Tulevaisuuden toimitilaturvallisuusohjeistuksen rakentaminen

19.Turvallisuusjohdon koulutusohjelma

Lopputyöraportti

Mikko Rikkonen

ISS Palvelut Oy

Helsinki xx.3.2026

Aalto University Executive Education and Professional Development

Tiivistelmä

Tämä työ tarkastelee, miten toimitilaturvallisuuden ohjeistus voidaan rakentaa johdonmukaiseksi, riskiperusteiseksi ja käytännössä toteuttamiskelpoiseksi kokonaisuudeksi. Tutkimus kuvaa takautuvasti suunnitteluprosessin, jossa yhdistettiin useita viitekehyksiä – kuten laatujohtaminen, tietoturva, tietosuoja ja ympäristöjohtaminen – toimitilaympäristön erityisvaatimuksiin. Tuloksena muodostui malli, jossa kaksi toisiaan täydentävää periaatetta, Privacy by Design ja Security (Facility) by Design, yhdistyvät rakenteelliseen Area–Zone-luokitteluun sekä työnkulkuun sidottuun RASCI-vastuunjakoon.

Mallin avulla ohjeistus kohdennetaan oikein hallittuihin ja vaikutettavissa oleviin ympäristöihin, mikä vähentää tulkinnanvaraa monivuokralais- ja monitoimittajaympäristöissä. Lisäksi kehitettiin tehtäväsoveltuvuusmalli, jossa työn sijainti toimii kontrollina ja määrittää turvallisen suoritusympäristön erityisesti hybridityössä. Järjestelmällinen evidenssinhallinta ja auditointivalmius muodostavat keskeisen osan mallia, sillä ne mahdollistavat poikkeamien hyödyntämisen organisaation oppimisessa ja jatkuvassa parantamisessa.

Tutkimus osoittaa, että toimitilaturvallisuuden ohjeistus voidaan rakentaa siten, että se on sekä standardeihin perustuva että käytännön toiminnassa sovellettava. Vaikuttavuutta voidaan arvioida kattavasti vasta käyttöönoton jälkeen, jolloin havaintojen perusteella voidaan tehdä hallittuja ja rajattuja jatkokehitystoimia.

Abstract

This report examines how a facility security guideline can be designed as a coherent, risk-based and operationally applicable framework. The study reconstructs the development process, in which multiple reference models—quality management, information security, data protection, environmental management and operational governance—were integrated with the practical requirements of diverse facility environments. The outcome is a model that combines two complementary principles, Privacy by Design and Security (Facility) by Design, with a structural Area–Zone classification and a RASCI-based responsibility assignment embedded in workflow design.

The model enables guidelines to be targeted appropriately in both controlled and influence-only environments, reducing ambiguity in multi-tenant and multi-vendor settings. In addition, a task-suitability model was developed in which the work location functions as a control, defining the secure operating environment particularly in hybrid work contexts. Systematic evidence management and audit readiness form an essential component of the model, enabling deviations to be used as learning data for continuous improvement.

The study demonstrates that a facility security guideline can be constructed to be both standards-aligned and practical to implement. Its effectiveness can be assessed after deployment, when sufficient observations on compliance, deviations and audit results are available, allowing controlled and incremental future refinements.

Sisältö

1 Johdanto

1.1 Tutkimuksen tausta ja lähtökohdat

Tämä raportti kuvaa takautuvasti ja metatasolla, miten tulevaisuuteen suuntautuva toimitilaturvallisuusohjeistus suunniteltiin ja koottiin vastaamaan samanaikaisia vaatimuksia laatujohtamisesta, tietoturvasta, tietosuojasta, ympäristöjohtamisesta ja operatiivisesta hallintamallista. Tarkoituksena ei ole esitellä ohjeistuksen yksityiskohtaista sisältöä, vaan selittää sen rakentumislogiikka: miten vaatimukset tunnistettiin, miten niistä muodostettiin johdonmukainen rakenne ja miten lopputulos validoitiin jäljitettävyyden ja vastuunjaon avulla.

Toimintaympäristö edellyttää monipaikkaista ja monimuotoista toimitilatoimintaa, usein monivuokralaisissa kiinteistöissä, joissa merkittävä osa perusinfrastruktuurista on vuokralaisen suoran hallinnan ulkopuolella. Tämä siirtää suunnittelun tavoitteen ideaalista ”täydellisestä perimetristä” kohti hallittavaa mallia, jossa erotetaan selkeästi, mikä on organisaation omassa kontrollissa, mihin voidaan vaikuttaa ja mitä voidaan ainoastaan valvoa ja käsitellä poikkeamien kautta.

Tutkimuksellinen kontribuutio on kaksiosainen. Ensinnäkin työ tuottaa jäsennellyn kuvauksen käytännöllisestä prosessista, jonka avulla toimitilaturvallisuuden ohjeistus voidaan rakentaa siten, että se on toteutettavissa Facility Management -toiminnoissa. Toiseksi työ tarjoaa esimerkin siitä, miten metakäsitteet (Area, Zone) ja vastuunjakoajattelu (RASCI) vähentävät tulkinnanvaraa ja parantavat ohjeistuksen auditointikelpoisuutta.

Raportin valmistelussa ja kirjoitusprosessissa on hyödynnetty tukiälypohjaisia välineitä kielenhuollon, aineiston rajauksen, tiedonhakuprosessien suuntaamisen ja argumentaation jäsentelyn tukena. Näitä välineitä on käytetty ainoastaan analyysin apuvälineinä, ja niiden tuottamat ehdotukset on arvioitu

kriittisesti ja sovellettu harkiten. Kaikki tekstissä esitettävät analyysit, tulkinnat ja johtopäätökset perustuvat tutkijan omiin näkemyksiin, työkokemukseen ja valittujen teoreettisten viitekehysten tarjoamiin reunaehtoihin.

Tukiälyn käyttö ei ole korvannut tutkijan omaa arviointikykyä tai analyyttistä vastuuta; se on toiminut ainoastaan apuna ilmaisun täsmentämisessä, kokonaisuuksien jäsentämisessä ja vaihtoehtoisten näkökulmien tunnistamisessa. Näin varmistetaan, että raportti täyttää tieteellisen kirjoittamisen keskeiset periaatteet; läpinäkyvyyden, toistettavuuden ja argumentaation loogisuuden, samalla kun tutkijan oma ääni ja asiantuntijuus säilyvät työn keskiössä.

1.2 Tutkimuksen tavoite ja tutkimuskysymykset

Tämän tutkimuksen tavoitteena on rekonstruoida ja selittää toimitilaturvallisuusohjeistuksen rakentumisprosessi evidenssipohjaisena hallintamallina sekä osoittaa, miten ohjeistus sidottiin useisiin viitekehyksiin ilman, että lopputuotteen yksityiskohtia paljastetaan.

Tutkimuskysymykset ovat seuraavat:

1. Miten toimitilaturvallisuusohjeistus voidaan jäsentää siten, että se on samanaikaisesti riskiperusteinen, auditoitava ja paikallisesti sovellettava
2. Miten Area- ja Zone-metakonseptit tukevat johdon mukasita kontrollisuunnittelua, tehtävien soveltuvuutta ja vastuunjakoa?
3. Miten Privacy by design ja Security (Facility) by Design voidaan integroida yhdeksi operatiiviseksi hallintalogiikaksi.
4. Miten RAS(C)I selkeyttää omistajuutta ja vähentää piiloriippuvuukisa monivuokralais- ja monitoimittajaympäristöissä

1.3 Rajaukset

Raportti on tarkoituksellisesti anonymisoitu: organisaation nimeä, kohdeosoitteita tai yksityiskohtaisia teknisiä konfiguraatioita ei esitetä. Analyysi tarkastelee periaatteita, rakennetta, hallintalogiikkaa ja jäljitettävyyttä. Työturvallisuutta käsitellään vain siltä osin kuin se liittyy toimitilaturvallisuuden operatiiviseen hallintaan, kuten hätätilanteiden kulku- ja poistumisjärjestelyihin. Pääpaino on toimitilaturvallisuuden johtamisessa ja ohjeistuksen toteutettavuudessa.

