Hanna Pikkusaari

RAKENNUKSEN JÄRJESTELMÄYMPÄRISTÖN DIGITAALISEN RESILIENSSIN LISÄÄMINEN JATKUVUUDENHALLINTAA KEHITTÄMÄLLÄ

Huoltovarmuuskeskeinen lähestymistapa

Opinnäytetyö

Ylempi AMK

Yrittäjyyden koulutus

2023

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Tradenomi (ylempi AMK)
Tekijä/Tekijät	Hanna Pikkusaari
Työn nimi	Rakennuksen järjestelmäympäristön digitaalisen resilienssin lisääminen jatkuvuudenhallintaa kehittämällä – Huoltovarmuuskeskeinen lähestymistapa
Toimeksiantaja	Yksityisen turva-alan pooli, Huoltovarmuusorganisaatio
Vuosi	2023
Sivut	88 sivua, liitteitä 19 sivua
Työn ohjaaja(t)	Nina Hartikainen, Atte Kokkinen

TIIVISTELMÄ

On yleisesti tiedossa, että kiinteistö- ja rakentamisala digitalisoituu parhaillaan nopeasti. Kuitenkin kriittisten toimijoiden järjestelmäympäristöön liittyvä jatkuvuudenhallinta on tutkimuksen kohteena vielä nuori. Tässä tutkimuksessa selvitettiin suomalaisten huoltovarmuuskriittisten organisaatioiden näkemyksiä ja kokemuksia käytössään olevien toiminnalleen kriittisten rakennusten järjestelmäympäristön eli OT-ympäristön jatkuvuudenhallintaan liittyen.

Tutkimuksen tavoitteena oli vastata kysymykseen, miten yleinen koko rakennuksen kattava OT-järjestelmäympäristö on kuvattavissa kokonaisuuden hallinnan näkökulmasta mahdollisimman yksinkertaisesti mutta kattavasti ja mitkä ovat tämän kokonaisuuden jatkuvuudenhallinnalle keskeisimmät ja parhaat käytännöt. Tutkimuksesta saadut tiedot valottavat suomalaisten huoltovarmuuskriittisten yritysten käytössä olevien rakennusten terveellisiä ja turvallisia olosuhteita ohjaavan OT-ympäristön jatkuvuudenhallinnan ja digitaalisen resilienssin tilaa yleisellä tasolla.

Tämä kyselytutkimuksen sekä puolistrukturoidun teemahaastattelun yhdistänyt monimenetelmäinen tapaustutkimus tuotti tietoa OT-järjestelmien jatkuvuudenhallinnan parhaista käytännöistä sekä vahvisti tarpeen OT-ympäristön läpileikkaavan jatkuvuudenhallinnan mallin kehittämiselle. Tutkimus osoitti, että rakennusten OT-ympäristöä ei kohderyhmässä tavallisesti käsitellä yhtenä kokonaisuutena, vaikka sen eri siiloilla ja niiden sisältämillä järjestelmillä on vahvoja vuorovaikutussuhteita. Näin ollen myöskään siihen liittyvä jatkuvuudenhallintaprosessi ei tue sellaisenaan kokonaisuuden digitaalista resilienssiä.

Tutkimusprojektin lopputuloksena syntyi yleiskäyttöinen työkalu, DIGIRES-kanvaasi, jota hyödyntämällä mikä tahansa organisaatio voi matalalla kynnyksellä kehittää oman OT-ympäristönsä jatkuvuudenhallintaa ja digitaalista resilienssiä. Johtopäätöksenä todettakoon, että tutkimusta aihealueella tulee jatkaa osin eri tutkimusmenetelmien välisten ristiriitaisten tulosten vuoksi.

Asiasanat: OT, rakennuksen järjestelmäympäristö, älykkäät rakennukset, digitaalinen resilienssi, jatkuvuudenhallinta, kyberturvallisuus

South-Eastern Finland
University of Applied Sciences

Degree title	Master of Business Administration
Author (authors)	Hanna Pikkusaari
Thesis title	Increasing digital resilience of building's operational technology environment by developing continuity management – Approach of critical built environment in terms of security of supply
Commissioned by	The National Emergency Supply Organization, Private security sector
Time	2023
Pages	88 pages, 19 pages of appendices
Supervisor	Nina Hartikainen, Atte Kokkinen

ABSTRACT

It is common knowledge that the field of real estate and construction is currently facing a rapid wave of digitalization. However, research on continuity management of critical organizations is still in its infancy. This study investigated perspectives and experiences related to operational technology (OT) environment's continuity management in Finnish organizations critical to the security of supply.

The objective of the study was to answer the question: How a general OT environment covering a building and facilities can be described comprehensively, and what are the best practices for the continuity management of operational technology, overall. The information obtained describes the state of digital resilience and continuity management of the OT environment in the target group on a general level.

This multi-method case study combining a survey and a semi-structured theme interview produced information on best practices of continuity management of operational technology. The research showed that usually the OT environment of a building is not managed holistically, although it may include several interconnections. Hence, the related continuity management process does not support the digital resilience of the entity as such either.

As a result of the research project, a continuity management process development tool, DIGIRES canvas, was created. The tool can be used to develop the continuity management and digital resilience of any company's OT environment. In conclusion, it should be stated that research in the topic area should be continued due to some conflicting results between different research methods.

Keywords: operational technology, smart building, digital resilience, continuity management, cybersecurity

SISÄLLYS

Kiitos rakkaani A, N, R & B. Ilman kannustustanne ja kärsivällisyyttänne
sekä kontrastia kirjoittamisen, arjen ja juhlan välillä tämä työ voisi olla vieläkin kesken.

1 JOHDANTO

Kiinteistöksi voidaan arkikielellä kutsua monia erilaisia rakennuksia. Koska Suomen laki ei kuitenkaan tunnista rakennusta kiinteistönä, vaan maa-alaan eli kiinteistöön kuuluvana osana (Kiinteistöverolaki 20.7.1992 / 654, 2 §), käytettiin tässä tutkimuksessa arkikielen kiinteistöstä nimitystä ”rakennus”.

Rakennuksessa sijaitseva toimitila on toimijan arvonluonnille keskeinen, mikäli toimija toimintaansa varten sellaisen tarvitsee. Toimitilan on tällöin luotava siellä tapahtuvalle toiminnalle terveelliset ja turvalliset olosuhteet. Näin organisaation toiminnan jatkuvuuden kannalta on olennaista varmistaa myös toimitilassa ja koko rakennuksessa tapahtuvan toiminnan kannalta kriittisimpien järjestelmien ja laitteiden toiminnan jatkuvuus. Rakennuksen tekee siis käyttökelpoiseksi siinä tapahtuvalle toiminnalle muun muassa oikeanlaiset olosuhteet luova tekninen ympäristö. Se koostuu ratkaisuista, jotka voivat sisältää uusissa sekä uudistetuissa rakennuksissa huomattavan paljon paikallisiin tietoverkkoihin sekä Internetiin kytkettäviä laitteita ja järjestelmiä.

Rakennus on tärkeä niin pienyrityksille kuin korporaatioillekin. Pienestä yrityksestä voi tulla hetkessä suuri – startupista voi tulla yksisarvinen. Tällöin myös toiminnan mahdollistavan rakennuksen merkitys voi korostua yllättävän paljon. Rakennus voi suojata ydinliiketoiminnan ja se voi varmistaa oikeanlaiset olosuhteet sekä palveluille että palvelimille. Rakennus voi myös auttaa luomaan tiedosta uutta liiketoimintaa.

Tämä tutkimus keskittyi rakennusten sekä toimitilojen toiminnan kannalta kriittisen järjestelmäkokonaisuuden jatkuvuudenhallinnan prosesseihin ja tämän toimintaympäristön digitaalisen resilienssin tutkimiseen ja kehittämiseen. Tutkimuksessa selvitettiin, millä tavalla näitä prosesseja voitaisiin kehittää aiempaa paremmiksi ja millaisia välineitä tai työkaluja se vaatii. Tutkimuksessa rakennuksen toimintaa ohjaavia järjestelmiä kutsuttiin OT-järjestelmiksi ja järjestelmäympäristöä kokonaisuutena OT-järjestelmäympäristöksi tai lyhyesti OT-ympäristöksi.

1.1 Makroympäristössä tapahtuvat muutokset

Rakennuksen OT-ympäristöä tarkasteltiin näkökulmasta, jossa voimakkaasti muuttuva maailma luo sekä mahdollisuuksia että haasteita kompleksiselle ympäristölle ja sen johtamiselle. Tämä neljänneksi teolliseksi vallankumoukseksi (teollisuus 4.0, industry 4.0) kutsuttu disruptiivisten innovaatioiden aikakausi aiheuttaa suuria muutoksia kiinteistö- ja rakentamisalalle (Woodhead ym. 2018, 35). Tällainen muutosten jakso sekä sitä seuraava viides teollinen vallankumous voivat luoda ennennäkemättömiä liiketoimintamahdollisuuksia alan uusille sekä vanhoille toimijoille. Se, että organisaatio sivuuttaisi riskin mahdollisesta toimialan disruptiosta tällaisen muutoksen myötä, ei ole taloudellisesti eikä strategisesti järkevää, sillä disruptioon varautuminen luo jo itsessään mahdollisuuden häiriöstä selviytymiseen eli vahvistaa organisaation resilienssiä (Williams & You 2022, 4).

Tutkimusten mukaan Euroopan rakennuskannasta jopa 90 % on käytössä vielä vuonna 2050 (Al Dakheel ym. 2020, 1). On siis välttämätöntä varmistaa näiden rakennusten teknisen ympäristön jatkuvuus sekä ympäristön digitaalinen resilienssi vielä pitkälle tulevaisuuteen. Samalla Sitran julkaisemien megatrendien mukaan kamppailu digivallasta kiihtyy (Dufva & Rekola 2023, 47). Digitaalisesta vallasta kiistellään vääntämällä kättä siitä, kuka kerää ja kuka hyödyntää dataa, millaiset ovat digitaalisen maailman pelisäännöt, millaisia resursseja teknologia vaatii ja mihin suuntaan teknologian pitäisi kehittyä (Dufva & Rekola 2023, 47). Koska rakennukset ovat merkittävä tiedonlähde, koskee digivaltaan liittyvä keskustelu myös rakennuksia ja koko rakennettua ympäristöä.

Jatkuvasti kehittyvä teknologia on nykypäivän ilmiönä merkittävä, eikä sitä aina ehditä arjen kiireessä kyseenalaistaa. On tärkeää pohtia millä ehdoilla ja mitä uutta teknologiaa kannattaa ja voidaan ottaa käyttöön. On arvioitava, onko valittu teknologia todella omien asetettujen linjausten mukaista. Koska digitaalisen ympäristön pelisääntöjä ei ole asetettu yhdessä eikä pohdittu riittävästi, päättävät säännöistä käytännössä monikansalliset teknologiayritykset. (Dufva & Rekola 2023, 47.) Tällä on suoria vaikutuksia rakennettuun ympäris-

töön, kiinteistöihin ja rakennuksiin eli Suomen kansallisvarallisuuteen. Rakennuksen OT-ympäristön jatkuvuudenhallintaa käsiteltäessä tuleekin vastattua moniin edellä mainittuihin pelisääntöihin koskeviin kysymyksiin.

Koska kaikki digitalisoituu vähitellen ja vuorovaikutus siirtyy tietoverkkoihin, syntyy uusia osaamistarpeita. Näihin on vastattava oikea-aikaisesti. Hajautettuun arkkitehtuuriin perustuvat ratkaisut mahdollistavat erilaisten ekosysteemien rakentamisen. Tiedon ja toimintojen orkestrointiin liittyvät kyvykkyydet korostuvat, dataa kertyy valtavia määriä ja sitä on osattava käsitellä tehokkaasti ja vastuullisesti. (Dufva & Rekola 2023, 47–48.) Koska teknologia sulautuu kaikkeen (Dufva 2020, 37), puhutaan digitaalisesta ja vihreästä kaksoissiirtymästä. Siinä digitalisaation ja datan hyödyntäminen edistää matkaa kohti hiilineutraalia yhteiskuntaa (Sitra s.a.). On siis pohdittava luonnon kantokyvyn rajoja ja toimittava tämän vihreän kaksoissiirtymän tavoitteiden mukaisesti (Dufva & Rekola 2023, 47–48). Nämä tavoitteet pyrkivät turvaamaan sekä luonnon että ihmisten hyvinvoinnin edellytykset sukupolvelta toiselle (Dufva & Rekola 2023, 12). Kaikki tämä on nykypäivää ja keskeinen osa rakennuksia ja niiden järjestelmäympäristöä koskevaa muutosta.

1.2 Toimialavertikaalit läpileikkaava näkökulma

Jokainen toimiala hyödyntää nykyisin IT-järjestelmiä tavalla tai toisella. Visuaalisesti voisi ajatella IT:n läpileikkaavan kaikki muut toimialat. Toisaalta jokainen toimiala tarvitsee myös rakennuksia. Näin ollen voi ajatella myös kiinteistö- ja rakentamisalan läpileikkaavan muut toimialat IT:n tavoin. Tätä ajatusta voi kehittää myös pidemmälle. COVID-19-pandemian aikana yleiseen keskusteluun nostettu rakennuksen sisäilmasto ja siihen liittyvät viruksen leviämistä edistävät tai vähentävät toimenpiteet nostivat ehkä huomaamatta rakennuksen terveelliset ja turvalliset olosuhteet mahdollistavan järjestelmäympäristön hetkeksi julkisen keskustelun ytimeen. Tampereen yliopiston ja Tampereen ammattikorkeakoulun selvityksen mukaan muun muassa ilmanvaihtojärjestelmän käyttötavoilla todettiin olevan merkitystä tartuntariskin kannalta (Silander & Sormunen s.a., 1–2). Toisaalta energiahinnat nousivat merkittävästi Venäjän Ukrainaa vastaan kohdistuvan hyökkäyssodan myötä (Tilastokeskus 2022, s.a.). Tämän jälkeen keväällä 2023 Euroopan parlamentti hyväksyikin EU:n aiempaa tiukemmat energiatehokkuustavoitteet, jotka tulevat

tiukentamaan energiatehokkuusdirektiiviä sekä vauhdittavat toimenpiteitä energiatehokkuuden optimointiin liittyen (Euroopan parlamentti 2023 a, s.a.). Näillä linjauksilla tuetaan kunnianhimoisia ilmastotavoitteita, mutta samalla pyritään irtaantumaan suurelta osin Venäjältä tuotaviin fossiilisiin polttoaineisiin liittyvästä riippuvuudesta (Euroopan parlamentti 2023 b, s.a.). Koska rakennuksen järjestelmäympäristöön liittyy merkittäviä turvallisuuteen, terveyteen ja tehokkuuteen liittyviä yleisiä vaatimuksia, voi myös OT-järjestelmiä ja niihin liittyviä palveluita olla hyödyllistä käsitellä yhtenä rakennusten lailla toimialat läpileikkaavana kokonaisuutena.

COVID-19 nopeutti selkeästi digitaalista transformaatiota eri aloilla. Esimerkiksi Saeedin ym. (2023, 5-6) tutkimuksen mukaan Yhdistyneen kuningaskunnan terveydenhuoltoalalla on tunnistettu nopea harppaus kehityksessä pilvilaskentaan, suurten tietomassojen hallintaan ja IoT:hen (Internet of Things, esineiden internet) liittyen. Samalla on havaittu kuitenkin myös, että digitalisaatio lisää järjestelmäympäristön haavoittuvuuksia, jolloin kyberhyökkäysten uhka kasvaa. Tutkimuksessa muistutetaan, että toiminnan resilienssin toteutumisen kannalta on olennaista lisätä tietoisuutta kyberturvallisuuteen liittyen. Tutkimuksessa todetaan myös, että digitaalisen resilienssin kehittäminen on välttämätöntä, jotta kyberuhilta voidaan suojautua mahdollisimman tehokkaasti. (Saeed ym. 2023, 5-6, 16.)

Digitaalinen transformaatio, jossa perinteiset liiketoimintaprosessit alkavat hyödyntää IT-järjestelmiä (Saeed ym. 2023, 1) luo uusia mahdollisuuksia kaikille toimialoille. Näin ollen se koskee myös kiinteistö- ja rakentamisalaa. Alan keskiössä olevan rakennuksen järjestelmäympäristöön toteutetaan tavallisesti useita siilomaisia rakenteita, joiden tuottamaa dataa voidaan hyödyntää läpi siilojen, kunhan kokonaisuus suunnitellaan ja toteutetaan hyvin integroituvaksi (Sinopoli 2016, 162). Tällaisen ratkaisun toteuttaminen vaatii kuitenkin hankkeen toimijoilta kykyä olla rakentamatta pistemäisiä järjestelmiä varmistaen näin mahdollisimman laajamittaiset hyödyt älykkääksi suunnitellun kokonaisuuden kannalta. (Woodhead ym. 2018, 43.)

OT-järjestelmäympäristön ekosysteeminäkökulman nostaminen osaksi IT:n strategisia linjauksia on keskeistä, jotta on mahdollista ottaa kantaa rakennuksen koko elinkaaren ajan ratkaisuihin (Woodhead ym. 2018, 35). Ja vaikka

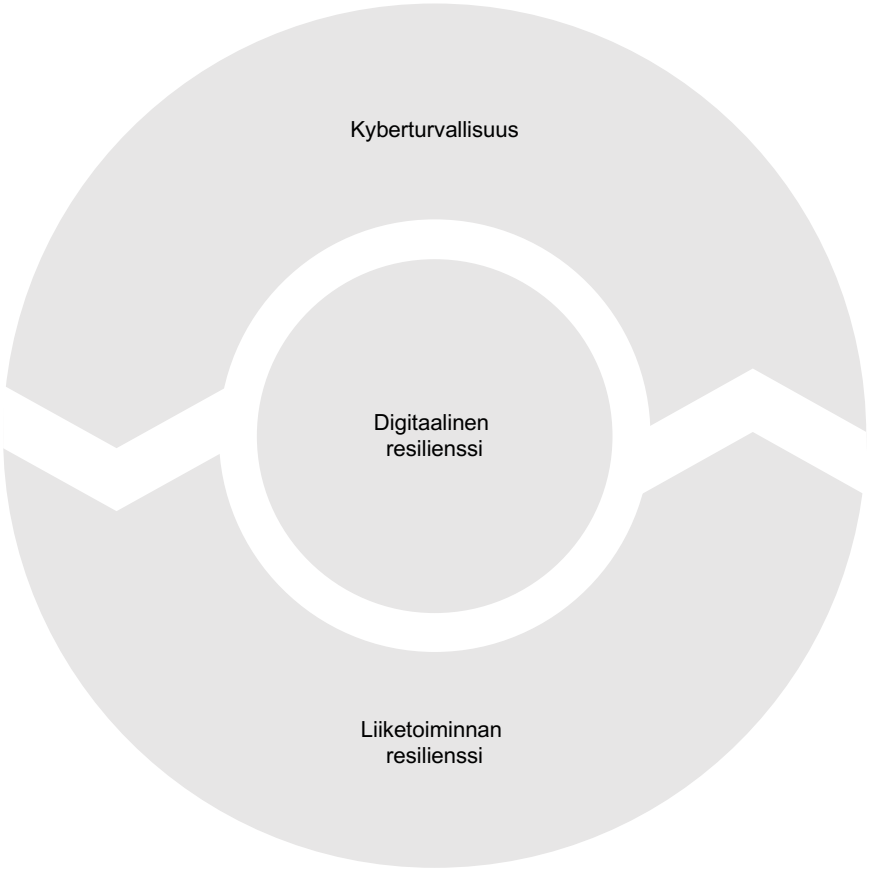
tuotannon OT-ympäristöön on havaittu kohdistuvan samankaltaisia uhkia kuin IT-ympäristöön, on OT-ympäristöstä vastaavilla tahoilla selkeästi erilaiset tavoitteet kyberturvallisuuteen ja kokonaisuudenhallintaan liittyen (Kosmowski ym. 2022, 2). Samanlaiset haasteet kohdistuvat tämän tutkimuksen tulosten perusteella myös rakennusten OT-ympäristöihin. Digitalisoituneen OT-järjestelmäympäristön johtamisen voi ajatella siis vaativan yhä enemmän IT-järjestelmäympäristön hallinnassa ja johtamisessa käytettävien keinojen ja mallien soveltamista, mutta myös digitalisoituneeseen ympäristöön liittyvien uudenlaisten riskien ja toiminnan jatkuvuudenhallintaa. Muun muassa tämän tutkimuksen otoksella voitiin vahvistaa se, että tällaiset kyvykkyydet vaativat uudenlaista osaamista niin kokonaisuuden johtamiseen, suunnitteluun, hankintaan, toteuttamiseen kuin myös koko rakennuksen elinkaaren prosesseihin liittyen.

1.3 Direktiivien sanelema tarve kehittämiselle

Euroopan unionin kyberturvallisuusdirektiivin 2022 / 2555 eli NIS 2 -direktiivin (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022 / 2555) sekä direktiivin kriittisten toimijoiden häiriönsietokyvystä (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022 / 2557) voimaanastuminen joulukuussa 2022 käynnistivät jäsenvaltioiden valmistelutoimenpiteet direktiivien paikalliseen käyttöönottoon liittyen. NIS 2 -direktiivin tarkoituksena on taata kriittiseksi luokiteltavien yritysten sekä julkisten toimijoiden toimintavarmuus ja varmistaa kyberturvallisuuden korkea taso EU:n sisämarkkinalla (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022 / 2555). Koska direktiivi koskee myös OT-ympäristöä, tukee tehty tutkimus direktiivin käyttöönottoon valmistautumista kansallisella tasolla.

Toisaalta COVID-19-pandemia sekä Venäjän pitkään jatkunut hyökkäyssota Ukrainassa ovat korostaneet tarvetta varmistaa kriittisten toimintojen jatkuvuus poikkeustilanteissa. Koska teknistä kyberturvallisuutta kehittämällä ei voi varautua kaikkiin mahdollisiin kyberturvallisuutta uhkaaviin skenaarioihin, on liiketoiminnan jatkuvuutta suojaavan digitaalisen resilienssin lisääminen käytännössä välttämätöntä (Petrenko 2019, 281). Petrenko (2019, 281) kuvaa digitaalisen resilienssin keskeistä roolia liiketoiminnan resilienssin ja kybertur-

vallisuuden keskiössä kuvan 1 mukaisesti. Hyvänä esimerkkinä välttämättömyydestä kehittää digitaalista resilienssiä voi toimia esimerkiksi voimalaitos. Koska kompleksisessa ympäristössä ei kyberiskuilta voi täysin suojautua, on panostettava digitaalisen resilienssin kehittämiseen. (Kosmowski ym. 2022, 18.)



Kuva 1. Käsitekaavio digitaalisen resilienssin, kyberturvallisuuden ja liiketoiminnan resilienssin välisistä riippuvuuksista (Petrenko 2019, 281.) (suomennettu alkuperäisestä kaaviosta)

Kuten Petrenko (2019, 281) kaaviossaankin osoittaa, on digitaalisella resilienssillä keskeinen ja oleellinen tehtävä. Se turvaa liiketoiminnan jatkuvuuden teknologian sulautuessa kaikkeen Sitran megatrendien (Dufva 2020, 37) mukaisesti. Organisaation toiminnalle keskeisten häiriötilanteiden tunnistaminen sekä palautumis- ja toipumisprosessien kuvaaminen ovatkin jatkuvuudenhallinnan keskeisiä osatekijöitä (Kosmowski 2022, 10). Tunnistettujen riskien pienentäminen voi kuitenkin olla haastavaa digitalisoituneessa järjestelmäympäristössä ja häiriöiden erittäin nopea laajeneminen digitaalisten kanavien kautta voi olla hyvinkin mahdollista (Huoltovarmuuskeskus 2021.).

1.4 Tutkimushypoteesi ja rajaus

Rakennuksen OT-ympäristön mukautumiskykyä jatkuvasti muuttuvassa ja digitalisoituvassa toimintaympäristössä on luontevaa käsitellä jatkuvuudenhallinnan sekä digitaalisen resilienssin kautta. Jatkuvuudenhallintaan ja palautumiskykyyn sekä jatkuvaan muutos- ja mukautumiskykyyn muuttuvassa ympäristössä viittaa muun muassa Björck ym. tutkimuksessaan (2015, 312). Toisaalta Kosmowski ym. nostaa digitaalisen resilienssin ja palautumisen kannalta yhtenä tärkeänä tekijänä OT-ympäristön keskeisten fyysisten varaosien saatavuuden (2022, 18). Tieteelliset tutkimukset eivät vaikuta keskittyneen nimenomaan rakennuksen OT-ympäristöön kokonaisuutena. Rajaaminen huoltovarmuuskriittisten toimijoiden toiminnan kannalta kriittisiin rakennuksiin avasi tämän tutkimuksen kautta kiinnostavaa lisätietoa tämän vähän tutkitun kokonaisuuden jatkuvuudenhallinnan tilasta ja aihealueen liiketoiminta- ja kehitysmahdollisuuksista.

Tutkimuksen lähtökohtana oli seuraava hypoteesi: *Rakennuksen OT-järjestelmäympäristöä ei ole käytännön tasolla tunnistettu yhtenäiseksi järjestelmäkokonaisuudeksi eikä näin ollen sen jatkuvuudenhallintaprosessia ole kehitetty tukemaan teknisen ympäristön digitaalista resilienssiä.* Tutkimuksessa keskityttiin erityisesti huoltovarmuuden näkökulmasta keskeisimpiin rakennuksiin ja toimitiloihin ja niissä toiminnan kannalta kriittisimpien OT-järjestelmien jatkuvuudenhallinnan kannalta parhaiksi koettuihin käytäntöihin. Käsitellyt toimialat rajautuvat NIS 2 -direktiivissä (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022 / 2555, liite I - liite II) määriteltyihin erittäin kriittisiin sekä osittain muihin kriittisiin toimialoihin. Tällä rajauksella tutkimus kohdistui organisaatioihin, jotka ovat kokoluokaltaan suuria tai huoltovarmuuden näkökulmasta merkittäviä.

1.5 Tavoite ja tutkimuskysymys

Tutkimuksen tavoitteena oli selvittää OT-ympäristön jatkuvuudenhallinnan tilaa ja parhaita käytäntöjä sekä laatia työkalu OT-järjestelmäympäristön digitaalista resilienssiä lisäävän jatkuvuudenhallinnan kehittämistä varten. Tavoitteen saavuttamiseksi vastattiin kyselytutkimuksen sekä teemahaastattelun keinoin seuraavaan tutkimuskysymykseen: *Miten yleinen koko rakennuksen ja toimitilat kattava OT-järjestelmäkokonaisuus on kuvattavissa mahdollisimman*

suoraviivaisesti ja helppolukuisesti, ja mitkä ovat tämän kokonaisuuden jatkuvuudenhallinnalle keskeisimmät ja parhaat käytännöt? Tutkimuksen tavoitteena oli jatkuvuudenhallinnan työkalun kehittämisen lisäksi lisätä toimialariippumattomasti ymmärrystä rakennuksen OT-järjestelmäympäristön roolista keskeisenä terveellisen ja turvallisen toiminnan varmistavana sekä konkreettisesti johdettavana, kehitettävänä ja tutkittavana kokonaisuutena.

Koska tutkimus toteutettiin opinnäytetyönä yrittäjyyden opintoihin liittyen, oli sen tehtävänä myös luoda mahdollisimman kantava tietopohja mahdollista uuden asiantuntijuuteen perustuvan yrityksen liiketoimintaa varten. Tutkittu aihealue on erittäin ajankohtainen, mutta samaan aikaan aiheeseen liittyen ei ole saatavilla ammattiin valmistavaa tai osaamista täydentävää koulutusta. Konsultointi aihealueella painottuu joko IT-ympäristön ja sen tukeman liiketoiminnan jatkuvuudenhallintaan ja resilienssiin tai automatisoituihin ja älykkäisiin tehdasympäristöihin. Rakennuksiin liittyen tämä OT-ympäristön jatkuvuudenhallinnan ja digitaalisen resilienssin yhdistävä tutkimus on yksi harvojen joukossa.

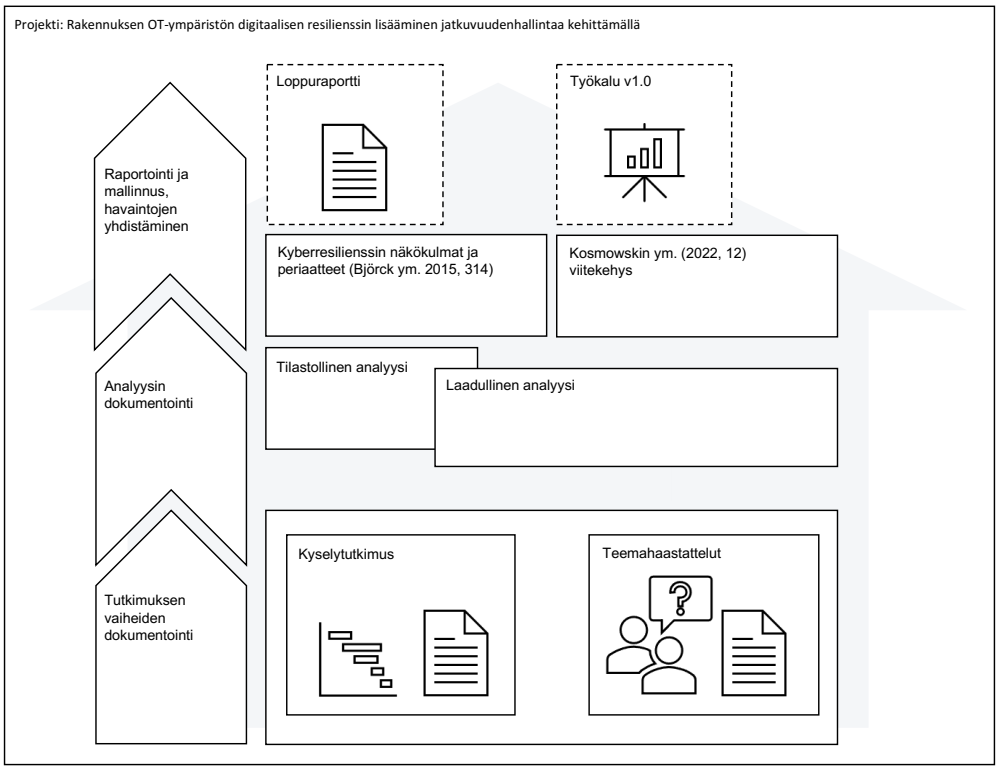
1.6 Monimenetelmäinen lähestymistapa työkalun kehittämiseen

Tapaustutkimus toteutettiin monimenetelmäisesti hyödyntäen kyselytutkimusta varmentavana ja tutkimukseen innoittavana menetelmänä laadullisen tutkimuksen rinnalla. Laadullisena tutkimusmenetelmänä käytettiin puolistrukturoitua teemahaastattelua. Tarve eri menetelmien yhdistämiseen nousi kontekstista sekä tutkimushypoteesista. Kummallakin menetelmällä oli itsenäinen rooli, mutta yhdistettynä ne syvensivät aihetta vastaten tutkimuskysymykseen kokonaisuudessaan. Tutkimuksen toteutustavalla saatiin myös luotua tilanne, jossa oli tunnistettavissa kontrasti eri toteutustapojen välillä.

Rakennuksen OT-järjestelmien digitaalista resilienssiä jatkuvasti muuttuvassa ja digitalisoituvassa toimintaympäristössä olisi luontevaa käsitellä systeemiteorian näkökulmasta kompleksisten järjestelmien välisten riippuvuuksien muodostamana riippuvuusongelmana eli useiden järjestelmätason ongelmien muodostamana ylätason ongelmana. Koska tutkimuksen mukaan OT-ympäristö sisältää hyvin monen tasoisia riippuvuuksia, olisi kokonaisuutta ollut luontevaa hahmotella kategorisoinnin lisäksi esimerkiksi eritasoisia riippuvuuksia

yhdistävän Nordes-konferenssissa vuonna 2011 Sevaldsonin (2011, 1) esittelemän GIGA-mapping -menetelmän avulla. Tämä kuitenkin rajattiin kaikessa laajuudessaan prosessin ulkopuolelle mahdollisena jatkotutkimuksen menetelmänä.

Tutkimuksen tuloksia peilattiin Björckin ym. (2015, 315) teoriaan kyberresilienssin näkökulmista ja periaatteista (”Cyber resilience aspects and principles”) ja riippuvuuksien osalta Kosmowskin ym. (2022, 12) viitekehykseen OT-ympäristön resilienssin käsittelystä. Kuva 2 osoittaa tehdyn tutkimuksen rakenteen sekä eri vaiheet tutkimusprosessin näkökulmasta.



Kuva 2. Tutkimuksen rakenne ja eteneminen tutkimukselle keskeisten Björckin ym. ja Kosmowskin ym. viitekehysten näkökulmasta (Björck ym. 2015, 314; Kosmowski ym. 2022, 12)

Kuvan 2 mukaisesti tutkimuksessa käsiteltiin laajaa kokonaisuutta. Tämä oli tarkoituksenmukaista, sekä sisällön että toteutetun jatkuvuudenhallinnan työkalun yleistettävyyden vuoksi. Jo tutkimuksen suunnitteluvaiheessa osattiin odottaa mahdollisia ristiriitaisuuksia haastattelujen ja kyselyn tulosten välillä, sillä tutkimuksen tekijä tunsi toimintaympäristön hyvin. Lopputuloksen yleistettävyyden kannalta ei siis olisi ollut mielekästä toteuttaa tutkimusta keskittyen ainoastaan yhteen tutkimusmenetelmään.

1.7 Toimeksiantajan esittely

Toimeksiantaja eli Yksityisen turva-alan pooli kuuluu verkostomaisesti toimivaan Huoltovarmuuskeskuksen (HVK) koordinoimaan Huoltovarmuusorganisaatioon (HVO). Huoltovarmuusorganisaation keskeisenä tehtävä on varmistaa Suomen huoltovarmuuden kannalta tärkeimpien organisaatioiden sekä koko yhteiskunnan toimintaedellytykset poikkeusoloissa. (Huoltovarmuuskeskus s.a.a.) Huoltovarmuusorganisaation poolit eli työryhmät vastaavat operatiivisesta varautumisesta toimiala- ja toimipaikkakohtaisesti. Poolit muun muassa seuraavat kriittisten toimialojen toimintaedellytyksiä, valmistelevat ja suunnittelevat poikkeusoloihin liittyviä toimenpiteitä sekä tukevat organisaatioita varautumiseen liittyen. (Huoltovarmuuskeskus s.a.b.) Yksityisen turva-alan poolin rooli Huoltovarmuusorganisaatiossa on toimialakohtaisen tilannekuvan tuottamisen lisäksi kriittisten siviilikohteiden suojaamisen varmistaminen. Poolin toiminnassa ovat mukana turvallisuusalan palveluita käyttävät organisaatiot sekä alan palveluita tarjoavat yritykset. (Huoltovarmuuskeskus s.a.c.)

1.8 Aiemmat tutkimukset aihepiiriin liittyen

Resilienssiä ja kriittisen infrastruktuurin sekä rakennusten digitalisoitumista on tutkittu jonkin verran. Painotus digitaaliseen resilienssiin ja jatkuvuudenhallintaan on jäänyt kuitenkin vähemmälle. Lecomte (2019, 128) on kuvannut älykkäiden rakennusten käsitteitä erityisesti liikekiinteistöjen näkökulmasta ja laatinut mittarointimallin älykkäiden rakennusten hintaindeksin kehittämistä varten. Lecomten tutkimus korostaa erityisesti teknologian hallitsevaa roolia omaisuudenhallinnassa ja sen ominaisuuksien määrittelyssä digitaalisella aikakaudella. Park ym. (2018, 10) taas arvioi IoT:n merkitystä älykaupunkikehityksessä ja korostaa tutkimus- ja kehitystoimintaa tukevien demoratkaisujen sekä IT:n kanssa tehtävän yhteistyön tärkeyttä. Starr ym. (2021, 164–165) kuvaa teollisuus 4.0:n (industry 4.0) soveltamismahdollisuuksia kaupallisiin kiinteistöihin liittyen. Tutkimuksen lopputuloksena nähdään kaupallisten kiinteistöjen digitalisoitumista tukeva Real Estate 4.0 -viitekehys. Starr ym. (2021, 164–165) painottaa tuloksissa uudelleenkouluttautumisen tärkeyttä sekä uusien teknologioiden ja ketterien toimintamallien hyötyjä kiinteistöalalla. Tätä edeltävä Woodheadin ym. (2018, 44–45) tutkimus kuvaa yleisesti teollisuus 4.0:n

vaikutuksia rakennusalaan korostaen digitalisaation myötä alkavaa luovan tuhon aikakautta, johon jokaisen alalla työskentelevän on syytä varautua. Moghaddam & Deshmukh (2019, 40) tutkivat kyberfyysisen tuotantojärjestelmien resilienssiä hajautetuissa ympäristöissä ja Nan & Sansavini (2017, 35) taas esittävät kriittisen infrastruktuurin toimintakyvyn arviointia varten mallinnukseen ja kvantifiointiin perustuvan resilienssin huomioon ottavan menetelmän. Sathursan ym. (2022, 1) vertailee omassa tutkimuksessaan eri viitekehyksiä ottaen huomioon resilienssin keskeisenä piirteenä arvioitaessa kriittisen infrastruktuurin toimintakykyä. Khatibi ym. (2022, 1556) taas arvioi tutkimuksessaan rakennuksen järjestelmäympäristön kestävyyttä ja resilienssiä peilaten tuloksia älykaupunkikehitykseen. Ryhmä esittelee tutkimuksen pohjalta laaditun viitekehyksen kaupungin älykkyyden sekä resilienssin arvioimista varten (Khatibi ym. 2022, 1556). Näistä tämän tutkimuksen teemoja käsittelevistä tutkimuksista erityisesti Khatibin ym. tutkimus kokoaa samoja teemoja, joskin kaupunkien tasolla. Tässä tutkimuksessa valittiin teoreettisen viitekehyksen keskeisimmiksi teorioiksi Kosmowskin ym. (2022, 12) OT-ympäristön jatkuvuudenhallinnan ja resilienssin yhdistävä viitekehys sekä Björckin ym. (2015, 314) digitaalista resilienssiä kuvaava malli. Kuten Khatibi ym. toteaa, tätä aihealuetta on tutkittu toistaiseksi hyvin vähän (Khatibi ym. 2022, 1556).

