisaatioturvallisuustoiminto tarpeelliseksi luoda toimitilaturvallisuuden tilan kehittämiseen ja ylläpitämiseen tähtäävän toimitilaturvallisuuden toteuttamismallin. Opinnäytetyön kehittämiskohteena syntyneitä toimitilaturvallisuuden toteuttamismallia on tarkoitus hyödyntää olemassa olevaa toimitilaturvallisuuden toimeenpano-ohjetta täydentävänä työkaluna. Tullin toimitilaturvallisuuden toteuttamismallia ei kokonaisuudessaan ole mahdollista liittää opinnäytetyöhön, mutta opinnäytetyössä kuvataan mallin syntyyn johtaneet tutkimusvaiheet ja -tulokset sekä toteuttamismallin pääpiirteet.

Toteuttamismallin lähtökohdat ja tarpeet määräytyivät hyvin vahvasti työelämälähtöisesti. Toimitilaturvallisuuden toteuttamismallilla tähdätään sekä valtioneuvoston tietoturvallisuusasetuksessa että Tullin omassa turvallisuusvaatimusmäärittelyssä toimitilaturvallisuudelle asetettujen vaatimusten toteuttamiseen Tullin kaikissa toimitiloissa. Toteuttamismallin sisältämien tilaturvallisuusvaatimusten määrittely pohjautui sekä toimipaikkojen nykytilakartoitukseen että organisaation sisäisiin tarpeisiin.

Toimitilaturvallisuuden toteuttamismalli luotiin vuoden 2016 aikana. Toteuttamismalli pohjautuu valtioneuvoston tietoturvallisuusasetuksen vaatimuksiin perustuvaan Tullin toimitilaturvallisuuden toteuttamisohjeeseen, mutta toteuttamismallissa on pyritty tekemään toteuttamisohjetta enemmän tila-, toiminto- ja toimintoympäristökohtaista riskianalyysia. Merkittävä rooli on ollut toimitilojen nykytilaa selvittäneen turvallisuuskartoituksen tuloksilla, joita on hyödynnetty toiminto- ja toimitilakohtaisessa riskianalyysissa sekä tilaturvapuutteiden kar-toittamisessa. Esimerkki toteuttamismallin rakenteesta on esitetty kuviossa 13.

Kuviossa on esitetty toteuttamismallin ensimmäinen sivu. Lisäksi malli sisältää omat vaatimustaulukkonsa koskien erilaisia erityistiloja. Juuri erityistilojen osalta oli tärkeää saada suoritettua niitä koskeva vaatimusmäärittely, jotta tilat ja niiden vaatimukset voidaan tulevaisuudessa paremmin huomioida jo suunnitteluvaiheessa. Aikaisemmin erityistilojen osalta ei ole ollut yhdenmukaista toteutusmallia, jolloin kyseisten tilojen tilaturvallisuustoteutuksissa on ollut suurta vaihtelua eri tullitoimipaikkojen välillä.

	PERUSTASO	KOROTETTU TASO	KOROTETTU+ TASO	ISPS-alue	24/7 miehitty	Miehittämättömät	Viranomaisyhteistilat
	<ul style="list-style-type: none"> • ST IV tietojen käsittely • Normaalit Tullin työtilat • Vyöhykkeen väri pohjapiirroksissa vihreä 	<ul style="list-style-type: none"> • ST III tietojen käsittely • Vyöhykkeen väri pohjapiirroksissa keltainen 	<ul style="list-style-type: none"> • ST II tietojen käsittely • Erityissuojausta vaativat tilat • Vyöhykkeen väri pohjapiirroksissa sininen 	Huomioidaan ISPS-alueen turvallisuusratkaisut ja -vaatimukset	Aina miehittyjen tilojen osalta huomioidaan teknisten valvontajärjestelmien käytön mahdollisuus	Riskienarvioinnissa huomioitava suojattavat kohteet: mm. onko kiinteät yhteydet/säilytetäänkö tilassa asiakirjoja/muuta suojattavaa.	Toteutus suunnitellaan yhteistyössä vastaamaan kaikkien toimijoiden vaatimuksia.
Aluevalvonta (kohderakennusta välittömästi ympäröivä alue) Tilan kuoren aukot							
Väliseinät							
Alakatto							
Ulko-ovet							
Väliovet							
Ikkunat, kattoikkunat ja lasiseinät							
Lukitus vyöhykkeen rajalla							

Kuvio 13: Toimitilaturvallisuuden toteuttamismallin rakenne

Toimitilaturvallisuuden toteuttamismallissa on pyritty mahdollisimman kattavasti huomioimaan erilaisia toimipaikkakohtaisia tekijöitä, jotka vaikuttavat turvallisuusjärjestelyjen toteuttamistarpeeseen. Erityispiirteet ja riskiarviot huomioiva toteuttamismalli auttaa yleistasoisia ohjeita paremmin saavuttamaan tila- ja turvallisuussuunnittelussa mahdollisimman kustannustehokkaan lopputuloksen, jossa turvallisuusjärjestelyjä ei ole yli- tai alimitoitettu.

Yleistä toteuttamisohjetta yksityiskohtaisempaa mallia on kaivattu etenkin uusien toimitilojen suunnitteluvaiheessa. Useat turvallisuusratkaisut on kyettävä linjaamaan riittävän yksityiskohtaisella tasolla jo tilasuunnitteluvaiheessa, jotta voidaan varmistua ratkaisujen vastaavan tilojen käyttötarkoituksen ja turvallisuusluokituksen mukaisia vaatimuksia. Etenkin osa tilojen rakenteelliseen turvallisuuteen liittyvistä vaatimuksista on kyettävä huomioimaan jo siinä vaiheessa, kun tehdään päätös tilan soveltuvuudesta organisaation käyttöön.

Tiettyjen tilojen rakenteellisista ratkaisuista voivat aiheuttaa tilanteen, että tila ei missään tapauksessa kykene täyttämään Tullin tilaturvallisuustarpeita. Esimerkkinä tällaisista tilanteista toimivat esimerkiksi kiinteistössä sijaitsevat lakisääteiset hätäpoistumistiet: kiinteistön mui-

den toimijoiden hätäpoistumistiet eivät voi kulkea Tullin tilojen kautta, joten tällaisten yhteiskäyttöisten hätäpoistumisteiden olemassaolo mahdollisesti aiheuttaa sen, että tila ei sovellu Tullin käyttöön. Toimitilaturvallisuuden toteuttamismallin avulla tällaiset tilanteet voidaan tunnistaa riittävän alustavassa vaiheessa tilan soveltuvuutta selvitetessä.