2 Tietoperusta

2.1 Tietoperusta

Toimitilaturvallisuusohjeistuksen tulee toimia siltana organisaation strategian ja arjen toteutuksen välillä. Käytännössä tämä tarkoittaa, että ulkoiset ja sisäiset odotukset muunnetaan kontrolli-, vastuu- ja päätössäännöiksi, joita voidaan soveltaa johdonmukaisesti eri kohteissa. Käyttökelpoinen tietoperusta yhdistää johtamisjärjestelmälähtöisen ajattelun, turvallisuuskontrollien periaatteet, tietosuojan reunaehdot sekä toimitilatoiminnan realiteetit.

2.2 Hallintamallin ja johtamisjärjestelmän yhteensopivuus

Toimitilaturvallisuuden hallintamallin tulee rakentua yhdenmukaisesti yleisesti hyväksyttyjen johtamisjärjestelmien periaatteiden kanssa, jotta kontrollit, vastuut ja päätöksenteon mekanismit voidaan esittää johdonmukaisina, todennettavina ja auditoitavina toimialasta tai organisaatiorakenteesta riippumatta. Kansainväliset johtamisjärjestelmästandardit, kuten ISO 9001 (laadunhallinta), ISO 14001 (ympäristöjohtaminen), ISO/IEC 27001 (tietoturvallisuuden hallinta) sekä uudempi laajennus ISO/IEC 27701 (tietosuojanhallinta), muodostavat yhteisen rakenteen, jossa korostuvat prosessiajattelu, dokumentoitu toimintalogiikka, riskiperusteinen toiminta ja jatkuva parantaminen (ISO 9001:2015; ISO 14001:2015; ISO/IEC 27001:2022; ISO/IEC 27701:2025).

ISO 9001 määrittää periaatteet, joiden mukaisesti prosessit, roolit ja kontrollit dokumentoidaan, omistetaan ja arvioidaan systemaattisesti; tämä tukee toimitilaturvallisuutta etenkin vaihtuvissa ja monitoimittajaympäristöissä (ISO 9001:2015). ISO 14001 laajentaa tarkastelua ympäristöriskeihin (esim. energiankulutus, kemikaalien käsittely, laitteiden elinkaarihallinta, jätteenkäsittely), mikä vahvistaa toimitilaturvallisuuden kokonaisvaltaisuutta (ISO 14001:2015). ISO/IEC 27001 asettaa vaatimukset kontrolloidulle pääsylle,

suojaustasojen erotukselle, ympäristönvalvonnalle ja tilojen turvallisuusluokitukselle, mikä on linjassa Area–Zone-mallin kanssa (ISO/IEC 27001:2022). ISO/IEC 27701 puolestaan korostaa henkilötietojen käsittelyn läpinäkyvyyttä, jäljitettävyyttä ja hallittua kontrollia, jolloin fyysisen ympäristön kontrollit ovat osa tietosuojan toteutusta (ISO/IEC 27701:2025).

Kokonaisuutena nämä standardit mahdollistavat hallintamallin, jossa toimitilaturvallisuus on osa johdonmukaista ja auditoitavaa johtamisjärjestelmää. Oma analyysini korostaa metatason rakenteita – RASCI-vastuunjakoa, Area/Zone-luokittelua ja kontrollilogiikkaa – yhdenmukaisuuden ja auditointivalmiuden varmistajina (Rikkonen 2026). Näin hallintamalli voidaan rakentaa sekä teoreettisesti perustelluksi että käytännössä toimivaksi kokonaisuudeksi myös monitoimittaja- ja monivuokralaisympäristöissä.

2.3 Privacy by Design operatiivisena reunaehtojärjestelmänä

Ohjeistuksen tulee yhdistää riskiperusteinen arviointikehys, vyöhykeloginen tilanhallinta ja tietosuojaperiaatteet tavalla, joka on auditoitava, operatiivisesti toteutettavissa ja yksilön kannalta ymmärrettävä. Tehokas turvallisuus perustuu uhkien, haavoittuvuuksien ja seurausten järjestelmälliseen tunnistamiseen sekä riskitasoon suhteutettuihin kontrolleihin (Coole & Brooks 2019; CISA 2015).

Area/Zone-malli tukee tätä kerroksellisella suojauksella: mitä kriittisempi toiminto, sitä syvemmälle suojausvyöhykkeeseen sen tulee sijoittua; näin vastuut ja tekniset kontrollit skaalautuvat riskin mukaan eivätkä oletettujen rakenteiden tai yleiskäytäntöjen perusteella (CISA 2015; NIST 2014). Privacy by Design (PbD) täydentää mallia siirtämällä painopisteen ennakoivaan suunnitteluun ja yksilön arjen toimintaan: vaikka tila olisi matalan riskin Zone/Area-kategoriassa, tietosuoja toteutuu vain, jos käyttäjä tunnistaa tietosuojaluokituksen ja toimii sen mukaisesti (Cavoukian 2012; Nampiina et al. 2020). Tutkimuskirjallisuus osoittaa, että riskit syntyvät usein työskentelytavoista, eivät yksin rakenteista (Nampiina et al. 2020; Cavoukian 2012; IEEE 2023).

PbD ja vyöhykelogia edellyttävät selkeää vastuunjakoa: RASCI tarjoaa viitekehyksen, jossa määritellään, kuka toteuttaa kontrollit (R), kuka omistaa vyöhykkeen/prosessin/kontrollin (A), kuka tukee (S), ketä konsultoidaan (C) ja kenelle tiedotetaan (I). Näin syntyy läpinäkyvä ja auditoitava toimintamalli,

joka toimii myös fyysisen ja digitaalisen turvallisuuden konvergenssissa (Railsware 2025; FacilityLead 2024; PNNL 2020; Betuš et al. 2026). Johtopäätöksenä toimitilaturvallisuus rakentuu neljästä toisiaan täydentävästä osa-alueesta: (1) riskiperusteinen uhka- ja haavoittuvuusarviointi, (2) vyöhykeloginen fyysinen ja organisatorinen rakenne, (3) PbD:n mukainen yksilön tieto- ja toimintavastuu sekä (4) RASCI-pohjainen läpinäkyvä vastuunjako. Tämä hallintamalli on standardoitavissa, paikallisesti sovellettavissa ja jatkuvasti kehitettävissä, ja se on linjassa oman aiemman analyysini kanssa (Rikkonen 2026).

2.4 Security (Facility) by Design kyvykkyysjärjestelmänä

Security (Facility) by Design määrittää tavan suunnitella toimitilojen turvallisuus siten, että fyysiset rakenteet, infrastruktuuri ja tekniset ratkaisut ovat sisäänrakennettuja eikä jälkikäteen lisättyjä. Security (Facility) by Design perustuu järjestelmälliseen ketjuun: uhka- ja haavoittuvuusanalyysi → arkkitehtuurivalinnat → implementointi → validointi (NIST 2022; NIST 2021). Lähestymistapa tukee turvallisia oletusarvoja ja suunnittelijan omistajuutta myös operatiivisissa ympäristöissä (CISA 2023).

Käytännössä Security (Facility) by Design tarkoittaa kerroksellista suojausta, selkeästi määriteltyjä vyöhykerajoja, tarkoituksenmukaista valvonnan sijoittelua, rakenteellisia viiveitä sekä kulunhallinnan peruslogiikkaa. Lähestymistapa on yhteismitallinen IEC 62443 -viitekehyksen kanssa (zones & conduits, roolijako omistaja–integraattori–toimittaja), ja sitä tukevat myös CPTED-periaatteet (ISO 22341:2021), joiden avulla ympäristö ohjaa oikeaan toimintaan ilman tarpeetonta monimutkaisuutta (IEC 62443; ISAGCA 2023; ISO 22341:2021).

Organisaatiotasolla Security (Facility) by Design konkretisoituu, kun periaatteet dokumentoidaan ja sidotaan Area/Zone-malleihin, pääsynhallinnan periaatteisiin ja teknisten kontrollien mitoitukseen (Rikkonen 2026(2)). Näin muodostuu johdonmukainen ja todennettavissa oleva turvallisuuskokonaisuus, jossa arkkitehtuuri, tekniset järjestelmät ja käyttäytymissäännöt tukevat toisiaan (NIST 2022; NIST 2021; CISA 2023; IEC 62443; ISAGCA 2023; ISO 22341:2021).