2 TEOREETTINEN VIITEKEHYS

Liiketoiminnan resilienssi voidaan määritellä lyhyesti häiriöistä selviytymisen kyvykkyytenä (Williams & You 2022, 10). Kuitenkaan palautuminen vakaaseen tilaan häiriön jälkeen ei välttämättä tarkoita sitä, että palattaisiin mahdollista disruptiota edeltävään tilaan (Williams & You 2022, 5). Tämä luku käsittelee tutkimuksen teoreettista viitekehystä resilienssin ja jatkuvuudenhallinnan kautta. On huomattava, että systeemiajattelun mukaisesti useiden muutosten yhteisvaikutus ja näistä palautuminen voi lopulta olla jotakin muuta kuin alkuperäinen konfiguraatio (Koffka 1935, 21). Tällä voi olla merkittävä vaikutus liiketoiminnan kyvykkyyteen jatkaa uudessa tilanteessa, mikäli toiminnan resilienssiä ei ole kehitetty riittävälle tasolle.

2.1 OT

OT (englanniksi operational technology) viittaa IT:tä vastaavaan teolliseen ympäristöön, jossa kokonaisuuteen sisältyy myös fyysiset laitteet ja niiden ohjaus. Tekninen OT-ympäristö kattaa teollisten toimintojen hallintaan, ohjaukseen ja monitorointiin liittyvän teknologian, järjestelmät sekä protokollat. (Akailvi ym. 2022, 1, 3; Stouffer 2022, 3.) OT:ta ovat myös muun muassa sähköverkon, kaasu-, vesi- ja jätevesijärjestelmien sekä ydinvoimaloiden ohjausjärjestelmät sekä näiden häiriötilanteiden ja turvallisuuden hallintajärjestelmät (Arora ym. 2022, 111; Stouffer 2022, 4). OT-ympäristö on ollut aiemmin tavallisesti suljettu eikä yhteyksiä muihin sisäisiin tai ulkoisiin verkkoihin ole ollut (Israel National Cyber Directorate 2020 / 2022, 9). OT kattaa siis fyysisen maailman kanssa yhteydessä olevat järjestelmät, niiden anturit ja erilaiset ohjauselementit, joilla voi olla tarvittaessa yhteys muihin verkkoihin (Adams ym. 2022, 4) ja jotka voivat olla kriittisen infrastruktuurin toiminnan kannalta välttämättömiä (Adams ym. 2022, 4; Stouffer ym. 2022, 4). OT-järjestelmillä seurataan ja valvotaan ympäristön tilaa ja olosuhteita, mutta myös ohjataan tähän liittyviä laitteita ja prosesseja halutun tilanteen saavuttamiseksi. Teollisuuden ohjausjärjestelmien lisäksi OT-järjestelmiä ovat muun muassa rakennusautomaatiojärjestelmät, kuljetusjärjestelmät, fyysiset kulunvalvontajärjestelmät ja muut fyysiseen ympäristöön liittyvät valvonta- ja mittausjärjestelmät. (Stouffer ym. 2022, 4–5.) Eri tutkimuksissa viitataan OT-ympäristöön myös muun muassa lyhenteillä CPS, ICS, E/E/PEC sekä SCADA (esimerkiksi Kosmowski ym. 2022, 5, 19).

OT-järjestelmäympäristö on IT-verkkojen tavoin altis kyberhyökkäyksille, josta syystä on tärkeää käsitellä IT-ympäristön lisäksi myös OT-ympäristöä ulkoisille uhille alttiina kokonaisuutena (Sarkar ym. 2022). Jotta kyberturvallisuutta voidaan luotettavasti hallita, on OT-verkoista ja niiden välisistä riippuvuuksista oltava käytettävissä kattavat tiedot (Rothrock 2022, 2).

2.2 Jatkuvuudenhallinta

ISO 22301 -standardi käsittelee jatkuvuudenhallintaa liiketoiminnan jatkuvuuden näkökulmasta (ISO 2019, 5). Standardi kuvaa liiketoiminnan jatkuvuutta kykynä jatkaa häiriön jälkeen tuotteiden ja palvelujen toimittamista toiminnan kannalta hyväksyttävän aikavälin puitteissa ennalta määritellyllä kapasiteetilla.

Jatkuvuussuunnitelma taas tarkoittaa standardin mukaan dokumentoitua organisaatiota ohjaavaa tietoa, jolla ohjataan organisaation jatkuvuudenhallintaa. (ISO 2019, 9.) Valtioneuvosto toteaa (2022, 40, 58) jatkuvuudenhallinnan olevan organisaatioiden omaehtoista varautumista kriiseihin sekä häiriötilanteisiin.

Jatkuvuudenhallinta on keskeinen osa organisaation riskienhallintaa. Sillä varaudutaan erityisesti sellaisiin häiriötilanteisiin, jotka voivat aiheuttaa merkittävää haittaa organisaation kyvylle tuottaa sen ydinpalveluita. (Drewitt 2013, 11; Hopkin 2012, 188; Kosmowski ym. 2022, 9.) Nämä palvelut ja toiminnot turvataan ennalta määriteltyjen toimintamallien mukaisesti koskien normaalioloja, häiriötilanteita sekä poikkeusoloja (Vahti 2016, 18). ISO 22301 -standardi kuvaa jatkuvuudenhallintaa kyvykkyytenä sekä toimintana, joka tunnistaa sekä toteuttaa organisaatiolle välttämättömät liiketoiminnan jatkuvuuden turvaavat käytännöt sekä toimenpiteet, joilla toiminta saadaan palautumaan häiriötilanteesta. Jatkuvuudenhallintaan sisältyvät standardin mukaisesti myös suorituskyvyn sekä toiminnan tehokkuuden ylläpito sekä toiminnan jatkuva kehittäminen perustuen laadullisiin sekä määrällisiin kyvykkyyttä mittaaviin tuloksiin. (ISO 2019, 5.)

Parkin ym. (2018, 356–357) mukaan varautuminen uhkiin riskianalyysin avulla ei sellaisenaan riitä kriittisen infrastruktuurin suojaamiseen. On käsiteltävä erikseen resilienssiä, joka auttaa suojautumaan ennalta arvaamattomilta tapahtumilta ja toipumaan niistä. (Park ym. 2018, 356–357.)

2.3 Digitaalinen resilienssi

Resilienssi on määritelty jo 1900-luvun alussa materiaalifysiikassa kappaleen elastiseksi ominaisuudeksi (Park ym. 2013, 356). 1900-luvun puolivälin jälkeen resilienssiä käsiteltiin jo eri näkökulmista. Oxfordin sanakirja tunnistaa resilienssin vuoden 1963 painoksessa nopeasti alkuperäiseen muotoonsa palaavan venytetyn, puristetun tai murskatun kappaleen ominaisuudeksi tai tilaksi viitaten niin materiaalifysiikkaan kuin myös esimerkiksi ihmiskehoon (Oxford 1963, 837). C. S. Holling (1970) määritteli resilienssin uudelleen seminaariartikkelissaan ekologian kontekstissa biodiversiteetin, elinympäristöjen pirstoutumisen ja ekologisten systeemien näkökulmasta. Hän tunnisti keskeisen

eron näiden teknisten ja ekologisten järjestelmien välillä. Erona hän tunnisti tarkoituksellisuuden, joka syntyy suunnittelun tuloksena tekniikassa, mutta puuttuu täysin luonnollisista ekosysteemeistä. (Park ym. 2013, 356–357.) Termiä resilienssi tulkitaan näin ollen monella eri tavalla eri asiayhteyksissä.

Resilienssi voi olla kyky korjata, korvata tai palauttaa menetetty suoritustaso tai -kyky kokonaan tai osittain onnettomuuden, vaurion tai epävakauttavan häiriön jälkeen (Alberts 2011, 218). Se voi olla myös järjestelmän kyky sopeuttaa toiminnot jatkuvuuden ylläpitämiseksi häiriötilanteessa (Alderson ym. 2015, 562) tai kyky kestää häiriötilanteen vaikutuksia ja toipua häiriöstä ennalleen (infrastruktuurin resilienssi) (Berkeley III & Wallace 2010, 15). Resilienssi voi kuvata järjestelmän kyvykkyyttä varmistaa toiminnan jatkuvuus mukauttamalla toimintaansa häiriötilanteen vallitessa (Alderson ym. 2015, 562–563) eli ylläpitää palvelutaso haitallisista kybertapahtumista huolimatta (Björck ym. 2015, 312). Holling (1996, 33) kuvaa resilienssin kahden eri näkökulman kautta, joista toinen keskittyy toiminnon tehokkuuden säilyttämiseen (tekninen resilienssi) ja toinen toiminnon olemassaolon säilyttämiseen (ekologinen resilienssi). Näistä ekologinen resilienssi tarkoittaa häiriönsietokykyä ennen systeemin ohjauksessa tai rakenteessa tapahtuvaa muutosta. Madnin (2009, 181, 185, 187) mukaan resilienssi voi olla kyky välttää onnettomuuksia ennakoimalla, palautua häiriötilanteista ja kehittyä mukautuen muutokseen. Resilienssi voi olla myös elastisuutta, jonka avulla järjestelmä voi palata alkuperäiseen muotoonsa, asentoonsa tai konfiguraatioon sen jälkeen, kun sitä on taivutettu, puristettu tai venytetty. Toisaalta se voi olla monitahoisen järjestelmän kyky välttää häiriöitä, sopeutua sekä toipua häiriötilanteesta. (Madni 2009, 181, 185, 187). Resilienssi voi olla toisiinsa kytkeytyvien järjestelmien välisten riippuvuussuhteiden kvantifiointia (Nan & Sansavini 2016, 35), kyky sopeutua yllätykseen, muutokseen tai häiriöön ja samalla välttää peruuttamattomat muutokset tai rekursiivisiin prosesseihin liittyvä ominaisuus, jota ei voida päätellä tutkimalla järjestelmän yksittäisiä komponentteja erikseen (Park ym. 2013, 356, 365).

Petrenkon (2019, 7) mukaan kyberresilienssi on toiminto, jonka avulla varmistetaan kyberjärjestelmien kyvykkyys kehittää immuniteetti tuhoavia vaikutuksia aiheuttaville häiriötilanteille. Sanchis ym. (2020, 1) taas kuvaa resilienssin ky-

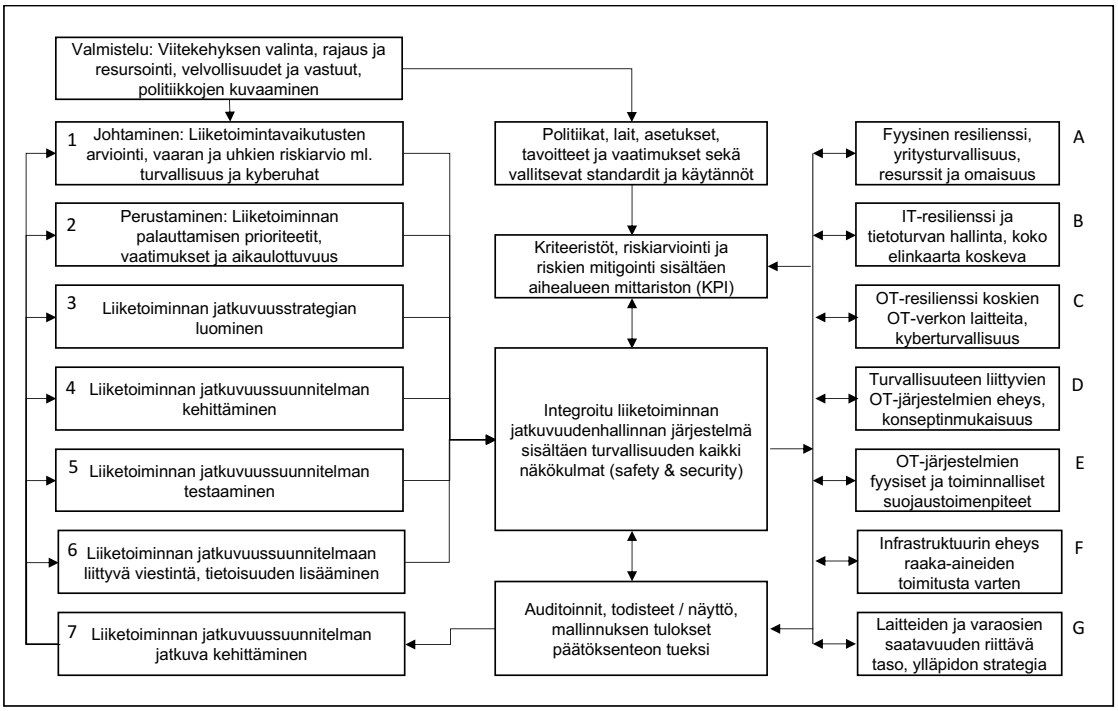
vykkyytenä taata organisaation toiminnan jatkuvuus pitkällä aikavälillä, kyvykkyytenä ennakoida ja varautua häiriöihin tai kykynä palautua häiriötilanteen vaikutuksesta (organisaation resilienssi) (Sanchis ym. 2020, 4, 14). Resilienssi voi myös olla kyky valmistautua ja sopeutua muuttuviin olosuhteisiin mukaan lukien tahalliset hyökkäykset, onnettomuudet sekä luonnonmullistukset sekä toipua nopeasti häiriötilanteesta (The White House 2013). Vugrin ym. (2010, 82) kuvaa resilienssin kyvykkyytenä vaimentaa tehokkaasti systeemin suorituskykyyn kohdistuvan häiriön voimakkuutta ja vähentää häiriön kestoa. Walker ym. (2004, 6) kuvaa resilienssin järjestelmän kykynä mukautua häiriötilanteeseen ja organisoitua uudelleen muutoksen aikana niin, että järjestelmä säilyttää olennaisilta osin samat toiminnot, rakenteen sekä identiteetin. Resilienssi voi kuvata myös sitä, kuinka hyvin systeemi pystyy mukautumaan tilanteeseen ja käsittelemään perusmekanismien ulkopuolelle jääviä häiriöitä ja prosessien variaatioita (Woods 2006, 21).

Resilienssin määritelmä riippuu näkökulmasta sekä kulloinkin asiayhteydessä käsiteltävistä suureista (Sathursan ym. 2022, 2). Koska tutkimus keskittyi teknisen ympäristön resilienssiin sekä jatkuvuudenhallintaan, oli kyse pääasiassa teknisestä ja digitaalisesta resilienssistä eli kyberresilienssistä (Alderson ym. 2015, 562; Björck ym. 2015, 311; Petrenko 2019, 7), mutta myös organisaation kyvykkyydestä sopeutua vallitsevaan tilanteeseen (Sanchis ym. 2020, 1). Björck ym. (2015, 315) toteavatkin verratessaan kyberturvallisuutta ja kyberresilienssiä, että kyberresilienssi on liiketoimintalähtöistä tavoitteenaan saavuttaa liiketoimintatavoitteet kyberhäiriöistä huolimatta toisin kuin teknislähtöinen kyberturvallisuus.

2.4 Kosmowskin viitekehys

Tutkimuksessa hyödynnettiin Kosmowskin ym. (2022, 12) kehittämää viitekehystä, joka yhdistää käsiteltävät teemat eli jatkuvuudenhallinnan OT-ympäristön resilienssin hallintaan (kuva 3). Kosmowski on tutkinut teollista OT-ympäristöä sekä sen riippuvuuksia liiketoiminnan jatkuvuudenhallintaan tuotantoympäristönäkökulmasta. Tutkimuksen mukaan tällaisessa ympäristössä on otettava tarkasti huomioon IT- ja OT-järjestelmien konvergenssi eli näiden kahden kohtaaminen teknisessä ja prosessiympäristössä. (Kosmowski ym. 2022, 4, 6.)

Kosmowskin ym. (2022, 12) kuvaama liiketoiminnan jatkuvuudenhallinnan viitekehys (kuva 3) yhdistää teknisen ympäristön hallinnan liiketoiminnan jatkuvuudenhallintaan. Mallin avulla voi käsitellä havainnollisesti teknisen ympäristön kriittisiä toimintoja ja tunnistaa niistä haavoittuvuuksia, jotka voivat vaikuttaa suoraan esimerkiksi tuotantolaitoksen toimintaan.



Kuva 3. Kosmowskin ym. (2022, 12) viitekehys, joka kuvaa yhteydet teknisen ympäristön jatkuvuudenhallinnan ja resilienssinhallinnan sekä liiketoiminnan jatkuvuudenhallinnan prosessien välillä (suomennettu alkuperäisestä)

Tässä tutkimuksessa peilattiin saatuja tuloksia tähän todellisessa ympäristössä testattuun Kosmowskin ym. (2022, 12) viitekehykseen (kuva 3). Viitekehystä, kirjallisuutta sekä muuta tutkimustietoa sovellettiin rakennuksen OT-ympäristöön ja näitä hyödynnettiin myös jatkuvuudenhallinnan työkalun kehittämisen tukena.

3 TUTKIMUKSEN TOTEUTUS

Tämä suomalaisten huoltovarmuuskriittisten toimijoiden keskeisimpien rakennusten OT-järjestelmäympäristön hallintaan keskittynyt tapaustutkimus toteutettiin monimenetelmällisesti soveltaen sekä laadullista että määrällistä tutkimusotetta. Useita eri organisaatioita koskevassa tutkimuksessa otettiin huomi-

oon Puusan & Juutin (2020, 88) mallin mukaisesti mahdollisimman kokonaisvaltaisesti sellaiset seikat, jotka liittyivät tutkittavaan ilmiöön. Sovellettu tutkimusote auttoi ymmärtämään kokonaisuutta ilmiön omassa toimintaympäristössä.

Määrällisenä aineistonkeruumenetelmänä käytettiin organisaatioiden jatkuvuudenhallinnan tilaa sekä vastaajien näkemyksiä kartoittavaa kyselytutkimusta. Kyselyn tarkoituksena oli vahvistaa laadullisen osuuden tulokset sekä tutkimuksen ja toteutetun toimintaympäristön kehittämistä tukevan työkalun tarpeellisuus yleisellä tasolla. Laadullinen tutkimusosuus taas painotti samalla Puusan & Juutin (2020, 74) näkemyksen mukaisesti haastateltavien henkilökohtaista kokemusta tilanteesta.

Tutkimusotteeksi valittiin monimenetelmällisyys, sillä se antoi edellä mainittujen hyötyjen lisäksi mahdollisuuden vaihtaa tarvittaessa tapaustutkimuksen näkökulmaa ja keskittyä siten kokonaisuuden kannalta olennaisiin asioihin, kuten Puusa & Juuti (2020, 73) toteavat. Tämä koettiin tärkeäksi ja tutkimukseen joustoa tuovaksi erityisesti työkalun kehittämisen osalta. Työkalun kehittämisen kannalta oli myös tärkeää voida yleistää tuloksia riittävästi, johon Puusan & Juutin (2020, 91) tulkinnan mukaan mahdollisuuden antoi määrällinen tiedonkeruumenetelmä laadullisen tutkimusotteen tukena.

3.1 Tutkimukseen tarvittava aineisto

Tavoiteltujen lopputulosten saavuttamiseksi tarvittiin tietoa OT-järjestelmäympäristöön liittyvän jatkuvuudenhallinnan tilasta ja ympäristöön liittyvistä toimintatavoista. Näillä tiedoilla voitiin todentaa jatkuvuudenhallinnan kehittämisen tarpeellisuus sekä erityiset painopisteet. Tätä varten varmistettiin mahdollisimman laajan ja samalla relevantin kohdejoukon saavuttaminen Huoltovarmuusorganisaation kautta. Tutkimukseen sitoutettiin myös Kiinteistönomistajat ja rakennuttajat Rakli ry:n Uudistuminen ja digitalisaatio -teemaverkosto, jonka avulla haettiin huoltovarmuuskriittisten toimijoiden ulkopuolelta referenssitietoa mahdollisesti erilaisen näkökulman tunnistamiseksi. Tuloksia ei kuitenkaan hyödynnetty vastaajamäärän jäätyä varsin vähäiseksi.

Määrällinen tutkimus tuotti sekä tutkimustietoa kehitettävästä ilmiöstä että kehittämistietoa jatkuvuudenhallinnan työkalun sekä koko toimialan kehittämisen tueksi. Vastaajat olivat pääasiassa Suomen huoltovarmuuden kannalta keskeisiä toimijoita ja otosjoukko suuruusluokaltaan satoja organisaatioita. Tutkimuksessa kerättiin tietoa jatkuvuudenhallintaprosessiin liittyvistä toimintatavoista, hyvistä ja huonoista kokemuksista, haasteista sekä parhaaksi todetuista käytännöistä. Vastaajat olivat kiinteistöjen omistajia ja käyttäjiä riittäväksi koetulla Huoltovarmuuskeskuksen toimialaluokitukset kattavalla otoksella, jotta voitiin yleistää tiedot jatkuvuudenhallinnan työkalun kehitystä varten.

3.2 Menetelmät

Tässä kartoittavassa monimenetelmäisessä tutkimuksessa käytetyt eri menetelmät mittasivat samoja asioita eri näkökulmista. Hirsjärven & Hurmeen (2022, 31) mukaan tällöin puhutaan varmentavasta käytöstä monimenetelmäisessä tutkimuksessa. Hirsjärvi & Hurme (2022, 31) linjaavat myös, että mikäli kvalitatiivisesta ja kvantitatiivisesta osiosta saadut tulokset eriävät toisistaan, on tähän reagoitava senhetkisiin tietoihin nojaten ja on syytä jatkaa tutkimusta aiheeseen liittyen. Tähän tilanteeseen päädyttiin osittain tässä tutkimuksessa. Hurmerinta & Nummela (2020, 299) toteavat, että monimenetelmäisyyteen voi tutkimusfilosofisesta näkökulmasta suhtautua monin eri tavoin. Tässä tutkimuksessa sallittiin vuoropuhelu kahden rinnakkain toteutetun eri tutkimusmenetelmän välillä. Näin pragmaattiset oletukset osoittivat ennemminkin suuntaviivoja kuin ohjasivat tutkimusta.

Tarve eri menetelmien yhdistämiseen nousi kontekstista sekä tutkimusongelmasta. Kummallakin tutkimusosalla oli itsenäinen rooli, mutta yhdistettynä tutkimuselementit vastasivat tutkimuskysymykseen kokonaisuudessaan Hurmerinnan & Nummelan (2020, 299) mukaisesti. Tämä loi tutkimukselle syvyyttä sitoen laadullisen tutkimuksen tulokset tarpeeseen kehittää OT-ympäristön jatkuvuudenhallinnan malleja ja menetelmiä.

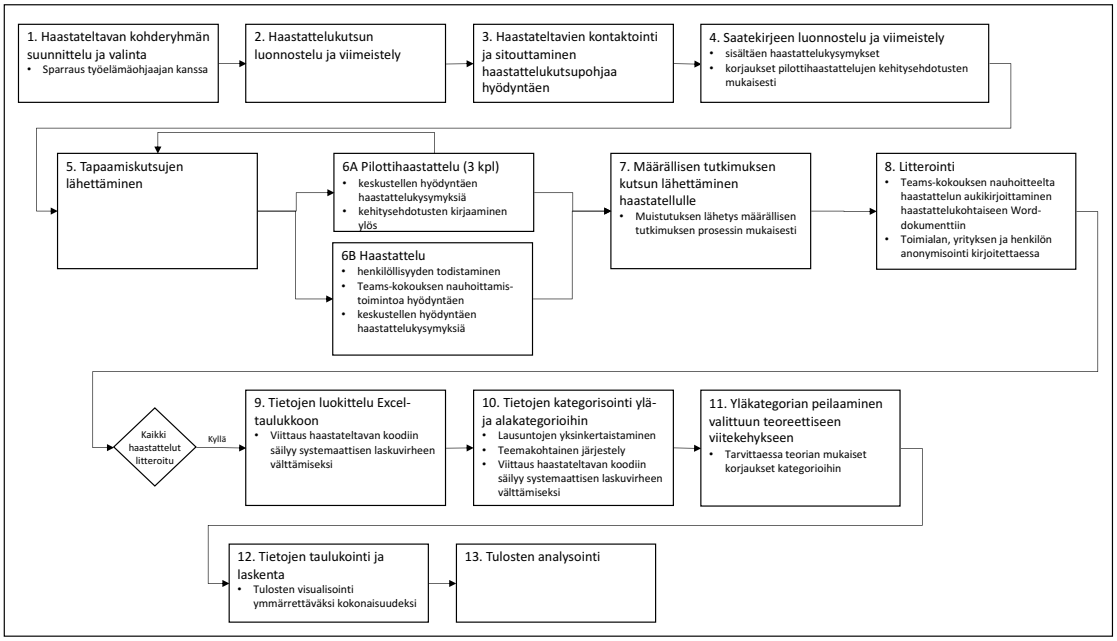
3.3 Puolistrukturoitu teemahaastattelu laadullisena tutkimusmenetelmänä

Laadullisen osuuden menetelmänä käytettiin puolistrukturoitua teemahaastattelua. Menetelmä soveltuu Hirsjärven & Hurmeen (2022, 47–48) mukaan hyvin tilanteeseen, jossa haastateltavilla henkilöillä voi olettaa olevan valmiiksi kokemusta haastatteluissa käsiteltävistä tilanteista ja tutkijalla toisaalta on jo alustavaa tietoa kokonaisuudesta, ilmiöistä ja tapahtumista käsiteltävään teemaan liittyen. Teemahaastattelu antoi myös Kallisen ym. (2022, 45) mukaan mahdollisuuden joustavuuteen läpikäytävien asioiden ja riippuvuuksien suhteen, jolloin suunnittelussa huomiotta jääneiden asioiden annettiin myös nousta esille haastatteluissa.

Haastatteluun päädyttiin tutkimusmenetelmänä myös sen vuoksi, että haastattelutilanteessa pystyttiin muodostamaan henkilökohtainen keskusteluyhteys haastateltavan kanssa ja tarkentamaan teemaa haastattelukohtaisesti riittävälle tasolle, jotta haastateltavalla oli mahdollisimman hyvät mahdollisuudet vastata omasta näkökulmastaan kysymyksiin. Haastatteluja varten laadittiin saateviestiin (liite 1) liitetty haastattelurunko (liite 3), joka käytiin läpi tilanteeseen soveltuvassa järjestyksessä kunkin haastateltavan kanssa, ja jonka kysymyksiin kukin haastateltava vastasi oman subjektiivisen näkemyksensä mukaisesti. Haastatteluja olisi ollut mahdollista järjestää myös ryhmä- tai parihaastatteluina Kallisen ym. (2022, 53) mukaisesti. Jokaista haastateltiin kuitenkin yksitellen yhtä parihaastattelua lukuun ottamatta, jotta kukin haastateltava sai mahdollisimman hyvin oman äänensä kuuluviin. Haastattelut toteutettiin maalis-huhtikuussa 2023.

Aineiston keräämisen vaiheet toteutettiin kuvan 4 mukaisesti. Ensimmäiset kolme haastattelua toteutettiin pilottihaastatteluina, joista saadun palautteen pohjalta tehtiin muutoksia sekä haastattelun kysymysrunkoon, haastattelutilanteen toimintatapoihin, että saatekirjeeseen. Haastatellut henkilöt osallistuivat myös kyselytutkimukseen (kuvan 4 kohta 7). Haastattelun kysymysrunko (liite 3) toimi erinomaisena keskustelurunkona. Yksi henkilö kieltäytyi vastaamasta yhteen kysymykseen.

Haastattelut pidettiin yhtä lukuun ottamatta Microsoft Teams -sovelluksen välityksellä. Yksi haastattelu pidettiin haastateltavan työpaikan neuvottelutilassa keskustellen ja yksi haastatteluista toteutettiin parihaastatteluna haastateltavien pyynnöstä. Jokainen haastattelu tallennettiin Microsoft Teams -sovelluksella. Haastattelut tallentuivat oppilaitoksen Microsoft 365 -ympäristöön. Jokainen haastattelu anonymisoitiin litterointivaiheessa kohderyhmän mahdollisen tunnistettavuuden vuoksi. Anonymisointi toteutettiin nimeämällä haastattelujen litteroinnista syntyneet dokumentit koodilla, jota ei linkitetty haastateltuihin henkilöihin. Toimialaan sekä organisaatioon, kilpailijoihin ja yhteistyökumppaneihin liittyvät viittaukset anonymisoitiin yleistämällä sanamuotoja.



Kuva 4. Empiirisen aineiston keräämisen prosessi

Tietojen kategorisointi ja analysointi

Tutkimuksessa käytettiin laadullisen analyysin menetelmänä abduktiivista sisällönanalyysiä, jossa asiasisältö toimi analyysiyksikkönä Puusan (2020, 147–148) mallin mukaisesti. Kerättyä aineistoa peilattiin valmiisiin teorioihin ja malleihin. Analyysin vaiheet olivat niin ikään Puusan (2020, 147–148) mallin mukaisesti luokittelu ja kategorisointi, joilla tunnistettiin teemoja, toistuvuuksia sekä samankaltaisuuksia. Saatuja tietoja peilattiin tutkimushypoteesiin sekä tutkimusongelmaan, jotta varmistettiin tulosten olennaisuus asiayhteydessä.

Litterointivaiheen valmistumisen jälkeen tiedot luokiteltiin ensin Microsoft Word -dokumentissa teemoiksi värikoodein, jotka siirrettiin seuraavaksi Microsoft Excel -dokumenttiin teemakohtaisiksi listoiksi. Tämän jälkeen hyödynnettiin Puusan (2020, 147) tulkintaa tietojen kategorisoinnista yksinkertaistamalla samaa asiaa tarkoittavat kommentit joukoiksi samankaltaisia ilmaisuja jatkokäsittelyn sujuvoittamiseksi. Näin muodostuivat tutkimusaineiston alakategoriat. Seuraava kategoriataso luotiin ryhmittelemällä alakategoriat saman aiheisiksi ryhmiksi ja nimeämällä ne kuvailevalla termillä. Nämä yhdistettiin vielä Puusan (2020, 148) ehdotuksen mukaisesti tutkimuksen kannalta mielekkäiksi seuraavan tason kategorioiksi. Samaa Puusan (2020, 150) ohjeistusta soveltaen yhdistettiin kategoriat lopulta kaikki kategoriat kattavaksi yläkategoriaksi, jota käsiteltiin jatkuvuudenhallinnan alaisena teemana. Haastatellun henkilön koodia kuljetettiin kommenttien mukana, jotta systemaattiselta määrälliseltä tulkintavirheeltä vältyttäisiin haastateltujen toistettua samoja asioita useaan kertaan.

Kategorisointivaiheen jälkeen teoreettisen viitekehyksen kannalta relevantteja ylätason kategorioita peilattiin valitun viitekehyksen asiasanoihin, jotta varmistettiin oikeiden tietojen kerääminen käytettyyn viitekehykseen nähden ja toisaalta tietojen vertailtavuus määrällisen sekä laadullisen tutkimuksen tulosten osalta. Tiedot taulukoitiin kuvan 5 mukaisesti yhteen lasketuiksi kokonaisuuksiksi, jotta saatiin näkyvyys väitteiden sekä teemojen esiintyvyystiheyteen. Tulokset kvantifioitiin niiden tietojen osalta, jotka olivat kvantifioitavissa. Tietoja verrattiin suoraan kyselytutkimuksen tuloksiin. Näin varmistettiin Puusan (2020, 148) tulkintaohjeen mukaisesti tiedon havainnollisuus yhteenvetoa varten.

Haastateltavan kommentti	Haasteen teema	Esiintymismäärä	Sitaatti
Dokumentaatio säilytetään toisinaan missä sattuu.	Dokumentaatio	8	Dokumentaatio tehdään, jos muistetaan
Dokumentaatio tehdään, jos muistetaan.	Johtaminen	34	IT:n ja OT:n välillä on kuilu eivätkä näiden prosessit kohtaa.
OT-arkkitehtuuria ei kuvata.	Hankinta	34	Ostaja ei aina välttämättä tiedä, onko ostanut rautaa vai palvelua.
OT-järjestelmien dokumentaatio ei ole riittävällä tasolla.	Jatkuvuudenhallinta	34	Tämä on keskeinen asia ja kiinnostavaksi sen tekee se, että siitä on keskitetysti hankala päättää.
OT-järjestelmien dokumentaatio ei ole riittävällä tasolla.	Kyberturvallisuus ja tietoturvapolitiikka	37	Tietoturva otetaan hankinnassa huomioon kysymällä "onhan tietoturva otettu huomioon?", joka osoittaa ymmärryksen tason hankintavaiheessa.
Rajapintadokumentaatio on harmaalla alueella			
Rakennuksen käytön aikana palveluntoimittajien vastuuhenkilöt vaihtuvat, mutta dokumentaation jakamiselle ei ole toimivia käytäntöjä.			
Vaikka automaatiotoimittaja tietää, mitä on toimittanut kohteeseen, kokonaisuuteen liitetään erilaisia sensoreita ja lisäpalveluita tuottavia IoT-laitteita. Tästä johtuen verkkotopologiakuvaus ei pysy ajan tasalla kenelläkään.			

Kuva 5. Ote tutkimusaineistosta (n = 13). Koska samat aiheet toistuivat saman haastattelun aikana useaan kertaan, voi aiheen esiintymismäärä olla suurempi kuin haastateltavien lukumäärä.

Koska aihealue oli tutkijalle tuttu entuudestaan, suhtauduttiin aiheen objektiiviseen käsittelyyn erityisellä huolellisuudella. Tämä lähtötilanne otettiin huomioon niin haastatteluissa kuin aineiston käsittelyssä pyrkien välttämään mahdollisia kognitiivisia vinoumia. Kuten Puusa & Juuti (2020, 139) kirjassaan toteavat, helpottivat lähtötiedot tietojen tulkitsemista eri näkökulmista ja myös tuloksena saadun ilmiön kuvailemista. Kerättyyn tietoon suhtauduttiin Puusan (2020, 141–142, 147) kirjoitusta mukaillen avoimen kiinnostuneesti antaen samalla mahdollisuus sellaisten seikkojen ilmenemisille, joita ei välttämättä olisi osattu ottaa tutkimusasettelussa huomioon.

Haastattelussa korostui haastateltavien omat näkemykset tilanteista, jolloin erityisesti tutkittavien henkilöiden ääni kuuluu voimakkaana tuloksissa tutkijan oman näkökulman sijasta kuten Hirsjärvi & Hurme (2022, 48) sekä Kallinen ym. (2022, 38) toteavat. Haastattelun tilanne- ja kontekstisidonnainen luonne sekä mahdollinen yhteisön paine oli kuitenkin otettava Kallisen ym. (2022, 43) mukaan huomioon sekä haastattelutilanteessa että tuloksia analysoitaessa.

3.4 Määrällinen tiedonkeruu

Tilastollinen kokonaisuus toteutettiin Ketokiven (2015, 7) esityksen mukaisesti pitäen näkökulma loogisena tutkimuksen etenemisen ja tilastollisen selittämisen kontekstissa. Tarkoituksena oli luoda Ketokiven (2015, 7) linjan mukai-

sesti laadullisen tutkimuksen osuuden kanssa yhdessä ristiriidaton kokonaisuus tutkimuskysymyksen, käytettävissä olevan tutkimustiedon, kerätyn aineiston sekä tutkimuksen vaiheiden kautta. Kyselyn tuloksella pyrittiin siis vahvistamaan hypoteesin mukaan tämän tutkimuksen tavoitteen toteutumisen tarve sekä tarkentamaan jatkuvuudenhallinnan työkalun toteutukseen liittyviä teemoja. Määrällinen tutkimus oli Hirsjärven & Hurmeen (2022, 31) mukaisesti kuitenkin tutkimuksessa sivuosassa ja ennemmin tutkimusta innoittavana sekä myös näkökulmaa syventävänä elementtinä.

Tutkimuksen tavoitteena oli toteuttaa alun perin kokonaistutkimus, mutta koska tutkimuksessa ei ollut mahdollista varmistaa koko perusjoukon saavutettavuutta, toteutettiin tutkimus otantatutkimuksena. Toteutettu kartoittava otantatutkimus mittasi Hirsjärven & Hurmeen (2022, 25) mukaisen tutkittavan teeman eli rakennuksen järjestelmäympäristön jatkuvuudenhallinnan kattavuutta sekä organisoitumistapaa aihealueeseen liittyen perusjoukosta valikoidussa otoksessa. Tiedonkeruumenetelmänä käytettiin survey-tutkimusta.

Tutkimuksen kohdeperusjoukkona käsiteltiin Huoltovarmuusorganisaation verkostoa ja kehikkoperusjoukoksi rajautuivat ne Huoltovarmuusorganisaation toimialojen poolit, joille kysely ositetun otannan pohjalta lähetettiin. Referenssijoukkona oli tarkoitus käsitellä Kiinteistönomistajat ja rakennuttajat Rakli ry:n Uudistuminen ja digitalisaatio -teemaverkostoa, mutta koska vastauksia saatiin hyvin vähän (13 kpl), jätettiin ne pääosin käsittelemättä. Jatkuvuudenhallinnan työkalun toteutustapaan sekä koulutustapaan liittyviä tuloksia (kohta 5) hyödynnettiin kuitenkin työkalun toteutukseen liittyen.

Määrällisessä tutkimuksessa tutkimusyksikkönä käsiteltiin yrityksiä, joiden edustajien näkökulmia liittyen rakennusten OT-järjestelmäympäristön jatkuvuudenhallintaan ja digitaaliseen resilienssiin kartoitettiin kyselyn avulla (liite 4). Kohderyhmän osalta pyrittiin saavuttamaan mahdollisimman suuri ja edustava otos perusjoukosta tutkittavan ilmiön kuvaamista varten. Tämä tavoite ei kuitenkaan toteutunut täysin, sillä alkuperäisestä tavoitteesta poiketen kaikki Huoltovarmuusorganisaation poolit eivät osallistuneet lopulta tutkimukseen eli tavoiteltua tasaista peittoa ei saavutettu. Kuitenkin monen haastatellun osallistuttua myös kyselytutkimukseen pystyttiin kattamaan osa puuttuneiden toimialojen vastauksista. Yksi Huoltovarmuuskeskuksen määrittämä toimiala

(Huoltovarmuuskeskus s.a.d), terveydenhuolto, jäi täysin tutkimuksen ulkopuolelle.