Tilaturvallisuusvaatimusten huomioiminen riittävän aikaisessa vaiheessa antaa myös mahdollisuuksia erilaisten vaihtoehtoisten turvallisuusratkaisuiden suunnittelulle, ja auttaa näin saattamaan tilat niille asetettujen vaatimusten tasolle kustannustehokkaasti. Uusien rakennusten tai tilojen peruskorjausten yhteydessä toimitilojen suojaus toteutetaan tai suojausta parannetaan tilojen sisältämien turvallisuusvyöhykkeiden vaatimusten mukaisesti.

Olemassa olevissa tiloissa turvallisuusratkaisuja toteutetaan suoritettuun riskianalyyysiin perustuen ja toteutustarpeen ollessa perusteltavissa. Pääsääntöisesti toimitilaturvallisuuden hankintatarpeet pyritään huomioimaan etukäteisesti vuosittaisen budjettisuunnitelman laadinnan yhteydessä. Lisäksi tulee jonkin verran toiminnan ja tilojen muutoksista johtuvia hankintatarpeita, jotka pyritään toteuttamaan tarveperusteisesti. Toimitilaturvallisuuden toteuttamismallin avulla tarpeenmukaiset turvallisuusratkaisut voidaan tunnistaa ja budjetoida jo tilahankkeen alkuvaiheessa.

Pääpiirteittäin Tullin toimitilaturvallisuuden tavoitetila on siis määritetty valtioneuvoston tietoturvasuosituksessa (681/2010) ja toimitilojen tietoturvaohjeessa (VAHTI 2/2013), mutta organisaation sisäisten tarpeiden huomioiminen on vaatinut tarkennuksia edellä mainittuihin. Organisaatiotasoisia tarkennuksia on tehty erilaisia tiloja koskeviin turvallisuusvaatimuksiin, ja toteuttamismallin tavoitteena on ollut kyetä määrittelemään vaatimukset aikaisempaa riskiperusteisemmin. Muun muassa toimitilojen sijainti, koko, käyttötarkoitus, käyttöaste, tiloissa käsiteltävän ja säilytettävän tiedon suojaustaso, muut kiinteistön toimijat ja ympäröivien kiinteistöjen toimijat ja yleinen toimintaympäristö ovat asioita, jotka vaikuttavat tiloille asetettaviin turvallisuusvaatimuksiin sekä turvallisuustoimenpiteiden suunnitteluun ja toteutukseen. Näitä tekijöitä on huomioitu määriteltäessä toimitilaturvallisuuden toteuttamismallin tilakohtaisia vaatimuksia riskiperusteisesti.

Toimitilaturvallisuuden toteuttamismallin hyödyntäminen on aloitettu uusien tilojen suunnittelemisessa ja toteuttamisessa, sekä myös olemassa olevien toimitilojen muutos- ja parannushankkeiden yhteydessä. Tulevaisuudessa mallia on mahdollista käyttää myös auditointityökaluna haluttaessa varmistua olemassa olevien tilojen tilaturvatoteutusten olevan vaatimusten mukaisia.

7.5.2 Toteuttamismallin turvallisuusvyöhykejaottelu

Toimitilaturvallisuuden toteuttamismallin on tarkoitus toimia apuvälineenä paitsi tilaturva-vaatimuksia määritettäessä, mutta myös tilojen turvallisuusvyöhykkeiden tunnistamisessa.

Vyöhykeluokittelu ei aina ole yksiselitteinen tehtävä, ja toteuttamismallin luomiseen liittyvää tilojen turvallisuusvyöhykeluokittelua suoritettaessa kohdattiin haasteita, joihin liittyen jouduttiin pohtimaan tilojen turvallisuusvyöhykejaon perusteita ja selvittämään suojaustarpeita melko yksityiskohtaisellakin tasolla. Useita erityistiloja ja niitä koskevien turvallisuustarpeiden selvittämiseksi jouduttiin tekemään sisäistä pohdintaa ja riskianalyysiä tiloille asetettavista tilaturvallisuusvaatimuksista.

Esimerkkitapauksena tällaisista selvityksistä toimivat arkistotilat, joiden osalta jouduttiin selvittämään tilojen suojaustasotarvetta sekä organisaation sisäisesti että myös ulkoisista lähteistä. Toimipaikoille lähetetyn nykytilakartoituksen yhteydessä tuli toimipaikoilta useita kysymyksiä arkistotiloja koskien. Monien toimipaikkojen vastauksissa arkistot oli luokiteltu kuuluvaksi korotetun tason tiloihin, vaikka lähtökohtaisesti arkistotilat kuuluvat perustason tiloihin, mikäli niissä arkistoidaan pelkästään perustason tietoa.

Tiedon elinkaaren toteuttamisessa, joka luonnollisestikin käsittää myös tiedon arkistoinnin, on tarkoitus noudattaa arkistolaissa (831/1994) määritettyä arkistonmuodostussuunnitelmaa. Myös ohje valtioneuvoston tietoturvallisuusasetuksen täytäntöönpanosta asettaa selkeät vaatimukset suojaustasoluokitellun tiedon säilyttämiselle. Sen mukaan suojaustasoille I-III luokitellut paperimuotoiset asiakirjat sekä luonnokset on säilytettävä suojaustason vaatimusten mukaisessa data- tai kassakaapissa. Suojaustasoon IV kuuluvien asiakirjoja koskee puolestaan vaatimus säilyttää kyseisen tason asiakirjat lukitussa paikassa. (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 28, 71.)

Kansallisessa turvallisuusauditointikriteeristöissä Katakriissa todetaan, että suojattavien tietojen kasautuminen saattaa joissain tapauksissa edellyttää tiukempien turvallisuusvaatimusten soveltamista, jolloin esimerkiksi huomattava määrä suojaustason IV tietoa voisi muodostaa suojaustason III mukaisen kokonaisuuden (Kansallinen turvallisuusauditointikriteeristö 2015, 16). Kohdeorganisaatiossa arkistotilat sijaitsevat kuitenkin pääsääntöisesti toimitilojen sisäpuolella, eli suojatulla alueella, jonka lisäksi suurella osalla tiloissa työskentelevistä henkilöistä on pääsytarve arkistossa säilytettäviin materiaaleihin, mikä puolestaan puoltaisi perustason tilaluokitusta. Kuitenkin oleellista on huomioida, että mikäli arkistotilassa säilytetään suojaustason III mukaista tietoa, nostaa se luonnollisesti arkiston suojaustasotarpeen korotetulle tasolle.