2.5 Area ja Zone meta käsitteinä

Area ja Zone muodostavat metatason rakenteen, jonka avulla fyysiset tilat ja suojaustarpeet muutetaan riskiperusteisiksi päätössäännöiksi. Area erottaa hallintarajan (Outside Secure Area vs Secure Area), kun taas Zone luo Secure Arean sisälle suojaustasojen porrastuksen (esim. Administrative Zone, Secure Zone One, Secure Zone Two). Arvo on operatiivinen: vaatimukset kytketään toistettaviin pääsy-, valvonta-, käyttäytymis- ja rakenteellisiin kontrolleihin (Rikkonen 2026(2)).

Mallin ydin on, että kontrollit mitoitetaan käsiteltävän toiminnon, tiedon ja järjestelmien mukaan; näin vältetään ali- ja ylisuojaus sekä parannetaan hallittavuutta monitoimittaja- ja monivuokralaisympäristöissä (IEC 62443; ISAGCA 2023). ISO 22341 tukee periaatetta korostamalla näkyvyyttä, kulkureittien hahmotettavuutta ja luonnollista valvottavuutta rikosten ehkäisyn rakenteellisina ratkaisuina (ISO 22341:2021). Malli toimii myös toiminnan ohjaajana: se määrittää, missä tehtävät voidaan suorittaa, millaisia riskejä niihin liittyy ja miten henkilöstön tulee toimia (Rikkonen 2026(2)).

Vyöhykkeiden määrittely edistää teknisten ja rakenteellisten kontrollien yhdenmukaisuutta. Sisäinen rakenteellisen ja teknisen kontrolliarkkitehtuurin ohjeistus kuvaa, miten rakenteelliset viiveet, suojaustasot ja valvonta mitoitetaan riskiperusteisesti eri vyöhykkeille, jotta suunnittelu, ylläpito ja turvallisuustoiminnot nojaavat yhteiseen viitekehykseen (Rikkonen 2026(2)).

2.6 Vastuunjako ja RASCI toimitilaturvallisuuden hallinnassa

Vastuunjaon selkeys varmistaa, että turvallisuusratkaisut perustuvat yhteisiin periaatteisiin eivätkä yksittäisten toimijoiden tulkintoihin. Accountability tarkoittaa päätösvaltaa ja lopullista vastuuta siitä, että tila tai prosessi täyttää riskiperusteiset vaatimukset; Responsible vastaa toteutuksesta (esim. kulunhallinnan konfiguraatio, valvontalaitteiden käyttöönotto, vyöhykkeiden tekninen määrittely); Support varmistaa resurssit; Consulted tuo asiantuntemuksen; Informed pitää sidosryhmät ajan tasalla (CISA 2023; FacilityLead 2024).

RASCI yhdistää rakenteelliset ja operatiiviset kontrollit yhdeksi hallintamalliksi, mikä on olennaista ympäristöissä, joissa kiinteistöinfrastruktuuri ja organisaation omat kontrollit limittyvät. Malli vähentää piiloriippuvuuksia ja

tekee omistajuudesta jäljitettävää ja auditoitavaa monitoimittaja- ja monivuokralaiskonteksteissa (Railsware 2025; Rikkonen 2026(2)). Näin turvallisuusarkkitehtuuri voidaan toteuttaa suunnitelmallisesti ja riskiperusteisesti, eikä päätöksenteko nojaa henkilökohtaisiin tulkintoihin.

2.7 Tehtävien soveltuvuus: sijainti kontrollina

Tehtävien soveltuvuus kääntää työympäristön valinnan osaksi kontrollia: tehtävä suoritetaan vain ympäristössä, jonka suojaustaso vastaa tehtävän tietoturva- ja tietosuojavaatimuksia. Näin ehkäistään tilanteet, joissa prosessit tai työnkulut irtautuvat fyysisen ympäristön tarjoamasta suojaustasosta.

Area/Zone-malli tarjoaa puitteet: matalan riskin tehtävät voidaan tehdä Outside Secure Areassa, kun taas luottamukselliset ja todennettavuutta vaativat tehtävät edellyttävät Secure Areaa tai korotettua Zone-tasoa (ISO 22341:2021). Tämä on erityisen tärkeää hybridityössä. Operatiivisesti malli edellyttää selkeästi dokumentoituja ja toistettavia sääntöjä (hyväksytyt/ei-hyväksytyt suoritusympäristöt, poikkeusten käsittely, siirtoperusteet), jolloin päätöksenteko on läpinäkyvää ja auditoitavaa (CISA 2023; Rikkonen 2026).

3 Menetelmät

3.1 Tutkimusasetelma

Tämän työn tutkimusasetelma on laadullinen, ja tavoitteena on jäsentää toimitilaturvallisuuden kokonaisuutta siten, että eri osa-alueista muodostuu selkeä ja käytännössä sovellettava malli. Laadullinen lähestymistapa soveltuu tilanteisiin, joissa pyritään ymmärtämään ilmiön rakenteita ja merkityksiä pikemminkin kuin mittaamaan niitä määrällisesti (Hirsjärvi, Remes & Sajavaara 2016). Tutkimus on luonteeltaan konstruktiivinen, sillä sen tarkoituksena on tuottaa uusi jäsennys toimitilaturvallisuuden periaatteista eikä vain kuvata olemassa olevia käytäntöjä.

3.2 Tutkimusmenetelmät

Tutkimusmenetelmänä käytetään dokumenttianalyysiä, joka sopii erityisesti tilanteisiin, joissa aineisto koostuu valmiista teksteistä, ohjeista ja suunnitteludokumenteista (Bowen 2009). Dokumenttianalyysi mahdollistaa sen, että eri lähteistä saadut tiedot voidaan yhdistää ja muodostaa niistä yhtenäinen kokonaisuus. Menetelmä tukee hyvin tutkimuksen tavoitetta yhdistää teoriaperusteiset viitekehykset ja käytännön työssä kehitetyt sisäiset mallit.

3.3 Aineisto ja analyysiprosessi

Tutkimuksen aineisto muodostuu kahdesta pääkokonaisuudesta. Ensimmäinen sisältää kansainvälisen kirjallisuuden ja turvallisuusstandardit, kuten NIST SP 800-160 -mallin, CISA:n Secure-by-Design-ohjeistuksen, IEC 62443 -sarjan vyöhykelogian sekä ISO 22341:n ympäristön suunnittelua koskevat periaatteet sekä muu ISO-standardiperheen oleellinen aineisto. Toinen osa koostuu tutkijan omassa työssä tuottamista sisäisistä dokumenteista, joissa kuvataan muun muassa Area/Zone-malli, toimitilaturvallisuuden käytännöt sekä rakenteellisiin ja teknisiin kontrolliratkaisuihin liittyvät ohjeistukset (Rikkonen 2026). Nämä

dokumentit täydentävät kansainvälisiä lähteitä tarjoamalla käytännön näkökulman siihen, miten teoriaa voidaan soveltaa organisaatiotasolla.

Aineistoa analysoitiin teorialähtöisen sisällönanalyysin avulla. Ensimmäisessä vaiheessa lähteistä tunnistettiin tutkimuskysymysten kannalta olennaiset teemat, kuten rakenteellinen suojaus, tekniset kontrollit, vyöhykelogia ja hallintamallit. Toisessa vaiheessa nämä teemat ryhmiteltiin laajemmiksi kokonaisuuksiksi ja yhdistettiin malliksi, joka kuvaa toimitilaturvallisuuden keskeisiä periaatteita (Tuomi & Sarajärvi 2018). Sisällönanalyysin etuna on sen joustavuus: monimuotoinen aineisto voidaan purkaa ja koota loogiseksi kokonaisuudeksi ilman, että sen keskeinen sisältö katoaa.