Tutkimus toteutettiin hyödyntämällä oppilaitoksen lisenssillä Webropol-kyselyjärjestelmää. Tutkimuslomakkeen sisältö on kuvattu liitteessä 4 ja saatekirje liitteessä 2. Jotta kyselyyn oli mahdollista vastata, oli hyväksyttävä tietosuojailmoitus (liite 5). Vastaajista kolme ei hyväksynyt tietosuojaselostetta. Näitä ei laskettu vastaajajoukkoon mukaan.

Kysely sisälsi viiden vastausvaihtoehdon strukturoituja kysymyksiä, kuvapohjaisia monivalintakysymyksiä sekä avoimia kysymyksiä. Taustatietoja kartoittavat kysymykset selvittivät täsmällisiä tosiasioita. Kontekstuaalisten kysymysten ja ilmiöosan avulla kartoitettiin arvionvaraisia tosiasioita sekä mielipiteitä. Kyselyn esitestaus toteutettiin neljän henkilön toimesta ja kyselyä muokattiin palautteiden perusteella.

Otannan vaiheistus toteutettiin Heikkilän (2014, 33) kuvaamien vaiheiden mukaisesti. Alussa määriteltiin perusjoukko sekä sitä kuvaava rekisteri. Otosyksikkö määriteltiin yritykseksi ja tavoitteena oli saada käyttöön koko perusjoukon rekisteri. Koska rekisterin tietoja ei voitu jakaa tutkimuksen käyttöön, sovittiin viestintä tehtäväksi yhteyshenkilön kautta. Rekisteri koostui useista osista, joista kullakin oli oma vastuuhenkilö. Otoksen koko oli linjassa Heikkilän (2014, 43) otoskokotavoitteiden kanssa. Otosjoukko oli suuruusluokaltaan noin 500 vastaajaa, jotka voivat edustaa samoja tai eri yrityksiä tai muita organisaatioita. Tutkimuksessa vertailtujen ryhmien koot olivat suuruusluokaltaan 50–70 vastaajaa.

Tutkimuksessa tavoiteltiin suuruusluokaltaan 30–50 vastaajan otosta, mutta saavutettiin yhteensä 64 vastaajan otos. Tämä ei sisällä Raklin 13 vastaajan otosta, jonka tuottamat vastaukset jätettiin pääosin tutkimuksen ulkopuolelle. Poolitoiminnan otos sisälsi myös laadullisessa tutkimuksessa haastateltuja henkilöitä, koska he edustivat poolitoiminnassa mukana olevia organisaatioita. Riittävän korkeaan otokseen päästiin muistuttamalla tutkimusaikana kohderyhmää kahdesti vastaamisen tärkeydestä.

Kyselytutkimuksen avulla selvitettiin seuraavia parametreja, joiden riippuvuuksia tutkimuksen ulottuvuuksiin nähden on kuvattu kuvassa 6 esitetyn mittausmallin avulla: taustatiedot (toimiala ja liikevaihto vastaajien luokittelua varten), kontekstuaaliset kysymykset (järjestelmäympäristöön liittyvät vastuut, järjestelmäympäristöön liittyvät prioriteetit, järjestelmäympäristön jatkuvuudenhallinnan toimintatavat) sekä ilmiöosa (järjestelmäympäristön resilienssin nykytila, jatkuvuudenhallinnan työkalun dokumentointitapa, osaamisen kehittämisen tavat, näkemys jatkuvuudenhallinnan maturiteettitasosta, mukaillen Huoltovarmuuskeskuksen aiempaa ISO 22301 jatkuvuudenhallintastandardiin perustuvan kyselyn otsikointia sekä kohdatut haasteet ja mahdollisuudet). Mittausmallin avulla varmistettiin, että kyselyn kysymykset mittaavat oikeita asioita toteutetun tutkimuksen kannalta riittävän monesta näkökulmasta.

Primaari tutkimusaineisto käsiteltiin ja analysoitiin Webropol-järjestelmän työkalujen avulla. Aineisto käsiteltiin tulosten esittämistä varten helppolukuiseen muotoon ja taulukoitiin MS Excelillä raportointia varten. Taustakysymysten esitystavaksi valittiin tulosten esitystä ja nopeaa käsittelyä varten suuruusjärjestyksessä suuremmasta pienempään järjestetty palkki pois lukien organisaation liikevaihtoa koskeva kysymys, joka esitettiin liikevaihdon mukaan järjestyksessä pienemmästä suurempaan. Palkkeihin jätettiin näkyville sekä vastausten lukumäärä että prosenttiosuus. Matriisikysymysten esitystavaksi valittiin pinottu palkki, jossa akseli osoittaa suhteellisen osuuden prosentteina ja palkki vastausten lukumäärän sekä prosenttiosuuden. Jokaiseen kysymykseen sekä matriisikysymysten vastausvaihtoehtoihin nostettiin kaikkien vastaajien lukumäärä sekä vastausten keskiarvo näkyville. Vertailutoiminnallisuutta testattiin rakennuksen omistajilla verrattuna kaikkiin vastaajiin. Tällä pyrittiin osoittamaan ero rakennukseen investoineen tahon sekä rakennukseen liittyviä palveluita tarjoavien tahojen välillä. Tilastollisesti merkitsevää eroa ei tunnistettu, joskin selkeitä painotuksia oli havaittavissa eri vastaajajoukkojen kesken. Vertailu rajattiin kuitenkin tutkimuksen ulkopuolelle.

Matriisikysymysten vastausvaihtoehtojen pitkät vaihtoehtoa avanneet selitteet poistettiin. Kysymyksen ”Arvioi yrityksenne / organisaationne käytössä olevien rakennusten toimintaa ohjaavien järjestelmien kriittisyyttä” viimeinen virheellisesti hissien ja liukutasojen ohjausjärjestelmiin viittaava vastausvaihtoehto poistettiin. Oikea vastausvaihtoehto olisi ollut ”Toiminnanohjausjärjestelmät”,

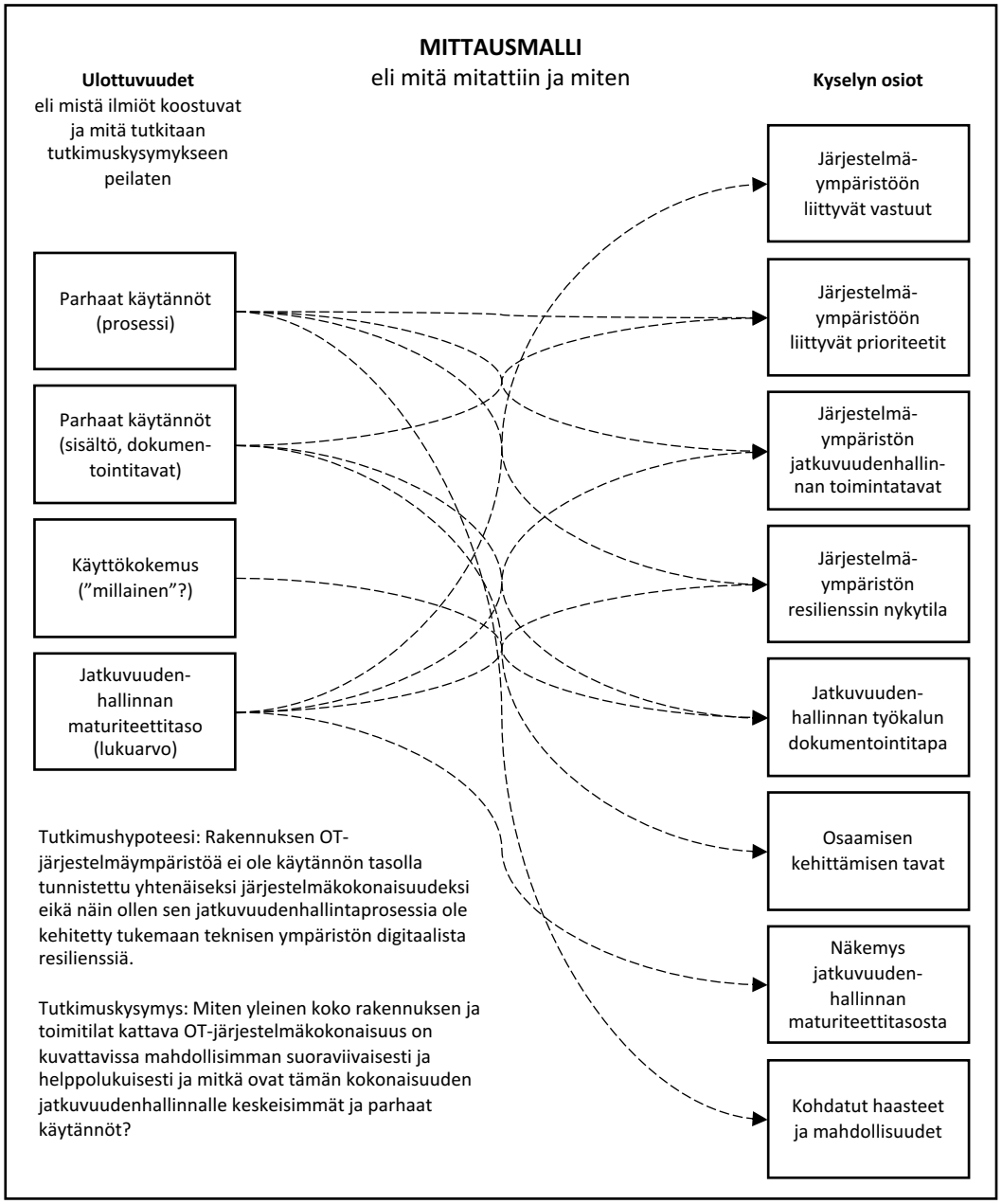
joka oli kyselyä muokatessa jäänyt tallentumatta oikein. Virhe ei ollut merkittävä. Kysymyksen tarkoituksena oli herättää vastaajan huomio erottamaan rakennuksen järjestelmäympäristön ja sen hallinta kiinteistömassan toiminnanohjauksesta.

Aineisto käsiteltiin Webropolin Professional Statistics -analyysityökalun avulla. Taustatiedot oli kysytty nominaaliasteikolla ja kontekstuaalisten sekä ilmiöosan kysymysten tiedot välimatka-asteikollisella Likert-asteikolla pois lukien kuvavalintakysymykset ja avoimet kysymykset. Järjestelmän avulla laskettiin tunnusluvut keskiarvo, luottamusväli, mediaani sekä keskihajonta kysymyskohtaisesti. Näiden lisäksi suoritettiin kontekstuaalisille sekä ilmiöosan kysymyksille Pearsonin korrelaatioanalyysi. Tämän avulla arvioitiin riippuvuuksia ja yhteyksiä valittujen tietojen suhteen käytettävissä olevan tiedon, korrelaatiokertoimen, selitysasteen sekä tilastollista riippuvuutta kuvaavan p-luvun avulla. Saatujen tietojen pohjalta tehtiin analyysi ja tiedon tulkinta. Aineiston testaaminen perustui ristiintaulukointiin. Jatkuvuudenhallinnan työkaluun sekä kouluttamiseen liittyviä kysymyksiä tarkasteltiin taustatietojen suhteen. Kyselyn vastaukset sekä lasketut tunnusluvut siirrettiin Excel-taulukkoon ja tunnusluvut tarkasteltiin kohta kohdalta mahdollisten tiedostonsiirtoon liittyneiden virheiden vuoksi. Havaitut siirrossa tapahtuneet virheet korjattiin. Otsikoinnin muokkaus suoritettiin MS Excelissä. Vastaajien raportin lähettämistä varten antamat sähköpostiosoitteet poistettiin tulostaulukosta.

Aineistosta tehtiin kuvaileva analyysi jäsentämällä väittämämuotoiset vertailukelpoiset muuttujat samaan taulukkoon keskiarvon perusteella järjestettynä pienimmästä suurimpaan, jotta tulokset saatiin kuvattua mittausmallin (kuva 6) mukaisesti. Väittämämuotoisten kysymysten avulla vastattiin mittausmallin kysymyksiin jatkuvuudenhallinnan prosessin parhaisiin käytäntöihin sekä jatkuvuudenhallinnan maturiteettitasoon liittyen. Jatkuvuudenhallinnan työkalua sekä koulutustapaa koskevat vastaukset järjestettiin valittujen prosenttiosuuksien mukaan suurimmasta pienimpään. Likert-asteikolla tutkittuja tietoja vertailtiin Pearsonin korrelaatiokertoimen avulla. Tiedoista pyrittiin tunnistamaan riippuvuuksia parhaiden käytäntöjen sekä OT-ympäristön jatkuvuudenhallinnan maturiteettitason välillä. Riippuvuuksista tilastollisesti erittäin merkitseviksi tulkittiin Heikkilän (2014, 240) mukaisesti tulokset, joissa $p \leq 0{,}001$. Tulokset

olivat tilastollisesti merkitseviä, jos $0{,}001 < p \leq 0{,}01$. Mikäli p:n arvot jäivät välille $0{,}01 < p \leq 0{,}05$, tulkittiin tulokset tilastollisesti melkein merkitseviksi. Muita tuloksia ei käsitelty. Kuitenkin mikäli korrelaatiokerroin jäi alle 0,3:een ja näin ollen selitysaste alle 10 %:een, oli tarkasteltava mahdollista riippuvuutta erityisen harkiten. Näin toteutetulla analyysillä pyrittiin tunnistamaan järjestelmäkokonaisuuden hallintaan liittyviä tapoja ja todentamaan tutkimushypoteesin paikkansapitävyys. Tutkimusotteena haluttiin kuvata ilmiötä ja verrata tunnistettua ilmiötä laadullisen tutkimuksen tuloksiin. Yksittäisiä poikkeavia havaintoja ei tutkittu erikseen, sillä tutkimusmenetelmän rooli tutkimuksessa oli toissijainen. Avoimet kysymykset käsiteltiin seuraavassa luvussa esitetyn mukaisesti.

Tulokset jäsenneltiin tapaustutkimukselle relevanttien tietojen osalta tutkimusongelmaa sekä tutkimushypoteesia mukaillen. Tutkimusongelman ulkopuolelle jäävät sekä muut epärelevantit asiat rajattiin tulosten käsittelyn ulkopuolelle. Ulos rajatuilla tutkimusongelmaan sisältyneillä asioilla ei ollut riittävästi näyttöä tai virhelähteet olivat liian suuria luotettavien johtopäätösten tekemistä ajatellen. Lopuksi havainnot tulkittiin peilaten aiempaan teoreettiseen viitekehykseen.



Kuva 6. Mittausmalli

Edellä kuvatussa (kuva 6) mittausmallissa käsiteltiin tutkimustuloksia kahtena eri kokonaisuutena määrällisen tutkimuksen näkökulmasta. Parhaat käytännöt (prosessi) vastasi tutkimuskysymykseen. Jatkuvuudenhallinnan maturiteettitasoa mittaavat kysymykset taas pyrkivät vahvistamaan tutkimushypoteesiin. Mittausmallin ulottuvuudet ”Parhaat käytännöt (sisältö ja dokumentointitavat)” sekä ”Käyttökokemus (’millainen’)” tuottivat sisältöä jatkuvuudenhallinnan työkaluun liittyen. Tätä kokonaisuutta on käsitelty seuraavassa luvussa.

3.5 Tutkimusmenetelmät yhdistävät kokonaisuudet

Tutkimuksen eri menetelmäosioissa tutkittiin samoja teemoja erilaisten näkökulmien varmistamiseksi sekä selvitettiin joitakin samoja asioita sisällön tuottamiseksi jatkuvuudenhallinnan kehittämisen työkalua varten. Tällaisia asioita olivat työkalun dokumentointitapa, jota tutkittiin mittausmallin (kuva 6) kohtien ”käyttökokemus” sekä ”parhaat käytännöt, sisältö ja dokumentointitavat” mukaisesti.

Tutkimuksessa nousi spontaanisti esille jatkuvuudenhallintaan liittyviä haasteita. Näitä ei ensisijaisesti kysytty haastateltavilta, sillä lähestymistapa oli positiivinen ja ratkaisuhakuinen. Haastateltavat nostivat kuitenkin haasteita omaaloitteisesti esille tarkentaakseen toimintaympäristöön liittyvää kontekstia ja nykytilaa. Näin saatiin eri näkökulmista negatiivisen kautta tulkiten sisältöä työkalun kehittämistä varten. Tästä syystä myös haasteet on sisällytetty tutkimustuloksiin sekä tulosten käsittelyosuuteen.

Tekstianalyysi toteutettiin luokittelemalla vastaukset määrällisen ja laadullisen tutkimusmenetelmän osalta samojen teemojen muodostamiksi kokonaisuuksiksi. Tunnistetut aiheet jaettiin kategorioiksi ja näiden alle tunnistettaviksi alakategorioiksi. Alakategorioita käsiteltiin tutkimuksessa OT-ympäristön jatkuvuudenhallintaan liittyvinä aiheina. Aiheiden esiintymismäärä kvantifioitiin ja aiheisiin liittyvistä maininnoista laskettiin teemakohtaiset prosenttiosuudet.

3.6 Tutkimuksen luotettavuus

Tutkimus kohdistui selkeästi rajattuun otosjoukkoon, joka kattaa kaikki huoltovarmuuskriittiset toimijat Suomessa. Kohderyhmän sensitiivisen luonteen takia yhteystietoja ei voitu kyselytutkimusta varten jakaa. Tästä syystä myöskään kyselytutkimuksen vastausprosenttia ei voitu laskea eksaktisti, vaikka otosjoukon koko olisikin teoriassa laskettavissa. Otosjoukon koko on tässä tutkimuksessa arvioitu suuruusluokan mukaan.

Haastateltavat valikoituivat tutkijan oman arvion pohjalta. Koska huoltovarmuuskriittisten toimijoiden listaa ei voitu jakaa tutkimusta varten edes organisaatiotasolla, oli tutkijan omia tietojaan hyödyntäen otettava yhteyttä oletetta-

vasti haastatteluun soveltuviin henkilöihin. Yhteydenotot tapahtuivat pääasiassa LinkedIn-palvelun kautta, sillä valtaosa haastatelluista ei ollut tutkijalle entuudestaan tuttuja. Prospektilistalla oli 25 organisaatiota, joista 13 henkilöä päätti osallistua tutkimukseen. Tutkimukseen osallistuneiden haastateltujen lisäksi haastattelun antoivat myös neljä informanttia, joiden haastattelujen vastauksia ei sisällytetty tutkimustuloksiin, koska nämä eivät kuuluneet ensisijaisesti kohderyhmään. Informanttien näkökulmia hyödynnettiin kuitenkin kerätyn tiedon jäsentelyssä ja jatkuvuudenhallinnan työkalun suunnittelussa.

Koska Huoltovarmuusorganisaatio koostuu useista poolitoiminnan ryhmistä, joilla on omat vastuuhenkilönsä, jäi kohderyhmän sitouttaminen pahimmillaan kahden peräkkäisen välikäden vastuulle. Tästä syystä alkuperäisestä tavoitteesta huolimatta ei kaikkia kyselytutkimuksen perusjoukkoon kuuluvia henkilöitä tavoitettu tai voitu sitouttaa yhtä aktiivisella viestinnällä kuin tehokkaimmin tutkimukseen sitoutettu kohderyhmä. Toisaalta kyselytutkimukseen osallistuivat myös haastatteluun osallistuneet perusjoukkoon kuuluneet henkilöt. Tämä aiheutti mahdollisesti lievää vinoumaa kysymysten tulkinnassa, sillä haastattelu tapahtui tällä otoksella ennen kyselytutkimukseen vastaamista. Haastateltujen osalta myöskään poimintatodennäköisyys perusjoukosta ei ollut sama kuin muilla kyselytutkimukseen kutsutuilla.

Epätasaisen jakelun takia kyselytutkimuksen vastauksissa korostuivat kuvan 14 mukaisesti tietyt toimialat. Näin ollen otos ei ollut täysin edustava kuvaus perusjoukosta yleisellä tasolla. Koska muun muassa Heikkilän (2014, 31) mukaan otoksen on tutkittavien ominaisuuksiensa suhteen vastattava riittävältä osin perusjoukkoa, pitäisi tutkittavan ilmiön osalta olla käytettävissä riittävät tiedot perusjoukosta. Koska kuitenkaan vastaavaa tutkimusta ei ole aiemmin toteutettu eikä näin ollen perusjoukon merkityksellisiä erityispiirteitä tunneta, ei tämän tutkimuksen perusteella voida vielä todeta vastaavuutta otoksen ja perusjoukon välillä.

Tutkimuksen tuloksissa vinoumaa saattoi aiheuttaa myös itse aihe, sillä tutkimuksessa käsiteltiin huoltovarmuudelle kriittisiä teemoja ja toimijoita. Tämä on voinut aiheuttaa taktikointia vastauksessa yleisen teemaan sitoutumisen näkökulmasta. Toisaalta kyselytutkimuksen varsin erilaiset vastaukset haastatteluihin nähden voivat johtua kysymysten tulkinnanvaraisuudesta taikka siitä, ettei

kyselyssä ollut mahdollista varmistaa vastaajan ymmärrystä siitä, mitä teemaa käsitellään ja mitä se tarkoittaa. Yleisesti ottaen kuitenkin erityisesti haastatteluissa kävi selväksi, että osaaminen aihealueeseen liittyen on liian vähäistä toimialalla.

Tutkimusajankohta vaikutti mahdollisesti vastauksiin, sillä joulukuussa 2022 oli vahvistettu EU-komissiossa NIS 2 tietoturvadirektiivi sekä kriittistä infrastruktuuria koskeva CER-direktiivi. Toisaalta samalla Venäjä jatkoi hyökkäyssotaa Ukrainassa tuhoten systemaattisesti paikallista kriittistä infrastruktuuria (Bailey ym. 2023, 1–2). Maailmanpoliittinen tilanne, kyberuhkiin liittyvien riskitasojen nousu sekä varautuminen direktiivien paikalliseen voimaanastumiseen voivat olla vastauksiin vaikuttaneita teemoja. Muun muassa Kosmowski ym. (2022, 13) mainitsee kyberhyökkäysten riskin olevan Euroopan alueella suhteellisen korkea.

Mahdollista vinoumaa aiheuttavista aikaan ja kohderyhmään liittyvistä maininnoista huolimatta kyselytutkimuksen tulokset vaikuttavat olevan suuntaa antavia ja tarkentuvia. Kerätyt tiedot kuvaavat tehokkaasti tutkitun ilmiön tilaa ja melko luotettavia tuloksia saavutettiin myös tällä kohtalaisen pienellä otoksella. Erot haastattelututkimuksen ja kyselytutkimuksen välillä on selitettävissä kysymyksenasettelun sekä haastattelutilanteessa tarkemmin kuvatun ja rajatun kontekstin avulla.

3.7 Tutkimuksessa käytetyt termit

Tutkimuksessa käytettiin järjestelmäkokonaisuuksista osittain kiinteistö- ja rakentamisalan nimeämiskäytännöstä poikkeavia nimityksiä, sillä yleisten käytäntöjen mukaiset nimitykset koettiin joiltakin osin liian rajoittuneiksi. Paloturvallisuustekniset järjestelmät tarkoittivat tässä tutkimuksessa esimerkiksi seuraavia: paloturvalaitteet, paloilmoitinjärjestelmä, sprinklerijärjestelmä, savunpoistoluukkujen ohjausjärjestelmä, äänievakuointijärjestelmä ja turvavalaistusjärjestelmä. Taloteknisillä järjestelmillä tarkoitettiin seuraavia: rakennusautomaatiojärjestelmä, kylmäjärjestelmä ja valaistuksen ohjausjärjestelmä, LVIA, talotekniikkavalvomojärjestelmä, energiatehokkuusjärjestelmä, olosuhteidenseurantajärjestelmä. Turvallisuusjärjestelmiin laskettiin mukaan muun muassa

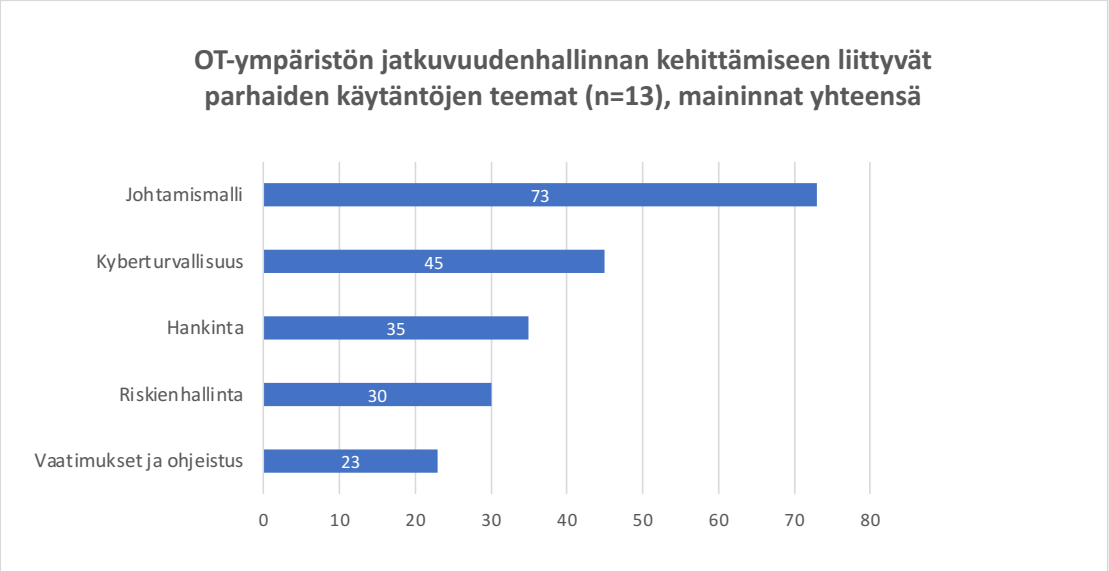
murtosuojajärjestelmä, kulunvalvonta- ja kameravalvontajärjestelmä, aluevalvontajärjestelmä sekä turvallisuusvalvomojärjestelmä. Liikkumiseen liittyen käsiteltiin hissien, liukuportaiden ja liukutasojen ohjausjärjestelmiä ja muita kulkemiseen liittyviä järjestelmiä, joita ovat esimerkiksi vierailijahallintajärjestelmä, kilpitunnistusjärjestelmä, porttipuhelinjärjestelmä, pysäköinninohjausjärjestelmä, sähköautojen, trukkien ynnä muiden latausjärjestelmät, ovien, porttien ja puomien ohjausjärjestelmät. Energiajärjestelmät kattoivat tutkimuksessa muun muassa sähköjärjestelmän, lämpöjärjestelmän, UPS-laitteet sekä varavoiman. Näiden lisäksi tutkimuksessa mainittiin toiminnanohjausjärjestelmät (esimerkiksi jätehuollon ja kierrätyksen järjestelmät, puhtaanapidon järjestelmät, toimitilapalveluiden järjestelmät, AV-järjestelmät, ravintolapalveluiden järjestelmät ja smart office -järjestelmät).

4 TULOKSET

Tutkimus tuotti runsaasti tietoa valitun kohderyhmän toiminnalleen kriittisimpien rakennusten järjestelmäympäristön jatkuvuudenhallintaan ja digitaaliseen resilienssiin liittyvistä prosesseista ja toimintatavoista. Tässä luvussa esitellään tutkimuksen tulokset tekstimuodossa, havainnollisin kuvin sekä taulukoin.

4.1 Jatkuvuudenhallinnan parhaat käytännöt laadullisen tutkimuksen näkökulmasta

Kohdissa 4.1.1–4.1.5 on esitetty haastateltujen esille nostamat jatkuvuudenhallinnan parhaat käytännöt kussakin kohdassa teemoittain, kategorioittain, joita käsitellään tässä teemoihin liittyvinä aiheina, sekä otsikoittain. Tulokset on esitetty kussakin kohdassa samanlaisin kaaviokuvin, joissa kaavion ydin osoittaa teemaan liittyvien aiheiden prosentuaalisen osuuden teemakohtaisesta kokonaisuudesta ja ulompi kerros osoittaa mainittujen parhaiden käytäntöjen kategoriakohtaisen lukumäärän. Kaavio sisältää myös palkkikaavion kategoriakohtaisten mainintojen lukumäärästä, joka joiltakin osin eroaa parhaiden käytäntöjen lukumäärästä. Tämä johtuu siitä, että eri henkilöt mainitsivat jonkin verran samoja aiheita parhaiksi käytännöiksi. Parhaisiin käytäntöihin liittyvät jatkuvuudenhallinnan kehittämisen teemat jakautuivat kuvan 7 mukaisesti. Haastateltavat kommentoivat selkeästi eniten johtamiseen liittyviä aiheita.



Kuva 7. OT-ympäristön jatkuvuudenhallinnan kehittämiseen liittyvät parhaiden käytäntöjen teemat haastattelututkimuksen mukaan (n = 13), maininnat yhteensä

Kuvassa 7 esitettyjen teemojen lisäksi haastatellut sekä kyselytutkimukseen vastanneet nostivat esille haasteita OT-ympäristön jatkuvuudenhallintaan liittyen. Näistä tunnistettiin tutkimuksessa yhteensä 183 yksittäistä haastetta tai ongelmaa, joita on käsitelty enemmän kohdassa 4.2.5.

4.1.1 Johtamismalli

Johtamiseen liittyvät teemat esiintyivät selkeästi useimmin (73 mainintaa, n = 13) haastatteluissa käsiteltäessä OT-ympäristön jatkuvuudenhallinnan parhaita käytäntöjä. Erillisiä aihealueita tunnistettiin yhdeksän kuvan 8 mukaisesti. Kuvassa on esitetty näihin liittyvät maininnat kappalemääräisenä sekä teemakohtaisina prosenttiosuuksina. Operatiivinen johtaminen mainittiin 22 kertaa (30 % teeman aiheista) ja yhteistyö 18 kertaa (25 %). Talouden johtaminen mainittiin kahdeksan (11 %) ja pitkän tähtäimen suunnittelu seitsemän kertaa (10 %). Tiedolla johtaminen nostettiin haastatteluissa esille kuusi kertaa (8 %). Osaamisen kehittäminen mainittiin neljästi (5 %), joskin se nousi esille myös muissa yhteyksissä johtamisen lisäksi. Elinkaarenhallinta ja riskienhallinta mainittiin osana johtamista kumpikin kolme kertaa (4 %) ja omaisuuden hallinta kahdesti (3 %).

Johtamiseen liittyviä parhaita käytäntöjä ja kokemuksia listattiin kategorioittain kuvan 8 mukaisesti. Johtamiseen liittyen johdon sitoutuminen mainittiin keskeisenä tekijänä. Elinkaarenhallinnassa korostui suunnitelmallisuus, tiedon

eheyden säilyminen, tarpeenmukaisuus sekä yleisesti kokonaisuuden reunaehtojen tunnistaminen. Omaisuuden hallinnasta nostettiin esille omaisuusstrategian tärkeys sekä jatkuvuudenhallinnan rooli omaisuudenhallintaa tukevana toimintona. Vastuullisuuden raportointiin liittyvät teemat mainittiin myös joitakin kertoja tiedolla johtamisen sekä regulaation näkökulmasta.

> "Meillä ainakin ympäristön näkökulmat ja ympäristövastuullisuus on iso asia. Sitä raportoidaan eli silloin jos ne järjestelmät palvelevat sitä kokonaisuutta, niin silloin hankinta on todennäköisimmin jollain tavalla perusteltavissa." (I)

Jatkuvuudenhallintaa pidettiin loogisena osana operatiivista toimintaa ja operatiivisen johtamisen alle listautui luontevasti useita eri tehtäviä ja toimintamalleja. Haastateltavat olivat jokseenkin eri mieltä siitä, miten toimintaa yleisesti ottaen pitäisi johtaa ja haastatteluissa nousi esille kolme eri näkökulmaa. Osan mielestä paras johtamismalli on jaettu vastuu IT:n ja rakennuksen toimintojen substanssin välillä ja samalla kuitenkin osa nosti esille jaetun vastuun toimimattomuuden. Osan mielestä IT:n pitäisi vastata kaikkien teknologiaan liittyvien toimintojen johtamisesta ja osa taas siirtäisi kaikkien OT-ympäristöön liittyvien toimintojen johtamisen substanssivastuulliselle yksikölle. Osa haastatelluista mainitsi tärkeänä säännöllisen seurannan, tavoitteellisuuden ja strategisten linjausten mukaisen toiminnan. Samalla nostettiin myös yhteistyön tärkeys IT:n, kiinteistö- ja turvallisuusalan välillä esille tärkeänä kokonaisuutena. Varautuminen, valvonnan tärkeys sekä reagointikyvyn ylläpitäminen mainittiin välttämättöminä toimintoina kokonaisuuden hallintaan ja johtamiseen liittyen.

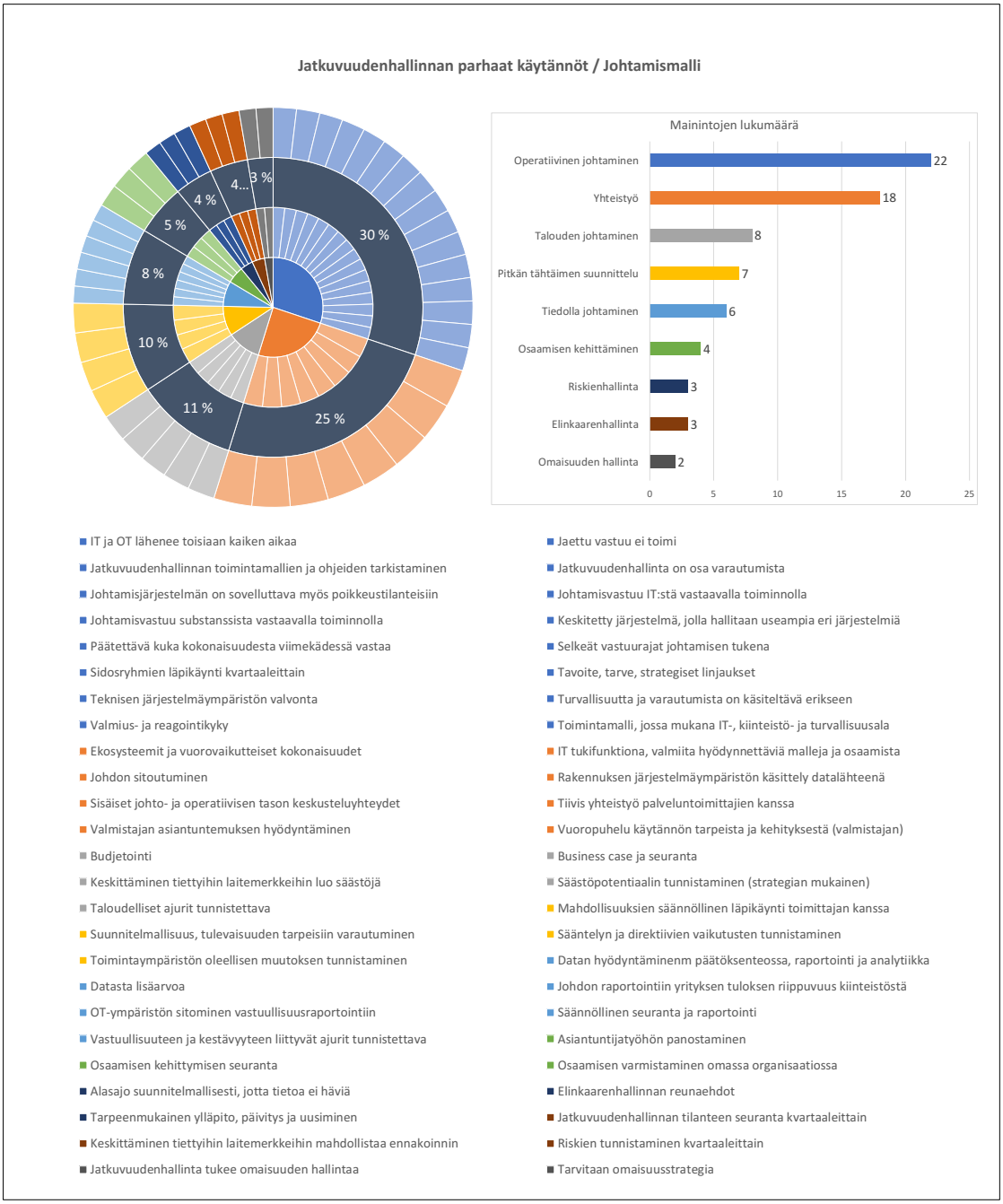
> "Nyt ollaan siinä ajassa, että pitää tehdä niitä oikeita valintoja, jotta pysytään kehityksessä mukana." (K)

Moni vastaajista piti osaamista ja sen ylläpitoa merkittävänä asiana ja sen puuttuminen nousi esille myös tunnistettujen haasteiden näkökulmasta. Osaamista käsiteltiin niin organisaation sisäisenä toiminnan johtamista ja ohjaamista kuin myös hankintaa koskevana kokonaisuutena, mutta myös palvelun-toimittajien kyvykkyytenä tuottaa tarvittavaa ja sovitun mukaista palvelua. Osaaminen ja toisaalta sen puuttuminen esiintyivät tutkimuksen eri aihealueet poikkileikkaavana kokonaisuutena.

Suunnitelmallisuuden näkökulmasta nostettiin esille varautuminen sekä riskienhallinnan että toiminnan jatkuvuuden näkökulmasta mutta myös sääntelyn ja direktiivien vaikutuksiin liittyvänä toimintaympäristön muutoksiin liittyvänä teemana. Yhteistyön tärkeys organisaation sisäisten ja ulkoisten suorien sidosryhmien kesken mainittiin lähes jokaisessa haastattelussa.