Muidenkin erityistilojen osalta on tiloja, joiden käyttötarkoituksen ja luokittelun osalta jouduttiin pohtimaan asiaa hyvin yksityiskohtaisella tasolla, ja pyrittiin näin saavuttamaan yhtenäinen luokittelumalli. Tällaisia haasteellisia tiloja olivat esimerkiksi erilaiset varastohuoneet sekä eritasoiset valvomo- ja toimistotilat. Kartoituksen vastauksissa edellä mainitut tiloja oli luokiteltu sekä perustason että korotetun tason tiloiksi, joten yhtenäisen luokittelumallin kehittäminen osoittautui tarpeelliseksi. Oikean suojaustason määrittäminen on tärkeää, koska tilojen luokittelu tarvetta korkeammalle tasolle voi aiheuttaa ylimääräisiä kustannuksia esimerkiksi valvontajärjestelmien osalta, mutta toisaalta aliluokittelu altistaa tilat ja tiloissa tapahtuvat toiminnot erilaisille uhille. Tiettyjen erityistilojen osalta ei siis ole valmista kaavaa vyöhykejaottelun suorittamiseksi, vaan jaottelu tehdään tapauskohtaiset tekijät huomioiden.

Kuten edellä kuvatussa toimitilojen turvallisuusvyöhykeluokittelun kuvauksesta ilmenee, on tärkeää ennen turvallisuusvaatimusten määrittelemistä kyetä luokittelemaan tilat tarpeenmukaiselle tasolle. Vasta onnistuneen ja oikeellisen turvallisuusvyöhykemäärittelyn jälkeen voidaan määrittää tiloilta edellytettävät turvallisuusvaatimukset yleisemmällä tasolla. Kuitenkin turvallisuusvaatimuksia tulee vielä tämänkin jälkeen kyetä soveltamaan tapauskohtaisesti, koska riskianalyysin tulokseen vaikuttavia tekijöitä on huomattava määrä. Täysin kaiken kattavan ja kaikissa tiloissa toimivan vaatimusmäärittelyn luominen on siis mahdoton tehtävä, koska kaikilla tiloilla ja toiminnoilla on omat erityispiirteensä, jotka voivat vaatia tilaturvallisuusvaatimusten soveltamista joko korkeammalle tai matalammalle tasolle.

8 Päätelmät

Luvussa käsitellään työn tutkimustulosten perusteella tehdyt johtopäätökset sekä työn tuloksia että käytettyjä tutkimusmenetelmiä koskien. Luvussa arvioidaan myös työn kehittämiskohteen hyödynnettävyyttä kohdeorganisaation toiminnassa. Lisäksi kuvataan kehittämiskohteen liittyviä esiin nousseita jatkokehittämis ja -tutkimusaiheita.

8.1 Johtopäätökset

Toimitilaturvallisuus on hyvin laaja kokonaisuus, jonka yksityiskohtaiset vaatimukset ja toteutusmallit määräytyvät organisaation suojattavien arvojen perusteella. Turvallisuustoiminnan sekä turvallisuusriskienhallinnan tavoitteet ja kehittämistoimet määräytyvät organisaation tavoitteiden sekä strategian mukaisesti. Jotta turvallisuustoimenpiteet eivät jää kehittämistoiminnan ulkopuoliseksi osioksi, tulee organisaation turvallisuustoiminnan ja riskienhallinnan tavoitteiden Leppäsen (2006, 175-176) mukaan olla riittävän selkeitä, ja ne tulee kyetä yhdistämään organisaation operatiivisiin ja strategiaan tavoitteisiin.

Kuten työn toisessa luvussa todettiin, on organisaation turvallisuuden tilalla tärkeä asema organisaation toimintaedellytysten ylläpitämisessä. Kuitenkin organisaatioiden toimintaan kohdistuvat turvallisuusriskit ovat yhä monimuotoisempia, ja niihin varautuminen vaatii organisaatioilta panostamista riskienhallintatyöhön niin riskien tunnistamisen kuin varautumistoinenpiteidenkin osalta. Opinnäytetyön kehittämiskohteena luotiin Tullin toimitilaturvallisuuden toteuttamismalli, jota hyödynnetään kohdeorganisaation turvallisuussuunnittelun apuvälineenä pyrittäessä varmistamaan, että organisaation tilaturvallisuus toteutuu tarpeenmukaisella tasolla. Toimitilaturvallisuuden toteuttamismallille oli selkeät työelämälähtöiset tarpeet, jotka ovat vahvasti auttaneet määrittämään toteuttamismallin sisältöä.

Toimitilaturvallisuuden toteuttamismallin luominen on nähty kohdeorganisaatiossa tarpeelliseksi, jotta pystyttäisiin varmistamaan organisaation toimitilaturvallisuuden tilan olevan vaatimusten mukainen. Opinnäytetyön aihe on kohdeorganisaatiossa erityisen ajankohtainen, koska meneillään ja suunnitteilla on runsas määrä toimitilamuutoksia, ja uusia toimitiloja suunniteltaessa ja toteutettaessa tulee muiden tiloille asetettujen vaatimusten lisäksi kyetä huomioimaan myös toimitilaturvallisuutta koskevat vaatimukset. Vaatimusten toteuttamissuunnitelmassa tulee huomioida monia eri tekijöitä; suunnittelua ohjaa paitsi edellä mainittu valtioneuvoston tietoturvallisuusasetus, mutta myös organisaation sisäiset riskiarviot eri toimintoja koskien sekä toisaalta paineita luovat myös julkisia toimijoita koskevat kustannustehokkuusvaatimukset.

Työn toiminnallinen osuus, joka käsitti lähinnä toimitilojen tilaturvallisuuden tason nykytilakartoituksen, toteutettiin osin projektimuotoisesti. Projektinhallinnan teorioihin tutustuminen oli täten ehdoton edellytys projektin suunnittelulle ja sen onnistuneelle toteuttamiselle. Projektien aikataulutukseen ja päättämiseen liittyvien vaikeuksien hallitsemiseksi projektille oli tärkeää määritellä selkeä tavoite. Toimitilaturvallisuusprojektille oli asetettu selkeä päämäärä, jonka saavuttaminen toimi tavoitteena, ja ohjasi vahvasti projektin kulkua ja sen päättämistä.

Tutkimuskysymysten asettelu ja tavoite

Opinnäytetyön aihe on hyvin ajankohtainen, koska työn kohdeorganisaation tuli täyttää valtioneuvoston tietoturvallisuusasetuksen vaatimukset perustason osalta syyskuuhun 2013 mennessä ja korotetun tason osalta lokakuuhun 2015 mennessä. Opinnäytetyön tutkimuskysymykset asetettiin siten, että ne tähtäsivät asetuksen korotetun tason vaatimusten täyttämiseen. Opinnäytetyössä kuvataan teoreettinen viitekehys sekä organisaation tilaturvallisuuden kehittämistarpeet, joiden perusteella kehitettiin Tullin toimitilaturvallisuuden toteuttamismalli. Toteuttamismallia hyödynnetään valtioneuvoston tietoturvallisuusasetuksen vaatimusten mukaisen toimitilaturvallisuustason saavuttamisessa ja ylläpitämisessä.