3.4 Triangulaatio ja validointi, Tutkijan rooli sekä vinoumien hallinta

Tutkimuksen luotettavuutta vahvistettiin triangulaatiolla käyttämällä useita eri aineistolähteitä ja vertaamalla niitä toisiinsa. Kansainväliset standardit, tutkimuskirjallisuus ja sisäiset dokumentit tarjoavat eri näkökulmia samaan ilmiöön, mikä vähentää yksittäiseen lähteeseen liittyvää tulkintariskiä (Bowen 2009; Nowell et al. 2017). Lisäksi analyysissa hyödynnettiin useita teoreettisia viitekehyksiä, mikä vahvistaa johtopäätösten uskottavuutta ja ehkäisee yhden lähteen ylikorostumista.

Tutkija toimii työssä sekä aineiston tuottajana (sisäiset dokumentit) että sen analysoijana. Tämän vuoksi oli tärkeää huolehtia siitä, etteivät omat kokemukset ohjanneet tulkintaa liikaa. Vinoumien hallitsemiseksi sisäisiä dokumentteja ei käytetty sellaisenaan tulkinnan perustana, vaan niitä tarkasteltiin rinnakkain kansainvälisten standardien ja tutkimuskirjallisuuden kanssa. Näin sisäisiä havaintoja voitiin suhteuttaa laajempaan viitekehykseen, mikä tukee tulkinnan tasapainoisuutta ja perusteltavuutta (Hirsjärvi, Remes & Sajavaara 2016).

3.5 Menetelmälliset rajoitteet ja työn luonne.

Tämä työ tuottaa ensisijaisesti jäsennyksen ja suunnittelulogikan toimitilaturvallisuusohjeistuksen rakentamiselle, eikä se mittaa mallin vaikuttavuutta käyttöönoton jälkeen. Tulokset perustuvat

dokumenttianalyysiin ja teorialähtöiseen sisällönanalyysiin, minkä vuoksi työ voi osoittaa mallin johdonmukaisuuden, auditointikelpoisuuden edellytykset sekä toteuttamiskelpoisuuden periaatteet, mutta ei vielä todentaa muutosta noudattamisessa, poikkeamien määrässä tai auditointihavainnoissa. Mallin vaikuttavuuden arviointi edellyttää käyttöönoton jälkeistä seurantaa ja vertailukelpoista evidenssiä, mikä on tässä työssä rajauksen ulkopuolella.

4 Tulokset ja johtopäätökset

4.1 Tulokset

Tutkimuksen tuloksena muodostui kokonaismalli, joka yhdistää toimitilaturvallisuuden rakenteellisen, teknisen ja organisatorisen suunnittelun yhdeksi johdonmukaiseksi kokonaisuudeksi. Analyysi osoitti, että ohjeistuksen rakentaminen ei onnistu pelkästään yksittäisiä kontrollitoimenpiteitä kokoamalla, vaan se edellyttää yhteistä rakennetta, jonka varaan eri vaatimukset, toimintatavat ja vastuut voidaan liittää. Tuloksissa korostui erityisesti se, että toimitilaturvallisuuden toimiva ohjeistus syntyy vasta silloin, kun fyysinen ympäristö, tehtävien sisältö, tietoon liittyvät vaatimukset, vastuunjako ja seuranta muodostavat keskenään yhteensopivan kokonaisuuden. Tällöin ohjeistus ei jää irralliseksi periaateasiakirjaksi, vaan siitä tulee käytännön johtamisen, päätöksenteon ja valvonnan väline.

Tulokset vastaavat erityisesti sellaisiin hallintaympäristön haasteisiin, joissa organisaatio toimii monivuokralaisissa kohteissa, hyödyntää useita palveluntuottajia, sovittaa yhteen useita viitekehyksiä ja joutuu samalla huomioimaan tietosuojan, tietoturvan, fyysisen turvallisuuden sekä käytännön toimitilaoperaatiot. Keskeiseksi tulokseksi ei muodostunut vain yksittäinen ohje tai malli, vaan toisiinsa liittyvä suunnittelulogiikka, jossa ensin määritellään mitä suojataan, sitten missä ympäristössä suojaus toteutetaan, tämän jälkeen millä ehdoilla toimintaa voidaan harjoittaa, kuka vastaa eri vaiheista ja lopuksi miten toteutuminen voidaan todentaa.

Tässä luvussa tulokset esitetään toisiaan tukevina osa-alueina, joita täydennetään kunkin alaluvun lopussa **“Näin pääset alkuun tässä”** -osuuksilla. Näiden tarkoituksena on tuoda tarkasteluun käytännöllistä konkretiaa ja ohjata lukijaa soveltamaan esitettyä mallia omaan toimintaympäristöönsä ilman, että ratkaisu esitetään valmiina tai yleistettävänä mallina.

4.1.1 Kahden suunnittelulogiikan yhdistäminen: Privacy by Design ja Security (Facility) by Design

Keskeinen tulos oli Privacy by Designin ja Security (Facility) by Designin yhdistäminen tavalla, joka tuottaa johdonmukaisen ja toisiaan täydentävän suunnittelulogiikan. Privacy by Design ohjaa sitä, miten työntekijä käsittelee tietoa, tekee arjen valintoja ja arvioi omaa toimintaansa suhteessa näkyvyyteen, kuultavuuteen, päätelaitteiden käyttöön ja ympäristön hallittavuuteen. Security (Facility) by Design puolestaan määrittää sen, millaista rakenteellista, teknistä ja toiminnallista suojaa fyysinen ympäristö pystyy tarjoamaan. Yhdistettynä nämä periaatteet muodostavat mallin, jossa tietosuoja ja turvallisuus eivät perustu yksin käyttäjän harkintaan eivätkä yksin tilan teknisiin ominaisuuksiin, vaan niiden yhteisvaikutukseen.

Tämä yhdistetty logiikka osoittautui erityisen tärkeäksi tilanteissa, joissa fyysinen tila voi olla rakenteellisesti riittävä, mutta tietosuoja vaarantuu silti käyttäjän toiminnan kautta. Vastaavasti havaittiin, että käyttäytymiseen perustuvat säännöt eivät yksin riitä, jos tehtävä, käsiteltävä tieto tai toiminnan luonne edellyttää ympäristöltä vahvempaa suojauskyvykkyyttä. Näin tuloksena syntyi lähestymistapa, jossa työn sisältö, tiedon luonne ja ympäristön suojaustaso voidaan tarkastella samassa mallissa ilman, että tietosuoja ja fyysinen turvallisuus jäävät erillisiksi tai keskenään ristiriitaisiksi osa-alueiksi.

Tämän tuloksen käytännöllinen merkitys oli siinä, että suunnittelun lähtökohta siirtyi tilojen nimeämisestä ja yksittäisten kontrollien luetteloinnista kohti tehtävän, tiedon ja ympäristön välistä suhdetta. Näin voitiin kuvata esimerkiksi tilanteita, joissa sama tila voi soveltua useaan käyttötarkoitukseen, mutta tehtävän sallittavuus määräytyy käsiteltävän tiedon, sivullisriskin ja käyttäytymiseen liittyvien vaatimusten perusteella. Ratkaisevaa ei siis ole vain se, missä työ tehdään, vaan myös se, mitä työssä tehdään ja millä ehdoilla se tapahtuu.

Näin pääset alkuun tässä: ensimmäinen vaihe on erottaa toisistaan käyttäytymiseen liittyvät vaatimukset ja fyysiseen ympäristöön liittyvät suojausvaatimukset. Käytännössä tämä tarkoittaa, että organisaation tulee tunnistaa keskeiset tehtävätyypit, niissä käsiteltävän tiedon luonne, näkyvyys- ja kuultavuusriskit, päätelaitteisiin liittyvät odotukset sekä tilanteet, joissa riski syntyy ensisijaisesti yksilön toiminnasta. Samanaikaisesti on kuvattava, mitä suojaa

fyysinen ympäristö voi tarjota rakenteiden, pääsynhallinnan, valvonnan, sijoittelun ja muiden käytännön ratkaisujen kautta. Kun nämä kaksi näkökulmaa on kuvattu rinnakkain, voidaan muodostaa ensimmäinen yhteinen perusmalli siitä, milloin käyttäytymiseen perustuvat kontrollit ovat riittäviä ja milloin niiden tueksi tarvitaan vahvempaa ympäristön tarjoamaa suojaa. Tämä vaihe luo perustan seuraavalle osa-alueelle, koska ilman sitä ei voida johdonmukaisesti määritellä, millaisia alueita ja vyöhykkeitä organisaatio ylipäätään tarvitsee.