> ”Meille on sisäänrakennettuna systeemi, jossa yksi osapuoli vastaa kiinteistöstä ja rakennuksista. Infrasta vastaa toinen osapuoli. Tällä mallilla tullaan pieniin intressiristiriitoihin. Käytännöt eroavat toisistaan, koska ei hahmoteta omistajuuden ja vastuullisen toiminnan tarpeita.” (I)

Osa painotti myös päämiesten eli järjestelmän kehittäjän tai laitevalmistajan ja loppukäyttäjän välisen yhteistyön tärkeyttä. Käytettävissä olevan tiedon hyödyntäminen johtamisen työkaluna mainittiin joitakin kertoja. Tavanomaisia talouden johtamisen välineitä kuten budjetointia, business case -laskentaa sekä seurantaa pidettiin merkittävinä toiminnan hallinnan välineinä. Osa, joskin vain harva, haastatelluista nosti näihin tukeutuen esille erilaisia mahdollisuuksia säästötoimenpiteisiin. Samalla mainittiin myös taloudelliset ajurit laadukkaan toiminnan mahdollistavana sekä estävänä teemana.



Kuva 8. Jatkuvuudenhallinnan parhaat käytännöt johtamisen näkökulmasta (n = 13)

Kuvan 8 aihealueet kategorisoitiin haastatteluista saatujen tietojen pohjalta. Operatiivinen johtaminen sekä yhteistyöhön liittyvät käytännöt nousivat jokaisessa haastattelussa esille merkittävänä kokonaisuutena kattaen yhdessä yli 50 % kaikista johtamismalliin liittyvistä maininnoista. Seuraava merkittävä kokonaisuus kattaa suunnitelmallisuuteen liittyviä teemoja eli taloudellisen johtamisen, pitkän tähtäimen suunnittelun sekä tiedolla johtamisen. Nämä yhdessä kattoivat yli neljänneksen kaikista johtamiseen liittyvistä kommenteista. Hyviä kommentteja aihekohtaisesti saatiin kerättyä useita, joista esimerkkejä on nostettu esimerkiksi taulukkoon 1.

Taulukko 1. Sitaatteja johtamismalliin liittyen

Kategoria	Sitaatti
Elinkaaren hallinta	"Miten sen elinkaarta pystytään hallitsemaan? Mitä se tarkoittaa? Millainen sen ympäristö tai alusta on? Mihin se järjestelmä perustetaan? Onko se ympäristö sellainen, että se on relevantti asia?" (L)
Omaisuuden hallinta	"Koen, että me pystymme hallitsemaan sekä meidän tekemistä ja meidän tietoa, että myös meidän omaisuutta paljon paremmin, jos meillä olisi tämän tyyppinen jatkuvuudenhallinta ja ylipäätään se omaisuusstrategia olisi aidosti käytössä." (M)
Operatiivinen johtaminen	"Tässä on ihan sellanen perusjuttu, että IT:hän haluais johtaa kaikkea, mutta käytännössä heillä ei ole substanssiosaamista. Se ei vaan wörki se toimintamalli. Yleensä on parasta, että asiaa johtaa se ihminen, joka ymmärtää, mitä sieltä tavoitellaan ja miten halutaan mennä eteenpäin." (H) "Me vihdoin aletaan käsittää ne (rakennuksen järjestelmät) IT-järjestelminä. Ne pitäisi mielestäni laittaa saman toimijan alle." (P)
Osaamisen kehittäminen	"Kyllä minä näen, että paremmat tulokset saadaan sillä, että on kokemuksia isoistakin organisaatioista. On kokemuksia siitä, että omalla osaamisella ja riittävällä resurssoinnilla pystytään tarjoamaan parempaa laatua, jatkuvuutta ja kustannustehokkuutta siihen omaan organisaatioon. Selkeästi suunta on se, että asiat kehittyvät ja muuttuvat koko ajan ja palvelutoimittajien asiantuntijapuolella tapahtuu sellasita liikehdintää, että sen oman osaamisen kehittäminen pitää nyt varmistaa ja resurssoida siihen. Se on todella tärkeää."(F)
Pitkän tähtäimen suunnittelu	"Meillä yleisesti tietysti EU-sääntely ja kansainvälinen sääntely on iso (vaikutin) ja sitä kautta tulee tosi paljon meille ympäristödirektiiviä ja ympäristösääntelyyn liittyviä asioita. Toisaalta, kun siihen voi liittyä myös tätä digitalisaation kysymyksiä, niin silloin varmasti juuri näin on (CER- ja NIS 2 -direktiivit nostavat esille sellaisia asioita, että johto tulee kiinnostumaan myös muista kuin IT-järjestelmistä)." (I)
Riskienhallinta	"Säästöjä syntyy siitä, että keskitytään tiettyjen globaalien valmistajien laitteisiin. Tällöin tiedetään, mitä laitteita on ja huollot sekä muut toimenpiteet on ennakoitavissa. Tiedetään elinkaaret ja tiimit tarvitsevat vähemmän resursseja. Se ei vie paikallisen kiinteistöpäällikön aikaa." (J)
Talouden johtaminen	"Suurin draiveri on varmasti talous eli se, että tuottaako jonkunlainen prosessi hyvää taloudellista lopputulosta - säästetäänkö rahaa toisin sanoen. Tai tuottaako vaikkapa investoinnit uusiin järjestelmiin ja niiden käyttöönotto ympäristön kannalta hyviä ratkaisuja." (M)
Tiedolla johtaminen	"Kiinteistön pitäis pystyä kertomaan johdolle (tilannetietoja) ja johdossa pitäis olla ymmärtäväisiä ihmisiä, jotka ymmärtävät sen, miten paljon organisaation tulos riippuu kiinteistöstä. Monella (organisaatiolla) riippuu aika radikaalisti oman yhtiön tulos siitä kiinteistöstä.” (A)
Yhteistyö	"Tämä on ollut meillä se muutoksen este tai haaste, että ei ole haluttu lähteä tällaiseen holistiseen keskusteluun siitä, että voisko tätä (kiinteistön järjestelmäympäristöä) miettiä kokonaisuutena ja tällaisena tiedonvaihtomahdollisuutena." (B)

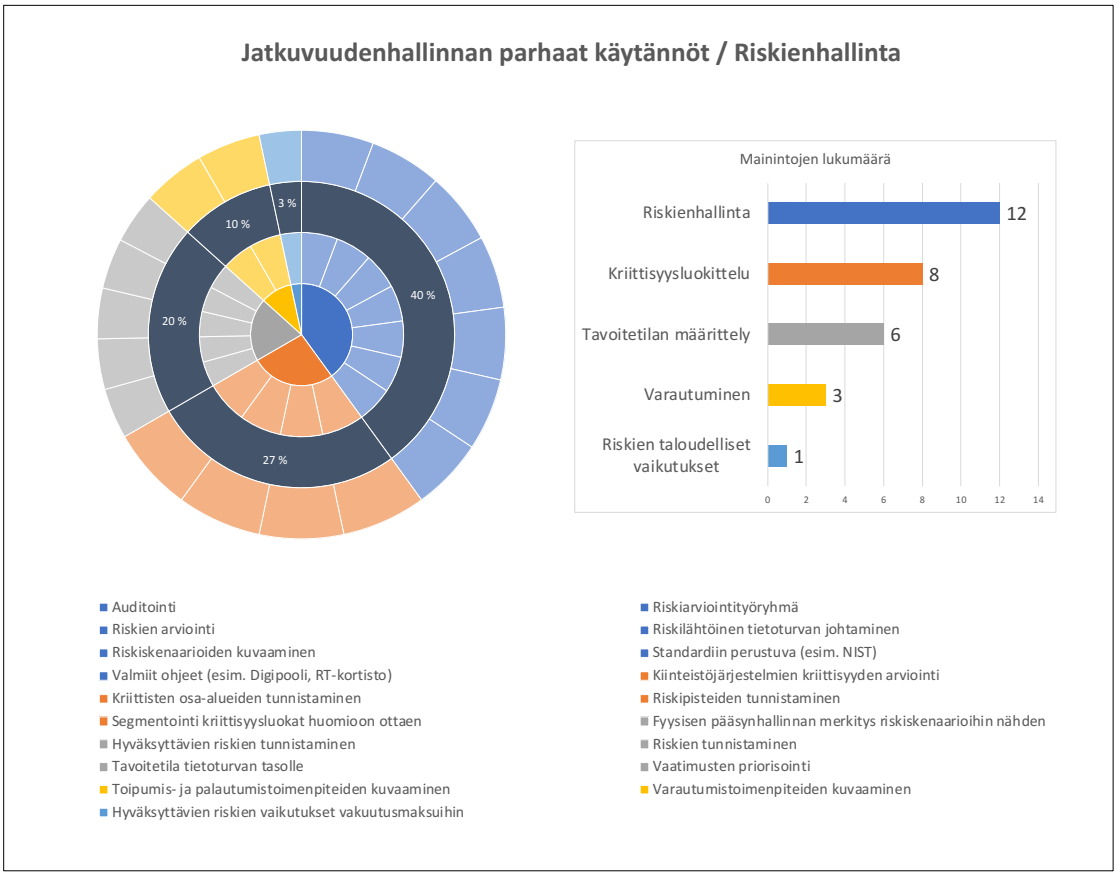
Taulukon 1 kommentit kuvaavat haastateltavien näkemystä hyvistä käytännöistä sekä toisaalta myös nykytilan ongelmista ja onnistumisista. Eräs haastateltu nosti muun muassa esille holistisen näkemyksen puuttumisen koko OT-järjestelmäympäristöön liittyen. Björck ym. (2015) taas toteaa, että holistinen näkökulma digitaalisen resilienssin varmistamiseksi on välttämättömyys. Haastatteluissa nousi esille johtamisen käytäntöjen lisäksi myös vastuullisuus sekä esimerkiksi teknisen ympäristön valintaan ja tämän aihealueen osaamisen kehittämiseen liittyvät tarpeet.

4.1.2 Riskienhallinta

Riskienhallinta mainittiin (30 mainintaa, n = 13) sen lisäksi, että se laskettiin osaksi johtamista, myös omana teemanaan liittyen OT-ympäristön jatkuvuudenhallintaan. Kosmowski ym. (2022, 8) mainitsee jatkuvuudenhallinnan osana organisaation holistista riskienhallintaa. Riskienhallintaan liittyviä aihealueita tunnistettiin viisi. Näihin liittyvät maininnat kappalemääräisenä sekä prosenttiosuuksina on esitetty kuvassa 9. Yleisesti riskienhallintaan liittyviä mainintoja oli 12 kappaletta (40 % teeman aiheista) ja kriittisyysluokitteluun liittyviä kahdeksan kappaletta (27 %). Tavoitetilan määrittely mainittiin kuusi kertaa (20 %) ja varautuminen kolmesti (10 %). Riskien taloudelliset vaikutukset mainittiin kerran (3 %).

> "Käytännössä yksi kriittinen osa tietoturvaa on fyysinen pääsynhallinta. Kyllähän se suurin riski on ne tyypit kuitenkin." (L)

Riskienhallintaan liittyviä parhaita käytäntöjä listattiin viideltä eri aihealueelta, jotka olivat riskienhallinta yleisesti, kriittisyysluokittelu, riskien taloudelliset vaikutukset, tavoitetilan määrittely ja varautuminen. Kriittisyysluokittelun näkökulmasta nostettiin esille muun muassa yleisesti kriittisten osa-alueiden tunnistaminen sekä OT-ympäristön tietoverkkojen segmentointi kriittisyysluokat huomioon ottaen. Riskien taloudellisten vaikutusten osalta mainittiin jatkuvuudenhallinnan ja OT-ympäristön tilaan liittyvien hyväksyttävien riskien mahdollinen vaikutus vakuutusmaksuihin. Riskienhallintaprosessille koettiin tärkeänä jokin standardi tai malli, johon toiminta voi tukeutua. Yleisesti tunnetuista malleista mainittiin yhdysvaltalaisen National Institute of Standards and Technologyn (NIST) laatima dokumentaatio sekä myös Huoltovarmuusorganisaation Digipoolin ja Rakennustiedon laatimat aineistot. Fyysisen pääsynhallinnan sekä priorisoinnin merkitys korostui joissakin haastatteluissa. Teknisen ympäristön riskienhallintaan liittyen toivottiin tavoitetila asetettavan samalle tasolle tietoturvan kanssa. Varautumis-, toipumis- ja palautumistoimenpiteiden kuvaamisen sekä priorisoinnin tärkeys mainittiin kukin kertaalleen.



Kuva 9. Jatkuvuudenhallinnan parhaat käytännöt / Riskienhallinta (n = 13)

Kuvan 9 aihealueet kategorisoitiin haastatteluista saatujen tietojen pohjalta. Maininnat sisälsivät keskeisiä teemoja riskienhallintaan liittyen. Tavoitetilan määrittelyyn liittyvät aiheet nousivat esille tärkeänä teemana erityisesti osaamisen näkökulmasta. On kyettävä määrittämään kompleksisessa ympäristössä kokonaisuuden tavoitetila niin, että palveluntoimittajat pystyvät sitä vastaavaa palvelua tarjoamaan. Toisaalta tavoitetilan määrittämisen yhteydessä nousi esille myös kustannukset. Hyväksyttävien riskien tunnistaminen voi olla haastateltujen mukaan joskus järkevämpää kuin arvokkaan kaikelta suojaamaan pyrkivän kokonaisuuden toteuttaminen. Kommentteja aihekohtaisesti saatiin kerättyä useita, joista osa nostettiin esimerkiksi taulukkoon 2.

Taulukko 2. Sitaatit riskienhallintaan liittyen

Kategoria	Sitaatti
Kriittisyysluokittelu	"Jos lähtee turvallisuudesta liikkeelle, niin kyllähän pitäis olla riskiperustainen lähestyminen siihen, että tämä malli, jossa tunnistetaan ne toiminnan kannalta kriittiset kiinteistöt tai ympäristöt joissa kiinteistöjärjestelmillä on merkitystä sille kohteelle tai toiminnan kohteelle." (B)
Riskien taloudelliset vaikutukset	"Joitain riskejähän voi olla ihan järkevää hyväksyäkin. Kyllä heidän (kiinteistöistä vastaavien tahojen) pitää asettaa myös tavoitetilaa tietoturvan tasolle, koska sehän vaikuttaa vakuutusmaksuihin ja muihin sit loppupeleissä." (L)

Riskienhallinta	"Lähtötilanne perustuu aina riskiarvioon ja riskiarviointityökaluun tehtyihin päätelmiin siitä, mitä meillä on ja mitä riskejä löytyy ja mihin pitäisi vastata ja miten niitä on priorisoitu." (K) "Nämä meillä auditoidaan meidän omistajien puolesta, koska he haluavat tietää (tilanteen), kun ovat sijoittaneet tähän. He haluavat tietää, että arvo säilyy ja millään muulla he eivät voi varmistaa sitä kuin katsomalla, että meillä tehdään kyberturvallisuusjutut, riskiarviot jne. He lähettävät omat tarkastajat tarkastamaan." (A) "Riskiarviointityöryhmän kautta (arvioidaan) se, että kuinka paljon siellä on niitä riskipisteitä tällasessa kiinteistössä ja mitä pitäisi tarkastella." (F)
Tavoitetilan määrittely	"Kyllähän he (riskienhallinta) tavallaan miettii sen sillä tavalla, että mikä haitta tulee, jos jotain käy. Kyllähän sieltä pitää tulla se tavoitetaso, mutta ei se tarkoita sitä, että tavoitetasoon on pakko mennä. Voi olla järkevämpää tehdä asioita jollain toisella tavalla kuin nostaa tietoturvan tasoa aina sille tasolle, mitä se riskienhallinta esittää." (L)
Varautuminen	"Jos mennään tähän varautumispuolelle, niin (on hyvä) ymmärtää taas se, että jos on sellaisia järjestelmiä tai kokonaisuuksia, jotka halvaantuessaan aiheuttaa kohteelle jotain katalia asioita, niin nekin (kriittisyys) nousee. Se jakautuu niin, että on se turvallisuus siinä mielessä, että ne laitteet ovat turvallisia, että sinne ei pääse kyberiskuja tekemään ja toisaalta jos sinne pääsee ja joku menee rikki, niin on sitten ne varautumistoimet, että joko ne pystytään eristämään tai sitten saadaan nopeesti jotain korjaavia liikkeitä tehtyä, että se kapasiteetti saadaan pystyyn ja toiminta jatkumaan." (B)

Taulukon 2 sitaatit kuvaavat ylätasolla sitä ilmapiiriä, joka haastatteluista jäi tutkijalle mieleen riskienhallintaan liittyen. Haastateltavat tunnistivat selkeästi fyysisen turvallisuuden roolin osana jatkuvuudenhallintaa ja erilaisten yhteistyöverkostojen tärkeyden kokonaisuuden kannalta oikeiden toimenpiteiden toteuttamiseen liittyen.

4.1.3 Hankinta

OT-ympäristön jatkuvuudenhallinnan tunnistetuista parhaista käytännöistä hankintateeman alle rajautui seitsemän aihealuetta. Näiden maininnat kappalemääräisenä (yhteensä 35, n = 13) sekä prosenttiosuuksina on esitetty kuvassa 10. Aiheista palvelusopimuksiin ja palvelutasosopimuksiin liittyviä mainintoja oli yhteensä 13 kpl (37 % teeman aiheista) ja vaatimusten määrittelyyn liittyviä 11 kpl (31 %). Yhteistyökumppanin valintaan liittyviä mainintoja oli neljä kappaletta (11 %) ja kokonaisuuden hallintaan, ratkaisun valintaan sekä sopimuksen kohteeseen liittyviä mainintoja oli kutakin kaksi kappaletta (6 %). Sopimuksen vakiolausekkeet sopimista helpottavana tekijänä mainittiin vain kerran (3 %).

> ”Kuudesta osastosta neljä hankkii järjestelmiä. Yksi hankkii järjestelmiä, joiden ylläpitovastuu on toisella yksiköllä. Nämä ovat ihan sekaisin. Kenen vastuulla kokonaisuus on? Kuka hoitaa sen, että oikeat piuhat menevät oikeaan paikkaan ja että oikeanlainen raportointi on ylipäätään mahdollista?” (M)

Hankintaan liittyviä parhaita käytäntöjä listattiin kategorioittain seitsemälle aihealueelle seuraavien otsikoiden alle kuvan 10 mukaisesti: kokonaisuuden hallinta, palvelusopimukset ja palvelutaso, ratkaisun valinta, sopimuksen kohde, sopimuksen vakiolausekkeet, vaatimukset ja yhteistyökumppanin valinta. Kokonaisuuden hallinnasta erityisesti huoltokirjajärjestelmän rooli nousi maininnoissa esille, mutta samalla myös järjestelmien kyvykkyydet tai kyvyttömyydet vastata nykyajan järjestelmäympäristön hallintaan liittyviin vaatimuksiin.

> "Jos ne (riippuvuudet ja palvelutasovaatimukset) kirjoitettaisiin auki ja pyydettäisiin niitä, niin pikkuhiljaa pakotetusti toimijat joutuvat mukautumaan siihen. Ja jos ei niitä pystytä tarjoamaan millään tavalla, niin ne jäävät aina ulos (kilpailutuksesta). Kyllähän se ajaa sitä alaa oikeaan suuntaan." (K)

Palvelusopimukset ja erityisesti palvelutasosopimukset nousivat esille haastatteluissa hankinnan osaamisen näkökulmasta. Vaatimusten määrittelyyn liittyen mainittiin useita keskeisiä hankintaan liittyviä asioita, jotka vaikuttavat ratkaisun elinkaaren aikana. Mahdollisimman oikeat valinnat ratkaisun sekä yhteistyökumppanin valinnan näkökulmasta nousivat jonkin verran esille. Myös sopimuksen kohteen, tavoitteiden ja kohteen erityispiirteiden kuvaamisen tärkeyttä painotettiin osana onnistunutta hankintaprosessia.

Kuva 10. Jatkuvuudenhallinnan parhaat käytännöt / Hankinta (n = 13)

Kuvan 10 aihealueet kategorisoitiin haastatteluista saatujen tietojen pohjalta. Sopimiseen liittyvät aiheet kattoivat teemakohtaisista maininnoista yhteensä 40 %. Tämän lisäksi vaatimuksiin liittyvät teemat korostuivat yli 30 prosentissa vastauksista. Nämä yhteensä kattoivat merkittävät lähes kolme neljäsosaa kaikista maininnoista hankintaan liittyen. Taulukossa 3 on listattu aihealuekohtaisesti esimerkinomaisesti haastateltavien sitaatteja.

Taulukko 3. Sitaatit hankintaan liittyen

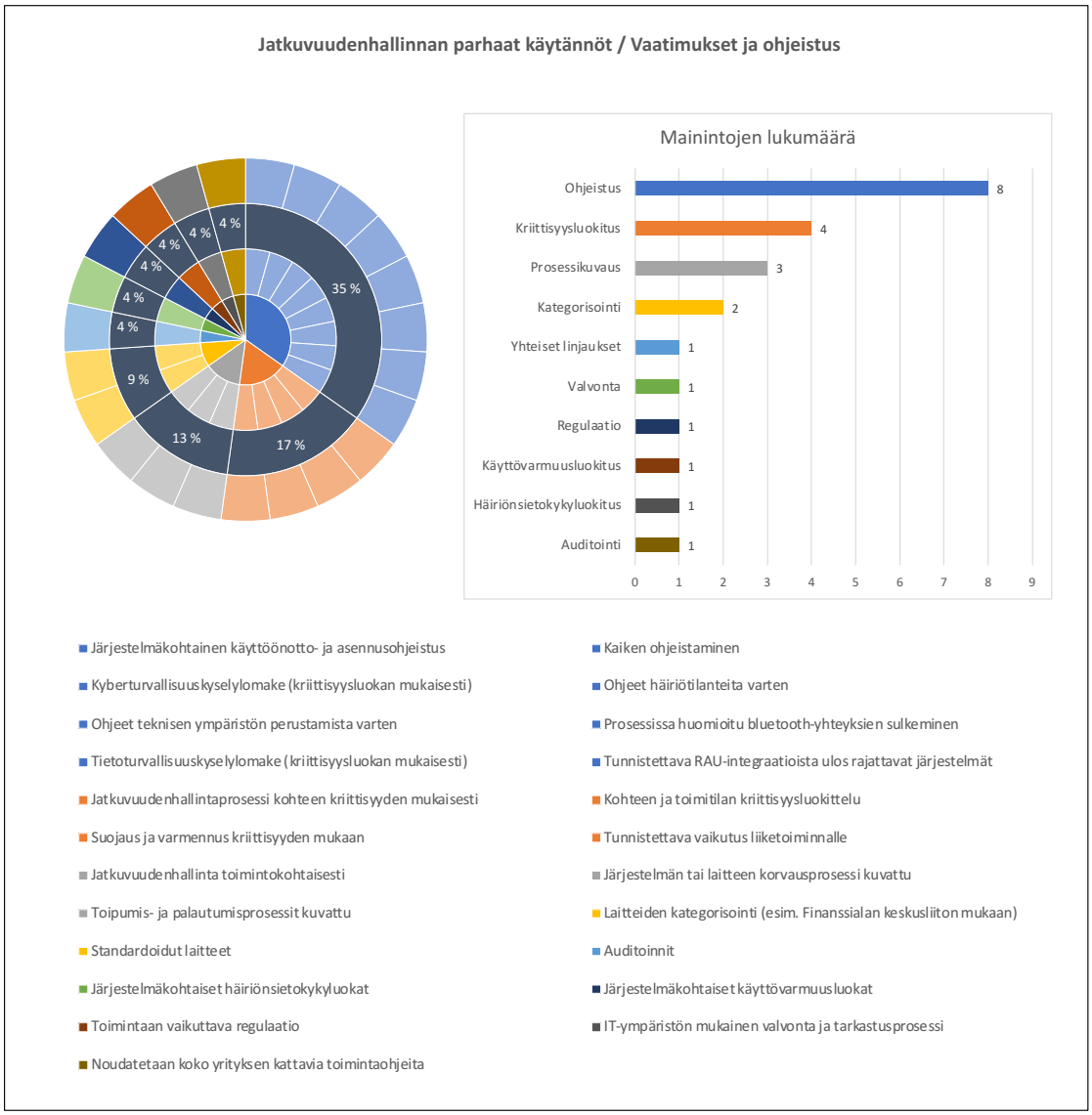
Kategoria	Sitaatti
Kokonaisuuden hallinta	"Sopimuskumppanit täytyy olla, sopimukset tehty ja huoltokirja, missä ne on hallittu. Sieltähän se kai näytti tulevan takaisin eli sopimuskumppanit ja huoltokirjat ja huolto-ohjelmat määriteltynä." (E)
Palvelusopimukset ja palvelutaso	"Olemme alkaneet pitää tällaisia varaosapooleja siten, että palveluntoimittaja ylläpitää ja varastoi varaosia ja me käytännössä ostamme heiltä laitteet itsellemme. Kun jotain hajoaa, niin tilataan sieltä varaosapoolista ja kohdistetaan lasku sitten sille kustannuspaikalle, mille se kuuluu." (E)

Ratkaisun valinta	"Me aloitamme arvioimalla sekä tuote että valmistaja, koska tuote voi olla hyvä, mutta sitten taas elinkaariajattelussa emme halua välttämättä ostaa taloteknistä järjestelmää, jonka hyödyllinen käyttöikä on kolme vuotta." (P)
Sopimuksen kohde	"Mihin (vaatimuksiin / tavoitteisiin) pitää vastata (järjestelmäympäristöllä)" (F)
Sopimuksen vakiolausekkeet	"Hankintasopimuksiin pitää saada uusia vaatimusvakiolausekkeita siitä, miten asioita hoidetaan. On tullut GDPR:ää ja on tullut tulossa näitä uusia vaatimuksia tänne tietoturvallisuudelle ja kyberturvallisuudelle. Sinne pitää saada ymmärrettävää vaatimusta ja vakiolauseketta niihin sopimuksiin, että toimittajat osaavat ja ymmärtävät tarjota niitä oikein ja ymmärtävät myös ne vastuut. Ne on nyt jollain tavalla yleisluonnollisia olleet tähän saakka." (K)
Vaatimukset	"Se käyttöikä pitää olla järkevästi mietitty ja se asettaa vähän haasteita tähän laiteympäristöön. On esimerkiks määritettävä mitä ne tekee eli sen pitää olla päivitettävä. Pitää olla sen verran tota järeitä laitteita, että ne myös toimii kymmenen vuoden päästä, kun ajetaan siihen uusimpia ohjelmistoja sun muita." (P) "Mitä halutaan? Millaisia laitteita? Nyt on tällainen laite - okei millaisessa ympäristössä? Kukaan (järjestelmäntoimittaja) ei kysy, että millaisissa olosuhteissa (järjestelmät) toimivat nykypäivänä tai mitä niiden pitäisi kestää tai millaisille asioille se järjestelmät altistuvat elinkaarensa aikana. Sellasia kysymyksiä ei (käydä läpi) hankintavaiheissa." (F)
Yhteistyökumppanin valinta	"Jos ajatellaan vaikka taloautomaatiojärjestelmää, niin sehän me ollaan tietenkin määritelty sillä tavalla, että sillä palveluntarjoajalla on tietyn tasoiset serveripalveluntuottajat." (C)

Haastateltavien kommentit (taulukko 3) kuvastavat tarvetta kokonaisuuden ymmärtämiselle jo hankintavaiheessa. Kiinnostavaa on, että haastatteluissa nostettiin esille myös hankinnan osaaminen yleisesti rakennuksen järjestelmäympäristöön liittyen. Yleisesti ottaen tehokkaan hankinnan optimoinnissa havaittiin osaoptimoinnin kaltaisia riskejä, jolloin hyvin optimoitu yksittäinen hankinta voi aiheuttaa haasteita kokonaisuuden kannalta.

4.1.4 Vaatimukset ja toimittajan ohjeistus

Hankinnan vaiheessa keskeiseksi koettu vaatimusmäärittelykyvykkyys sekä toiminnan ohjeistaminen nousivat luontevasti yhdeksi jatkuvuudenhallintaan ja sen parhaisiin käytäntöihin liittyväksi erilliseksi kokonaisuudeksi. Mainintoja teemaan liittyen oli yhteensä 23 kpl (n = 13). Teeman alla erillisiä aihealueita oli yhteensä kymmenen. Näiden maininnat kappalemääräisenä sekä prosenttiosuuksina on esitetty kuvassa 11. Keskeisin aihe oli ohjeistus (8 mainintaa, 35 % teeman aiheista). Tämän lisäksi merkittäviä olivat kriittisyysluokitus (4, 17 %) ja prosessien kuvaus (3, 13 %) sekä kategorisointi (2, 9 %). Näiden lisäksi yksittäisiä mainintoja saatiin seuraavista (jokainen erikseen 1, 4 %): auditointi, häiriönsietokykyluokitus, käyttövarmuusluokitus, regulaatio, valvonta ja yhteiset linjaukset.



Kuva 11. Jatkuvuudenhallinnan parhaat käytännöt / Vaatimukset ja ohjeistus (n = 13)

Kuvan 11 aihealueet kategorisoitiin haastatteluista saatujen tietojen pohjalta. Jatkuvuudenhallintaa tukevista vaatimuksiin ja toimittajan ohjeistamiseen liittyvistä parhaista käytännöistä (kuva 11) painottivat vastaajat yli neljänneksessä maininnoista kriittisyysluokittelua sekä kategorisointia. Ohjeistuksen tärkeyttä sekä tilaajan että palveluntoimittajan näkökulmasta pidettiin kuitenkin kaikkein tärkeimpänä aiheena muiden aiheiden jäädessä yksittäisiksi maininnoiksi. Kommentteja aihealuekohtaisesti on listattu taulukkoon 4.

Taulukko 4. Sitaatit vaatimuksiin ja toimittajan ohjeistukseen liittyen

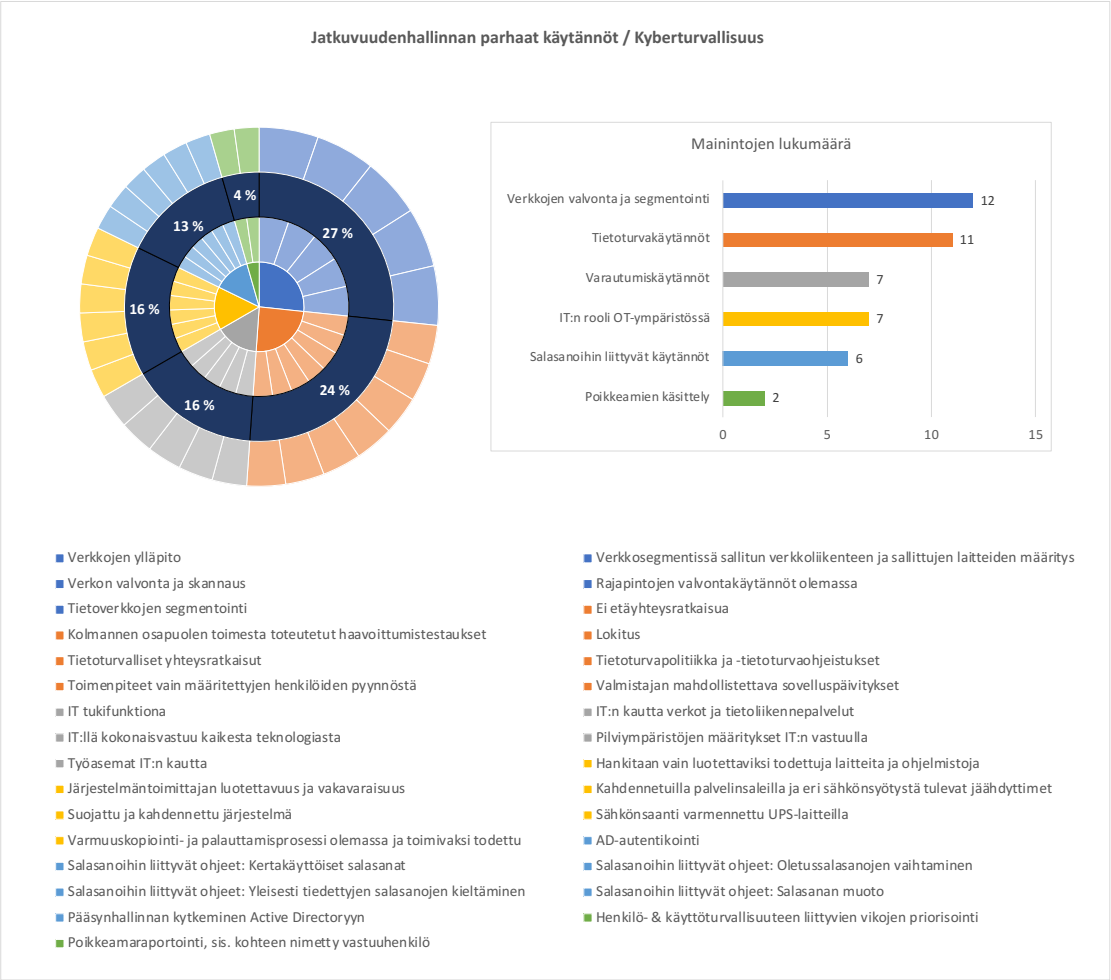
Kategoria	Sitaatti
Auditointi	"Ainoo mikä on osoittautunut semmoseks, et se oikeesti toimii, on auditoinnit." (P)
Häiriönsietokyky-luokitus	"(Pitäisi käyttää) finanssialan toimesta hyväksyttäviä laitteita. Niiden luokitukset ei ota (kuitenkaan) kantaa ollenkaan siihen häiriönsietokykyyn. Ton tyyppisessä energiakatkoksessa

	tai jonkunlaisessa palvelunestohyökkäyksessä tai muuten sabotoinnissa turvaudutaan tällaisiin asioihin. Ja sit siihen on rakennettu jonkunlainen palvelu, mikä nopeuttaa tai pystyy määritteleen, et miten ne saadaan kuntoon joko varajärjestelmillä tai korjaamalla." (K)
Kategorisointi	"Etsitään semmonen yks perusmalli, minkä pitäis kattaa vähintään 85% kaikista tarpeista. Elikkä tarpeeksi tehokas, että sen vois tökätä vähän niinku mihin tahansa ja se ajaa asiansa. Se on nyt sitten tulossa uudelleen tämä, mikä ehkä meni pois muodista eli nää varaosavarastot." (O)
Kriittisyysluokitus	"Suojaus ja varmennus kriittisyyden mukaan. Eli mikä on business impacti siihen, että mitä menetetään." (J)
Käyttövarmuusluokitus	"Käyttövarmuus. kun meillä tarvii olla 99% ja jotain käyttövarmuus." (A)
Ohjeistus	"Meil on hyvin tarkat ohjeet siitä, että kun esimerkiks kulunvalvontajärjestelmät, kun ne otetaan käyttöön tai asennetaan, niin nämä, nämä ja nämä pitää olla tehty näin, näin ja näin. Käyttäjätunnukset ja salasanat pitää olla tätä muotoa, koska sit kun me otetaan ne kiinni taustajärjestelmiin, niin me ne vaihdetaan. Siin on ihan step by step asennusohjeet, mitkä ne käy luovutuspöytäkirjassa läpi, että nää on tehty. Sitten me tarkistetaan ne tekemällä pistotarkastuksia." (P)
Prosessikuvaus	"Siihen täytyy liittää ehdottomasti se, että miten ne laitteet on varmuuskopioitu, korvattavissa ja vaihdettavissa ja kuka ne tekee ja niin poispäin, että on suunnitelmat olemassa. " (G)
Regulaatio	"Ehkä se koko ekosysteemi siellä taustalla tulis niin kuin kenties tämmöisen regulaation kautta varmasti pikkuhiljaa hoidettua paremmin, mä oletan, koska silloin se koskee kaikkia yleisesti" (I)
Valvonta	"Taloa ohjaa ja valvoo käytännössä tietokoneet, niin ne tarvii samanlaista ylläpitoa ja valvontaa ja tarkastusta, kuten muutkin IT-ympäristön järjestelmät." (J)
Yhteiset linjaukset	"Konsernilähtöiset toimintaohjeet" (C)

Taulukon 4 kommenteista voi havaita sekä tavoitteellisuuden sekä selkeyden tärkeyden ohjeistamiseen liittyen, mutta myös joiltakin osin taustalta voi havaita myös haasteita. Selkeästi haastatellut pitivät tässä yhteisiä linjauksia tärkeinä, mutta toisaalta nousi esille myös regulaation toimialaa velvoittava ja päätöskykyä helpottava rooli.

4.1.5 Kyberturvallisuus

Jatkuvuudenhallinnan parhaista käytännöistä kyberturvallisuuteen liittyviä mainintoja oli kaiken kaikkiaan 45 kappaletta (n = 13). Maininnat jakautuivat kuuden eri aihealueen alle. Mainintojen esiintyminen kappaleina sekä prosentuaalisina osuuksina on esitetty kuvassa 12. Verkkojen valvonta ja segmentointi (12 mainintaa, 27 % teeman aiheista) ja tietoturvakäytännöt (11, 24 %) nousivat keskeisimmiksi aiheiksi kyberturvallisuuteen liittyen. Muita aiheita olivat IT:n rooli OT-ympäristössä sekä varautumiskäytännöt kumpikin seitsemällä maininnalla (16 %), salasanoihin liittyvät käytännöt kuudella (13 %) ja poikkeamien käsittely kahdella maininnalla (4 %).



Kuva 12. Jatkuvuudenhallinnan parhaat käytännöt / Kyberturvallisuus (n = 13)

Kuvan 12 aihealueet kategorisoitiin haastatteluista saatujen tietojen pohjalta tutkimuksen kannalta loogisiksi kokonaisuuksiksi. Kyberturvallisuus tunnistettiin tärkeäksi osaksi rakennuksen järjestelmäympäristön jatkuvuudenhallintaan liittyviä teemoja. Maininnat olivat varsin teknisiä sekä palveluntoimittajia velvoittavia. Myös osaamisen kehittämisen tarve on tunnistettavissa selkeästi sekä palveluiden tilaajan että toimittajan puolella. Haastateltujen sitaatteja teemaan liittyen on lueteltu taulukossa 5.