Ensimmäiseen tutkimuskysymykseen vastaamiseksi selvitettiin Tullin toimipaikkojen toimitilaturvallisuuden nykytila. Tutkimusaineiston laajuuden vuoksi aineiston keruumenetelmänä hyödynnettiin pääasiallisesti kyselytutkimusta. Kyselytutkimuksen tueksi suoritettiin tarpeen vaatiessa haastatteluja sekä havainnointia empiirisen tutkimuksen keinoin. Kyselytutkimusten tulosten perusteella voitiin todeta selkeä tarve selvittää vastaukset myös kahden muun tutkimuskysymyksen osalta, jotta niiden avulla saataisiin apua tarvittavien tilaturvallisuuden kehittämistoimenpiteiden suunnitteluun ja toteuttamiseen.

Toisen tutkimuskysymyksen aineisto ja teoriapohja muodostuivat verrattaessa ensimmäisen tutkimuskysymyksen avulla saatua aineistoa kohdeorganisaation tilaturvallisuuden tavoitetilaan. Tavoittila muodostuu valtioneuvoston tietoturvaluusasetuksen sekä Tullin omien toimitilaturvallisuuden toteuttamista koskevien tavoitteiden perusteella. Näitä vertaamalla saatiin tilakohtaiset tiedot toimitilaturvallisuuden puutteista.

Organisaatioturvallisuuden yleisten teorioiden avulla pyrittiin löytämään selityksiä sille, miksi kohdeorganisaation tilaturvallisuudessa havaitut puutteet kenties ovat olemassa, ja millä toimenpiteillä niihin olisi mahdollista pyrkiä vaikuttamaan. Kolme keskeisintä taustatekijää ja samalla kehittämiskohdetta tilaturvallisuuden puutteille tunnistettiin olevan tilaturvallisuuden ennakkosuunnittelu ja yhdenmukaisuus sekä organisaation turvallisuustietoisuus koskien tilaturvallisuuden toteuttamista.

Toimitilaturvallisuuden toteuttamismalli työn varsinaisena kehittämistehtävänä

Tullin toimitilaturvallisuuden toteuttamismallin luomista voidaan pitää opinnäytetyön varsinaisena kehittämistehtävänä. Ensimmäiseen ja toiseen tutkimuskysymykseen liittyvä tutkimusaineisto oli edellytys toteuttamismallin sisällön yksityiskohtien määrittämiselle. Kohdeorganisaation toimitilaturvallisuuden nykytila sekä sen perusteella tehty analyysi tarvittavista kehittämistoimenpiteistä siis toimivat oleellisen tärkeänä taustatietona, jotta kriittiset puutteet tilaturvallisuusjärjestelyissä oli mahdollista tunnistaa. Toimitilaturvallisuuden toteuttamismallissa on pyritty kuvaamaan riittävät riskienhallintatoimenpiteet tunnistettujen puutteiden korjaamiseksi.

Tehdyn toimitilaturvallisuuden nykytilakartoituksen sekä jo olemassa olevien vaatimusten avulla määriteltiin toimintokohtaiseen riskiarvion avulla vaatimuskriteeristö, jonka perusteella syntyi Tullin toimitilaturvallisuuden toteuttamismalli. Tilaturvavaatimukset olivat sekä organisaation sisäisiä että ulkopuolisten asetusten mukaisia, ja ne pyrittiin määrittämään tarpeenmukaiselle tasolle organisaation ja tilojen toimintaympäristöön ja toimintoihin kohdistuvan riskienarvioinnin perusteella.

Toimintokohtaisesti suoritettu riskienarviointi oli yksi oleellisimpia tekijöitä, jonka avulla turvallisuusvaatimukset saatiin asetettua kohdeorganisaation tarpeiden mukaiselle tasolle. Tulevaisuudessa toteuttamismallin sisältöä on kyettävä muokkaamaan toimintaympäristössä sekä kohdeorganisaation toiminnoissa tapahtuvien muutosten johdosta, jotta toteuttamismallin sisältämien turvallisuusvaatimusten riskiperusteisuus säilyy, ja varmistaa näin turvallisuusratkaisuiden tarkoituksenmukaisuuden. Riskiperusteisuutta on tarpeen myös painottaa entistä enemmän toteuttamismallin seuraavien päivitysten yhteydessä.

Tullin sisäiset toimitilaturvallisuuden vaatimukset määräytyivät tilojen toimintaympäristöön ja tiloissa suoritettaviin toimintoihin kohdistuvan sisäisen turvallisuusriskikartoituksen perusteella, jonka avulla pystytään huomioimaan turvallisuusvaatimusten määräytymiseen vaikuttavat organisaation erityispiirteet. Opinnäytetyön tutkimuksellisen osion sekä teoreettisen viitekehyksen tarkoituksena oli tukea toteuttamismallin sisällön määrittämistä.

Toteuttamismalli on otettu käyttöön olemassa olevien tilojen turvallisuusratkaisujen linjauksissa ja turvallisuussuunnittelussa

Toimitilaturvallisuuden toteuttamismallia hyödynnetään Tullin meneillään olevissa ja tulevaisuudessa toimitilahankkeissa turvallisuussuunnittelun apuvälineenä, jotta saadaan varmistettua toimitilojen turvallisuusratkaisuiden tarpeenmukainen ja yhdenmukainen taso. Seuraavaksi malli on tarkoitus viedä laajemmin käyttöön myös toimipaikkojen paikallisille vastuuhenkilöille, jotka ovat osallisena toimitilahankkeiden suunnittelussa ja toteutuksessa.

Toimitilahankkeiden yhteydessä on hyvin tärkeää, että tiloja koskevat vaatimukset on yksilöity riittävän tarkasti, sillä tilojen turvallisuusjärjestelyt suunnitellaan ja toteutetaan yhteistyössä osastojen ja ulkoisten toimijoiden kanssa. Yksityiskohtaisten vaatimusten avulla voidaan varmistua siitä, että ulkopuoliset toimittajat, kuten esimerkiksi vuokranantaja, kiinteistön omistaja tai järjestelmätoimittaja, ovat riittävän ajoissa tietoisia tiloilta edellytetyistä turvallisuusratkaisuista. Kustannustehokkuuden takaamiseksi turvallisuusvaatimukset on tärkeää huomioida jo tilojen suunnitteluvaiheessa, jolloin voidaan pyrkiä valitsemaan tarkoituksenmukaisin ratkaisu turvallisuusvaatimusten täyttämiseksi.