4.1.2 Area–Zone-malli ohjeistuksen yhdistävänä rakenteena

Area–Zone-malli osoittautui tuloksissa keskeiseksi jäsentelytavaksi, joka mahdollisti kontrollien, vastuiden ja käyttösääntöjen yhdenmukaisen kuvaamisen. Mallin lähtökohtana oli rakenteellinen jako ympäristöihin, joita organisaatio hallitsee suoraan, sekä ympäristöihin, joita se hallitsee vain osittain tai joihin se voi vaikuttaa rajallisesti. Tämän jälkeen hallittujen ympäristöjen sisälle voitiin määritellä vyöhykkeitä, jotka erosivat toisistaan suojaustason, käyttötarkoituksen, pääsyperiaatteen ja valvonnan perusteella. Tällainen rakenne toi samaan malliin sekä yleiset toimitilaperiaatteet että korkeamman suojauksen alueita koskevat tarkemmat vaatimukset.

Mallin merkittävä etu oli sen realistisuus erityisesti monivuokralaisissa kiinteistöissä. Kaikki tilat, kulkureitit, tekniset ratkaisut tai tukipalvelut eivät ole organisaation omassa päätösvallassa, vaikka ne vaikuttavat suoraan turvallisuuden toteutumiseen. Tämän vuoksi pelkkä sisäisiin sääntöihin perustuva malli ei riitä, jos se ei samalla tunnista organisaation tosiasiallisia vaikutusmahdollisuuksia. Area–Zone-rakenne mahdollisti sen, että ohjeistuksessa voitiin erottaa toisistaan ympäristöt, joissa organisaatio voi itsenäisesti asettaa ja toteuttaa kontrollit, sekä ympäristöt, joissa turvallisuus rakentuu osittain vuokranantajan, palveluntuottajien tai muiden osapuolten ratkaisujen varaan.

Rakenteen vahvuus oli myös siinä, että se tarjosi yhteisen rungon useille eri ohjeistuksen osa-alueille. Sama rakenne mahdollisti pääsynhallinnan, vierailijakäytäntöjen, toimittajien liikkumisen, valvonnan käyttöperiaatteiden, poikkeamien käsittelyn ja tehtävien soveltuvuuden kuvaamisen yhdenmukaisessa muodossa. Näin vyöhykemalli ei jäänyt pelkäksi tilaluokitteluksi, vaan siitä muodostui koko ohjeistuksen yhdistävä rakenne.

Näin pääset alkuun tässä: kun tietoon, käyttäytymiseen ja ympäristön suojauskyvykkyyteen liittyvät perusvaatimukset on tunnistettu, seuraava vaihe on rakentaa niille tilallinen rakenne. Tämä kannattaa tehdä ensin hyvin yksinkertaisesti erottamalla toisistaan ympäristöt, joita organisaatio hallitsee suoraan, ja ympäristöt, joissa hallinta on osittaista tai välillistä. Tämän jälkeen hallittuun ympäristöön rakennetaan 2–4 vyöhykettä, joille määritellään vähintään tarkoitus, pääsyperiaate, sallittu käyttö, valvonnan taso ja muut keskeiset kontrollit. Tässä vaiheessa ei ole vielä tarpeen kuvata kaikkia yksityiskohtia, vaan luoda runko, johon seuraavat osa-alueet voidaan liittää johdonmukaisesti. Area–Zone-malli toimii siten siltana ensimmäisessä vaiheessa tunnistettujen suojausvaatimusten ja seuraavan vaiheen tehtäväsoveltuvuuden välillä. Kun ympäristörakenne on olemassa, voidaan siirtyä tarkastelemaan, millaiset tehtävät kuuluvat mihinkin ympäristöön ja millä ehdoilla.

4.1.3 Tehtävien soveltuvuus ja sijainnin käyttö kontrollina

Tutkimuksen konkreettisimpia tuloksia oli tehtävien soveltuvuusmalli, jossa työympäristön sijainti toimii kontrollina. Tarkastelun lähtökohtana ei ollut vain se, onko tila teknisesti turvallinen, vaan myös se, minkä tyyppisiä tehtäviä kyseisessä ympäristössä voidaan suorittaa hyväksyttävällä riskitasolla. Tämä korostui erityisesti hybridityössä ja etätyössä, joissa fyysinen työympäristö vaihtuu, mutta tiedon luottamuksellisuus, todennettavuuden tarve ja toiminnan riskit eivät muutu vastaavasti.

Tuloksena muodostui jäsennys, jossa tehtävät voidaan erottaa sen mukaan, millaisia ympäristövaatimuksia niiden suorittamiseen liittyy. Osa tehtävistä voidaan suorittaa ympäristössä, jonka hallittavuus on rajallinen, kunhan perustason käyttäytymissäännöt ja tekniset minimikontrollit toteutuvat. Osa tehtävistä voidaan suorittaa vastaavassa ympäristössä vain lisäkontrollein, kuten vahvennetulla päätelaitteella, rajatulla näkyvyydellä, hyväksytyillä työkaluketjuilla tai keskustelurajoitteilla. Kolmas ryhmä sisältää tehtäviä, jotka tulee sijoittaa hallittuun sisäympäristöön niiden sisältämän luottamuksellisuuden, todennettavuusvaatimuksen tai häiriöherkkyyden vuoksi. Neljäs ryhmä puolestaan sisältää tehtäviä, jotka edellyttävät korkeamman suojaustason vyöhykettä esimerkiksi privilegioitujen operaatioiden, sensitiivisten käsittelytilanteiden tai poikkeustilanteiden vuoksi.

Tämän tuloksen merkitys oli siinä, että sijainti muuttui logistisesta valinnasta tietoiseksi riskienhallinnan keinoksi. Tehtävien soveltuvuus ei siis määräytynyt pelkästään sen perusteella, mitä henkilö tekee työssään, vaan myös sen perusteella, missä ympäristössä kyseinen tehtävä voidaan toteuttaa turvallisesti. Samalla syntyi käytännöllinen perusta koulutukselle, käyttöoikeusperiaatteille, hyväksyntäprosesseille ja auditointikriteereille, koska tehtäväryhmät voitiin liittää suoraan ympäristörakenteeseen.

Näin pääset alkuun tässä: kun Area–Zone-rakenne on määritelty, seuraava vaihe on liittää siihen tehtävät. Tämä kannattaa tehdä tehtäväryhmittäin eikä yksittäisiin rooleihin tai nimikkeisiin takertuen, jotta malli kestää organisaation muutoksia. Organisaation tulee tunnistaa, millaiset tehtävät sisältävät perustason tietojenkäsittelyä, millaiset tehtävät edellyttävät lisäkontrolleja, mitkä tehtävät tulee rajata hallittuun sisäympäristöön ja mitkä vaativat korkeamman suojaustason vyöhykettä. Arvioinnissa on huomioitava vähintään tiedon luottamuksellisuus, näkyvyys- ja kuultavuusriski, todennettavuuden tarve, käytettävät oikeustasot sekä väärän suoritusympäristön vaikutukset. Kun tehtävät on ryhmitelty tällä tavalla, sijainti alkaa toimia varsinaisena kontrollina.

Tässä vaiheessa muodostuu myös perusta poikkeuslogiikalle: osa tehtävistä voidaan sallia alemmassa suojausympäristössä vain lisäehdoin, kun taas osa tehtävistä tulee rajata yksiselitteisesti korkeamman suojaustason ympäristöihin. Tämä vaihe antaa sisällön vyöhykemallille ja luo samalla tarpeen seuraavalle kysymykselle, eli sille, kuka päättää tehtävien sijoittelusta, poikkeuksista, toteutuksesta ja valvonnasta.

4.1.4 RASCI ja vastuut käytännön työnkulkuina

Tulokset osoittivat, että RASCI tuottaa arvoa vasta silloin, kun se sidotaan konkreettisiin työnkulkuihin. Pelkkä organisaatiokaavioon perustuva vastuunjako ei riitä, jos ei ole näkyvää kuvausta siitä, kuka käynnistää prosessin, kuka tekee valmistelun, kuka hyväksyy lopputuloksen, kuka tukee toteutusta, ketä kuullaan ja kenelle tieto annetaan. Tästä syystä RASCI-malli kytkettiin erityisesti sellaisiin työnkulkuihin, joissa päätöksiä tehdään toistuvasti ja joissa vastuurajat jäävät helposti epäselviksi.