Taulukko 5. Sitaatit kyberturvallisuuteen liittyen

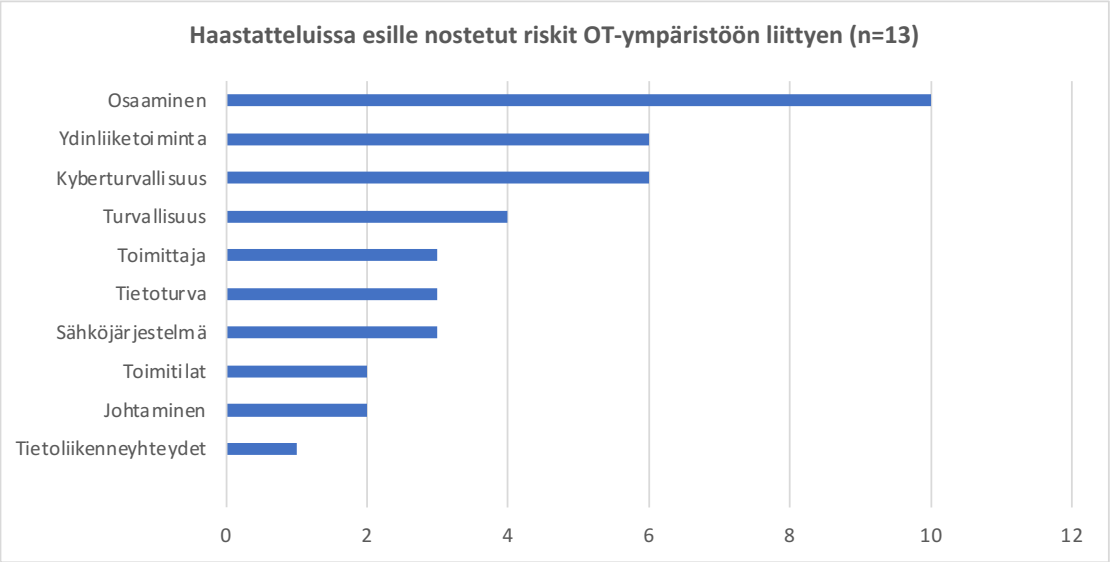
Kategoria	Sitaatti
IT:n rooli OT-ympäristössä	"IT:n rooli tulee pysymään mun mielestä jonkun aikaan vielä sillä tavalla, et se on avustavassa roolissa tässä ympäristössä ja auttaa sen arkkitehtuurin kuvaamisessa ja tota tarjoaa niitä perinteisiä IT-tyyppisiä palveluita siihen ympäristöön, mitä tarvitaan. Verkot, niiden segmentoinnit, tietoliikennepalvelut, ja ehkä sit sen ympärille vielä mitä mikä on tulossa niin nimenomaan nää julkipilvi tai yksityiset pilvet ja niihin liittyvät määritykset, miten niitä hankitaan." (F)
Poikkeamien käsittely	"Mä näkisin, että kiinteistössä, jossa on ihmisiä töissä tai oleskelee kauppakeskuksessa, niin siel pitäis herkällä korvalla korjata jopa pikkasen enemmän kuin et haluaako kiinteistö ottaa vastuun niistä kuolleista, jotka siellä tapahtuu sitten sen seurauksena että ei ole korjattu." (A)

Salasanoihin liittyvät käytännöt	"Se on vasta niinkun hiljattain tullu, että sä et voi enää käyttää admin/adminia tai admin/passwordia tai root/rootia ja vastaavia. Kirjautuessa ekan kerran se pakottaa tekemään käyttäjätunnukset ja salasanat, jotka on tietyn mittaisia ja näin poispäin. Sehän ei tietenkään poista sitä ongelmaa, et sama käyttäjätunnus ja salasana on niis kaikissa laitteissa oli se asiakkuus mikä vaan." (P)
Tietoturvakäytännöt	"Mitä enemmän niitä reikiä teet siihen järjestelmään, sitä enemmän sul pitää olla tietoa, että kuinka se turvallisesti tehdään, ettei sinne kukaan pääse tunkeutumaan." (H) "Ylläpidollisesti mitään päivityksiä (ei saa tehtyä) tai tällaista haavoittuvaisuuksia sieltä ei kovin jouheasti saa poistettu eli tärkeää on, että se on turvattu se ympäristö muuten." (N)
Varautumiskäytännöt	"Siihen täytyy liittää ehdottomasti se, että miten ne laitteet on varmuuskopioitu, korvattavissa ja vaihdettavissa ja kuka ne tekee ja niin poispäin, että on suunnitelmat olemassa." (N)
Verkkojen valvonta ja segmentointi	"Kyberturvan puolesta voin sanoa, et ihan ensimmäisenä on segmentointi. Et taloautomaatio tai mikä tahansa automaatioympäristö on erillään muusta verkosta, et se on oma kokonaisuutensa." (N) "OT-verkon baselinen määritys. Toisin kuin toimistoverkko, missä kohisee, vaikka minkänäköstä liikennettä, niin OT-ympäristössä pitäisi olla hyvinkin vakio, että mitä siellä liikkuu. Ja se pitäis olla määritettynä." (N)

Taulukon 5 sitaateista voi tunnistaa tarpeen hyödyntää IT:n parhaita käytäntöjä teknisen ympäristön hallintaan liittyen. Samalla voi havaita, että OT-järjestelmille sallitaan sellaisia puutteita, jotka jo IT:ssä ratkaisun hankintavaiheessa suljettaisiin pois. Kyberturvallisuuteen liittyvissä keskusteluissa nousivatkin esille selkeästi myös kyberturvallisuuden prosessia tukeviin teemoihin liittyvät haasteet, joita on käsitelty kohdassa 4.2.5.

4.1.6 Tunnistetut riskit

Haastatellut nostivat teemaan liittyen proaktiivisesti esille riskejä, joiden todennäköisyyttä OT-ympäristön huolellisella jatkuvuudenhallintaprosessilla voidaan vähentää. Tutkimuksen kannalta riskien tunnistaminen on tärkeää jatkuvuudenhallinnan keinojen tunnistamisen ja samalla jatkuvuudenhallinnan työkalun kuvaamisen näkökulmasta. Yksittäisiä riskejä mainittiin yhteensä 40, jotka jakautuivat kuvan 13 mukaisesti kymmenen eri teeman alle. Osaamisen puuttumisen koettiin aiheuttavan eniten riskejä (kymmenen mainintaa) ja kyberturvallisuuteen ja ydinliiketoimintaan liittyviä riskejä mainittiin kumpiakin kuusi. Turvallisuuteen liittyviä riskejä mainittiin neljä. Sähköjärjestelmään, tietoturvaan sekä toimittajiin liittyviä riskejä mainittiin kolme. Johtamiseen ja toimitiloihin liittyen mainittiin kumpaankin kaksi riskiä ja tietoliikenneyhteyksiin yksi.



Kuva 13. Haastatteluissa esille nostetut riskit rakennuksen OT-ympäristöön liittyen (n = 13)

Kuvasta 13 voi havaita, että osaamiseen liittyvät riskit ovat nousseet esille useimmin. Osaaminen ja sen kehittäminen olikin tutkimuksessa selkeästi kaikki teemat läpileikkaava kokonaisuus. Jos turvallisuutta käsitellään yhtenä kokonaisuutena sisältäen kyberturvallisuuden, yritysturvallisuuden sekä tietoturvallisuuden, on tunnistettujen riskien määrä suurin (yhteensä 13 eri mainintaa).

4.2 Järjestelmäympäristö kokonaisuutena tilastollisen tutkimuksen näkökulmasta

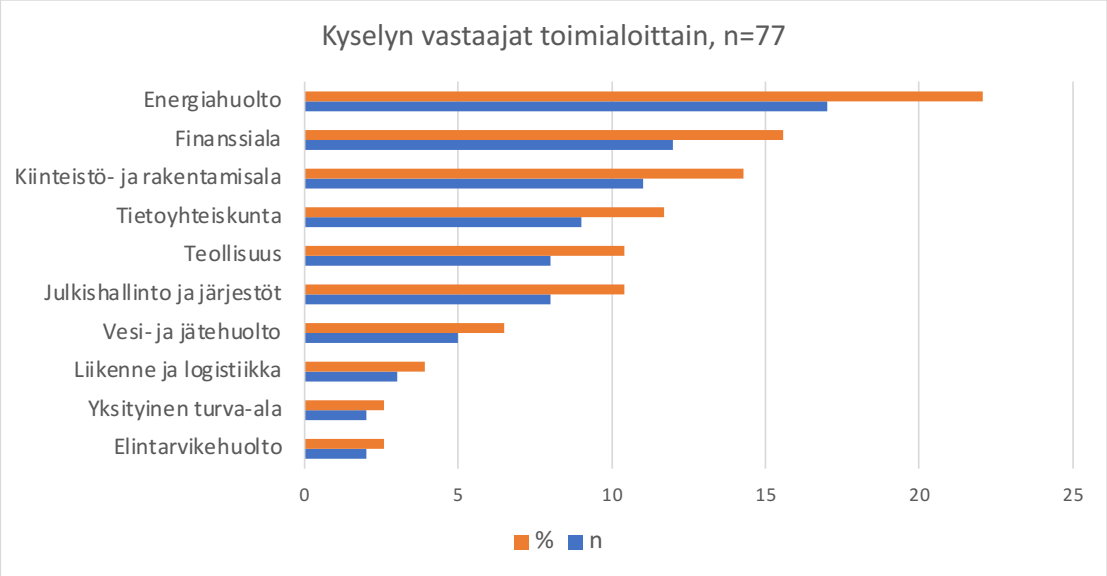
Tässä luvussa käsitellään tilastollisen tutkimusosan tulokset tutkimushypoteesin asettamien rajausten valossa. Jatkuvuudenhallintaan sekä resilienssiin liittyvien käytäntöjen sekä jatkuvuudenhallinnan maturiteettikokemuksen väliset mahdolliset riippuvuudet on esitetty Pearsonin korrelaatiokertoimen sekä siihen liittyvien tulkintojen avulla. Vastaukset on järjestetty taulukoissa keskiarvon perusteella pienimmästä suurimpaan. Kuvat osoittavat prosenttiosuudet kunkin valitun vastausvaihtoehdon osalta. Jokaiseen tässä luvussa käsiteltyyn kysymykseen on vastattu Likertin asteikon mukaisesti valitsemalla väittämät väliltä 1–5 taustatietokysymykset pois lukien. Organisaatioiden maturiteettia resilienssin käsittelyyn liittyen arvioitiin verraten tuloksia Björckin ym. (2015, 315) malliin ”Cyber resilience aspects and principles”, jota resilienssiin liittyvät väittämät mukailivat. Jatkuvuudenhallinnan osalta saatuja tuloksia peilattiin Kosmowskin ym. (2022, 12) liiketoiminnan jatkuvuudenhallinnan viitekehykseen (kuva 3). Näiden tietojen avulla pyrittiin todentamaan tarve rakennuksen

OT-ympäristön jatkuvuudenhallinnan kehittämiselle sekä sitä tukevalle työkalulle. Huolimatta siitä, että määrällinen tutkimus toteutettiin kuvailevana tutkimuksena tukien laadullista kartoittavaa tutkimusta, hyödynnettiin kuitenkin tunnuslukuja aineiston analyysissä.

4.2.1 Taustatiedot

Kyselytutkimuksen taustatietoina kysyttiin vastaajan organisaation toimialaa ja liikevaihtoa sekä roolia kiinteistö- ja rakentamisalalla. Kysytyistä taustatiedoista toimiala toimi luokittelevana piirteenä. Edellä mainittujen lisäksi kysyttiin, ovatko yrityksen / organisaation käytössä olevat rakennukset jonkin tahon vastuulla kyseisessä organisaatiossa. Tämä kysymys luokitteli vastaajat kahteen eri ryhmään, sillä kolmanteen vaihtoehtoon ei tullut yhtään vastausta. Tutkimuksen kannalta yllättävää on, että 25 % (n = 64) vastasi, ettei vastuutahoa rakennuksiin liittyen ollut erikseen nimetty.

Kyselytutkimukseen vastasi yhteensä 77 henkilöä (kuva 14), joista 13 oli Kiinteistönomistajat ja rakennuttajat Rakli ry:n Uudistuminen ja digitalisaatio -teemaverkoston jäseniä. Raklin vastaajien osalta vastauksia hyödynnettiin ainoastaan avointen kysymysten sekä jatkuvuudenhallinnan työkaluun ja koulutustapoihin liittyvien kysymysten osalta. Verrokkiryhmänä tätä ei hyödynnetty, koska vastaajamäärä jäi varsin pieneksi. Tutkimukseen vastausprosentti oli noin 13 (64 vastaajaa) laskettuna arvioidun otosjoukon koon (500) mukaan.



Kuva 14. Kyselyn vastaajat toimialoittain (n = 77)

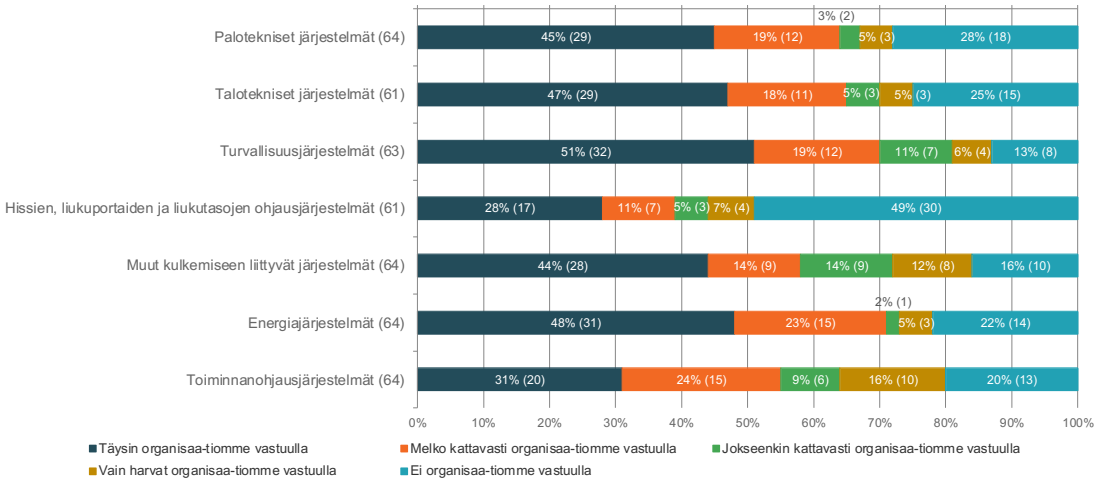
Kun kaikkien vastaajien toimialat luokitellaan Huoltovarmuuskeskuksen toimialaluokituksen (HVK s.a.) mukaisesti (kuva 14), voidaan todeta yhtä lukuun ottamatta kaikkien toimialojen olevan sekä laadullisessa että määrällisessä tutkimuksessa edustettuna; Ainoastaan terveydenhuolto jäi vaille edustusta niin kyselytutkimuksessa kuin myös haastatteluissakin.

Vajaa 80 % vastaajista (n = 64) koki, että organisaatiolla on rooli rakennuksen käyttäjänä (Rakli: 31 % n = 13), vaikkakin olisi voinut ajatella jokaisen olevan jollakin tavalla rakennuksen käyttäjä. Hieman alle 65 % vastaajista toimi rakennuksen omistajan roolissa (Rakli: 77 %). Rakennuksen ylläpitäjiä oli 25 % (Rakli: 54 %) ja rakennuttajia lähes 22% (Rakli: 77 %). Muita tunnistettuja rooleja olivat rahoittaja ja suunnittelija (kumpikin noin 10 %, Rakli: 0 % ja 8 %) sekä järjestelmäntoimittaja, laitetoimittaja, vakuutusliike, urakoitsija ja konsultti (Rakli/konsultti: 15 %, muut 0 %).

Noin 25 % (n = 64) vastaajista kuului organisaatioon, jonka liikevaihto on yli 0,5 miljardia (Rakli: 23 %, n = 13) ja reilu 25 % organisaatioon, jonka liikevaihto on välillä 50–500 miljoonaa euroa (Rakli: 31 %). Noin 25 % jäi välille 10–50 miljoonaa (Rakli: 31 %) ja reilu 20 % kuului ryhmään, jonka liikevaihto on väillä 1–10 miljoonaa (Rakli: 15 %). Loput vastaajista työskentelivät organisaatioille, joiden liikevaihto on alle miljoona euroa (Rakli: 0 %).

4.2.2 Järjestelmien kriittisyyden yhteys jatkuvuudenhallintaan ja resilienssiin

Vastaajat arvioivat kokemusta organisaationsa vastuusta organisaation toiminnan kannalta kriittisten rakennusten järjestelmiin liittyen Likert-asteikolla täysin (1), melko kattavasti (2), jokseenkin kattavasti (3), vain harvat (4) ja ei (5) organisaatiomme vastuulla. Vastaukset on esitetty kuvassa 15 prosenttiosuuksina ja taulukkoon 6 on koottu tilastollisia tunnuslukuja järjestettynä keskiarvon mukaan pienimmästä suurimpaan.



Kuva 15. Organisaation vastuu järjestelmäkokonaisuuteen liittyen eli vastuu varmistaa päätösvaltaisena toimijana niiden lainmukaisuus ja olemassaolo sekä toimivuus ja kehittäminen (n = 64)

Vastaajista 51 % (n = 63) koki, että turvallisuusjärjestelmät ovat täysin oman organisaation vastuulla (kuva 15). Tämän osalta vastaajat olivat eniten samaa mieltä (s = 1,43) (taulukko 6). Lähes viidesosa vastaajista totesi kuitenkin, että turvallisuusjärjestelmistä vain harvat järjestelmät ovat tai järjestelmät eivät ole lainkaan organisaation vastuulla. Vastaajista odotetusti noin 70 % (n = 64) totesi energiajärjestelmien sekä myös turvallisuusjärjestelmien olevan täysin tai melko kattavasti organisaation vastuulla. Hissien osalta 49 % (n = 61) vastaajista koki, ettei hissien, liukuportaiden ja liukutasojen järjestelmät ole lainkaan organisaation vastuulla. Saadut tulokset kertovat, että yleisesti ottaen turvalliset ja terveelliset olosuhteet ovat organisaatioille varsin tärkeitä. Hissiä taas ei pidetä organisaation toiminnalle niinkään välttämättömänä. Kokonaisuuden hallinnan kannalta hissi toimii tässä digitaalisen resilienssin näkökulmasta riskifaktorina, mikäli se on yhdistetty esimerkiksi kulunvalvonnan kokonaisuuteen. Tulokset eivät kerro siitä, miten paljon osaamista organisaatioissa on ulkoistettu tai miten paljon sitä on organisaatiolla itsellään rakennuksen OT-ympäristön kokonaisuuden hallintaan tai johtamiseen liittyen.

Taulukosta 6 voidaan todeta vastaajien lukumäärän perusteella, että kysymykset oli asetettu niin, että niihin oli luontevaa vastata. Tämän kertoo korkea vastaajien lukumäärä suhteessa koko kyselyn vastaajamäärään (n_{alin} = 61). Keskiarvo ei tässä anna luotettavaa kuvaa vastauksista, sillä numerot kuvasivat sanallista arviota, vaikkakin keskihajonta kuvaa vastausten varsin suurta hajontaa hyvin. Parhaiten vastauksia kuvaa mediaani, joka osoittaa varsin hyvin

kuvan 15 tilanteen osoittamalla, mikä sanallisista vastausvaihtoehdoista osuu keskimmäiseksi.

Taulukko 6. Organisaation vastuu järjestelmäkokonaisuuteen liittyen eli vastuu varmistaa päätösvaltaisena toimijana niiden lainmukaisuus ja olemassaolo sekä toimivuus ja kehittäminen

Muuttuja	n	k.a.	Luottamusväli	Md	s	s^2
Turvallisuusjärjestelmät (esim. murtosuojajärjestelmä, kulunvalvonta- ja kameravalvontajärjestelmä, aluevalvontajärjestelmä, turvallisuusvalvomojärjestelmä)	63	2,11	1,76 – 2,46	1	1,43	2,04
Energiajärjestelmät (esim. sähkö, lämpö ja varavoima)	64	2,28	1,88 – 2,68	2	1,62	2,62
Talotekniset järjestelmät (esim. rakennusautomaatiojärjestelmä, kylmäjärjestelmä ja valaistuksen ohjausjärjestelmä, LVIA, talotekniikkavalvomojärjestelmä, energiatehokkuusjärjestelmä, olosuhteidenseurantajärjestelmä)	61	2,41	1,99 – 2,83	2	1,68	2,81
Muut kulkemiseen liittyvät järjestelmät (esim. vierailijahallintajärjestelmä, kilpitunnistusjärjestelmä, porttipuhelinjärjestelmä, pysäköinninohjausjärjestelmä, sähköautojen, trukkien ym, latausjärjestelmät, ovien, porttien ja puomien ohjausjärjestelmät)	64	2,42	2,05 – 2,80	2	1,53	2,34
Palotekniset järjestelmät (esim. paloilmoitinjärjestelmä, sprinklerijärjestelmä, savunpoistoluukkujen ohjausjärjestelmä, äänievakuointijärjestelmä, turvavalaistusjärjestelmä)	64	2,52	2,09 – 2,94	2	1,73	2,98
Toiminnanohjausjärjestelmät (esim. jätehuollon ja kierrätyksen järjestelmät, puhtaanapidon järjestelmät, toimitilapalveluiden järjestelmät, AV-järjestelmät, ravintolapalveluiden järjestelmät, smart office -järjestelmät)	64	2,70	2,32 – 3,08	2	1,55	2,40
Hissien, liukuportaiden ja liukutasojen ohjausjärjestelmät	61	3,38	2,93 – 3,82	4	1,78	3,17

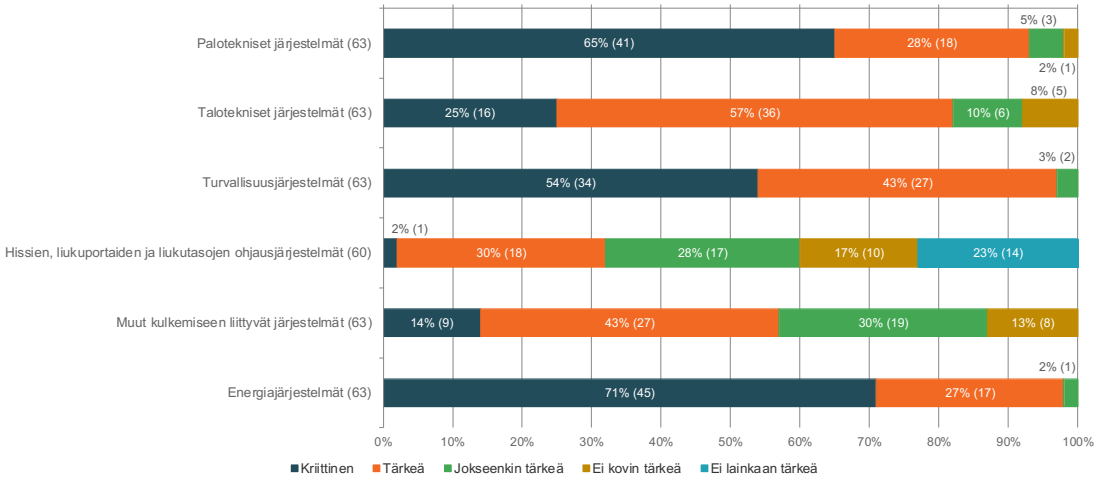
n = vastausten lukumäärä
k.a. = keskiarvo
Md = mediaani
s = keskihajonta
s^2 = varianssi

Tulosten mukaan, mikäli vaatimusmäärittelyprosessi tai hankinnan prosessi on ulkoistettu (taulukko 8), organisaatiolla ei nähdä olevan niinkään merkittävää vastuuta järjestelmäkokonaisuuteen liittyen (taulukko 6). Kääntäen tämä voi tarkoittaa sitä, että mitä vahvemman vastuun organisaatiolla koetaan olevan järjestelmistään, sitä epätodennäköisemmin vaatimusmäärittelyvaihe tai hankintaprosessi ulkoistetaan. Esimerkkinä koska kolmasosa vastaajista ei koe organisaation olevan vastuussa paloteknisestä ympäristöstä, voidaan tulkita, että siihen liittyviä prosesseja on suoraviivaista ulkoistaa. Kaikista vastaajista lähes 30 % totesi, että järjestelmien vaatimusmäärittely *on* ulkoistettu (täysin tai osittain) ja hankinnan on ulkoistanut reilu neljännes. Esimerkiksi energiajärjestelmien vaatimusmäärittely näyttäisi olevan vähemmän tärkeä, kun vaatimusmäärittely on ulkoistettu ($n = 61$, $r_p = -0{,}31$, $p = 0{,}014$).

Mikäli järjestelmiin liittyvä hankinta on ulkoistettu, ei organisaatiossa koeta olevan kovinkaan merkittävää vastuuta järjestelmiin liittyen (taulukot 6 ja 8). Esimerkiksi hankintojen ulkoistaminen näyttää aineiston perusteella madaltavan turvallisuusteknisten ($n = 61$, $r_p = -0{,}43$, $p = 0{,}001$), taloteknisten ($n = 61$, $r_p = -0{,}6$, $p = 0{,}000$), paloteknisten ($n = 64$, $r_p = -0{,}55$, $p = 0{,}000$) ja energiajärjestelmien ($n = 64$, $r_p = -0{,}54$, $p = 0{,}000$) määrittelyn vastuuta. Tulos vaikuttaa hankinnan käytäntöjen näkökulmasta loogiselta eli mikäli vastuu järjestelmistä koetaan heikoksi, ulkoistetaan todennäköisesti järjestelmän vaatimusmäärit-

tely- sekä hankintaprosessit. Tutkimuksen mukaan yli 35 % (n = 61) oli ulkoistanut vähintäänkin jokseenkin kattavasti OT-järjestelmien vaatimusmäärittelyn ja kolmannes hankintaprosessin. Tämän lisäksi vajaa 25% (n=61) vastanneista totesi olevansa täysin tai jokseenkin eri mieltä sen kanssa, että liiketoimintaa ja järjestelmiä käsiteltäisiin yhteen liitettynä kokonaisuutena. Ainakin näiltä osin voidaan saatujen tietojen pohjalta organisaation OT-ympäristön olevan siiloutunut. Myös Sinopoli (2016, 162) toteaa tutkimuksessaan OT-ympäristöön toteutuvan siilomaisia rakenteita.

Vastaajat arvioivat organisaation käytössä olevien rakennuksen toimintaa ohjaavien järjestelmien kriittisyyttä niin ikään Likert-asteikolla kriittinen (1), tärkeä (2), jokseenkin tärkeä (3), ei kovin tärkeä (4), ei lainkaan tärkeä (5). Vastaajat pitivät energiaan sekä yleisesti turvallisuuteen liittyviä järjestelmiä selkeästi kriittisimpinä (kuva 16) ratkaisuina kussakin mediaanin ollessa 1 eli kriittinen (taulukko 7). 71 % (n = 63) vastaajista koki energiajärjestelmät kriittisiksi ja 27 % tärkeiksi (kuva 16). Loput vastaajista koki energiajärjestelmät jokseenkin tärkeiksi. 65 % (n = 63) koki palotekniset järjestelmät kriittisiksi ja 28 % tärkeiksi, mutta 2 % ei kokenut paloteknisiä järjestelmiä kovin tärkeiksi. 97 % (n = 63) vastaajista koki turvallisuusjärjestelmät kriittisiksi (54 %) tai tärkeiksi (43 %) ja loput jokseenkin tärkeiksi. Hissit, liukuportaat ja liukutasot olivat kriittisiä vain kahdelle prosentille (n = 60) vastaajista ja 40 % vastaajista vastasi niiden olevan ei kovin tai ei lainkaan tärkeitä organisaatiolle. 82 % (n = 63) vastaajista piti taloteknisiä järjestelmiä kriittisinä tai tärkeinä ratkaisuina omalle organisaatiolleen.



Kuva 16. Organisaation käytössä olevien rakennusten toimintaa ohjaavien järjestelmien kriittisyys (n=63)

Yleisesti ottaen vastaajat olivat väittämissä varsin samanmielisiä (0,50 ≤ s ≤ 1,18) (taulukko 7). Tuloksista voi tulkita, että energiajärjestelmien (k.a. = 1,30, Md = 1) kaiken mahdollistava rooli on ilmeinen käytännössä jokaiselle organisaatiolle. Samoin turvallisuus niin paloturvallisuuden (k.a. = 1,43, Md = 1) kuin fyysisenkin turvallisuuden (k.a. = 1,49, Md = 1) näkökulmasta ovat toiminnalle välttämättömiä (taulukko 7). Talotekniset järjestelmät koetaan myös (k.a. = 2,00, Md = 2) tärkeiksi, joskin lähes viidesosalle kokonaisuus ei ole niinkään tärkeä. Tämä voi johtua organisaation roolista toimitilassa, jolloin jokin muu toimija vastaa terveellisestä ja turvallisesta toimintaympäristöstä ja sisäilmastosta. Hissien rooli pääasiassa ei niin välttämättömänä rakennuksen ominaisuutena näkyy selkeästi tilastosta (k.a. = 3,3, Md = 3).

Taulukosta 7 voidaan todeta vastaajien lukumäärän perusteella, että kysymykset oli asetettu helposti vastattaviksi, joskaan yhteenkään kysymykseen ei saatu vastausta jokaiselta koko kyselyyn vastanneelta (n_{alin} = 60). Keskiarvo ei anna luotettavaa kuvaa vastauksista numeroiden kuvatessa sanallista arviota. Keskihajonta oli varsin pieni lähes jokaisessa kysymyksessä, joka tarkoittaa sitä, että vastaajat olivat varsin samanmielisiä vastauksissaan. Parhaiten vastauksia kuvaa mediaani, joka osoittaa varsin hyvin kuvan 16 tilanteen osoittamalla, mikä sanallisista vastausvaihtoehdoista osuu keskimmäiseksi.

Taulukko 7. Organisaation käytössä olevien rakennusten toimintaa ohjaavien järjestelmien kriittisyys

Muuttuja	n	k.a.	Luottamusväli	Md	s	s^2
Energiajärjestelmät (esim. sähkö, lämpö ja varavoima)	63	1,30	1,18 – 1,42	1	0,50	0,25
Palotekniset järjestelmät (esim. paloilmoitinjärjestelmä, sprinklerijärjestelmä, savunpoistoluukkujen ohjausjärjestelmä, äänievakuointijärjestelmä, turvavalaistusjärjestelmä)	63	1,43	1,26 – 1,59	1	0,67	0,44
Turvallisuusjärjestelmät (esim. murtosuojajärjestelmä, kulunvalvonta- ja kameravalvontajärjestelmä, aluevalvontajärjestelmä, turvallisuusvalvomojärjestelmä)	63	1,49	1,35 – 1,63	1	0,56	0,32
Talotekniset järjestelmät (esim. rakennusautomaatiojärjestelmä, kylmäjärjestelmä ja valaistuksen ohjausjärjestelmä, LVIA, talotekniikkavalvomojärjestelmä, energiatehokkuusjärjestelmä, olosuhteidenseurantajärjestelmä)	63	2,00	1,80 – 2,20	2	0,82	0,68
Muut kulkemiseen liittyvät järjestelmät (esim. vierailijahallintajärjestelmä, kilpitunnistusjärjestelmä, porttipuhelinjärjestelmä, pysäköinninohjausjärjestelmä, sähköautojen, trukkien ym, latausjärjestelmät, ovien, porttien ja puomien ohjausjärjestelmät)	63	2,41	2,19 – 2,63	2	0,89	0,79
Hissien, liukuportaiden ja liukutasojen ohjausjärjestelmät	60	3,30	3,00 – 3,60	3	1,18	1,40

n = vastausten lukumäärä
k.a. = keskiarvo
Md = mediaani
s = keskihajonta
s^2 = varianssi

Jatkuvuudenhallinnan prosessit (taulukko 8) oli vastaajien mukaan kuvattu todennäköisimmin siinä tapauksessa, että palotekniset (n = 61, r_p = 0,31, p = 0,017), turvallisuus- (n = 61, r_p = 0,31, p = 0,018) tai energiajärjestelmät (n =

61, $r_p = 0,35$, $p = 0,008$) koettiin kriittisiksi (taulukko 7). 54 % (n = 57) vastanneista totesi jatkuvuudenhallinnan prosessien olevan kuvattu täysin tai osittain. Vastaajista yli 98 % (n = 63) koki energiajärjestelmät tärkeiksi tai kriittisiksi (k.a. = 1,30, Md = 1). Paloteknisten (k.a. = 1,43, Md = 1) ja turvallisuusjärjestelmien (k.a. = 1,49, Md = 1) osalta prosenttiosuudet olivat 93 % (n = 63) ja 97 % (n = 63). Koska prosenttiosuudet ovat lähellä sataa, on tulokseen suhtauduttava varauksella. Muiden järjestelmien osalta tätä jatkuvuudenhallinnan prosessien kuvaamisen ja järjestelmien kriittisyyden välistä yhteyttä ei löytynyt.

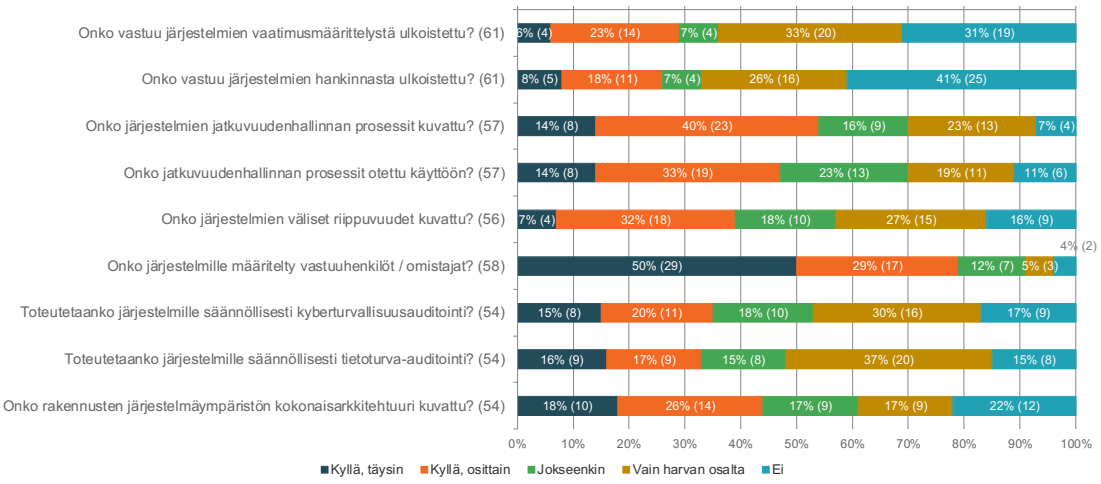
Mikäli organisaatio kokee talotekniset järjestelmät kriittisiksi (taulukko 7), on todennäköisesti ratkaisuarkkitehtuuri toteutettu kerroksellisuutta noudattaen (taulukko 9) ja tällöin kukin toteutettu kerros pystyy toipumaan erikseen mahdollisessa häiriötilanteessa (n = 46, $r_p = 0,32$, $p = 0,031$). 47 % (n = 46) vastaajista oli täysin tai lähes samaa mieltä sen kanssa, että ”Järjestelmien ratkaisuarkkitehtuuri koostuu kerroksista, joista jokainen pystyy toipumaan erikseen yhden suojatun kerroksen sijasta” (kuva 18). Tämän väittämän osalta on otettava kuitenkin tulkinnassa huomioon yllättävän alhainen vastaajamäärä, joka on voinut vaikuttaa lopputulokseen. Muiden järjestelmien osalta tällaista mahdollista yhteyttä ei ollut nähtävissä.

Kun vastaajat kokivat energiajärjestelmät kriittisiksi (taulukko 7) (n = 56, $r_p = -0,37$, $p = 0,004$) häiriöön reagointia ja näistä hallittua toipumista *ei* suosittu (taulukko 9). Tämä on ristiriidassa digitaaliseen resilienssiin liittyvän tarkoituksen ”safe-to-fail” (Björck ym. 2015, 313) kanssa. Käytännössä kyselyyn vastanneiden organisaatiot pyrkivät välttämään häiriötilanteet kokonaan sen sijasta, että reagoisi niihin hallitusti. Yhteyttä muiden järjestelmien osalta ei ollut tunnistettavissa. Kuitenkin mikäli palotekniset (n = 56, $r_p = -0,31$, $p = 0,021$), talotekniset (n = 56, $r_p = -0,29$, $p = 0,036$) tai energiajärjestelmät (n = 56, $r_p = -0.27$, $p = 0,045$) olivat vastaajien mukaan organisaation vastuulla (taulukko 6), suhtauduttiin hallittuun reagointiin kielteisesti ja pyrittiin ennemminkin suojautumaan kyberhäiriötilanteilta (taulukko 9). Vastaajista 32 % (n = 56) oli täysin tai lähes samaa mieltä väittämän ”Tavoitteemme ei ole suojata järjestelmiä täysin kyberhäiriöiltä, vaan ympäristön sallitaan reagoida häiriötilanteisiin ja toipua niistä hallitusti” (kuva 18) kanssa. Vaikka nämä tulokset ovat tilastollisesti merkitseviä, saattoi vastauksiin vaikuttaa myös väittämän sanamuoto,

joka voi alun negaation takia ohjata vastaajan kannalta väärän vastausvaihtoehdon valintaan.

4.2.3 Jatkuvuudenhallinnan käytännöt ja digitaalinen resilienssi

Rakennuksen järjestelmäympäristön jatkuvuudenhallintaan liittyviä käytäntöjä arvioitiin taulukon 8 mukaisesti. Vastaukset annettiin Likert-asteikolla kyllä täysin (1), kyllä osittain (2), jokseenkin (3), vain harvan osalta (4), ei (5). Vastaajat olivat hyvin yksimielisiä vastausten suhteen (1,06 ≤ s ≤ 1,45). Eniten eroavaisuuksia ilmeni kokonaisarkkitehtuuriin liittyvän kysymyksen kohdalla (kuva 17). Kuvan 17 mukaisesti 50 % (n = 58) vastanneista totesi, että kaikille järjestelmille (täysin) on määritelty vastuuhenkilöt / omistajat. 54 % (n = 57) taas mainitsi, että jatkuvuudenhallinnan prosessit on kuvattu täysin tai osittain ja 47 % (n = 57) vastaajista totesi, että ne on otettu käyttöön. Tutkimuksen kannalta merkittävä 44 % (n = 54) totesi, että rakennuksen järjestelmäympäristön kokonaisarkkitehtuuri on kuvattu täysin tai osittain. Tietoturva-auditointi on toteutettu 52 %:n (n = 54) mukaan vain harvan osalta tai ei ollenkaan ja kyberturvallisuusauditoinnin osalta luku on 47 % (n = 54). Vastaajat totesivat, että järjestelmien vaatimusmäärittely on ulkoistettu täysin, osittain tai jokseenkin 36 %:n (n = 61) mukaan ja hankintakin 34 %:n (n = 61) mukaan.