Meneillään olevien ja tulevien tilahankkeiden lisäksi mallia tullaan hyödyntämään olemassa olevien tilojen tilaturvaparannusten suunnittelussa ja toteutuksessa, jotta kaikkien tilojen tilaturvallisuus saadaan vaatimustenmukaiselle tasolle. Laajemmassa mittakaavassa toteuttamismallin käyttöönoton avulla on mahdollista tehostaa tässä työssä kohdeorganisaation kehittämishaasteiksi kuvattuja asioita: tilaturvallisuuden ennakosuunnittelua, yhdenmukaisuutta ja organisaation turvallisuustietoisuutta tilaturvallisuusasioista. Näissä kehittämiskohteissa

tapahtuneet muutokset voidaan todeta vasta pidemmän aikavälin jälkeen, kun toimitilaturvallisuuden toteuttamismallia on ehditty hyödyntää useamman toimitilan turvallisuusratkaisujen suunnittelemisessa ja toteuttamisessa.

8.2 Tutkimuksen luotettavuus ja arviointi

Tutkimuksen teossa on tärkeää varmistua tutkimuksessa saatujen tutkimustulosten luotettavuudesta. Hirsjärven (2004, 216-217) mukaan tutkimuksen ja sen tulosten luotettavuutta arvioidaan rebligateetin sekä validiteetin kautta. Reliabiliteetilla tarkoitetaan tutkimuksen luotettavuutta ja validiteetilla tutkimuksessa käytetyn tutkimusmenetelmän soveltuvuutta mittaamaan haluttua asiaa.

Toimitilojen nykytilakartoituksen suorittamiseksi tuli toimipaikoilta saada tiedot niiden nykyistä tilaturvallisuuden ratkaisuista. Aineiston kerääminen toimipaikkojen toimitilaturvallisuuden lähtötason määrittelemiseksi kyselytutkimuksen keinoin osoittautui vaativaksi tehtäväksi. Lähtötietojen luotettavuus ja kattavuus oli oleellisen tärkeää, eli tietojen tuli olla paikkansa pitäviä ja vastaukset tuli saada kaikilta toimipaikoilta.

Kyselytutkimuksen vastausten luotettavuuden ja kattavuuden varmistamiseksi jouduttiin ole-malla yhteydessä kyselyyn vastanneisiin tahoihin toimipaikoilla ja esittämään tarkentavia kysymyksiä. Kyselytutkimuksen ohella päädyttiin siis esittämään tarkentavia kysymyksiä *haastattelun* keinoin sekä suorittamaan tilaturva-auditointeja eli *havainnointia*. Näin ollen tutkimus suoritettiin menetelmätriangulaation avulla, eli käytettiin useampaa tiedonhankintakeino-a saadun aineiston luotettavuuden ja kattavuuden varmistamiseksi.

Haasteet nykytilakartoituksen suorittamisessa

Tutkimuksen luotettavuuden osalta riskinä oli ennen kaikkea kartoitukseen sisältyvän tilaturvallisuusvyöhykejaottelun oikeellisuus. Tilojen luokittelu todellista korkeampaan turvallisuusvyöhykkeeseen voisi aiheuttaa huomattavia lisäkustannuksia turvajärjestelyjen toteuttamisvaiheessa. Toisaalta tilojen luokittelu todellista matalampaan turvallisuusvyöhykkeeseen kuuluvaksi aiheuttaisi helposti puutteita todellisen turvallisuusvyöhykkeen mukaisten turvallisuusvaatimusten toteutumisen osalta. Tilojen vyöhykeluokittelun suorittaminen vaatii kuitenkin laajahkoa turvallisuustietämystä, eikä kaikilla kyselyyn vastaajilla tällaista pohjaosaamista välttämättä ollut. Vyöhykeluokittelua koskevan tiedon saaminen vaati tutkijan suoria yhteydenottoja toimipaikoille, jolloin vyöhykeluokittelun oikeellisuudesta voitiin todennäköisemmin varmistua.

Koska toimipaikkojen turvallisuusvyöhykejaottelua ja turvallisuusratkaisuja koskevien tietojen oikeellisuus oli tärkeää, jouduttiin kartoituksen suunnitellusta aikataulusta tinkimään, ja

käyttämään kartoitukseen aiottua enemmän aikaa. Osasyynä vastausten puutteellisuuteen oli kyselylomakkeen liiallinen suppeus, osin taas vastaajatahojen epätietoisuus turvallisuusvyöhykeluokittelun suorittamisesta tai tilojen turvallisuusteknisistä ratkaisuista.

8.3 Jatkotutkimusmahdollisuudet

Toteuttamismallin käyttökokemusten perusteella suoritetaan tarvittavia muokkauksia sekä mallin sisältöön että ulkoiseen toteutukseen. Oletettavasti toteuttamismallin tilaturvallisuusvaatimukset tarkentuvat ja muokkaantuvat huomattavastikin, kun mallia riittävästi hyödynnetään erityyppisten tilahankkeiden yhteydessä.

Uudenlaiset työskentelytavat ja -tilat edellyttävät uudistumista myös tilojen turvallisuusratkaisuilta

Tullissa on meneillään merkittäviä uudistuksia niin tilojen kuin toiminnankin osalta. Esimerkiksi siirtyminen monitoimityötiloihin ja nimeämättömiin työpisteisiin vaatii myös uusien turvallisuusvaatimusten ja -ratkaisuiden linjaamista. Toimitilojen tietoturvaohjeen (VAHTI 2/2013) mukaisesti perustason ja korotetun tason vyöhykkeillä on mahdollista hyödyntää avotai monitoimityötilatoteutusta, mutta kuitenkin pääsy perustasoa korkeamman turvallisuustason vyöhykkeelle tulee olla vain niillä henkilöillä, joiden työtehtävät tätä edellyttävät. Näin ollen vallitsevan toimitilakonseptin mukaiset monitoimityötilaratkaisut vaativat turvallisuusvaatimusten huomioimista perinteisempiä työtilatoteutuksia laajemmin, mikä tulee tulevaisuudessa nykyistä laajemmin huomioida myös tilojen turvallisuussuunnittelussa.

Lisäksi tulevaisuudessa mahdollisesti tapahtuva nimeämättömiin työpisteisiin siirtyminen vaatii yhä tarkempaa etukäteissuunnittelua, jotta tällaisissa tiloissa saadaan toteutettua tarpeenmukaiset turvallisuusratkaisut ja henkilöiden kulkuoikeusrajaukset tilojen välillä. Nimeämättömät työpisteet ja lisääntyvä etätyöskentely siis vaativat linjauksia vaadituista turvallisuusratkaisuista sekä uudistuksia toimitilaturvallisuuden toteuttamismallin sisältöön. Nämä ovat organisaation lähitulevaisuuden suunnitelmia, ja samalla tilaturvallisuuden kehittämishaasteita ja -kohteita jo aivan lähitulevaisuudessa.