Tällaisia työnkulkuja olivat esimerkiksi vyöhykeluokittelun muuttaminen, uuden valvontaratkaisun käyttöönotto, toimittajan pääsynhallinta, poikkeuksellisen työtehtävän sijoittaminen alempaan suojausympäristöön sekä auditoinnissa havaitun puutteen korjaaminen. Näissä tilanteissa RASCI siirtää vastuun oletuksista näkyviksi rooleiksi. Esimerkiksi corporate-tason turvallisuustoiminto voi omistaa periaatteen, kohdetason vastuuhenkilö toteuttaa käytännön muutoksen, juridinen tuki arvioi tietosuojaan liittyvän vaikutuksen, ICT tukee teknistä toteutusta ja area- tai zone owner varmistaa paikallisen soveltamisen. Tällöin vastuunjako ei jää muodolliseksi, vaan siitä tulee osa toteutuksen käytännön logiikkaa.

Merkittävä havainto oli myös se, että yksilön vastuu tulee näkyä osana työnkulkuja eikä vain ohjeiden kohteena. Käyttäjä tai työn suorittaja ei ole pelkästään informoitava osapuoli, vaan monissa tilanteissa vastuullinen toimija. Tämä näkyy esimerkiksi kulkutunnisteen asianmukaisessa käytössä, vierailijoiden saattamisessa, työympäristön valinnassa, poikkeamien ilmoittamisessa ja käyttörajojen noudattamisessa. Näin RASCI ei kuvaa vain hallinnollista rakennetta, vaan myös sitä, miten turvallisuus toteutuu päivittäisessä toiminnassa.

Näin pääset alkuun tässä: kun tehtävät ja ympäristöt on sidottu toisiinsa, seuraava vaihe on tehdä näkyväksi, kuka omistaa tämän mallin eri osat ja miten päätökset etenevät käytännössä. RASCI kannattaa rakentaa ensisijaisesti työnkulkujen ympärille, ei yleisluontoiseksi organisaatiokaavioksi. Ensimmäisessä vaiheessa on syytä valita muutama ydintyönkulku, joilla on suurin vaikutus mallin toimivuuteen, kuten uuden alueen tai vyöhykkeen määrittely, tehtävän sijoittaminen tiettyyn suojausympäristöön, poikkeusluvan käsittely, toimittajan pääsyn hyväksyntä, valvontaratkaisun käyttöönotto sekä auditointihavaintojen korjaaminen. Näissä prosesseissa tulee määritellä, kuka valmistelee asian, kuka hyväksyy lopputuloksen, kuka tukee toteutusta, ketä konsultoidaan ja kenelle tieto annetaan. Samalla on varmistettava, että vastuunjako tukee sekä Area–Zone-mallia että tehtävien soveltuvuuslogiikkaa. Jos vyöhykemalli määrittelee korkeamman suojaustason alueen, mutta sen muuttamiseen liittyvä omistajuus jää epäselväksi, rakenne ei toimi käytännössä. Jos taas tehtävä voidaan suorittaa alemmassa suojausympäristössä vain poikkeusluvalla, on oltava selkeä prosessi sille, kuka arvioi ehdot, kuka hyväksyy riskin ja kuka seuraa toteutusta. Tähän vaiheeseen kuuluu myös yksilön vastuun

näkyväksi tekeminen: käyttäjän tulee näkyä aktiivisena toimijana niissä kohdissa, joissa turvallisuus toteutuu sääntöjen noudattamisen, oikean ympäristön valinnan ja poikkeamien ilmoittamisen kautta. Kun RASCI rakennetaan osaksi käytännön työnkulkuja, syntyy pohja viimeiselle vaiheelle eli sille, miten mallin toimivuutta todennetaan ja seurataan.

4.1.5 Evidenssi, seuranta ja auditointivalmius

Tutkimus osoitti, että toimitilaturvallisuus on rakennettava tavalla, joka mahdollistaa auditoinnin, seurannan ja jatkuvan parantamisen. Tämän vuoksi kontrollit määriteltiin siten, että niihin liittyy aina todennettava evidenssi: mitä kirjataan, milloin kirjataan, miten tieto säilytetään ja kuka tarkastaa sen. Tällainen lähestymistapa siirtää huomion yksittäisistä virheistä järjestelmätason kyvykkyyteen ja siihen, miten organisaatio oppii poikkeamista.

Evidenssiketju (havainnollistava, ei organisaatiokohtainen). Auditointivalmius syntyy käytännössä siitä, että kontrollit on sidottu ennalta määritettyihin todennettaviin jälkiin. Yksinkertaisimmillaan tämä tarkoittaa ketjua: (1) määritelty kontrolli tai päätöskohta, (2) sovittu evidenssi (mitä tietoa syntyy ja mihin), (3) tarkastusvastuu (kuka varmistaa toteuman), ja (4) käsittelysääntö (mitä tehdään, jos havaitaan poikkeama). Kun tämä ketju on kuvattu jo suunnitteluvaiheessa, kontrollit eivät jää periaatteiksi, vaan niiden toteutumista voidaan osoittaa ilman erillistä “jälkikäteen keksittyä” raportointia.

Keskeiseksi tulokseksi muodostui ajatus siitä, että jokaiselle olennaiselle kontrollille tulee olla näkyvä jälki. Esimerkiksi vyöhykemuutoksesta voi syntyä hyväksyntäpäätös, poikkeamasta havaintokirjaus, toimittajapääsystä rekisterimerkintä ja koulutuksesta osallistumistieto. Kun evidenssi liitetään osaksi ohjeistuksen rakennetta alusta lähtien, kontrollit eivät jää pelkiksi periaatteiksi, vaan niiden toteutumista voidaan tarkastaa, vertailla ja kehittää systemaattisesti.

Tuloksissa korostui myös se, että poikkeamia ei tule tarkastella vain epäonnistumisina, vaan datapisteinä, jotka kertovat, missä ohjeistus, käyttötavat, vastuut tai kontrollit eivät vielä toimi riittävän hyvin. Tällöin seuranta ei ole vain valvontaa, vaan myös oppimisen väline. Auditointivalmius ja jatkuva parantaminen eivät näin muodosta erillistä jälkivaihetta, vaan kuuluvat osaksi koko toimitilaturvallisuuden johtamisrakennetta.

Näin pääset alkuun tässä: kun periaatteet, ympäristörakenne, tehtäväsoveltuvuus ja vastuunjako on määritelty, viimeinen vaihe on varmistaa, että mallin toteutumisesta syntyy todennettava jälki. Tämä tarkoittaa sitä, että jokaiselle keskeiselle kontrollille, päätökselle ja poikkeukselle on määriteltävä etukäteen, mitä evidenssiä syntyy, missä sitä säilytetään, kuka tarkastaa sen ja missä tilanteessa havainto johtaa korjaavaan toimenpiteeseen. Ensimmäisessä vaiheessa kannattaa valita ne kontrollit, joista halutaan aina näkyvä jälki, kuten vyöhykemuutokset, poikkeusluvat, toimittajapääsyt, koulutusten suorittaminen, tarkastusten toteutuminen ja havaitut poikkeamat. Tämän jälkeen näille tulee kuvata seurantatapa, tarkastusvastuu ja käsittelyrytmi. Tämä vaihe sitoo kaikki aiemmat vaiheet yhteen: käyttäytymiseen liittyvät vaatimukset näkyvät havaintoina ja koulutustietoina, Area–Zone-malli näkyy ympäristökohtaisina vaatimuksina, tehtävien soveltuvuus näkyy poikkeamien ja hyväksyntöjen kautta, ja RASCI näkyy siinä, että evidenssille on nimetty omistaja, tarkastaja ja käsittelyprosessi. Kun evidenssi ja seuranta rakennetaan mukaan jo suunnitteluvaiheessa, ohjeistus ei jää staattiseksi dokumentiksi, vaan muuttuu johtamisen välineeksi, jonka avulla voidaan arvioida toteutusta, tunnistaa puutteita ja tehdä jatkuvaa parantamista.