Kuva 17. Järjestelmäympäristön jatkuvuudenhallintaan liittyvät käytännöt (n=61)

Yleisesti ottaen jatkuvuudenhallinnan käytännöissä on tunnistettavissa vastausten perusteella melko paljon kehitettävää perustuen negatiivisten vastausten määrään (vain harvan osalta tai ei). Kuitenkin suurelle osalle järjestelmistä

on kyselyn mukaan määritetty vastuuhenkilöt / omistajat. Tämä ei tulosten perusteella takaa toimivaa jatkuvuudenhallinnan prosessia, mutta auttaa osoittamaan yhteyshenkilön haasteiden kohdatessa. Ulkoistusta koskevien kysymysten osalta pohdinta on tehtävä päinvastaisesti, sillä kyselyn kontekstissa positiivinen vastaus on tulkittava negatiivisesti jatkuvuudenhallinnan ja digitaalisen resilienssin näkökulmasta. Tästä syystä kyseinen kohta sijoittuu ehkä hieman harhaanjohtavasti taulukon 8 hännille.

Taulukon 8 lukujen perusteella voidaan todeta, että kysymykset olivat selvästi edellisiä haastavampia, sillä vastaajien määrä putosi merkittävästi (n_{alin} = 54). Keskiarvo ei anna luotettavaa kuvaa vastauksista numeroiden kuvatessa sanallista arviota. Keskihajontaa oli jonkin verran, joka näkyy parhaiten kuvasta 17. Parhaiten vastauksia kuvaa mediaani, joka osoittaa varsin hyvin kuvan 17 tilanteen osoittamalla, mikä sanallisista vastausvaihtoehdoista osuu keskimmäiseksi. Yhdistämällä mediaani tietoon keskihajonnasta voidaan tulkita tulosten sisältävän jonkin verran hajontaa.

Taulukko 8. Järjestelmäympäristön jatkuvuudenhallintaan liittyvät käytännöt

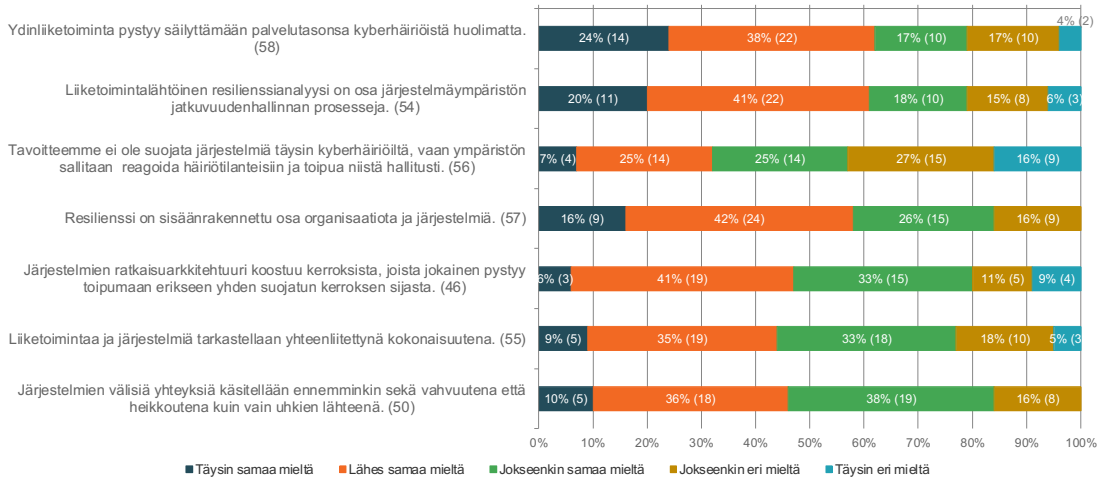
Muuttuja	n	k.a.	Luottamusväli	Md	s	s^2
Onko järjestelmille määritelty vastuuhenkilöt / omistajat?	58	1,83	1,55 – 2,10	1,5	1,06	1,13
Onko järjestelmien jatkuvuudenhallinnan prosessit kuvattu?	57	2,68	2,38 – 2,99	2	1,18	1,40
Onko jatkuvuudenhallinnan prosessit otettu käyttöön?	57	2,79	2,47 – 3,11	3	1,22	1,49
Onko rakennusten järjestelmäympäristön kokonaisarkkitehtuuri kuvattu?	54	2,98	2,60 – 3,37	3	1,45	2,09
Onko järjestelmien väliset riippuvuudet kuvattu?	56	3,13	2,80 – 3,45	3	1,24	1,53
Toteutetaanko järjestelmille säännöllisesti kyberturvallisuusauditointi?	54	3,13	2,77 – 3,49	3	1,33	1,78
Toteutetaanko järjestelmille säännöllisesti tietoturva-auditointi?	54	3,17	2,81 – 3,52	4	1,34	1,80
Onko vastuu järjestelmien vaatimusmäärittelystä ulkoistettu?	61	3,59	3,26 – 3,92	4	1,32	1,75
Onko vastuu järjestelmien hankinnasta ulkoistettu?	61	3,74	3,39 – 4,08	4	1,38	1,90

n = vastausten lukumäärä
k.a. = keskiarvo
Md = mediaani
s = keskihajonta
s^2 = varianssi

Vastaajia pyydettiin arvioimaan digitaalista resilienssiä osana organisaation toimintaa mukaillen Björckin ym. (2015, 315) kehittämiä väittämiä (”Cyber resilience aspects and principles”). Taulukossa 9 on esitetty Likert-asteikolla (täysin samaa mieltä (1), lähes samaa mieltä (2), jokseenkin samaa mieltä (3), jokseenkin eri mieltä (4) ja täysin eri mieltä (5)) tilastolliset tunnusluvut esitettyihin väittämiin liittyen. Kuvassa 18 on kuvattu valitut vastausvaihtoehdot prosentteina. Eniten *eri mieltä* vastaajat olivat taulukon alimmaisen kohdan kanssa eli 43 % (n = 56) oli jokseenkin tai täysin eri mieltä sen suhteen, että tavoitteena *ei ole* suojata järjestelmiä täysin kyberhäiriöiltä. Tämän voi tulkita toisin päin eli vastaajista 43 % pyrkii suojaamaan järjestelmäympäristön täysin

tai lähes täysin kyberhäiriöiltä. Tämä on linjassa kyberturvallisuuden käytäntöjen kanssa, jossa tavoitellaan *fail-safe* -mallia eli tilannetta, jossa tekninen ympäristö pystyy vastustamaan kyberhäiriöitä (Björck ym. 2015, 314). Digitaalisen resilienssin toteutumisen näkökulmasta on kuitenkin keskeisintä mahdollistaa Björckin ym. (2015, 314) mukaan häiriötilanteisiin reagointi kontrolloidulla ja liiketoiminnan jatkuvuuden mahdollistavalla tavalla (*safe-to-fail*). Väittämän muotoilun takia voi olla todennäköistä, että osa vastaajista vastasi tähän väittämään epähuomiossa toisin kuin mitä oli tarkoittanut. Toisaalta vastauksissa voi myös näkyä vastaajien eri näkökulmat teknisen ympäristön ja liiketoiminnan jatkuvuuden suojaamiseen liittyen.

79 % (n = 58) vastaajista arvioi organisaation pystyvän säilyttää ydinliiketoimintansa kyberhäiriöistä huolimatta vähintäänkin jokseenkin hyvin (taulukko 9). Samoin 79 % (n = 54) totesi liiketoimintalähtöisen resilienssianalyysin olevan vähintään jokseenkin osa järjestelmäympäristön jatkuvuudenhallinnan prosesseja. 84 % (n = 57) vastaajista totesi resilienssin olevan vähintäänkin jokseenkin sisäänrakennettu osa organisaation järjestelmiä. Tutkimushypoteesin kannalta kiinnostava 44 % (n = 55) vastaajista totesi olevansa täysin tai lähes samaa mieltä sen kanssa, että liiketoimintaa ja järjestelmiä tarkastellaan yhtenä kokonaisuutena ja vain vajaa neljännes totesi olevansa väittämän kanssa jokseenkin tai täysin eri mieltä.



Kuva 18. Digitaalinen resilienssi osana organisaation toimintaa (n = 59), jossa väittämät on laadittu mukaillen Björckin ym. (2015, 315) kehittämiä väittämiä ”Cyber resilience aspects and principles”.

Digitaalisen resilienssin osalta vastaukset vaikuttavat positiivisilta tutkimushypoteesiin verrattuna. Toisaalta väittämä liittyen järjestelmän suojaamiseen kyberhäiriöltä voi olla tulkittavissa helposti väärin, josta syystä vastausprofiili voi olla kyseisen väittämän osalta hyvin erilainen kuin muissa väittämissä. Tilanne on tulkittavissa myös taulukosta 9, jossa kyseinen väittämä jää keskiarvon mukaan järjestettynä alimmaiseksi korkeimmalla keskiarvolla. Kyseisen väittämän osalta vastauksissa ilmenee eniten erimielisyyttä vastaajien kesken (s = 1,20). Tulosten perusteella joko tilanne on digitaalisen resilienssin osalta varsin hyvä, ulkoiset vaikuttimet ohjasivat yleisesti vastaamaan tietyllä tavalla tai vaihtoehtoisesti kysymyksen asettelu ohjasi vastaajia arvioimaan yleisesti liiketoiminnan resilienssiä. Tähän voi hyvinkin viitata se, että avoimissa kysymyksissä mainittiin nopea tulipalosta toipuminen osoituksena organisaation resilienssistä. Kuten Björck ym. (2015, 311) toteaa, on yksilöille, yrityksille ja yhteiskunnalle luotava yhteinen kieli digitaaliseen resilienssiin liittyen, jotta sitä pystytään tehokkaasti hyödyntämään ja kehittämään.

Resilienssiin liittyvät kysymykset olivat selvästi vastaajille haastavia, sillä vastausmäärät putosivat entisestään (n_{alin} = 46). Keskiarvo anna luotettavaa kuvaa vastauksista, sillä numerot kuvasivat sanallista arviota, vaikkakin varsin tasainen keskihajonta kuvaa vastausten hajontaa hyvin. Parhaiten vastauksia kuvaa mediaani, joka osoittaa varsin hyvin kuvan 15 tilanteen osoittamalla, mikä sanallisista vastausvaihtoehdoista osuu keskimmäiseksi.

Taulukko 9. Resilienssi osana organisaation toimintaa

Muuttuja	n	k.a.	Luottamusväli	Md	s	s^2
Ydinliiketoiminta pystyy säilyttämään palvelutasonsa kyberhäiriöistä huolimatta.	58	2,38	2,09 – 2,67	2	1,14	1,29
Resilienssi on sisäänrakennettu osa organisaatiota ja järjestelmiä.	57	2,42	2,18 – 2,67	2	0,94	0,89
Liiketoimintalähtöinen resilienssianalyysi on osa järjestelmäympäristön jatkuvuudenhallinnan prosesseja.	54	2,44	2,14 – 2,75	2	1,14	1,31
Järjestelmien välisiä yhteyksiä käsitellään ennemminkin sekä vahvuutena että heikkoutena kuin vain uhkien lähteenä.	50	2,60	2,36 – 2,84	3	0,88	0,78
Järjestelmien ratkaisuarkkitehtuuri koostuu kerroksista, joista jokainen pystyy toipumaan erikseen yhden suojatun kerroksen sijasta.	46	2,74	2,44 – 3,04	3	1,04	1,09
Liiketoimintaa ja järjestelmiä on tarkastellaan yhteenliitettynä kokonaisuutena.	55	2,76	2,49 – 3,04	3	1,04	1,07
Tavoitteemme ei ole suojata järjestelmiä täysin kyberhäiriöiltä, vaan ympäristön sallitaan reagoida häiriötilanteisiin ja toipua niistä hallitusti.	56	3,20	2,88 – 3,51	3	1,20	1,43

n = vastausten lukumäärä
k.a. = keskiarvo
Md = mediaani
s = keskihajonta
s^2 = varianssi

Taulukon 9 tulosten perusteella vastaajat olivat väittämistä varsin samanmielisiä (0,88 ≤ s ≤ 1,20). Organisaatiot pyrkivät ensisijaisesti säilyttämään ydinliiketoiminnan palvelutason kohdatuista häiriötilanteista huolimatta (k.a. = 2,38, Md = 2). Tätä tukee prosesseihin sekä teknisiin ratkaisuihin sisäänrakennettu

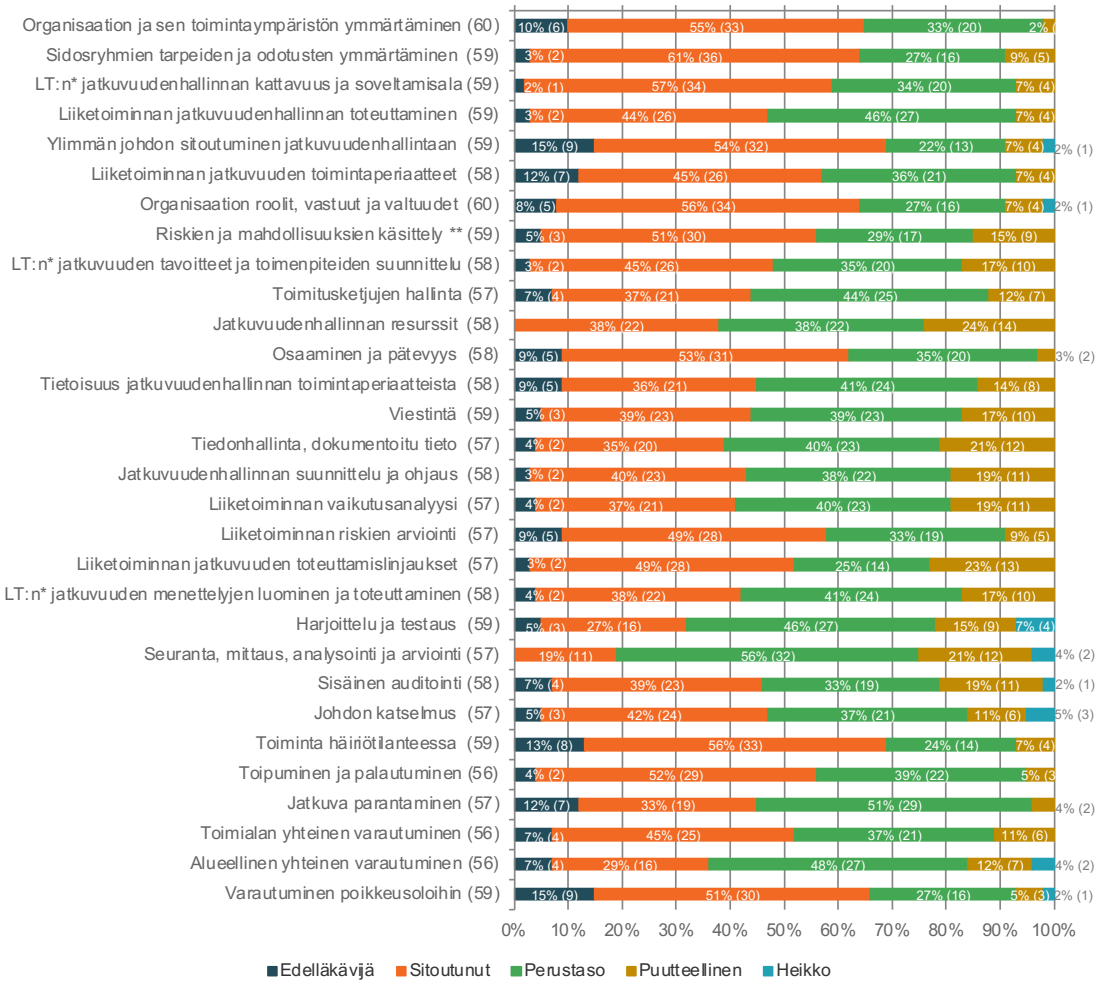
resilienssi (k.a. = 2,42, Md = 2). Jotta tällaisiin tuloksiin päästään, on hyvinkin loogista, että resilienssianalyysi pyritään tekemään liiketoimintalähtöisesti (k.a. = 2,44, Md = 2).

4.2.4 Järjestelmäympäristön jatkuvuudenhallinnan maturiteettitason arviointi

Järjestelmäympäristön jatkuvuudenhallintaan liittyvää maturiteettitasoa tutkittiin mukaillen Huoltovarmuuskeskuksen aiemmin teettämän ISO 22301 -standardiin perustuvan jatkuvuudenhallintakyselyn teemakohtaista otsikointia sovellettuna rakennuksen järjestelmäympäristöön. Väittämät ja tulokset on lueteltu taulukossa 10 järjestyksessä keskiarvon suhteen pienimmästä suurimpaan. Vastaajat arvioivat organisaation maturiteettitasoa jatkuvuudenhallinnan käytäntöihin liittyen vastaamalla väittämiin Likert-asteikolla edelläkävijä (1), sitoutunut (2), perustaso (3), puutteellinen (4), heikko (5).

Rakennuksen järjestelmäympäristöä koskeva jatkuvuudenhallinnan maturiteettitaso koettiin yleisesti ottaen varsin hyväksi (kuva 19). 75 % (n = 57) vastaajista arvioi, että seuranta, mittaus, analysointi ja arviointi on maturiteetiltaan vähintään perustasolla ja muut vastausprosentit olivat tätä suurempia perustasoa tarkasteltaessa. Suurimmillaan vastanneista lähes 100 % (kuva 18) koki, että maturiteettitaso järjestelmäympäristön jatkuvuudenhallinnan näkökulmasta on vähintään perustasolla. Tällaisia aiheita olivat jatkuva parantaminen 96 % (n = 57), organisaation ja sen toimintaympäristön ymmärtäminen 98 % (n = 60) ja osaaminen ja pätevyys 97 % (n = 58).

Vaikka tulosten perusteella vastaajat kokivat maturiteettitason olevan pääasiassa vähintään perustasoa, nousi tietyt aiheet joiltakin osin esille puutteellisina tai heikkoina. Tällaisia olivat muun muassa seuranta, mittaus, analysointi ja arviointi (25 %, n = 57), jota ISO 22301 -standardi (ISO 2019, 28) edellyttää osana jatkuvan parantamisen prosessia. Näiden lisäksi kehitystoimenpiteitä vaativat erityisesti jatkuvuudenhallinnan liian vähäiset resurssit (24 %, n = 58), liiketoiminnan jatkuvuuden puutteelliset toteuttamislinjaukset (23 %, n = 57), sisäinen auditointi (21 %, n = 57) ja tiedon hallinta sekä dokumentointi (21 %, 57).



Kuva 19. Jatkuvuudenhallinnan maturiteettitaso (n = 60) (*liiketoiminta, **Jatkuvuudenhallintaan kohdistuvien riskien ja mahdollisuuksien käsittely)

Koska perustasoa ei erikseen määritelty, jäivät vastaukset siltä osin hyvin epätarkoiksi (kuva 19). Perustasoksi voi muun muassa tulkita lain ja asetusten määrittämän teknisen ympäristön perustason. Jokainen organisaatio tulkitsee todennäköisesti kuitenkin perustason subjektiivisesti omasta näkökulmastaan. Taulukosta 10 voidaan nähdä, että operatiiviset toiminnot, joista esimerkkeinä mainittakoon toiminta häiriötilanteessa (k.a. = 2,24, Md = 2), johdon sitoutuminen (k.a. = 2,25, Md = 2), organisaation ja sen toimintaympäristön ymmärtäminen (k.a. = 2,27, Md = 2) ja varautuminen poikkeusoloihin (k.a. = 2,27, Md = 2) koetaan olevan rakennusten järjestelmäympäristön jatkuvuudenhallinnan osalta erinomaisella tasolla. Myös muiden kohtien osalta näkemys jatkuvuudenhallinnan maturiteettitasosta on varsin hyvä ja myös vastaajat erittäin samanmielisiä ($0{,}65 \leq s \leq 0{,}95$).

Vaikka kysymyksen asettelussa painotettiin näkökulmaa järjestelmäympäristön kautta, on mahdollista, että osa vastaajista on kuitenkin vastannut kysymyksiin liiketoiminnan jatkuvuudenhallinnan maturiteetin näkökulmasta. Toisaalta digitaalisen resilienssin lähtökohtana tuleekin olla aina liiketoiminta ja sen tavoitteet (Björck ym. 2015, 313) toisin kuin kyberturvallisuudessa, jossa näkökulma on tekninen ja usein vahvasti IT-lähtöinen. Vastaajien oli tarkoitus vastata jokaiseen kysymykseen vain kriittisimpien organisaation käytössä olevien rakennusten näkökulmasta, joka myös selittää varsin positiiviset tulokset.

Viimeistä kysymystä (taulukko 10) kohti vastausmäärät nousivat, joka osoittaa, että vastaajat olivat varsin sitoutuneita kyselyyn. Viimeinen kysymys sisälsi eniten väittämiä, joten se vaati vastaajilta erityistä keskittymistä. Keskiarvo ei tässä anna luotettavaa kuvaa vastauksista, sillä numerot kuvasivat sanallista arviota. Kuitenkin keskihajonta oli varsin tasainen jokaisen väittämän osalta, joka kuvaa hyvin vastaajien samanmielisyyttä.

Taulukko 10. Järjestelmäympäristön jatkuvuudenhallinnan maturiteettitaso

Muuttuja	n	k.a.	Md	s	s^2
Toiminta häiriötilanteessa	59	2,24	2	0,77	0,60
Ylimmän johdon sitoutuminen jatkuvuudenhallintaan	59	2,25	2	0,86	0,74
Organisaation ja sen toimintaympäristön ymmärtäminen	60	2,27	2	0,66	0,44
Varautuminen poikkeusoloihin	59	2,27	2	0,85	0,72
Osaaminen ja pätevyys	58	2,33	2	0,69	0,47
Organisaation roolit, vastuut ja valtuudet	60	2,37	2	0,80	0,64
Liiketoiminnan jatkuvuuden toimintaperiaatteet	58	2,38	2	0,79	0,63
Sidosryhmien tarpeiden ja odotusten ymmärtäminen	59	2,41	2	0,70	0,49
Liiketoiminnan riskien arviointi	57	2,42	2	0,78	0,61
Jatkuva parantaminen	57	2,46	3	0,76	0,57
Liiketoiminnan jatkuvuudenhallinnan kattavuus ja soveltamisala	59	2,46	2	0,65	0,42
Toipuminen ja palautuminen	56	2,46	2	0,66	0,44
Toimialan yhteinen varautuminen	56	2,52	2	0,79	0,62
Jatkuvuudenhallintaan kohdistuvien riskien ja mahdollisuuksien käsittely	59	2,54	2	0,82	0,67
Liiketoiminnan jatkuvuudenhallinnan toteuttaminen	59	2,56	3	0,68	0,46
Tietoisuus jatkuvuudenhallinnan toimintaperiaatteista	58	2,60	3	0,84	0,70
Toimitusketjujen hallinta	57	2,61	3	0,80	0,63
Liiketoiminnan jatkuvuuden tavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu	58	2,66	3	0,81	0,65
Liiketoiminnan jatkuvuuden toteuttamislinjaukset	57	2,67	2	0,87	0,76
Viestintä	59	2,68	3	0,82	0,67
Johdon katselmus	57	2,68	3	0,93	0,86
Sisäinen auditointi	58	2,69	3	0,92	0,85
Jatkuvuudenhallinnan suunnittelu ja ohjaus	58	2,72	3	0,81	0,66
Liiketoiminnan jatkuvuuden menettelyjen luominen ja toteuttaminen	58	2,72	3	0,79	0,62
Liiketoiminnan vaikutusanalyysi	57	2,75	3	0,81	0,65
Alueellinen yhteinen varautuminen	56	2,77	3	0,89	0,80
Tiedonhallinta, dokumentoitu tieto	57	2,79	3	0,82	0,67
Jatkuvuudenhallinnan resurssit	58	2,86	3	0,78	0,61
Harjoittelu ja testaus	59	2,92	3	0,95	0,91
Seuranta, mittaus, analysointi ja arviointi	57	3,09	3	0,74	0,55

n = vastausten lukumäärä
k.a. = keskiarvo
Md = mediaani
s = keskihajonta
s^2 = varianssi

Kyberhäiriöiltä suojautumisen ja hallitun häiriöön reagoimisen (taulukko 9) sekä jatkuvuudenhallinnan maturiteettitasoa mittaavien väittämien välille (taulukko 10) väliltä ei löytynyt lainkaan yhteyttä. Toisaalta tulokset osoittivat, että mikäli ylin johto on sitoutunut jatkuvuudenhallintaan (taulukko 10), vaikuttaisi todennäköisimmin jatkuvuudenhallinnan prosessien olevan kuvattu ($n = 57$, $r_p = 0,4$, $p = 0,002$) ja otettu käyttöön ($n = 57$, $r_p = 0,42$, $p = 0,001$) (taulukko 8). Tällöin myös vastuuhenkilöt / omistajat on todennäköisimmin määritelty järjestelmille ($n = 58$, $r_p = 0,45$, $p = 0,001$) (taulukko 8). Mikäli ylin johto on jatkuvuudenhallintaan sitoutunut, on myös järjestelmien väliset riippuvuudet ($n = 56$, $r_p = 0,33$, $p = 0,015$) ja kokonaisarkkitehtuuri kuvattu ($n = 54$, $r_p = 0,36$, $p = 0,008$) (taulukko 8). Myös usean muun jatkuvuudenhallinnan käytäntöjä ja digitaalista resilienssiä kuvaavan väittämän osalta johdon sitoutuminen osoitti lineaarista riippuvuutta. Kuitenkaan johdon sitoutumisen ja tietoturva- tai kyberturvallisuusauditoinnin (taulukko 8) välillä ei ollut tunnistettavissa yhteyttä, joka taas voi tukea haastatteluissa esille nostettua kyberturvallisuuteen liittyvän osaamisen kehittämisen tarvetta ja tiedonjanoa nimenomaan rakennuksiin ja niiden järjestelmäympäristöön liittyen.

Yksittäisenä erityisyytenä mainittakoon vielä toimitusketjun hallintaan (taulukko 10) liittyvän maturiteettitason yhteys jatkuvuudenhallinnan käytäntöihin ja digitaalisen resilienssiin (taulukot 8 ja 9). Tulosten mukaan, mikäli organisaation OT-ympäristön jatkuvuudenhallinnan maturiteettitaso on korkea, on tällä yhteys lähes jokaiseen jatkuvuudenhallinnan käytäntöjä ja resilienssiä mittaavaan väittämään. Poimintoina nostettakoon esille riippuvuudet, jotka koskevat toimitusketjun hallintaa suhteessa liiketoimintalähtöiseen resilienssianalyysiin ($n = 54$, $r_p = 0,46$, $p = 0,001$) (taulukko 9), liiketoiminnan ja järjestelmien tarkasteluun yhteen liitettynä kokonaisuutena ($n = 55$, $r_p = 0,42$, $p = 0,002$) (taulukko 9) ja kokemukseen, jossa resilienssi koetaan sisäänrakennetuksi osaksi organisaatiota ja sen järjestelmiä ($n = 57$, $r_p = 0,4$, $p = 0,003$) (taulukko 9). 44 % ($n = 57$) vastaajista *kokee olevansa* toimitusketjun hallintaan liittyen edelläkävijä tai sitoutunut.

Jos maturiteettitasoa mittaavia väittämiä käsitellään kokonaisuutena, on tuloksista havaittavissa, että mitä korkeampi maturiteettitaso (taulukko 10) järjestelmäympäristön jatkuvuudenhallintaan liittyen koetaan olevan, sitä todennäköi-

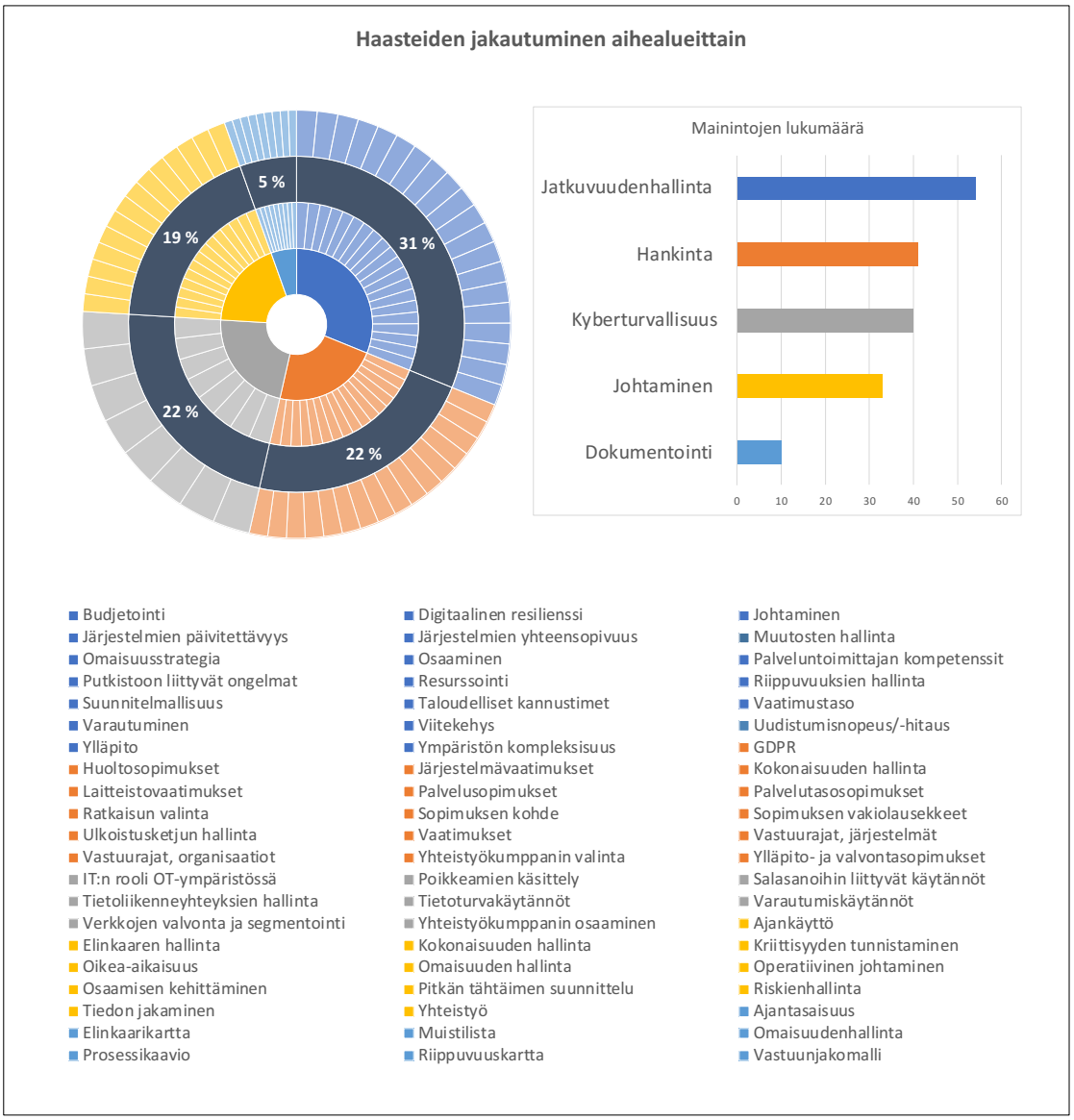
semmin jatkuvuudenhallinnan prosessit on kuvattu ja käyttöönotettu, järjestelmien väliset riippuvuudet on kuvattu ja järjestelmien vastuuhenkilöt / omistajat on nimetty (taulukko 8). Tällöin resilienssi on myös todennäköisimmin sisäänrakennettu osa organisaatiota ja liiketoimintalähtöinen resilienssianalyysi koetaan osaksi järjestelmäkokonaisuuteen liittyvää jatkuvuudenhallinnan prosessia (taulukko 9). Tämä on linjassa Kosmowskin ym. (2022, 14) mallin kanssa, jossa painotetaan IT:n ja OT:n välisten riippuvuuksien sekä tämän kokonaisuuden turvallisuuteen liittyvien vaikutusten tärkeyttä liiketoiminnan jatkuvuudenhallinnalle. Tulokset ovat näiltä osin tilastollisesti merkitseviä tai erittäin merkitseviä. Yleisesti ottaen verrattaessa järjestelmäympäristön jatkuvuudenhallinnan maturiteettitasoa mittaavia väittämiä toisiinsa, oli havaittavissa jokaisen väittämän välillä riippuvuus, joista valtaosassa se oli melko vahva tai vahva. Tämä voidaan tulkita niin, että OT-ympäristön jatkuvuudenhallintaa kuten muutakin jatkuvuudenhallintaa käsitellään kohderyhmässä yleisesti ISO 22301 -standardin mukaisesti (ISO 2019, 2) laajana kokonaisuutena eikä yksittäisten tehtävien listana.

4.2.5 Vastaukset avoimiin kysymyksiin

Tutkimuksessa annettiin vastaajille mahdollisuus kommentoida rakennuksen järjestelmäympäristöön liittyviä teemoja myös avoimilla vastauksilla. Avoimia vastauksia saatiin varsin runsaasti tutkimukseen osallistuneiden lukumäärään verrattuna. 64:stä vastaajasta 20 kertoi onnistumisista, 15 mahdollisuuksista ja teemahaastattelut mukaan lukien 39 vastaajaa kertoi haasteista, joita rakennuksen järjestelmäympäristön jatkuvuudenhallintaan liittyy. Kerättyjä tietoja hyödynnettiin muiden tietojen ohella rakennuksen jatkuvuudenhallinnan työkalun hahmottelussa. Koska tutkimuksen teema on hyvin ajankohtainen, näkyi maailmanpoliittinen tilanne myös monissa vastauksissa. Onnistumisiin liittyvissä vastauksissa korostuivat muun muassa viestintä, energiansaanti, varavoima ja varautuminen. Toisaalta onnistumisena mainittiin myös suljetun ympäristön rooli häiriöttömyyden mahdollistajana.

> ”Vielä mitään todella hankalaa ei ole sattunut, vaikka geopoliittisen tilanteen muutoksen myötä riskitasot ovat kasvaneet. Riskit on tiedostettu.” (D)

Rakennuksen järjestelmäympäristöön liittyvistä mahdollisuuksista tunnistettiin muun muassa ulkoistaminen, reaaliaikainen tieto ja tunnistetut parannustoimenpiteet. Laadullisessa tutkimuksessa pyrittiin positiiviseen näkökulmaan eli tarkoituksena oli selvittää miten ja millaisin keinoin rakennuksen OT-ympäristön jatkuvuudenhallintaa kannattaisi toteuttaa ja kehittää. Silti keskusteluissa nousi esille useita haasteita. Haastateltavien oli todennäköisesti tarkoitus luoda haasteiden avulla kontrastia ja tarkentaa näillä kontekstiin liittyviä asioita. Erillisiä haasteita (kuva 20) mainittiin 183 kappaletta 38 vastaajan toimesta eli yhteensä enemmän kuin yhteenkään muuhun teemaan liittyviä asioita ja suhteessa enemmän kuin muita mainittuja asioita yhteensä. Muihin teemoihin liittyviä asioita mainittiin kaikki yhteensä 246 kappaletta. Haasteet luokiteltiin teemakohtaisesti ja yksinkertaistettiin jatkuvuudenhallinnan näkökulmasta tärkeiksi aiheiksi.



Kuva 20. Haasteiden teemakohteinen esiintyminen lukumäärinä ja prosentteina (n = 38)

Kuvassa 20 on esitetty tutkimuksen teemoittain järjestettynä lueteltujen haasteiden aiheet. OT-ympäristön jatkuvuudenhallintaan liittyvistä haasteista yleiset jatkuvuudenhallintaprosessiin liittyvät toimenpiteet toistuivat useimmin. Tämän lisäksi kymmeniä mainintoja sai hankinta, kyberturvallisuus ja johtaminen. Myös dokumentointi mainittiin, mutta harvemmin. Tutkimuksen positiivisesta näkökulmasta huolimatta OT-ympäristön jatkuvuudenhallintaan liittyvät haasteet nousivat jokaisessa haastattelussa keskeisimmäksi teemaksi.

4.3 Jatkuvuudenhallinnan kehittämisen työkalu, DIGIRES

Kyberturvallisuus nousi haastatteluissa esille yhtenä merkittävänä teemana. Näkökulma kyberturvallisuuteen oli pitkälti lisää tietoa janoava sekä riskit ja haasteet tunnistava. Haastatteluista jäi erityisesti mielikuva, että tarve sekä uudelle osaamiselle että yhteistyölle digitaalisen resilienssin varmistamisen sekä kyberuhkiin varautumisen osalta on suuri. Kuitenkin aikaa kaiken omaksumiselle ja yhteistyön rakentamiselle vaikuttaa olevan liian vähän sekä työarjen että maailmantilanteen näkökulmasta.

> ”Turvallisuuden näkökulmasta KATAKRI on hyvä, mutta se ei ota kantaa jatkuvuudenhallintaan. Se ottaa kantaa siihen, että miten järjestelmiä käytetään, ei siihen, että miten niitä on hoidettu ja ylläpidetty, joka on se suurin kompastuskivi. Tietääkseni ei ole sellaista viitekehystä, joka sopisi suoraan näihin rakennusten järjestelmäympäristön jatkuvuudenhallinnan taklaamiseen.” (J)

Tilanne vaikutti olevan sama kiinteistön omistajan, ylläpitäjän sekä palveluntoimittajan kannalta. Jotta digitaalista resilienssiä voi lisätä ja kyberturvallisuutta hallita, on tiedettävä, mitä hallitaan. Siihen jatkuvuudenhallinnan työkalu voi olla erinomainen väline. Tutkimuksen tulosten perusteella syntyi DIGIRES-kanvaasi, jota on kuvattu tarkemmin kohdassa 6.