Ulkoisten toimijoiden suorittamien tilaturvallisuusratkaisuiden toteuttamiseen kaivataan apuvälinettä

Toinen suunnitelmavaiheessa oleva jatkokehitysaihe on toimitilaturvallisuuden vaatimusten huomioiminen tilasuunnitteluvaiheessa ulkopuolisten toteuttajien kanssa. Tullin tilaturvallisuusvaatimukset tulisi kyetä viemään soveltuvien osien esimerkiksi tilojen omistajien, vuokranantajien, rakentajien ja muiden sidosryhmien tietoisuuteen jo tilahankkeiden alkuvaiheessa, jotta vaatimusten toteuttamisratkaisut saadaan toteutettua oikealla tasolla.

Toimitilaturvallisuuden toteuttamismallista tultaneen siis tekemään ulkopuolisille tahoille tarkoitettu supistettu versio, joka ei sisällä salassa pidettävää tietoa, ja jota näin ollen voidaan jakaa tarpeenmukaisille yhteistyötahoille kohdeorganisaation ulkopuolelle. Tällöin voidaan varmistua siitä, että kaikilla osapuolilla on riittävä tieto tarvittavista tilaturvallisuusratkaisuista, eikä puutteellisia tai virheellisiä ratkaisuja synny tiedon puutteesta johtuen. Riittävän tarkka etukäteinen vaatimusmäärittely auttaa myös toteuttamaan toimenpiteet sovitussa aikataulussa.

Toteuttamismallia voidaan hyödyntää myös olemassa olevien tilojen turvallisuustason auditoinnissa ja tiedon jakamisessa

Tavoitteena on, että tulevaisuudessa toimitilaturvallisuuden toteuttamismalli toimii paitsi turvallisuussuunnittelun apuna, mutta myös olemassa olevien tilojen auditointityökaluna. Näin tiloihin voitaisiin säännöllisesti suorittaa turvallisuuden tilan tarkastuksia, ja näin varmistaa vaatimusten toteutuminen. Tarpeen mukaan mallia on mahdollista laajentaa koskemaan soveltuvien osien myös turvallisuuden muita osa-alueita, jolloin sen avulla voidaan auditoida kohteen turvallisuustasoa laajemmaltikin.

Kuten työssä aiemmin jo useasti on ilmennyt, on henkilöstön turvallisuustietoisuus ratkaisevan tärkeässä osassa turvallisuusratkaisuiden käytäntöön viemisessä ja organisaation turvallisuuden tilan ylläpitämisessä. Toimitilaturvallisuuden toteuttamismallia kannattaa ehdottomasti pyrkiä hyödyntämään myös turvallisuusperehdytyksen ja -koulutuksen apuvälineenä niille henkilöille, jotka toimipaikoilla turvallisuuden kehittämisestä ja turvallisuushankinnoista vastaavat. Turvallisuusosaamisen lisäämisen avulla päästään aiempaa yhdenmukaisempiin tilaturvallisuuden toteutusmalleihin, ja voidaan näin varmistua vaadittavan tilaturvallisuustason toteutumisesta yhä laajemmin.

Kokonaisuudessaan toimitilaturvallisuuden toteuttamismalli tulee varmasti elämään tulevaisuudessa, koska muutoksia tapahtuu jatkuvasti niin organisaation sisä- kuin ulkopuolellakin. Toteuttamismallin pitäminen ajantasaisena on tärkeää, jotta se kykenee vastaamaan tilojen kehittämistarpeisiin mahdollisimman kattavasti ja oikeellisesti. Toteuttamismallin päivittämisessä on huomioitava lainsäädännössä mahdollisesti tapahtuvat uudistukset, toiminnassa sekä toimintaympäristössä tapahtuvat muutokset, jotka mahdollisesti voivat vaikuttaa tiloihin kohdistuviin riskeihin.

Painetut lähteet

- Aaltola, J., & Valli, R. 2001. Ikkunoita tutkimusmetodeihin II. Näkökulmia aloittelevalle tutkijalle tutkimuksen teoreettisiin lähtökohtiin ja analyysimenetelmiin. Jyväskylä: PS-kustannus.
- Aaltonen, T., Pitkänen, E. & Ristikangas, V. 2008. Asiantuntijasta esimies. Innostusta ja arvostusta esimiestyöhön. Helsinki: WSOYpro.
- ASIS Crime/Loss Prevention Council. 2010. Future of Corporate Security. Teoksessa Security in 2020. Alexandria: ASIS International.
- Berg, M. 2012. Sosiaalinen media yrityksen positiivisen maineriskin näkökulmasta. Pro gradu - tutkielma. Valtiotieteellinen tiedekunta. Helsinki: Helsingin yliopisto.
- Fennelly, L. 2013. Effective Physical Security. Elsevier.
- Halibozek, E. & Kovacich, G. 2009. The Manager's Handbook for Corporate Security. Elsevier.
- Heinonen, Keinänen, Paasonen 2013. Turvallisuustutkimuksen tekeminen: Kuinka tuottaa luotettavaa tietoa turvallisuudesta. Helsinki: Tietosanoma.
- Heljaste, J-M., Korkiamäki, J., Laukkala, H., Mustonen, J., Peltonen, J., Vesterinen, P. 2008. Yrityksen turvallisuusopas. Kauppakamari Helsinki.
- Hirsjärvi, S., Remes, P. & Sajavaara, P. 2004. Tutki ja kirjoita. Helsinki: Tammi.
- Hirsjärvi, S., Remes, P. & Sajavaara, P. 2012. Tutki ja kirjoita. Helsinki: Tammi.
- Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. 2010. Johda riskejä: käytännön opas yrityksen riskienhallintaan. Helsinki: Finva.
- Kansallinen turvallisuusauditointikriteeristö KATAKRI 2015.
- Kerko, P. 2001. Turvallisuusjohtaminen. Jyväskylä: PS-kustannus.
- Koskenranta, H. 2007. Luentomuistiinpanot opintojaksolta Fyysinen turvallisuus.
- Laki kansainvälisistä tietoturvallisuusvelvoitteista 588/2004.
- Laki viranomaisten toiminnan julkisuudesta 621/1999.
- Leppänen, J. 2006. Yritysturvallisuus käytännössä. Turvallisuusjohtamisen portfolio.
- Lämsä, A-M. & Päivike, T. 2013. Organisaatiokäyttötymisen perusteet. Edita.
- Metsämuuronen, J. 2001. Laadullisen tutkimuksen käsikirja. Helsinki: International Methelp.
- Puhakainen, P. & Siponen, M. 2010. Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. MIS Quarterly 34(4): 757-778.
- Reid, R. 2004. Facility Manager's Guide to Security: Protecting Your Assets. The Fairmont Press.
- Sennewald, C. 2011. Effective Security Management. 5. painos. Elsevier.
- SFS-ISO 31000 Riskienhallinta. Periaatteet ja ohjeet. Helsinki: Suomen Standardisoimisliitto.