Yhteenvetona tulokset osoittivat, että toimitilaturvallisuuden toimiva kokonaismalli rakentuu viidestä toisiaan tukevasta osa-alueesta. Ensin määritellään käyttäytymiseen ja fyysiseen ympäristöön liittyvien suojausvaatimusten yhteinen logiikka. Tämän jälkeen rakennetaan Area–Zone-rakenne, joka toimii ohjeistuksen tilallisena runkona. Kolmannessa vaiheessa tehtävät sidotaan ympäristöihin siten, että sijainti toimii kontrollina. Neljännessä vaiheessa vastuut liitetään käytännön työnkulkuihin RASCI-mallin avulla. Viimeisessä vaiheessa kokonaisuus sidotaan evidenssiin, seurantaan ja auditointivalmiuteen. Juuri näiden osa-alueiden yhteensopivuus muodosti tutkimuksen keskeisen tuloksen.

4.2 Johtopäätökset

Tutkimuksen perusteella toimitilaturvallisuuden ohjeistus on mahdollista rakentaa kokonaisuutena, jossa fyysinen ympäristö, työn tekemisen ehdot, vastuunjako ja seuranta tukevat toisiaan. Johtopäätösten tasolla olennaista ei ole yksittäisten kontrollien luettelointi, vaan se, että ohjeistus rakentuu vaiheittain eteneväksi malliksi: ensin tunnistetaan, mitä suojataan ja millaisia vaatimuksia toimintaan liittyy, tämän jälkeen määritellään ympäristöt, joissa

työtä voidaan tehdä, sen jälkeen kuvataan tehtävien soveltuvuus eri ympäristöihin, liitetään tähän selkeä vastuunjako ja lopuksi varmistetaan toteutumisen seuranta. Tällainen etenemislogiikka tekee toimitilaturvallisuudesta hallittavamman kokonaisuuden myös ympäristöissä, joissa omistajuus, kontrollit ja käytännön vaikutusmahdollisuudet jakautuvat usean toimijan kesken.

Työn keskeinen kontribuutio on metatason malli, joka yhdistää toimitilaturvallisuuden suunnittelun kahden toisiaan täydentävän periaatteen (Privacy by Design ja Security (Facility) by Design) kautta tilalliseen Area–Zone-rakenteeseen, työnkulkuun sidottuun RASCI-vastuunjakoon sekä evidenssi- ja auditointivalmiuden logiikkaan. Uutta on erityisesti tehtäväsoveltuvuuden jäsentäminen siten, että työn sijainti toimii eksplisiittisenä kontrollina hybridityössä ja estää ristiriitaiset “toimisto-only”-vaatimukset tilanteissa, joissa sama työ on hyväksytty tehtäväksi myös etänä. Lisäksi työ tekee näkyväksi, miten auditointikelpoisuus voidaan rakentaa jo suunnitteluvaiheessa sitomalla kontrollit todennettaviin jälkiin ja vastuut konkreettisiin työnkulkuihin.

Tutkimuksen perusteella voidaan myös todeta, että ohjeistuksen toimivuus ei ratkea vain sillä, kuinka vahvoja yksittäiset turvallisuustoimenpiteet ovat, vaan sillä, kuinka johdonmukaisesti ne liittyvät toisiinsa. Jos tilaluokittelu, tehtävien sijoittelu, vastuunjako ja seuranta rakennetaan erillisinä osioina, lopputuloksena on helposti vaikeasti ylläpidettävä ja tulkinnanvarainen kokonaisuus. Kun nämä sen sijaan sidotaan samaan rakenteeseen, ohjeistus tukee paremmin sekä päätöksentekoa että käytännön toteutusta.

Ohjeistuksen vaikutuksia voidaan arvioida kattavasti vasta pidemmän käyttövaiheen jälkeen. Ensimmäinen realistinen tarkasteluhetki on vuoden 2027 aikana, jolloin noudattamista, poikkeamia, hyväksyntäkäytäntöjä ja auditointihavaintoja voidaan vertailla järjestelmällisemmin. Vasta tällöin on mahdollista arvioida luotettavammin, missä määrin rakennettu malli toimii käytännössä eri kohteissa ja missä kohdin sitä tulee tarkentaa.

4.2.1 Keskeiset johtopäätökset

Keskeinen johtopäätös on, että toimitilaturvallisuuden ohjeistus hyötyy mallista, jossa tietoon liittyvät vaatimukset, fyysisen ympäristön suojauskyvyk-

kyys ja työn käytännön toteutus tarkastellaan samassa kokonaisuudessa. Tällöin fyysinen turvallisuus ei jää pelkäksi rakenteelliseksi tai tekniseksi kysymykseksi, eikä tietosuoja vastaavasti jää vain yksilön harkinnan varaan, vaan molemmat liittyvät toisiinsa osana samaa toimintaympäristöä.

Toinen keskeinen johtopäätös on, että tilallinen jäsentely on tarpeellinen, mutta ei yksin riittävä ratkaisu. Area–Zone-rakenne toimii vasta silloin, kun se kytketään käytännön toimintaan, erityisesti siihen, millaisia tehtäviä eri ympäristöissä voidaan suorittaa ja millä ehdoilla. Tämän vuoksi sijainnin käyttö kontrollina nousee tärkeäksi johtopäätökseksi erityisesti hybridityön, liikkuvan työn ja vaihtelevien toimitilaympäristöjen näkökulmasta. Työn suorituspaikka ei ole neutraali taustatekijä, vaan osa riskienhallintaa.

Kolmas johtopäätös liittyy vastuunjakoon. RASCI-tyyppinen vastuunjako on hyödyllinen vasta silloin, kun se sidotaan selvästi määriteltyihin työnkulkuihin. Tällöin vastuu ei jää muodolliseksi, vaan muuttuu näkyväksi osaksi käytännön toteutusta. Erityisen tärkeää on, että mallissa näkyvät samanaikaisesti corporate-tason omistajuus, paikallinen toimeenpano sekä yksilön rooli sääntöjen noudattajana ja poikkeamien tunnistajana. Toimitilaturvallisuuden vaikuttavuus ei siten rakennu vain hallinnollisesta ohjauksesta, vaan myös siitä, että yksilön toiminta on huomioitu osana kokonaismallia.

Neljäs johtopäätös on, että seuranta ja auditointivalmius eivät ole erillinen loppuvaihe, vaan osa ohjeistuksen rakennetta jo suunnitteluvaiheesta alkaen. Kun päätöksistä, poikkeuksista, käyttöoikeuksista, koulutuksista ja kontrollien toteutumisesta syntyy todennettava jälki, turvallisuuden johtaminen siirtyy oletuksista havaittavaan ja arvioitavaan muotoon. Tämä vahvistaa myös jatkuvan parantamisen mahdollisuuksia, koska organisaatiolla on käytettävissään tietoa siitä, missä kohdin malli toimii ja missä ei.

4.2.2 Kriittinen tarkastelu ja kehittämismahdollisuudet

Keskeinen haaste tämänkaltaisessa tutkimuksessa on varmistaa, että johtopäätökset perustuvat dokumentoituun aineistoon, havaittaviin ratkaisuihin ja jäljitettäviin perusteluihin eivätkä tutkijan omaan muistikuvapohjaiseen tulkintaan. Tämä korostuu erityisesti silloin, kun tutkimus kohdistuu käytännön kehittämistyöhön, jossa tutkija on itse ollut lähellä suunnittelua tai toteutusta. Luotettavuuden kannalta ratkaisevaa on

tällöin se, että aineistoa tarkastellaan useasta näkökulmasta ja että päätöksenteon logiikka tehdään näkyväksi.

Tutkimus osoittaa, että tutkijan osallistuminen ei itsessään heikennä työn uskottavuutta, jos analyysin eteneminen, aineiston käyttö ja tulosten perustelut ovat läpinäkyviä. Menetelmällisesti tarkasteltuna työ asettuu kvalitatiivisen tapaustutkimuksen alueelle, jota tukevat dokumenttianalyysi ja triangulaatio. Kehittämisorientoitunut näkökulma on tutkimuksessa läsnä, mutta johtopäätösten arvo perustuu siihen, että syntynyttä mallia ei kuvata vain ratkaisuna, vaan myös arvioidaan sen ehtoja, rajoja ja sovellettavuutta.