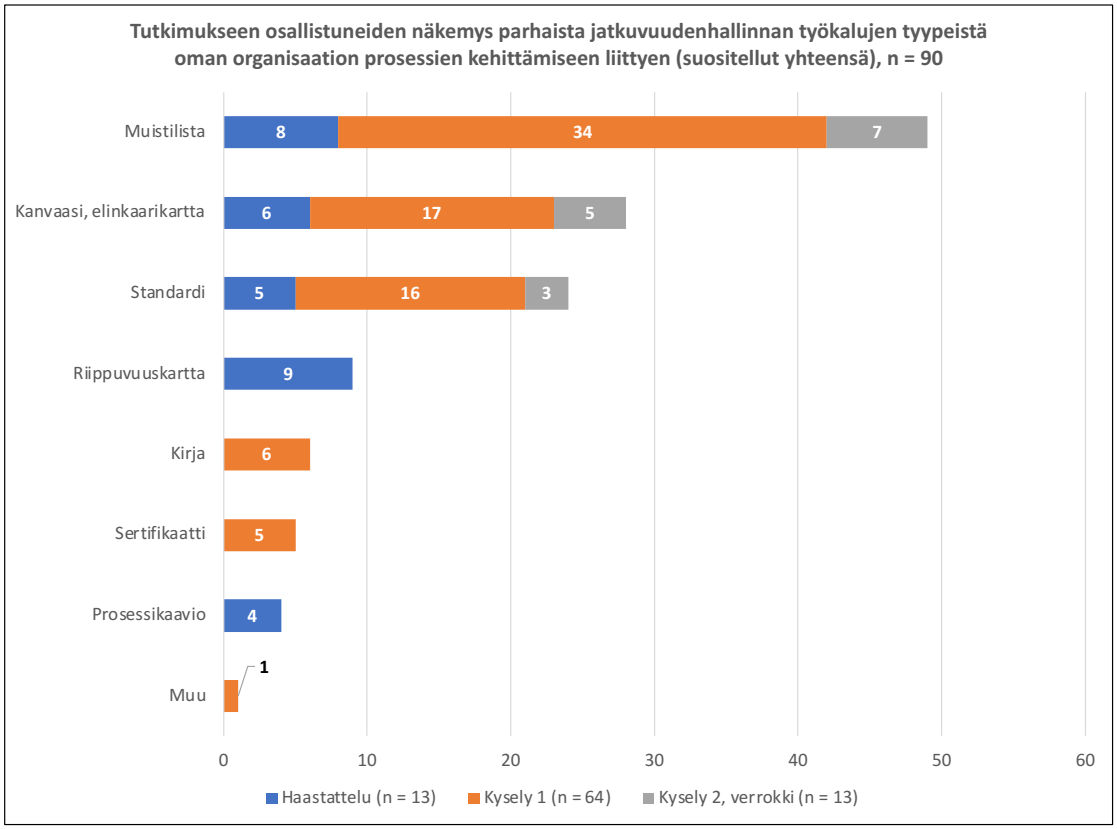
4.4 Ehdotukset työkalun toteutustavasta

Haastatteluissa sekä kyselytutkimuksessa käsiteltiin parhaita tiedon jakamisen käytäntöjä jatkuvuudenhallinnan kehittämiseen liittyen toteutettavan jatkuvuudenhallinnan työkalun näkökulmasta (kuva 21). Haastatteluissa vastausvaihtoehtoja ei ollut rajattu, joten vastaajat voivat esittää mitä tahansa vaihtoehtoja

parhaiksi käytännöiksi. Parhaina tapoina haastatteluissa mainittiin riippuvuuskartta, joka mainittiin yhdeksän, ja muistilista, joka mainittiin kahdeksan kertaa. Näiden lisäksi mainittiin kanvaasi tai tätä vastaava elinkaarikartta kuudesti, standardi viidesti ja prosessikaavio neljä kertaa. Kosmowski ym. (2022, 9) mainitsee erilaiset kyvykkyyksiä kehittävät toimenpiteet kuten resilienssin rakentamista hyödyttävän viitekehyksen sekä tehtävälistat tärkeänä liiketoiminnan jatkuvuudenhallinnan välineenä.

> ”(Tarvittaisiin) päivitetty näkymä eli jonkinlainen kvartaalisykli ja päivittäinen näkymä siihen et missä me mennään sen koko jatkuvuuden osalta” (K)

Jatkuvuudenhallinnan työkaluja käsiteltiin myös kyselytutkimuksessa (Kysely 1 ja Kysely 2). Muistilista oli kyselyssä ylivoimaisesti suosituin työn tukemisen väline 41 maininnalla (n = 90). Kanvaasi valittiin 22 kertaa ja standardi yhdeksän. Kirja valittiin kuudesti ja sertifikaatti viidesti. Näiden lisäksi ehdotettiin, että laadittaisiin standardiin perustuvat prosessikuvaukset sekä mahdollisuus suorittaa sertifiointiauditointi. Näin olisi erään tutkimukseen osallistuneen näkemyksen mukaan ”mahdollista todentaa toiminnan vaatimustenmukaisuus puolueettoman tahon toimesta” (D). Prosessikaaviota ja riippuvuuskarttaa ei ollut sisällytetty kyselyyn vaihtoehdoiksi. Myös jatkuvan parantamisen malleja sekä uhka-analyysejä ehdotettiin osaksi kokonaisuutta jaksotettuna toiminnan vuosikelloon. Toisaalta eräs vastaajista totesi, että ”jollei regulatiivista vaatimusta ole, niin todennäköisesti jatkuvuudenhallinnan kehittämiselle ei tule olemaan aikaa eikä muita resursseja” (D).



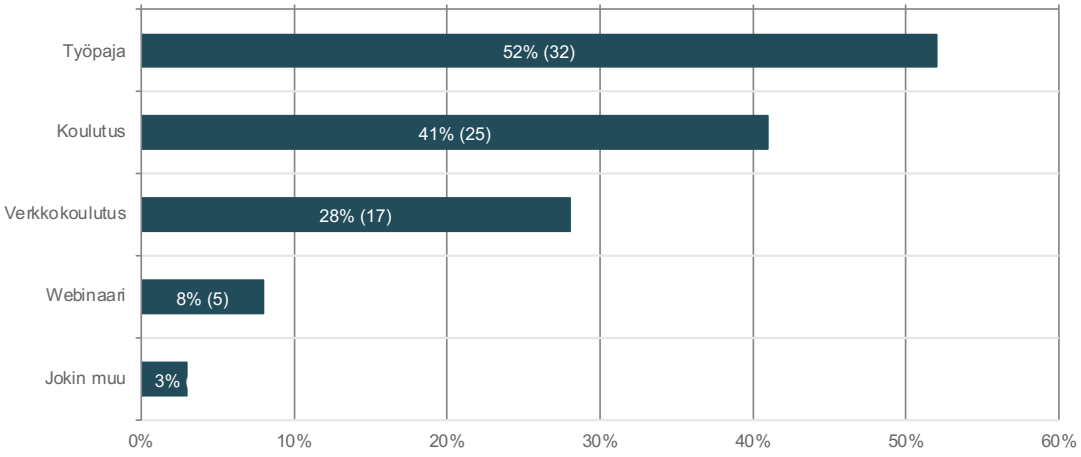
Kuva 21. Tutkimukseen osallistuneiden näkemys parhaista jatkuvuudenhallinnan työkalujen tyypeistä oman organisaation prosessien kehittämiseen liittyen (n = 90)

Suosittuihin jatkuvuudenhallinnan työkaluihin liittyen kolmen ensimmäisen eli muistilistan, kanvaasin ja standardin suosittuudet ovat linjassa toistensa kanssa. Näistä huolimatta riippuvuuskartta oli haastatteluissa suosituin. Mikäli tämä olisi ollut valintamahdollisuutena myös kyselytutkimuksessa, voi olla, että tulos olisi erilainen.

Vastauksista saatuja tietoja hyödynnettiin jatkuvuudenhallinnan työkalun toteuttamisessa mittausmallin (kuva 6) mukaisesti. Kyselyyn vastanneiden avoimista kommenteista saatiin hyvää osviittaa jatkuvuudenhallinnan kehittämisen tarpeen vahvistamiseen liittyen. Vastanneet mainitsivat muun muassa ylätason kokonaiskuvan kokonaisuuden hahmottamista selkeyttävän roolin useamman kerran ja myös lyhyiden käytännönläheisten ohjeiden merkitys kokonaisuuden digitaalisen resilienssin kehittämisessä mainittiin. Vaikka standardia pidettiin toisaalta liian raskaana osana arjen työtehtäviä, pidettiin sitä kuitenkin hyvänä lähtökohtana ja tukena kaikelle tekemiselle muun muassa seuraavin kommentein: ”Standardi palvelisi kokonaisuutta elinkaaren osalta vaatimusmäärittelystä hankintaan, toteutukseen ja ylläpitoon.” (D).

4.5 Oppimisen ja tiedonjakamisen parhaat käytännöt

Kyselytutkimuksen perusteella yli puolet vastaajista piti oppimisen osalta parhaana tapana työpajaa ja yli 40 % äänesti läsnäolokoulutuksen puolesta (n=61). Verkkokoulutusta piti tärkeänä reilu neljännes vastaajista ja webinaaria parhaana tapana kehittää osaamista piti vain alle 10 % vastaajista. Tulokset on esitetty kuvassa 22 sekä äänestysmäärinä että prosentteina kaikista vastaajista. Kysymyksessä sallittiin useampi vastausvaihtoehto. Kouluttamisen ja osaamisen ylläpitämisen tärkeyttä painottaa myös Kosmowski ym. (2022, 10) tutkimuksessaan, jossa mainitaan koulutusten ja harjoitusten lisäksi liiketoiminnan jatkuvuudenhallintaprosessin auditoinnit sekä katselmoinnit välineinä varmistaa osaamisen pysyminen ajan tasalla. Samoja teemoja käsiteltiin niin haastatteluissa kuin myös avoimien kysymysten vastauksissakin.



Kuva 22. Suosituimmat jatkuvuudenhallintaan liittyvän osaamisen kehittämisen tavat (n = 61)

Tällä kysymyksellä haettiin suuntaa mittausmallin (kuva 6) mukaisesti dokumentoinnin ja uuden tiedon sisäistämisen parhaiden käytäntöjen tunnistamiseksi aihealueella. Tietoa hyödynnettiin jatkuvuudenhallinnan työkalun laatimisessa. Jokin muu -vastaukset nostivat esille vastuuhenkilöille suunnatun täsmäkoulutuksen ja näiden vastuulle siirrettävän osaamisen jakamisen muille tietoa tarvitseville. Toisaalta ehdotettiin työpajan ja koulutuksen yhdistelmää sekä joustavasti kaikkia vaihtoehtoja kulloinkin tarkoitukseensa sopivalla lähestymistavalla. Tarve osaamisen kehittämiselle oli joka tapauksessa ilmeinen, vaikka OT-ympäristön jatkuvuudenhallinnan maturiteettitasoon liittyvässä kyselyssä osaaminen vaikuttikin olevan erittäin hyvällä tasolla.

5 HAVAINTOJEN YHTEENSOVITTAMINEN JA TULKINTA

Koska tutkimus toteutettiin monimenetelmäisenä, on saatuja tietoja vielä tulkittu tässä luvussa toisiinsa verraten relevanttien tulosten osalta. Kokemusta jatkuvuudenhallinnan käytännöistä ja maturiteettitasosta kyselytutkimuksen perusteella on verrattu tässä laadullisesta tutkimuksesta kerättyihin tietoihin. Myös digitaalisen resilienssin osalta on tehty vertailua eri tutkimusmenetelmien välillä.

5.1 Yleisesti

Tutkimuksen tulosten perusteella voidaan yleisesti todeta, että OT- järjestelmiin liittyy hyvin eripituisia elinkaaria, tavoitteita ja erityispiirteitä. IT:n parhaiden käytäntöjen hyödyntäminen sellaisenaan ei vaikuta tulosten perusteella olevan mahdollista OT-ympäristön jatkuvuudenhallinnan maturiteettitason kehittämisessä, mutta sovellettuna OT:n toimintoihin, voi joistakin IT:n tavoista toimia olla hyvinkin hyötyä. Tätä tukee myös Kosmowskin ym. (2022,18) liiketoiminnan jatkuvuudenhallinnan viitekehys (kuva 3), jossa käsitellään fyysistä ja kyberturvallisuusympäristöä samassa raamissa liiketoiminnan tavoitteiden kanssa ottaen huomioon koko toimintaympäristön resilienssin ja liiketoiminnan tavoitteet. Ja kuten eräs haastateltu totesi: ”Tämä on keskeinen asia ja kiinnostavaksi sen tekee se, että siitä on keskitetysti hankala päättää.” (M).

Haastateltujen esille nostamat haasteet alleviivasivat IT:n vastuiden ulkopuolelle jäävän teknologian johtamiseen, hankintaan ja ylläpitoon liittyviä ongelmakohtia. Toisaalta kyselytutkimuksen perusteella OT-ympäristön jatkuvuudenhallinnan maturiteettitaso vaikutti olevan erittäin hyvällä tasolla, ylin johto sitoutunutta ja hankinnan prosessit pääosin omalla vastuulla (kuva 19). Tämä ristiriita lienee selitettävissä tutkimuksen eri osioiden erilaisen luonteen vuoksi ja kyselyn mahdollisesti harhaanjohtavan kysymyksenasetannan vuoksi. Yleisesti kuitenkin tarve jatkuvuudenhallinnan kehittämiseen nousi huolimatta tutkimusotteesta ja jatkuvuudenhallinnan kehittämistä tukemaan toivottiin helppokäyttöisiä työkaluja. Lähes kukaan haastateltavista ei tunnistanut sellaisia valmiita viitekehyksiä tai parhaita käytäntöjä, joita voisi hyödyntää rakennuksen järjestelmäympäristön jatkuvuudenhallinnassa. Kuitenkin tutkimuksen jälkeen versioksi 2.0 päivitetty NIST-viitekehys (NIST 2023) mainittiin yhtenä hyvänä, joskin raskaana mallina.

5.2 Kohderyhmän kokemus digitaalisesta resilienssistä omassa organisaatiossa

Sekä haastattelujen että kyselyn tulosten perusteella (kuva 18) voidaan todeta organisaatioiden käsittelevän digitaalista resilienssiä käsitteenä liiketoimintalähtöisesti tavoitteena ylläpitää palvelutaso sekä varmistaa liiketoimintatavoitteiden saavuttaminen mahdollisista kyberhäiriöistä huolimatta. Tämä on täysin linjassa Björckin ym. (2015, 312) sekä Aldersonin ym. (2015, 562–563) tulosten kanssa. Toisaalta osa tutkimukseen osallistuneista piti organisaatiolle tärkeänä luoda immuniteetti kriittisiä häiriötilanteita vastaan eli suojautua täysin häiriöiltä, joka taas vastaa Petrenkon (2019, 7) näkemystä digitaalisesta resilienssistä (kuva 18).

Park ym. (2018, 356–357) toteavat riskianalyysin olevan riittämätön varautumisen tapa kriittistä infrastruktuuria suojatessa. Tutkimusryhmä painottaa resilienssin tärkeyttä käsiteltävänä teemana, jonka avulla voidaan suojautua ennalta arvaamattomilta tapahtumilta ja niiden toteutuessa toipua niistä. Haastatteluissa resilienssi ei niinkään noussut esille teemana spontaanisti yksittäisiä mainintoja lukuun ottamatta toisin kuin riskienhallintaan liittyvät aiheet. Digitaalista resilienssiä pidettiin kuitenkin yleisesti hyvin tärkeänä organisaation ominaisuutena ydintoimintoja suojattaessa. Samalla haastateltavat kokivat puutteellisen jatkuvuudenhallinnan suurena riskinä digitaalisen resilienssin toteutumiselle, vaikka kyselytutkimuksessa taas yli puolet vastanneista koki, että jatkuvuudenhallinnan prosessit on kuvattu täysin tai osittain ja hieman alle puolet totesi niiden olevan jo käytössä (kuva 17).

Kyselytutkimuksessa Björckin ym. (2015, 315) kyberresilienssin näkökulmat ja periaatteet -mallin (”Cyber resilience aspects and principles”) mukaisesti kuvattuna kyselyyn vastaajat arvioivat organisaationsa digitaalisen resilienssin olevan varsin hyvällä tasolla (kuva 18). Jopa yli neljä viidestä arvioi resilienssin olevan sisäänrakennettu osa organisaation järjestelmiä (kuva 18). Toisaalta saman kyselyn mukaan reilu puolet vastaajista koki, että tietoturva-auditointeja on tehty vain harvoille järjestelmille tai ei ollenkaan (kuva 17). Kyberturvallisuusauditointi jää samalla mittarilla alle puoleen vastaajista (kuva 17). Haastattelujen perusteella voidaan todeta, että tutkittujen organisaatioiden

prosesseissa riskienhallinnan käytännöt vaikuttavat olevan puhekielessä tuttuja, mutta vaikka digitaalisen resilienssin varmistamiseen olisi käytännöt olemassa, vaikuttaa näiden sanoittaminen kohderyhmälle olevan enimmäkseen vierasta.

Osa haastatelluista koki hankinnalla olevan liian vähän osaamista nopeasti digitalisoituneeseen OT-järjestelmäympäristöön liittyen. Tämän koettiin vaikuttavan koko elinkaarella, sillä yksittäisen hankinnan taloudellisen optimoinnin tunnistettiin aiheuttavan riskejä ja lisäkustannuksia rakennuksen ja OT-järjestelmän elinkaarella. Toisaalta osa haastatelluista piti hankintaa hyvin suoraviivaisena ja tavoitteita tukevana toimintona, sillä näillä organisaatioilla oli erittäin tarkasti määritellyt vaatimukset kullekin OT-järjestelmälle ja järjestelmäympäristölle. Moni haastateltu tunnisti parhaillaan käynnissä olevan selkeän murrosvaiheen OT-järjestelmien myynnissä ja palveluntarjonnassa, joka omalta osaltaan vaikuttaa aiheuttavan häiriötä ja epäselvyyttä niin hankinnan kuin palveluntoimittajankin päässä.

Kosmowski ym. (2022, 12) kuvaa mallissaan (kuva 3) teknisen ympäristön digitaalisen resilienssin ja jatkuvuudenhallinnan suhdetta liiketoiminnan ja tuotannon jatkuvuudenhallintaan. Malli kuvaa havainnollisesti mahdollisten kriittisten haavoittuvuuksien riippuvuuksia organisaation ydintoimintoihin. Malli on tässä tutkimuksessa kerätyn tiedon perusteella hyvin sovellettavissa jokaiseen tutkimuksen kohteena olleeseen organisaatioon huolimatta siitä, että OT-ympäristöä käsitellään rakennuksen järjestelmäympäristön eikä tuotannon ympäristön näkökulmasta. Haastateltavat sekä kyselyyn vastanneet nostivat esille teemaan liittyen kuitenkin niin paljon haasteita (kuva 20), että digitaalisen resilienssin ja OT-ympäristön jatkuvuudenhallinnan kehittäminen lienee syytä aloittaa varsin matalalta maturiteettitasolta pienin askelin jatkuvasti toimintaa parantaen, kuten ISO 22301 edellyttää (ISO 2019, 27). Mallin hyödyntäminen tutkimuksessa OT-ympäristön jatkuvuudenhallinnan kehittämisen tukena on ollut kuitenkin valintana hyvä ja oikeita suuntaviivoja korostava.

5.3 Rakennuksen järjestelmäympäristö yhtenäisenä järjestelmäkokonaisuutena

OT-järjestelmien suunnittelu-, hankinta- ja käyttöönottoprosessit voivat tutkimuksen perusteella hajautua useisiin eri siiloihin ilman läpileikkaavaa kokonaisuudenhallintaa tai johtamista, jolloin näkemys kokonaisarkkitehtuurista jää saavuttamatta. Tämän lisäksi varsin merkittävä osa kohderyhmästä kertoi hyödyntävänsä ulkoistettua osaamista sekä vaatimusmäärittely- että hankintavaiheessa, jolloin ymmärrys kokonaisuudesta ei jää välttämättä työn tilaajalle hyödynnettäväksi elinkaaren eri vaiheissa, vaan siirtyy suoraan konsulteille. Rakennuksen OT-ympäristöä pidettiinkin haastattelujen perusteella kaiken kaikkiaan hyvin kompleksisena ja hallittavuudeltaan haastavana kokonaisuutena ja osaamista yleisesti aiheeseen liittyen riittämättömänä digitalisoitunutta OT-ympäristöä tarkasteltaessa.

Kyselytutkimus (kuva 15) osoittaa, että kyselyyn vastanneet kokivat järjestelmiin liittyvät vastuut hyvin monella tavalla. Vaikka jokin järjestelmä olisi organisaation vastuulla, jää todennäköisesti muita järjestelmiä organisaation vastuiden ulkopuolelle. Tämä tulos ei täysin todenna sitä, etteikö järjestelmiä käsiteltäisi yhtenä kokonaisuutena, mutta vahvistaa sen, että vastuut ovat hajautuneet usealle eri taholle. Tähän viitattiin myös haastatteluissa siilomaisena toimintana. Kun kyselytutkimuksessa selvitettiin jatkuvuudenhallinnan tilaa kokonaisarkkitehtuurin näkökulmasta, lähes puolet vastaajista totesi OT-ympäristön kokonaisarkkitehtuurin olevan täysin tai osittain kuvattu (kuva 17). Luku vaikuttaa yllättävän korkealta, joskin vastaajien määrä on kyseisen kysymyksen osalta tavallista alhaisempi. Näin ollen voi olla, että kokonaisarkkitehtuurin periaatteita enemmän tuntevat ovat vastanneet kyseiseen kysymykseen, joka vääristää lopputulosta hieman. Toisaalta lähes puolet vastaajista totesi, että liiketoimintaa ja järjestelmiä tarkastellaan yhteen liitettynä kokonaisuutena (kuva 18). Neljäsosa oli täysin eri mieltä.

Osa haastatelluista nosti esille riskinä rakennuksen järjestelmien elinkaaren merkittävän lyhenemisen lähemmäs IT-järjestelmien elinkaaritavoitteita. Asian esille nostaneet pitivät muutosta realistisena teknologian erittäin nopean kehittymisen ja sitä kautta ratkaisujen nopean rapautumisen sekä toisaalta nykyis-

ten ratkaisujen puutteiden vuoksi. Puutteina nostettiin esille muun muassa vaikeaksi tai jopa mahdottomaksi tehty järjestelmien ja laitteiden päivittäminen sekä nimenomaan kokonaisuudenhallinnan puuttuminen. Osa haastatelluista tunnisti puutteellisen kokonaisuudenhallinnan aiheuttavan epäjatkuvuuskohtia jatkuvuudenhallinnan kannalta oleellisiin järjestelmien välisiin yhteyksiin liittyen.

Osa haastateltavista mainitsi suhtautuvansa ymmärtäväisesti tilanteeseen, jossa rakennuttaja tai kohteesta vastaava toteuttaa parhaan ymmärryksensä tai urakoitsijan valintojen pohjalta ratkaisuja. Tämä kuitenkin koettiin elinkaaren ja kokonaisuuden hallinnan kannalta haastavana, sillä joissakin tilanteissa urakka-aikana tehdyt valinnat ovat joidenkin haastateltujen mukaan jopa häirinneet merkittävästi kohteeseen muuttavan organisaation toiminnan ydinprosesseja.

Tutkimuksen perusteella haastatellut olivat varsin yhtä mieltä siitä, että siilojen sekä näiden sisälle rakentuvien järjestelmien välinen tiedonsiirto mahdollistaa tehokkaita päättelyketjuja automatisoiduille prosesseille läpi koko OT-ympäristön. Järjestelmien välistä tiedonsiirtoa pidettiin lähes kaikkien haastateltujen toimesta mahdollisuutena. Samalla tunnistettiin riippuvuuksien aiheuttama kompleksisuus sekä haavoittuvuuksiin liittyvät riskit. Jo valmiiksi kompleksisen ympäristön sisäisten ja ulkoisten riippuvuuksien lisääminen vaikuttikin olevan laadulliseen tutkimukseen osallistuneille yleinen huolenaihe. Yhtenä erityisenä haasteena nostettiin esille toimintaympäristön siilomainen rakenne, jossa muihin toimintoihin vaikuttavia päätöksiä tehdään toisissa toiminnoissa ilman riittävää vuoropuhelua.

Tutkimuksen otoksella sai vastausten perusteella sellaisen mielikuvan, että viestintää ja yhteistyötä eri toimintojen, yksiköiden ja siilojen välillä pitäisi lisätä merkittävästi OT-ympäristön jatkuvuudenhallinnan kehittämiseksi. Björck ym. (2015, 312) painottaakin välttämättömänä digitaalisen resilienssin tehokkaan toteutumisen kannalta, että sitä on käsiteltävä holistisesti, usealla eri tasolla ja rinnakkain.

5.4 Jatkuvuudenhallinta digitaalisen resilienssin tukena

Tutkimuksen haastatteluosiossa nousi onnistuneen jatkuvuudenhallinnan mahdollistamisen osalta keskeisimpään osaan johtamiseen ja sen kehittämiseen liittyvät teemat. Kyselytutkimuksen vastausten perusteella ylin johto vaikutti olevan erittäin sitoutunutta OT-ympäristön jatkuvuudenhallintaan (kuva 19). Samoin operatiivisten jatkuvuudenhallinnan toimintojen maturiteettitaso oli kyselytutkimuksen tulosten perusteella erinomaisella tasolla (kuva 19). Tähän kontrastina haastateltavat tunnistivat kuitenkin useita johtamiseen liittyviä haasteita, mutta myös johtamismallin muutosten kautta saavutettavia mahdollisuuksia. Erityisesti operatiivisen toiminnan johtamiseen liittyvät kyvykkyydet korostuvat tuloksissa ja tähän selkeästi liittyvä yhteistyö tai sen puuttuminen.

Riskienhallintaa käsiteltiin laadullisessa tutkimuksessa johtamiseen liittyen kustannusten hallinnan ja ennakoinnin näkökulmasta. Riskienhallintaan liittyen haastatteluissa nousivat esille erityisesti hyviksi koetut standardeihin ja parhaisiin käytäntöihin perustuvat riskienhallintakäytännöt, sitoutuminen riskienhallintatyöhön sekä tiivis yhteistyö tietoturvan johtamisen ja riskienhallinnan välillä. Erityisesti painotettiin rakennusten sekä yleensä OT-ympäristön kriittisyyteen liittyvän arvioinnin tärkeyttä osana jatkuvuudenhallintaa ja toimenpiteiden priorisointia. OT-ympäristön jatkuvuudenhallintaan liittyvien menetelmien ja mallien puuttuminen tunnistettiin haastatteluissa. Ja vaikka kyselytutkimuksessa mittaamisen ja arvioinnin käytännöt vaikuttivat olevan maturiteettitasoltaan korkealla (kuva 19), jäi neljänneksellä vastaajista arvioksi puutteellinen tai heikko. Samoin sisäisen auditoinnin aihealueella koki reilu viidesosa vastanneista organisaation jatkuvuudenhallinnan auditoinnin olevan samalla tasolla (kuva 19). Ottaen huomioon kohderyhmän ja fokusoitumisen vastaajan organisaation kriittisimpinä pitämiin rakennuksiin, voi tuloksia pitää varsin heikkoina. Toisaalta koska auditointia tukevaa standardia OT-ympäristön jatkuvuudenhallintaan liittyen ei vielä ole ollut käytettävissä, lienee tulos ymmärrettävä.

Riskeistä ja niiden toteutumisesta aiheutuvia taloudellisia vaikutuksia käsiteltiin hyvin vähän johtuen tutkimuksen positiivisesta näkökulmasta. Kuitenkin haastatellut halusivat nostaa esille omasta näkökulmastaan realistisia riskejä

spontaanisti yli neljä kymmentä. Kyselytutkimuksessa yli puolet koki organisaationsa olevan sitoutunut tai edelläkävijä OT-ympäristön jatkuvuudenhallintaan kohdistuvien riskien ja mahdollisuuksien käsittelyyn liittyen (kuva 19) ja vain 15 % mainitsi tässä olevan puutteita. Kohderyhmän ollessa huoltovarmuuskriittiset toimijat, lienee ilmeistä, että riskienhallintaprosessien koetaan olevan hyvällä mallilla.

Lähes neljännes kyselytutkimukseen vastanneista totesi jatkuvuudenhallinnan resurssien olevan puutteellisella tai heikolla tasolla (kuva 19). Toisaalta yhdeksän kymmenestä totesi, että vastuuhenkilöt OT-järjestelmäympäristöön liittyen on vähintäänkin jokseenkin varmasti nimetty (kuva 17). Puolet vastaajista totesi jokaiselle järjestelmälle löytyvän vastuuhenkilön. Haastattelussa resursseihin liittyvää keskustelua käytiin enemmän tarvenäkökulmasta, joskin selkeiden roolien tärkeyttä painotettiin joidenkin haastateltujen toimesta. Resursseista eräs tutkimukseen osallistunut kuitenkin totesi, että ”vain regulaatio on riittävän voimakas kannustin riittävien resurssien varmistamiseksi” (D).

Rakennuksen kriittisyyden ja roolin tunnistaminen nostettiin useamman haastatellun toimesta yhdeksi OT-ympäristön jatkuvuudenhallinnan onnistumisen edellytykseksi. Osa koki, että vahvasti talousohjatussa organisaatiossa taloudellisten päätösten tueksi rakennuksen olisi itsessään pystyttävä osoittaa taloudellisten sekä muiden tunnuslukujen kautta roolinsa organisaation toiminnan kannalta keskeisenä tekijänä. Lähes neljännes kyselytutkimuksen vastaajista taas totesi liiketoiminnalta saatavien jatkuvuudenhallintaa koskevien linjausten olevan puutteellisia tai heikkoja (kuva 19). Vaikka moni kyselyyn vastanneista totesikin maturiteettitason olevan tiedonhallinnan ja dokumentoinnin osalta varsin hyvällä mallilla (kuva 19), yli viidesosa kaikista vastanneista koki sen olevan puutteellinen tai heikko.

Haastatellut tunnistivat haasteita parhaiden käytäntöjen puuttumisen osalta kompleksisen OT-ympäristön hallinnan ja kehittämisen suunnitelmallisuuteen liittyen. Samalla IT:n toimintamallien hyödyntäminen nostettiin mahdollisuudeksi oppia vastaavanlaisesta toimintaympäristöstä. Haastatellut olivat eri mieltä siitä, pitäisikö IT:n johtaa koko teknologiaportfoliota parhaita käytäntöjään soveltaen myös rakennuksen OT-ympäristöön, pitäisikö johtamisvastuun

olla substanssista vastaavalla taholla vai pitäisikö näiden organisaatioiden välille muodostaa yhteisiin tavoitteisiin perustuva yhteistyömalli. Haastatteluissa nostettiin kuitenkin esille myös se, että IT:n johtamismallejakin on erilaisia, joten jokaisen mallin pitäisi olla valittu juuri kyseistä organisaatiota, sen tavoitteita ja toimintaympäristöä ajatellen.

6 DIGIRES-KANVAASI

Tutkimuksen avulla määritettiin jatkuvuudenhallintaan liittyviä keskeisiä teemoja ja näihin liittyen tärkeitä aiheita. Tulosten pohjalta laadittiin OT-ympäristön jatkuvuudenhallintaa ja digitaalisen resilienssin kehittämistä tukeva työkalu, DIGIRES-kanvaasi (liite 6). Kanvaasi testattiin kolmella asiantuntijalla ja tarvittavat muutokset ensimmäistä versiota varten tehtiin kommenttien pohjalta. Kaikki oikeudet pidätetään DIGIRES-kanvaasin eli tutkimuksen tekijällä.

DIGIRES-kanvaasi kuvattiin A0-pohjalle, jotta sitä voidaan hyödyntää kollaboraatiotyökalussa (esimerkiksi Miro) tai läsnäolotyöpajassa A0-kokoiseksi tulostettuna. DIGIRES-kanvaasi sisältää 24 tutkimuksen pohjalta tunnistettua rakennuksen järjestelmäympäristöä kuvaavaa kohtaa, joihin lisätään tiedot käsiteltävään rakennukseen liittyen. Kanvaasi sisältää kohdekohtaisen ohjeistuksen. Järjestelmien välisiä riippuvuuksia ei sisällytetty kanvaasiin, sillä sitä varten on olemassa hyviä arkkitehtuurin mallinnustyökaluja.

Työskentely DIGIRES-kanvaasin avulla tuottaa tietoa rakennuksen järjestelmäympäristön jatkuvuudenhallintaan sekä häiriöhallintaan liittyen. Vaikka tietoa on paljon, on tiedot nähtävissä yhdellä silmäyksellä. Kriittiseksi koetut ja erityisiä toimenpiteitä vaativat kohdat voidaan kirjoittaa esimerkiksi huomioväriselle lapulle tai merkitä tarralla. Näin tilanteen sekä muutosten seuranta ylätasolla on mahdollista yhdellä silmäyksellä. Koska rakennuksen järjestelmäympäristö muuttuu paljon rakennuksen elinkaaren aikana, on DIGIRES-kanvaasin sisältöä päivitettävä aika-ajoin.

DIGIRES-kanvaasi toteutettiin Huoltovarmuusorganisaation yksityisen turvaalan poolin toimeksiannosta ensisijaisesti jaettavaksi Huoltovarmuusorganisaatiolle tukemaan huoltovarmuuskriittisten rakennusten jatkuvuudenhallintaa.

DIGIRES-kanvaasin käyttö hyödyttää kuitenkin mitä tahansa rakennusten järjestelmäympäristöstä vastaavaa tahoa. Koska kanvaasi oikein täytettynä sisältää rakennuksen toiminnan kannalta tärkeää ja jopa kriittistä tietoa, on sen säilytyksestä tai pääsynhallinnasta huolehdittava erityisellä tarkkuudella.

Suomenkielisen DIGIRES-kanvaasin rinnalle on suunniteltu toteutettavaksi ruotsinkielinen versio, jotta kanvaasi tarjoaisi hyödyn mahdollisimman kattavasti Suomessa sijaitsevien rakennusten jatkuvuudenhallintaan liittyen. Kanvaasin käytettävyydestä saatiin palautetta testaajilta ja jatkokehitykselle relevantit muutokset on tarkoitus toteuttaa seuraavaan versioon. Myös kanvaasin digitalisointi on suunnitteilla.

7 JOHTOPÄÄTÖKSET

Tutkimushypoteesi asetettiin rohkeasti kyseenalaistaen joiltakin osin rakennuksen OT-ympäristön kokonaisuudenhallintaan ja digitaaliseen resilienssiin liittyvät prosessit. Johtopäätöksenä voidaan todeta tutkimushypoteesia tukevat seuraavat tutkimustuloksista ilmenevät seikat: Haastattelujen perusteella rakennuksen OT-järjestelmäympäristöä ei käsitellä kokonaisuutena, vaan yksittäisinä eri toimintoihin liittyvinä järjestelminä ja siiloina. Kokonaisuudenhallinta on puutteellista ja se aiheuttaa digitalisoituneeseen ympäristöön epäjatkuvuuskohtia. Neljännes (n = 64) kyselyyn vastanneista totesi, ettei organisaatio ole osoittanut käytössään olevia rakennuksia minkään tahon vastuulle ja enintään 39 % (n = 64) kyselyyn vastanneista totesi kriittisissä tai organisaation toiminnalle keskeisissä kohteissa olevien OT-järjestelmien olevan melko kattavasti tai täysin kyseisen organisaation vastuulla. Haastatteluista tai kyselytutkimuksesta ei löytynyt linjassa olevia seikkoja, jotka olisivat vahvistaneet sen, että rakennuksen OT-ympäristö olisi tunnistettu yhtenäiseksi järjestelmäkokonaisuudeksi ja sitä sellaisena johdettaisi. Ennemminkin painotettiin sitä, että näin ei tehdä. Björckin ym. (2015, 312) mukaan digitaalisen resilienssin varmistamiseksi ympäristöä on nimenomaan käsiteltävä holistisesti, useilla eri tasoilla ja rinnakkain. Jatkuvuudenhallintaan sisältyy ISO 22301 -standardin (ISO 2015, 25–28) mukaisesti suorituskyvyn sekä toiminnan tehokkuuden ylläpito sekä toiminnan jatkuva kehittäminen perustuen laadullisiin ja määrällisiin jatkuvuudenhallintajärjestelmän soveltuvuutta ja vaikuttavuutta mittaaviin tu-

loksiin. Haastateltavat eivät tunnistaneet yhtä vastaajaa lukuun ottamatta sellaista standardia, mallia tai työkalua, jolla jatkuvuudenhallintaa voisi toteuttaa kaikki OT-järjestelmät kattavasti ja jota vasten auditointeja voisi tehdä ja onnistumista mitata. Toisaalta 75% kyselyyn vastanneista (n=57) totesi seurannan, mittaamisen, analysoinnin sekä arvioinnin olevan maturiteettitasoltaan vähintään perustasolla. Mittaamisen osalta olikin tunnistettava selkeä eroavaisuus haastattelujen ja kyselytutkimuksen välillä ja näiden osalta tutkimusta on syytä jatkaa. Kuitenkin ylätasolla tutkimustuloksista voidaan päätellä, että rakennuksen OT-ympäristön jatkuvuudenhallintaa ei ole kehitetty tukemaan ympäristön digitaalista resilienssiä ja näin ollen tutkimushypoteesi pätee valitulla kohderyhmällä.

Vaikka tulokset olivat tutkimushypoteesin osalta osin ristiriitaisia keskenään, voidaan siitä huolimatta sekä määrällisen että laadullisen tutkimuksen tutkimuksesta löytää yhtenäinen linja. Yhtenäistä koko rakennuksen OT-ympäristön läpileikkaavaa johtamismallia, linjaa tai johtamisen tapaa ei löytynyt, eikä näin ollen koko ympäristön kattavaa jatkuvuudenhallintamallia vaikuta olevan yleisesti käytössä. Osittain ristiriitaisista tuloksista sekä aiempien tutkimustulosten vähyydestä tai puuttumisesta johtuen tutkimusta on kuitenkin syytä jatkaa.