Strauchs, J. 2010a. Convergence of IT and Security. Teoksessa Security in 2020. Alexandria: ASIS International.

Strauchs, T. 2010b. Future of Information Security and Intellectual Property. Teoksessa Security in 2020. Alexandria: ASIS International.

Sähköiset lähteet

Liiketoimintaa turvallisesti. Kansallinen strategia yritystoiminnan turvallisuuden parantamiseksi. 2012. Sisäasiainministeriö. Viitattu 2.8.2016.
<http://www.intermin.fi/julkaisu/302012?docID=35892>

Murtohälytysjärjestelmät ja -palvelut ohje 2008. Finanssialan keskusliitto. Viitattu 28.1.2016.
http://www.finanssiala.fi/vahingontorjunta/dokumentit/Murtohalytysjarjestelmat_ja_palvelut_ohje_2008.pdf

Ohje riskienarvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. 2003. Valtionhallinnon tietoturvallisuuden johtoryhmä. Viitattu 17.1.2016. https://www.vahtiohje.fi/c/document_library/get_file?uuid=d1bcc4b1-789e-4ce1-a44a-e591a60985b5&groupId=10128

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. 2010. Valtionhallinnon tietoturvallisuuden johtoryhmä. Viitattu 13.1.2016.
https://www.vahtiohje.fi/c/document_library/get_file?uuid=b4a90e50-7307-4004-ac8e-b9103220db6a&groupId=10128&groupId=10229

Ohje riskienarvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. 2003. Valtionhallinnon tietoturvallisuuden johtoryhmä. Viitattu 2.8.2016.
https://www.vahtiohje.fi/c/document_library/get_file?uuid=d1bcc4b1-789e-4ce1-a44a-e591a60985b5&groupId=10128

Sidosryhmäyhteistyön riskit. Pk-yrityksen riskienhallinnan työvälinesarja. Viitattu 12.8.2016.
<http://www.pk-rh.fi/uploads/henkiloriskit/sidosryhmayhteistyon-riskit-tietokortti.pdf>

Suomen tullin palvelu- ja lainvalvontaorganisaatio. 2009. Tulli. Viitattu 10.8.2016. http://www.tulli.fi/fi/suomen_tulli/tulli_tutuksi/tehtavat/index.jsp

Tietoturvallisuus 2016. Elinkeinoelämän keskusliitto. Viitattu 11.8.2016. <https://ek.fi/mita-temme/tyoelama/yritysturvallisuus/tietoturvallisuus/>

Tietoturvallisuuden arviointi valtionhallinnossa. 2006. Valtionhallinnon tietoturvallisuuden johtoryhmä. Viitattu 16.1.2016. <http://vm.fi/dms-portlet/document/0/371333>

Tietoturvallisuus ja tulosohtaus. 2004. Valtionhallinnon tietoturvallisuuden johtoryhmä. Viitattu 13.8.2016. https://www.vahtiohje.fi/c/document_library/get_file?uuid=d67f9f1e-74e3-4a74-af67-71f7552f9f38&groupId=10229

Toiminnan jatkuvuuden hallinta. 2016. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä. Viitattu 13.9.2016. https://www.vahtiohje.fi/c/document_library/get_file?uuid=11459f91-91c8-4ebe-a34f-9d8d9bfc964c&groupId=10229

Toimitilojen tietoturvaohje. 2013. Valtionhallinnon tietoturvallisuuden johtoryhmä. Viitattu 13.1.2016. https://www.vahtiohje.fi/c/document_library/get_file?uuid=78751ee8-c2c8-4ac4-945c-72cb9ec4a01b&groupId=10229

Tullitoimipaikat kartalla. 2015. Tulli. Viitattu 15.9.2016. http://www.tulli.fi/fi/suomen_tulli/tulli_tutuksi/lisatietoa/tullitoimipaikat_kartalla.pdf

Tulli tutuksi. 2016. Tulli. Viitattu 10.8.2016. http://www.tulli.fi/fi/suomen_tulli/tulli_tutuksi/index.jsp

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010. 2010. Viitattu 13.8.2016. <http://www.finlex.fi/fi/laki/ajantasa/2010/20100681>

Valtioneuvoston periaatepäätös valtion toimitilastrategiaksi 2014. Valtiovarainministeriö. Viitattu 3.8.2016. <http://vm.fi/documents/10623/307565/Valtioneuvoston+periaatep%C3%A4%C3%A4t%C3%B6s+valtion+toimitilastrategiaksi/0a92ff49-8d57-43fe-b49a-ae911c98b59d>

Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekatsaus nro 15. Yrityksiin kohdistuva tietoverkkorikollisuus. 2014. Yritysturvallisuuden kansallinen yhteistyöryhmä. Viitattu 20.7.2016. https://ek.fi/wp-content/uploads/Tilannekuva_kevat_2014.pdf

Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva. 2012. Keskusrikospoliisi. https://www.intermin.fi/download/37646_Yrityksiin_kohdistuvan_rikollisuuden_tilannekuva_syksy_2012_20121011_2_.pdf?2b4b6f14c65ad288

Yritysten rikosturvallisuus 2012: Riskit ja niiden hallinta. 2012. Keskuskauppakamari ja Helsingin seudun kauppakamari. Viitattu 20.7.2016. http://kauppakamari.fi/wp-content/uploads/2012/01/Yritysten_rikosturvallisuus_2012-.pdf

Yritysturvallisuus. 2016. Elinkeinoelämän keskusliitto. Viitattu 11.8.2016. <http://ek.fi/mita-temme/tyoelama/yritysturvallisuus/>