Kehittämismahdollisuuksien näkökulmasta voidaan todeta, että mallin toimivuus riippuu pitkälti siitä, kuinka hyvin se pystytään pitämään riittävän yksinkertaisena. Jos ympäristörakenne, tehtäväsoveltuvuus, vastuunjako ja evidenssivaatimukset kasvavat liian raskaiksi, ohjeistus voi menettää käytännöllisyytensä. Toisaalta liian kevyt malli ei välttämättä riitä ympäristöissä, joissa käsitellään korkean luottamuksellisuuden tietoa, käytetään useita toimittajia tai toimitaan hallinnallisesti hajautetussa rakenteessa. Jatkokehityksen kannalta olennaista onkin löytää tasapaino yhdenmukaisuuden ja paikallisen sovellettavuuden välillä.

4.2.3 Jatkotutkimus ja kehittäminen

Jatkotutkimuksen kannalta keskeinen kysymys on, miten hyvin tässä muodostettu malli toimii erilaisissa toimitilaympäristöissä ja organisaatiorakenteissa. Erityisen kiinnostavia ovat tilanteet, joissa toimitilat, hallintarajat, vuokrasuhteet ja työn tekemisen käytännöt poikkeavat toisistaan merkittävästi. Tällöin voidaan arvioida, mitkä osat mallista ovat yleispäteviä ja mitkä vaativat vahvempaa paikallista sovittamista.

Toinen jatkotutkimuksen alue liittyy mittaamiseen. Tarvitaan tarkempia tapoja arvioida, miten tehtäväsoveltuvuuden määrittely, ympäristöjen käyttö kontrollina, vastuunjaon selkeys ja evidenssipohjainen seuranta vaikuttavat poikkeamien määrään, auditointivalmiuteen ja käytännön noudattamiseen. Ilman tällaista mittaristoa mallin vaikuttavuutta voidaan arvioida vain osittain.

Kolmas tärkeä jatkotutkimuksen alue liittyy yksilötason toimintaan. Vaikka ohjeistus voidaan rakentaa rakenteellisesti ja hallinnollisesti johdonmukaiseksi, turvallisuus toteutuu lopulta päivittäisessä käyttäytymisessä. Siksi

olisi hyödyllistä tarkastella tarkemmin, miten käyttäjät tekevät päätöksiä työympäristön valinnasta, miten he tulkitsevat tehtäväsoveltuvuutta käytännössä ja millaiset ohjauskeinot tukevat sääntöjen noudattamista tehokkaimmin.

Lisäksi jatkokehitystä tukisi kevyen päätöslokin tai muun vastaavan käytännön mallin kehittäminen. Tällainen ratkaisu voisi vahvistaa päätöksenteon läpinäkyvyyttä, helpottaa auditointeja ja tukea myöhempää ohjeistustyötä erityisesti tilanteissa, joissa ympäristöluokituksia, poikkeusratkaisuja tai käyttöoikeuksiin liittyviä linjauksia joudutaan tarkentamaan ajan myötä.

5 Lähdeviitteet ja kirjallisuusluettelo

Kirjat:

Eskola, J. & Suoranta, J. 1998. Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2016. Tutki ja kirjoita. Helsinki: Tammi.

Tuomi, J. & Sarajärvi, A. 2018. *Laadullinen tutkimus ja sisällönanalyysi.* Helsinki: Tammi.

Julkaisut

IEC 62443 -sarja. Security for Industrial Automation and Control Systems. Viitattu 15.3.2026. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

International Organization for Standardization. 2026. ISO 9001:2015 – Quality management systems — Requirements. Viitattu 15.3.2026. https://www.iso.org/standard/62085.html

International Organization for Standardization. 2026. ISO 14001 – Environmental management systems — Requirements with guidance for use. Viitattu 15.3.2026. https://www.iso.org/standard/14001

International Organization for Standardization. 2021. ISO 22341:2021 – Security and resilience — Protective security — Guidelines for crime prevention through environmental design. Viitatttu 15.3.2026 https://www.iso.org/standard/50078.html

International Organization for Standardization. 2026. ISO/IEC 27001:2022 – Information security management systems — Requirements. Viitattu 15.3.2026. https://www.iso.org/standard/27001

International Organization for Standardization. 2026. ISO/IEC 27701:2025 – Privacy information management systems — Requirements and guidance. Viitattu 15.3.2026. https://www.iso.org/standard/27701

NIST. 2021. SP 800-160 Vol. 2 Rev.1 — Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. Viitattu 15.3.2026 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

NIST. 2022. SP 800-160 Vol. 1 Rev. 1 — Engineering Trustworthy Secure Systems. Viitattu 15.3.2026 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf

NIST. 2014. SP 800-12: Physical and Environmental Security. Viitattu 15.3.2026. https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter15.html

Betuš, M. et al. 2026. Building Safe and Sustainable Universities: Integrated Governance Framework for Physical, Cyber and Psychosocial Security. Sustainability 18(5). Viitattu 15.3.2026. https://www.mdpi.com/2071-1050/18/5/2581

Artikkelit

Bowen, G. 2009. Document Analysis as a Qualitative Research Method. Qualitative Research Journal, 9(2). Viitattu 15.3.2026. https://doi.org/10.3316/QRJ0902027

ISAGCA. 2023. Quick Start Guide: An Overview of ISA/IEC 62443 Standards. Viitattu 15.3.2026. https://isasecure.org/hubfs/2023%20ISA%20Website%20Re-designs/ISAGCA/PDFs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf

IEEE. 2023. Architecting Privacy by Design: From Concept to Application. Viitattu 15.3.2026. https://digitalprivacy.ieee.org/publications/topics/architecting-privacy-by-design-from-concept-to-application/

FacilityLead. 2024. RACI in Facility Management: Clarifying Roles and Responsibilities. Viitattu 15.3.2026. https://facilitylead.com/raci-in-facility-management-clarifying-roles-and-responsibilities/

Nowell, L.S., Norris, J., White, D. & Moules, N. 2017. Thematic Analysis: Striving to Meet the Trustworthiness Criteria. International Journal of Qualitative Methods, 16(1). Viitattu 15.3.2026. https://doi.org/10.1177/1609406917733847

Railsware. 2025. Full Guide to RASCI Model. Viitattu 15.3.2026. https://railsware.com/blog/rasci-chart-with-examples/

Sähköiset Lähteet

Cavoukian, A. 2012. A Guide to Implementing Strong Privacy Practices – Operationalizing Privacy by Design. Viitattu 15.3.2026. https://gpsbydesigncentre.com/wp-content/uploads/2021/08/Doc-5-Operationalizing-pbd-guide.pdf

CISA. 2015. Facility Security Plan: An Interagency Security Committee Guide. Viitattu 15.3.2026. https://www.cisa.gov/sites/default/files/publications/ISC-Facility-Security-Plan-Guide-2015-508.pdf

CISA. 2023. Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure-by-Design and -Default. Viitattu 15.3.2026 https://www.cisa.gov/sites/default/files/2023-04/secure-by-design_and_-default_508c_0.pdf

Coole, M. & Brooks, D. 2019. Physical Security: Best Practices. Springer. Viitattu 15.3.2026. https://link.springer.com/content/pdf/10.1007/978-3-319-69891-5_220-1.pdf

PNNL / DOE. 2020. Facility Cybersecurity Framework Best Practices. OSTI.gov. Viitattu 15.3.2026. https://www.osti.gov/biblio/1660771

Opinnäytteet

Nampiina, E., Lkhagvasuren, M. & Madjidian, A. 2020. Privacy by Design – A Qualitative Study. Lund University. Viitattu 15.3.2026. https://lup.lub.lu.se/student-papers/record/9017931/file/9018102.pdf

Julkaisemattomat lähteet

Rikkonen, M. 2026. Analyysi toimitilaturvallisuuden ohjeistuksen rakenteesta. Sisäinen analyysi.

Rikkonen, M. 2026 (2). Sisäiset toimitilaturvallisuuden suunnittelu- ja ohjeistusmallit. Sisäiset dokumentit