Kuviot

Kuvio 1: Opinnäytetyön rakenne kuvamuodossa	16
Kuvio 2: Organisaation riskienhallintaprosessi	24
Kuvio 3: Tilaturvallisuustoimenpiteiden toteuttamismalli (mukailtu Koskenranta 2007) ...	28
Kuvio 4: Riskienhallinnan kustannusten ja toimenpiteiden suhde (mukailtu Leppänen 2006, 164).....	30
Kuvio 5: Organisaatioturvallisuuden osa-alueet (mukailtu Yritysturvallisuus 2016)	31
Kuvio 6: Tilojen turvallisuusvyöhykeluokittelu (mukailtu Toimitilojen tietoturvaohje 2013, 20)	36
Kuvio 7: Tiedon käsittelyn vaiheet (mukailtu Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2013)	40
Kuvio 8: Tullin toimipaikat vuonna 2015 (Tullitoimipaikat kartalla)	48
Kuvio 9: Kyselytutkimuksen suorittamisen aikataulu	49
Kuvio 10: Esimerkki kyselytutkimuksen vastauksena saadusta tilaturvallisuuskuvauksesta	55
Kuvio 11: Tilaturvallisuuden kehittämistarpeet taulukoituna toimipaikoittain.....	56

Taulukot

Taulukko 1: Työn tutkimuskysymykset	13
Taulukko 2: Työn tutkimuskysymykset ja -vastaukset.....	54

Liitteet

Liite 1: Toimitilaturvallisuuskartoituksen kyselylomake



Tulli

24.4.2015

Hallinto-osasto / Organisaatioturvallisuus

Toimitilaturvallisuusprojekti - korotettu taso

Rakenteellisen ja teknisen murto- ja tilasuojelun kartoitus

Turva-hankkeeseen (Asetus tietoturvallisuudesta täytäntöönpanohanke) liittyvän Toimitilaturvallisuusprojektin tehtävänä on kartoittaa ja kuvata Tullin toimitilojen rakenteellisen ja teknisen murto- ja tilasuojelun nykytila. Nykytilan kartoituksen jälkeen tullaan laatimaan parannus- ja kehitysehdotukset perustuen Tullin toimitilaturvallisuuden toteuttamisohjeeseen.

Nykytilanteen kartoittamiseksi projektin ensimmäisessä vaiheessa (perustason vaatimukset) pyydettiin toimipaikoilta syksyllä 2013 ja keväällä 2014 vastauksia toimitilojen yleisiin turvallisuusjärjestelyihin.

Projektin seuraavassa vaiheessa (korotetun tason vaatimukset) tarvitaan tarkemmat tiedot toimipaikkojen toimitilaturvallisuuden tilasta. Pyydämme toimipaikkoja merkitsemään toimitilojen pohjakuviin tiedot toimitilojen turvallisuusvyöhykkeistä (turvallisuusvyöhykkeet kuvattu seuraavalla sivulla, sekä liitteenä olevassa Tullin toimitilaturvallisuuden toteuttamisohjeessa) sekä turvallisuusjärjestelmien toteutuksesta (esimerkiksi kameravalvontalaitteisto, rikosilmoitinjärjestelmään liittyvä tekniikka, kulunvalvontajärjestelmät).

Tiedot voi toimittaa joko muokkaamalla tarvittavat tiedot pohjakuviin sähköisesti tai piirtämällä ne paperiseen pohjakuvaan. Toimitilojen ajantasaiset pohjakuvat ovat saatavilla Optimaze-järjestelmässä, johon käyttöoikeuksia on paikallisilla toimitilaryhmän edustajilla. Lisätietoja ja -ohjeita saa allekirjoittaneilta.



Jakelu:
Tiedoksi:

Hallintopalvelupäälliköt
TURJO

Tulli

24.4.2015

Hallinto-osasto / Organisaatioturvallisuus

Toimitilojen turvallisuusvyöhykejako:

Valtionhallinnon toimitilaturvallisuuden toteuttamisohje VAHTI määrittelee toimitilojen suojaustasot seuraavasti: Toimitilat jaetaan turvallisuusvyöhykkeisiin käsiteltävän ja säilytettävän tiedon turvaamiseksi asiakirjojen suojaustasoluokittelun perusteella: Julkisen, Perustason, Korotetun tason ja Korkean tason vyöhykkeisiin. Turvallisuusvyöhykejako perustuu sekä kansalliseen lainsäädäntöön (TTA 14 §) että kansainvälisten velvoitteiden toteuttamiseen.

Tullissa tilat jaetaan ja merkitään Tullin toimitilaturvallisuuden toteuttamisohjetta noudattaen: Julkisen, Perustason, Korotetun tason ja Korotettu+ -tason vyöhykkeisiin. Lähtökohtaisesti Tullilla ei ole tarvetta Korkean tason tilaturvallisuustoteutuksille.

Vyöhykkeiden sisällä voidaan tehdä tullitoimintokohtaista tasoluokittelua, jolla mahdollistetaan tarvittava työskentelyn ja tietojen käsittelyn "need to know" -periaate (tiedot ovat niiden käytettävissä, joilla on ko. tietoihin pääsyyn oikeus ja tarve).

Turvallisuusvyöhykkeiden sisälle on mahdollista toteuttaa erillisiä tiloja, jotka kuuluvat joko samalle tai korkeammalle turvallisuusvyöhykkeelle. Mikäli tilat ovat osittain tai kokonaan kahden tai useamman valtionhallinnon toimijan käytössä, toteutetaan turvallisuusratkaisut ylintä tiloissa käsiteltävää tai säilytettävää salassa pidettävää tietoa vastaaviksi.

Seuraavassa on kuvattu tiivistetysti tilojen jaottelu käsiteltävän tiedon suojaustason mukaisiin turvallisuusvyöhykkeisiin, jota tulisi toteuttaa merkittäessä toimitilojen turvallisuusvyöhykeitä pohjakuviin. Laajempi kuvaus turvallisuusvyöhykkeistä löytyy liitteenä olevasta Tullin toimitilaturvallisuuden toteuttamisohjeesta.

Julkinen vyöhyke VALKOINEN VÄRI:

- Asiakaspalvelutilat, koulutustilat, kokoustitilat asiakkaille
- Tilat, joihin tarvitaan kontrolloitu kulku, mutta joihin pääsyä ei voida rajata tietyille henkilöryhmälle.
- Tiloissa voidaan käsitellä ST-IV aineistoa

Perustaso VIHREÄ VÄRI:

- Normaalit työ- ja toimistotilat (perustason tilat).
- Lähtökohtainen toimitilaturvallisuuden suojaustaso.
- Tiloissa voidaan käsitellä ST-IV aineistoa ja satunnaisesti ST-III aineistoa

Korotettu taso KELTAINEN VÄRI:

- Tiloissa voidaan käsitellä ST-III aineistoa ja satunnaisesti ST-II aineistoa

Korotettu+ -taso SININEN VÄRI (korkea taso soveltaen):

- Tiloissa voidaan käsitellä ST-III aineistoa ja satunnaisesti ST-II aineistoa