Tutkimuskysymyksen osalta voidaan todeta, että tutkimus tuotti erinomaista aineistoa OT-ympäristön jatkuvuudenhallinnan työkalun toteuttamista varten. Kuhunkin kysymykseen saatiin tutkimuksen aikana vastaukset niin laadullisen kuin määrällisen tutkimuksen osalta. Vastaukset olivat varsin hyvin linjassa keskenään ja näiden perusteella laadittiin kohdassa 6 sekä liitteessä 7 esitetty Rakennuksen digitaalinen resilienssi DIGIRES -kanvaasi.

7.1 Pohdinta

Tutkimus avasi mielenkiintoisen näkökulman digitalisoituvan kiinteistö- ja rakentamisalan ytimeen. Se vahvisti tutkimuksen lähtötilanteessa olleen näkemyksen rakennuksen järjestelmäympäristön johtamiseen ja hallintaan liittyvistä haasteista. Se myös vahvisti uusien palveluiden ja mallien kehittämisen

tarpeen nopeasti muuttuvassa rakennetussa ympäristössä. Se vahvisti yhteistyön, uteliaisuuden ja avoimuuden ilmapiirin välttämättömyyden uuden oppimisen ja uuden luomisen edellytyksenä.

Tutkimus myös nosti esille osaltaan Suomen huoltovarmuuskriittisten toimijoiden sitoutuneisuuden rakennuksen OT-ympäristön jatkuvuudenhallinnan kehittämiseen ja ylläpitoon. Tutkimukseen osallistuneet tekivät sen mielenkiinnosta ajankohtaista aihetta kohtaan ja oppiakseen uutta. Järjestäen jokaisella haastatellulla henkilöllä oli vankka ymmärrys teemaan liittyen omasta näkökulmastaan. Jokainen piti erinomaisena sitä, että tällaista tutkimusta tehdään ja moni toivoi sitä tehtävän enemmänkin. Jokainen piti OT-ympäristön jatkuvuudenhallinnan mallin kehittämistä tervetulleena keinona oman organisaationsa järjestelmäympäristön digitaalisen resilienssin varmistamiseksi siitäkin huolimatta, että joukossa oli myös perinteisemmän suljetun järjestelmäympäristön toteutustavan edustajia.

Monimenetelmäinen tutkimusote osoitti eroavaisuuksia eri tutkimusmenetelmistä saatujen tulosten välillä. Se herätti kysymyksiä, mutta antoi myös riittävästi vastauksia tutkimuksen loppuunsaattamiseksi. Tutkimuksen mahdollistikin huolellisesti laadittu laaja tutkimussuunnitelma, vaikka yleisesti aihealueeseen liittyvien tieteellisten tutkimusten vähäisyys uhkasi kasvattaa työmäärää liian suureksi. Kuitenkin tutkimussuunnitelman ansiosta tähän monimenetelmäiseen tutkimukseen käytetty työmäärä ja lopputulos pysyivät maltillisissa rajoissa, vaikka monimenetelmäisyys lisäsikin tutkimuksen haasteellisuutta.

On asioita, joita olisi kannattanut tehdä toisin. Keskeisimpinä mainittakoon haastavaksi tunnistetun kohderyhmän saavutettavuuden varmistaminen. Johtuen suljetusta kohderyhmästä, olisi kyselytutkimuksen kohderyhmän peiton varmistamiseksi pitänyt prosessia tarkentaa tehtyä huolellisemmin. Tämä olisi varmistanut tutkimuksen lopputuloksen paremman luotettavuuden ja vertailtavuuden yli kaikkien määriteltyjen toimialojen. Kyselytutkimuksen kysymykset laadittiin kuitenkin niin, että tutkimus on mahdollista ja myös mielekästä toistaa määrävälein tulosten kehittymisen seuraamiseksi.

7.2 Jatkotoimenpiteet

Määrällinen tutkimus voidaan kohdistaa kattamaan kaikki kohderyhmän kiinteistöt sekä myös kohderyhmän ulkopuolelle jäävät toimijat. Näin saadaan yleistä vertailutietoa rakennuksen OT-ympäristön jatkuvuudenhallinnan maturiteettitasosta sekä digitaalisen resilienssin tilasta.

Tutkimus ei ottanut suoranaisesti kantaa Suomen huoltovarmuudelle kriittisten rakennusten järjestelmäympäristön tulevaisuuden näkymiin. Digitalisoituneen rakennuksen OT-ympäristön jatkuvuudenhallinta tunnistettiin kuitenkin tärkeäksi rakennuksen digitaalista resilienssiä tukevaksi teemaksi. Koska eri menetelmistä saatiin osin ristiriitaisia tuloksia, on syytä pohtia, miten rakennuksista vastaavien organisaatioiden vastuuhenkilöiden osaaminen saadaan riittävälle tasolle. Koska kyse ei ole vain yhden toiminnon kehittämisestä, on osaamista kehitettävä organisaation matriisissa kattaen kaikki teemaan liittyvät toiminnot. Yhteisen tavoitteen löytäminen eri toimintojen välillä tuleekin varmasti luomaan uusia mahdollisuuksia, kustannussäästöjä ja toiminnan tehostamisen väyliä. Toiminnan laadun parantaminen taas lisää yleisesti organisaation resilienssiä ulkoisia uhkia vastaan.

Nopeasti muuttuvassa maailmassa tämän päivän haastavimmat uhat voivat muistuttaa tulevaisuudessa vanhoista hyvistä ajoista. Tekoäly kehittyy prosesseja palvelevaksi automaatioksi korvaten useita työtehtäviä ja avaten huikeita mahdollisuuksia. Samalla uhat tekoälyn hyödyntämiseksi rikollisiin toimiin lisääntyvät. Kvanttitietokoneista kirjoitetaan jo uhkana vahvalle tunnistautumiselle ja kaikelle pääsynhallinnalle fyysisessä ja digitaalisessa maailmassa. Vaikka digitalisoitunut OT-ympäristö voi vaikuttaa vielä etäiseltä ja vaikeasti hahmotettavalta kokonaisuudelta, kannattaa silti jo seuraavaksi ottaa selvää, mitä nurkan takana näkyy ja miltä tulevaisuus mahdollisesti näyttää.

Koska tutkimus oli rajattu käsittelemään huoltovarmuuskriittisiä toimijoita Suomessa, näkyi vastauksissa joiltakin osin systemaattisuus, huoli ja toimijan vastuu osana huoltovarmuusorganisaatiota. Kehitettäviä asioita ja haasteita tunnistettiin kuitenkin paljon ja voikin olettaa, että koska muilla organisaatioilla ei ole vastaavanlaista huoltovarmuusvelvoitetta, voi tilanne näiden osalta olla ra-

kennusten digitaalisen resilienssin ja jatkuvuudenhallinnan kannalta huomattavasti heikompi. Näin ollen onkin syytä arvioida tutkimuksen laajentamista kattamaan myös tutkimuksen ulkopuolelle rajatut rakennuksista vastuussa olevat organisaatiot. Tämä tukisi yleisesti Suomen digitaalista resilienssiä ja osaamisen lisääntymistä sekä kriittisten toimenpiteiden tunnistamista aikana, jolloin kyberturvallisuuteen liittyvät teemat ovat erittäin ajankohtaisia. Voidaan myös todeta tämän tutkimuksen herättäneen sellaisia kysymyksiä ja ajatuksia tutkimukseen osallistuneiden tahojen joukossa, että tämä tutkimus toivottavasti toimii ponnahduslautana monelle innovatiiviselle idealle, yhteistyölle ja jopa uusien liikeideoiden kehittämiselle. Koska tarve on olemassa, mutta teema on vielä vieras, on juuri tämä hyvä hetki uudelle alulle.

Tutkimuksen teemaan liittyen on syytä jatkaa jatkuvuudenhallinnan työkalun kehittämistä sitä käyttäviltä organisaatioilta saatavan palautteen perusteella. Koska tietokirjallisuutta digitalisoituneiden ja älykkäiden rakennusten ja kiinteistöjen suunnitteluun, toteuttamiseen ja ylläpitoon liittyen ei vielä ole riittävästi saatavilla, on tämän tutkimuksen pohjalta mahdollista vastata myös tähän tarpeeseen.

7.3 Lopuksi

Tutkimusprosessi oli mielenkiintoinen, pitkä ja haastava. Se sisälsi ylämäkiä, alamäkiä ja aavoja lakeuksia. Se alkoi hitaasti ja päättyi nopeasti. Ja mikä tärkeintä, se tiivisti otsikon ytimen; Rakennusten järjestelmäympäristön digitaalista resilienssiä on lisättävä jatkuvuudenhallintaa kehittämällä.

LÄHTEET

Adams, E. K., Gunter, D., Kiser, R., Krenz, M., Peisert, S., Sons, S. & Zage, J. 2022. Findings of the 2022 Trusted CI Study on the Security of Operational Technology in NSF Scientific Research. PDF-dokumentti. Saatavissa: https://doi.org/10.5281/zenodo.6828675 [viitattu 20.2.2023]

Akailvi, S., Gautam, U., Bhandari, P., Rashid, H., Huff, P. D. & Springer, J. P. 2022. HELOT – Hunting Evil Life in Operational Technology. *IEEE Transactions on Smart Grid* 2022, 1–14. Saatavissa: https://doi.org/10.1109/TSG.2022.3222261 [viitattu 13.2.2023]

Alberts, D. S. 2011. The Agility Advantage: A Survival Guide for Complex Enterprises and Endeavors. Department of Defence: CCRP Publication Series 09/2011, 1–616. PDF-dokumentti. Saatavissa: https://apps.dtic.mil/dtic/tr/fulltext/u2/a631225.pdf [viitattu 16.2.2023]

Al Dakheel, J., Del Pero, C., Aste, N. & Leonforte, F. 2020. Smart buildings features and key performance indicators: A review. *Sustainable cities and society 2020* 61, 102328. Saatavissa: https://doi.org/10.1016/j.scs.2020.102328 [viitattu 29.7.2023]

Alderson, D. L., Brown, G. G. & Carlyle, W. M. 2015. Operational Models of Infrastructure Resilience. *Risk Analysis* 4, 562–586. Saatavissa: https://doi.org/10.1111/risa.12333 [viitattu 13.2.2023]

Arora, A., Wright, V. & Garman, C. 2022. Strengthening the Security of Operational Technology: Understanding Contemporary Bill of Materials. *Journal of Critical Infrastructure Policy* 1, 111–135. Saatavissa: https://doi.org/10.18278/jcip.3.1.8 [viitattu 19.2.2023]

Bailey, R., Stepanenko, K., Mappes, G., Howard, A., Barros, G., Philipson, L. & Kagan, F. 2023. Russian Offensive Campaign Assessment, March 9, 2023. Institute for the Study of War and the Critical Threats Project 2023, 1–2. PDF-dokumentti. Saatavissa: https://www.understandingwar.org/sites/default/files/Russian%20Operations%20Assessments%20March%209%202023.pdf [viitattu 5.7.2023]

Berkeley III, A. R. & Wallace, M. 2010. A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations. *National Infrastructure Advisory Council: Washington DC, USA,* 1–85. PDF-dokumentti. Saatavissa: https://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf [viitattu 16.2.2023]

Björck, F.; Henkel, M.; Stirna, J.; Zdravkovic, J. 2015. Cyber resilience - Fundamentals for a definition. *Advances in Intelligent Systems and Computing* , 311–316. Saatavissa: https://doi.org/10.1007/978-3-319-16486-1_31 [viitattu 16.2.2023]

Drewitt, T. 2013. A Manager's Guide to ISO22301: A practical guide to developing and implementing a business continuity management system. IT Governance Publishing: Cambridgeshire, UK. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 19.2.2023]

Dufva, M. 2020. Megatrendit 2020. PDF-dokumentti. Saatavissa: https://www.sitra.fi/app/uploads/2019/12/megatrendit-2020.pdf [viitattu 29.7.2023]

Dufva, M. & Rekola, S. 2023. Megatrendit 2023 – ymmärrystä yllätysten aikaan. PDF-dokumentti. Saatavissa: https://www.sitra.fi/app/uploads/2023/01/sitra_megatrendit-2023_ymmarrysta-yllatysten-aikaan.pdf [viitattu 29.7.2023]

Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555.

Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557.

Euroopan parlamentti. 2023 a. Rakennusten energiatehokkuus: EU-parlamentti hyväksyi kantansa. Lehdistötiedote 14.3.2023. WWW-dokumentti. Saatavissa: https://www.europarl.europa.eu/news/fi/press-room/20230310IPR77228/rakennusten-energiatehokkuus-eu-parlamentti-hyvaksyi-kantansa [viitattu 19.8.2023]

Euroopan parlamentti. 2023 b. EU:n toimet energiankulutuksen vähentämiseksi. WWW-dokumentti. Saatavissa: https://www.europarl.europa.eu/news/fi/headlines/society/20221128STO58002/eu-n-toimet-energiankulutuksen-vahentamiseksi [viitattu 19.8.2023]

Heikkilä, T. 2014. Tilastollinen tutkimus. E-kirja. Helsinki: Edita

Hirsjärvi, S. & Hurme, H. 2022. Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö. Gaudeamus: Helsinki. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 19.2.2023]

Holling, C. S. 1996. Engineering Resilience versus Ecological Resilience. Teoksessa: National Academy of Engineering (toim.) Engineering Resilience within Ecological Constraints. Washington, DC: The National Academies Press, 31–44. Saatavissa: https://doi.org/10.17226/4919 [viitattu 16.2.2023]

Huoltovarmuuskeskus. 2021. Digitaalinen turvallisuus 2030. WWW-dokumentti. Saatavissa: https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio/huoltovarmuuskeskus/4962-2/digitaalinen-turvallisuus-2030 [viitattu 11.1.2023]

Huoltovarmuuskeskus. s.a.a. Huoltovarmuusorganisaatio. WWW-dokumentti. Saatavissa: https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio [viitattu 11.1.2023]

Huoltovarmuuskeskus. s.a.b. Sektorit ja poolit. WWW-dokumentti. Saatavissa: https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio/sektorit-ja-poolit [viitattu 11.1.2023]

Huoltovarmuuskeskus. s.a.c. Yksityinen turva-ala. WWW-dokumentti. Saatavissa: https://www.huoltovarmuuskeskus.fi/toimialat/yksityinen-turva-ala [viitattu 11.1.2023]

Huoltovarmuuskeskus. s.a.d. Toimialat. WWW-dokumentti. Saatavissa: https://www.huoltovarmuuskeskus.fi/toimialat [viitattu 3.7.2023]

Hurmerinta, L. & Nummela, N. 2020. Monimenetelmätutkimus. Teoksessa Juuti, P. & Puusa, A. (toim.) Laadullisen tutkimuksen näkökulmat ja menetelmät. Helsinki: Gaudeamus. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 19.2.2023]

ISO. 2019. SFS-EN ISO 22301:2019 Turvallisuus ja kriisinkestävyys. Vaatimukset. Käännös alkuperäisestä julkaisusta SFS-EN ISO 22301:2019:en Security and resilience. Business continuity management systems. Requirements. *Suomen Standardoimisliitto SFS Ry*, 2, 5, 27–28. PDF-dokumentti. Saatavissa: https://online.sfs.fi/fi/index/tuotteet/SFS/CENISO/ID2/2/871697.html.stx [viitattu 25.5.2023]

Israel National Cyber Directorate. 2020/2022. Cyberrisk Management in the Operational Technology (OT) Environment A Guide for Boards of Directors. *INCD Cybersecurity Best Practices* A10, 1–31. PDF-dokumentti. Saatavissa: https://doi.org/10.18235/0004370 [viitattu 19.2.2023]

Kallinen, K., Pirskanen, H. & Rautio, S. 2022. Sensitiivinen tutkimuksessa : menetelmät, kohderyhmät, haasteet ja mahdollisuudet. Boca Raton, FL: United Press. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 19.2.2023]

Ketokivi M. 2015. Tilastollinen päättely ja tieteellinen argumentointi. E-kirja. Helsinki: Gaudeamus

Khatibi, H., Wilkinson, S., Eriwata, G., Sweya, L. N., Baghersad, M., Dianat, H. & Javanmardi, A. 2022. An integrated framework for assessment of smart city resilience. *Urban Analytics and City Science* 5, 1556–1577. Saatavissa: https://doi.org/10.1177/23998083221092422 [viitattu 12.2.2023]

Kiinteistöverolaki 20.7.1992/654.

Koffka, K. 1935. Principles of Gestalt Psycologhy. New York: Harcourt, Brace and Company. Saatavissa: https://archive.org/details/in.ernet.dli.2015.7888/mode/2up [viitattu 9.3.2023]

Kosmowski, K. T., Piesik, E., Piesik, J. & Sliwinski, M. 2022. Integrated Functional Safety and Cybersecurity Evaluation in a Framework for Business Continuity Management. *Energies* 15, 3610. Saatavissa: https://doi.org/10.3390/en15103610 [viitattu 13.2.2023]

Madni, A. M. & Jackson, S. 2009. Towards a conceptual framework for resilience engineering. *IEEE Systems Journal* 2, 181–191. Saatavissa: https://doi.org/10.1109/JSYST.2009.2017397 [viitattu 16.2.2023]

Moghaddam, A. & Deshmukh, A. 2019. Resilience of cyber-physical manufacturing control systems. *Manufacturing Letters* 20, 40–44. Saatavissa: https://doi.org/10.1016/j.mfglet.2019.05.002 [viitattu 21.8.2023]

Nan, C. & Sansavini, G. 2016. A quantitative method for assessing resilience of interdependent infrastructures. *Reliability Engineering and System Safety* 157, 35–53. Saatavissa: https://doi.org/10.1016/j.ress.2016.08.013 [viitattu 12.2.2023]

NIST. 2023. Updating the NIST Cybersecurity Framework – Journey To CSF 2.0. WWW-sivu. Saatavissa: https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20 [viitattu 20.8.2023]

Oxford. 1963. The Advanced Learner's Dictionary of Current English. Oxford: Oxford University Press.

Park, J., Seager, T. P., Rao, P. S. C., Convertino, M. & Linkov, I. 2013. Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems. *Risk Analysis* 3, 356–367. Saatavissa: https://doi.org/10.1111/j.1539-6924.2012.01885.x [viitattu 16.2.2023]

Park, E., del Pobil, A. P. & Kwon, S. J. 2018. The Role of Internet of Things (IoT) in Smart Cities: Technology Roadmap-oriented Approaches. *Sustainability* 10, 1–13. Saatavissa: https://doi.org/doi:10.3390/su10051388 [viitattu 13.2.2023]

Petrenko, S. 2019. Cyber Resilience. E-kirja. Gistrup: River Publishers.

Petrenko, S. 2021. Developing an Enterprise Continuity Program. E-kirja. Gisturp: River Publishers.

Puusa, A. 2020. Näkökulmia laadullisen aineiston analysointiin. Teoksessa Juuti, P. & Puusa, A. (toim.) Laadullisen tutkimuksen näkökulmat ja menetelmät. E-kirja. Helsinki: Gaudeamus

Puusa, A. & Juuti, P. 2020. Laadullisen tutkimuksen näkökulmat ja menetelmät. E-kirja. Helsinki: Gaudeamus.

Rothrock, R. A. 2022. Digital Resilience: Is Your Company Ready for the Next Cyber Threat? Äänikirja. New York: Gildan Media

Saaed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E. & Alabbad, D.A. 2023. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors 2023*, 23, 6666. Saatavissa: https://doi.org/10.3390/s23156666 viitattu [19.8.2023]

Sanchis, R., Canetta, L. & Poler, R. 2020. A Conceptual Reference Framework for Enterprise Resilience Enhancement. *Sustainability* 12, 1–27. Saatavissa: https://doi.org/doi:10.3390/su12041464 [viitattu 13.2.2023]

Sarkar, S., Teo, Y. T. & Chang, E-C. 2022. A cybersecurity assessment framework for virtual operational technology in power system automation. *Simulation Modelling Practice and Theory* 117, 102453. Saatavissa:

https://doi.org/10.1016/j.simpat.2021.102453 [viitattu 12.2.2023]

Sathurshan, M., Saja, A., Thamboo, J., Haraguchi, M. & Navaratnam, S. 2022. Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Framework. *Infrastructures* 67 1–26. Saatavissa: https://doi.org/10.3390/infrastructures7050067 [viitattu 13.2.2023]

Sevaldson, B. 2011. GIGA-mapping: Visualisation for complexity and systems thinking in design. PDF-dokumentti. Saatavissa: https://dl.designresearchsociety.org/cgi/viewcontent.cgi?article=1252&context=nordes [viitattu 20.8.2023]

Sitra. s.a. Tulevaisuussanasto: Digitaalinen ja vihreä kaksoissiirtymä. WWW-sivu. Saatavissa: https://www.sitra.fi/tulevaisuussanasto/digitaalinen-ja-vihrea-kaksoissiirtyma/ [viitattu 29.7.2023]

Silander, H. & Sormunen, P. s.a. Licence to Breathe, artikla 9: Case KampusAreena – Ilmanvaihdon käyttötapojen merkitys Covid-19-tartunnoissa. Saatavissa: https://content-webapi.tuni.fi/proxy/public/2021-05/09-case-kampusareena-ilmanvaihdon-kayttotapojen-merkitys.pdf [viitattu 19.8.2023]

Sinopoli, J. 2016. Advanced Technology for Smart Buildings. London: Artech House. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 19.2.2023]

Starr, C. W., Saginor, J. & Worzala, E. 2021. The rise of PropTech: emerging industrial technologies and their impact on real estate. *Journal of Property Investment & Finance* 39, 157–169. Saatavissa: https://doi.org/10.1108/JPIF-08-2020-0090 [viitattu 21.8.2023]

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri & V., Lightman, S. 2022. Guide to Operational Technology (OT) Security. *NIST Special Publication 800-82r3 ipd*, 1–142. PDF-dokumentti. Saatavissa: https://doi.org/10.6028/NIST.SP.800-82r3.ipd [viitattu 19.2.2023]

Tilastokeskus. 2022. Venäjältä tuodun energian osuus 18 % energian kokonaiskulutuksesta vuonna 2022. WWW-sivu. Saatavissa: https://www.stat.fi/julkaisu/clhomy00rtq7g0buvlkdxhfig [viitattu 19.8.2023]

The White House. 2013. Presidential Policy Directive -- Critical Infrastructure Security and Resilience. *Presidential Policy Directive/PPD-21.* WWW-dokumentti. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [viitattu 16.2.2023]

Trimintzios, P., Chatzichristos, G., Portesi, S., Drogkaris, P., Palkmets, L., Liveri, D. & Dufkova, A. 2017. Cybersecurity in the EU Common Security and Defence Policy (CSDP) – Challenges and risks for the EU. *European Parliamentary Research Service* EPRS/STOA/SER/16/214N. PDF-dokumentti. Saatavissa: https://doi.org/10.2861/853031 [viitattu 13.2.2023]

VAHTI. 2016. Toiminnan jatkuvuuden hallinta. *Valtiovarainministeriön julkaisu VAHTI 2/2016*. PDF-dokumentti. Saatavissa: http://urn.fi/URN:ISBN:978-952-251-779-1 [viitattu 13.2.2023]

Valtioneuvosto. 2022. Valtioneuvoston huoltovarmuusselonteko. *Valtioneuvoston julkaisuja* 2022:59. PDF-dokumentti. Saatavissa: http://urn.fi/URN:ISBN:978-952-383-803-1 [viitattu 13.2.2023]

Vugrin, E. D., Warren, D. E., Ehlen, M. A., Camphouse, R. C. 2010. A Framework for Assessing the Resilience of Infrastructure and Economic Systems. Teoksessa Gopalakrishnan, K., Peeta, S. (toim.) Sustainable and Resilient Critical Infrastructure Systems. Berlin: Springer, 77–116. Saatavissa: https://doi.org/10.1007/978-3-642-11405-2_3 [viitattu 16.2.2023]

Walker, B., Holling, C. S., Carpenter, S. & Kinzig, A. 2004. Resilience, adaptability and transformability in social-ecologigal systems. *Ecology and society* 2, 1–9. Saatavissa: https://doi.org/10.5751/ES-00650-090205 [viitattu 16.2.2023]

Williams, C. & You, J. J. 2022. Organizing for Resilience: Leading and Managing Risk in a Disruptive World. E-kirja. New York: Routledge

Woodhead, R., Stephenson, P. & Morrey, D. 2018. Digital construction: From point solutions to IoT ecosystem. *Automation in Construction* 93, 35–46. Saatavissa: https://doi.org/10.1016/j.autcon.2018.05.004 [viitattu 13.2.2023]

Woods, D. D. 2006. Essential characteristics of resilience. Teoksessa Hollnagel, E., Woods, D.D., Leveson, N. (toim.) Resilience Engineering: Concepts and Precepts. Burlington, VT: Ashgate, 21–34. Saatavissa: https://www.researchgate.net/publication/284328979_Essential_characteristics_of_resilience [viitattu 16.2.2023]

Saate haastatteluun osallistuville

Hei,

tulen haastattelemaan sinua Kaakkois-Suomen ammattikorkeakoulun (XAMK) opintoihini kuuluvaan YAMK-opinnäytetyöhön liittyen. Tutkimukseni keskittyy rakennusten järjestelmäympäristön jatkuvuudenhallintaan sekä digitaaliseen resilienssiin. Tutkimuksen tilaaja on Huoltovarmuusorganisaation Yksityisen turva-alan pooli. Työtä ohjaa Atte Kokkinen Huoltovarmuuskeskuksesta ja Nina Hartikainen XAMKista. Osallistumalla haastatteluun tuotat arvokasta tietoa siitä, millä tavalla rakennusten järjestelmäympäristön jatkuvuutta tulisi hallita ja kehittää ja mitkä tähän omasta mielestäsi ovat parhaat menetelmät ja välineet. Hyödynnän saamaani tietoa rakennusten toimintaa ohjaavan järjestelmäympäristön jatkuvuudenhallintaa tukevan työkalun kehittämisessä.

Haastattelu kohdistuu erityisesti huoltovarmuuden kannalta keskeisiin toimijoihin. Haastattelu on täysin luottamuksellinen, eikä vastaajan henkilöllisyys, yritys tai toimiala paljastu tutkimuksen missään vaiheessa. Noudatan tutkimuksessa Tutkimuseettisen neuvottelukunnan ohjeistoa (https://www.tenk.fi/fi/hyva-tieteellinen-kaytanto). Lähetän haastattelun saatekirjeen tiedoksi (cc) myös Atte Kokkiselle ja todistan henkilöllisyyteni tilaisuuden alussa.

Kyseessä on monimenetelmäiseen tapaustutkimukseen kuuluva puolistrukturoitu teemahaastattelu, joka tarjoaa mahdollisuuden tarvittaessa joustavalle keskustelulle. Lähetän ohessa kysymyksiä käsiteltävään teemaan liittyen. Voit tutustua niihin halutessasi ja ehtiessäsi etukäteen. Olen varannut Teamsin kautta pidettävään haastatteluun 30 minuuttia. Tallennan haastattelun tutkimustyön ajaksi, mikäli se sinulle sopii. Tutkimusaika on maalis-huhtikuu 2023. Mikäli organisaationne vaatii tutkimusluvan ja/tai NDA:n haastattelua varten, sovin näistä mielelläni.

Ystävällisin terveisin,

Hanna Pikkusaari
dhapi003@edu.xamk.fi
+358 50 310 4984

Konteksti:

Jatkuvuudenhallinta on organisaatioiden omaehtoista varautumista kriiseihin sekä häiriötilanteisiin (Valtioneuvosto 2022, 40, 58). Jatkuvuudenhallinta on myös keskeinen osa organisaation riskienhallintaa. Sillä varaudutaan erityisesti sellaisiin häiriötilanteisiin, jotka voivat aiheuttaa merkittävää haittaa organisaation kyvylle tuottaa sen ydinpalveluita. (Drewitt 2013, 11; Hopkin 2012, 188.)

Resilienssin määritelmä riippuu näkökulmasta sekä kulloinkin asiayhteydessä käsiteltävistä suureista (Sathursan ym. 2022, 2). Koska tutkimus keskittyy teknisen ympäristön resilienssiin sekä jatkuvuuden hallintaan, on tässä kyse pääasiassa teknisestä ja digitaalisesta eli kyberresilienssistä (Alderson ym. 2015, 562, Björck ym. 2015, 311, Petrenko 2019, 7), mutta myös organisaation kyvykkyydestä sopeutua vallitsevaan tilanteeseen (Sanchis ym. 2020, 1).

Teemahaastattelun kysymyksiä:

- Miten hallitset tai hallitsisit rakennuksen järjestelmäympäristön jatkuvuutta käytännön tasolla? Mikä tekee prosessista mahdollisimman helppoa tai suoraviivaista?
- Tunnistatko omasta näkökulmastasi hyviä malleja, käytännön menetelmiä tai työkaluja aiheeseen liittyen? Voisitko kuvailla näitä tarkemmin? Mitkä teemat/asiat/järjestelmät/järjestelmäkokonaisuudet niissä korostuvat? Mitä puuttuu, mitä lisäisit?
- Minkälaisia haasteita olet kohdannut rakennuksen järjestelmäympäristön hallintaan ja jatkuvuudenhallintaan liittyen? Eroavatko ne eri elinkaaren vaiheissa? Jos kyllä, niin miten?
- Eroavatko eri aihealueiden jatkuvuudenhallinnan (esimerkiksi liiketoiminta, IT, OT) käytännöt toisistaan? Miten? Voisiko joitakin eri aihealueiden käytäntöjä soveltaa rakennuksen järjestelmäympäristöön liittyen?
- Millaisia sidosryhmiä aihealueeseen liittyy? Millaista yhteistyötä näiden välillä tehdään? Miten näitä johdetaan tai pitäisi johtaa? Prosessit, vuosikello, aikataulutus?
- Miten koet digitaalisen resilienssin merkityksen teidän ydinprosessien kannalta tärkeimpiin rakennuksiin liittyen?
- Näetkö, että rakennusten järjestelmäympäristön jatkuvuus on kriittistä teidän liiketoiminnallenne?

Lähteet:

Alderson, D. L., Brown, G. G. & Carlyle, W. M. 2015. Operational Models of Infrastructure Resilience. *Risk Analysis* 4, 562-586. Saatavissa: https://doi.org/10.1111/risa.12333 [viitattu 14.2.2023]
Björck, F.; Henkel, M.; Stirna, J.; Zdravkovic, J. 2015. Cyber resilience - Fundamentals for a definition. Advances in Intelligent Systems and Computing , 311–316. Saatavissa: https://doi.org/10.1007/978-3-319-16486-1_31 [viitattu 16.2.2023]
Drewitt, T. 2013. A Manager's Guide to ISO22301: A practical guide to developing and implementing a business continuity management system. IT Governance Publishing: Cambridgeshire, UK. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 19.2.2023]
Hopkin, P. 2012. Fundamentals of risk management – understanding, evaluating, and implementing effective risk management. London: Kogan Page.
Petrenko, S. 2019. Cyber Resilience. Gistrup: River Publishers. E-kirja. Saatavissa: https://ebookcentral.proquest.com/lib/xamk-ebooks/detail.action?docID=5963879 [viitattu 9.3.2023]
Sanchis, R., Canetta, L. & Poler, R. 2020. A Conceptual Reference Framework for Enterprise Resilience Enhancement. *Sustainability* 1-27, 1464. Saatavissa: https://doi.org/10.3390/su12041464 [viitattu 11.2.2023]
Sathursan, M., Saja, A., Thamboo, J., Haraguchi, M. & Navaratnam, S. 2022. Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Frameworks. *Infrastructures* 67, 1. Saatavissa: https://doi.org/10.3390/infrastructures7050067 [viitattu 19.2.2023]
Valtioneuvosto. 2022. Valtioneuvoston huoltovarmuusselonteko. *Valtioneuvoston julkaisuja* 2022:59. PDF-dokumentti. Saatavissa: http://urn.fi/URN:ISBN:978-952-383-803-1 [viitattu 14.2.2023]

Kyselyn saate

Ajankohtainen kysely rakennusten järjestelmäympäristön kyberresilienssiin ja toiminnan jatkuvuudenhallintaan liittyen

Tervetuloa vastaamaan rakennuksen järjestelmäympäristön jatkuvuudenhallintaan liittyvään kyselyyn. Vastaamalla tuotat arvokasta tietoa siitä, miten itse näet organisaationne käytössä tai vastuulla olevien rakennusten järjestelmäympäristön tilan, siihen liittyvät uhat sekä mahdollisuudet ja millaisia prosesseja aihealueeseen liittyy tai tulisi liittyä. Saatua tietoa hyödynnetään rakennusten toimintaa ohjaavan järjestelmäympäristön jatkuvuudenhallintaa tukevan työkalun kehittämisessä.

Tutkimus on osa Kaakkois-Suomen Ammattikorkeakoululle tehtävää monimenetelmäistä YAMK-opinnäytetyötä. Työn on tilannut Huoltovarmuusorganisaation Yksityisen turva-alan pooli. Kysely on kohdistettu poolitoiminnan verkostolle. Kysely on täysin luottamuksellinen, eikä vastaajan henkilöllisyys paljastu tutkimuksen missään vaiheessa. Tutkimuksessa noudatetaan Tutkimuseettisen neuvottelukunnan ohjeistoa (https://www.tenk.fi/fi/hyva-tieteellinen-kaytanto).

Kyselyyn vastaaminen kestää noin 10 minuuttia. Kysely sisältää taustatietoja sekä aiheeseen liittyviä käytäntöjä kartoittavat osiot. Tutkimusaika on 28.3.-11.4.2023.

Linkki kysekyyn: https://link.webropol.com/s/jatkuvuuskysely

Mikäli haluat tutkimusraportin tutkimuksen valmistuttua, jätä sähköpostiosoitteesi tiedoksi kyselyn lopussa tai ilmoita yhteystietosi tutkimuksen tekijälle, jolta saat myös halutessasi lisätietoja aiheesta.

Hanna Pikkusaari, YAMK-opiskelija, tutkimuksen tekijä
dhapi003@edu.xamk.fi
p. 050 310 4984

Ohjaajat
Atte Kokkinen, Huoltovarmuuskeskus, atte.kokkinen@nesa.fi
Nina Hartikainen, Kaakkois-Suomen ammattikorkeakoulu (XAMK), nina.hartikainen@xamk.fi

Liite 3

Teemahaastattelurunko

- Miten hallitset tai hallitsisit rakennuksen järjestelmäympäristön jatkuvuutta käytännön tasolla?
    - Mikä tekee prosessista mahdollisimman helppoa tai suoraviivaista?
- Tunnistatko omasta näkökulmastasi hyviä malleja, käytännön menetelmiä tai työkaluja aiheeseen liittyen?
    - Voisitko kuvailla näitä tarkemmin?
    - Mitkä teemat/asiat/järjestelmät/järjestelmäkokonaisuudet niissä korostuvat? Mitä puuttuu, mitä lisäisit?
- Minkälaisia haasteita olet kohdannut rakennuksen järjestelmäympäristön hallintaan ja jatkuvuudenhallintaan liittyen?
    - Eroavatko ne eri elinkaaren vaiheissa?
    - Jos kyllä, niin miten?
- Eroavatko eri aihealueiden jatkuvuudenhallinnan (esimerkiksi liiketoiminta, IT, OT) käytännöt toisistaan?
    - Miten?
    - Voisiko joitakin eri aihealueiden käytäntöjä soveltaa rakennuksen järjestelmäympäristöön liittyen?
- Millaisia sidosryhmiä aihealueeseen liittyy?
    - Millaista yhteistyötä näiden välillä tehdään?
    - Miten näitä johdetaan tai pitäisi johtaa?
    - Prosessit, vuosikello, aikataulutus?
- Miten koet digitaalisen resilienssin merkityksen teidän ydinprosessien kannalta tärkeimpiin rakennuksiin liittyen?
    - Näetkö, että rakennusten järjestelmäympäristön jatkuvuus on kriittistä teidän liiketoiminnallenne?
    - Jäikö jotakin keskeistä käsittelemättä?

Kyselytutkimuksen kysymykset

Kysely rakennusten omistajille, käyttäjille ja ylläpitäjille: Rakennuksen järjestelmäympäristön jatkuvuudenhallinta ja digitaalinen resilienssi

Tervetuloa vastaamaan rakennuksen järjestelmäympäristön jatkuvuudenhallintaan liittyvään kyselyyn. Vastaamalla tuotat arvokasta tietoa siitä, miten itse näet yrityksenne / organisaationne käytössä olevien rakennusten järjestelmäympäristön tilan, siihen liittyvät uhat sekä mahdollisuudet ja millaisia prosesseja aihealueeseen liittyy tai tulisi liittyä. Saatua tietoa hyödynnetään rakennusten toimintaa ohjaavan järjestelmäympäristön jatkuvuudenhallintaa tukevan työkalun kehittämisessä.

Tutkimus on osa Kaakkois-Suomen Ammattikorkeakoululle tehtävää YAMK-opinnäytetyötä. Työn on tilannut Huoltovarmuusorganisaation Yksityisen turva-alan pooli. Kysely on kohdistettu poolitoiminnan verkostolle. Kysely on täysin luottamuksellinen, eikä vastaajan henkilöllisyys paljastu tutkimuksen missään vaiheessa. Tutkimuksessa noudatetaan Tutkimuseettisen neuvottelukunnan ohjeistoa (https://www.tenk.fi/fi/hyva-tieteellinen-kaytanto). Kyselyyn vastaaminen kestää noin 10 minuuttia. Kysely sisältää taustatietoja sekä aiheeseen liittyviä käytäntöjä kartoittavat osiot. Kyselyä voi jakaa organisaation sisällä. Tutkimusaika on 28.3.-11.4.2023. (vastausaikaa jatkettu 16.4.2023 saakka)

Mikäli haluat tutkimusraportin tutkimuksen valmistuttua, jätä sähköpostiosoitteesi tiedoksi kyselyn lopussa tai ilmoita yhteystietosi tutkimuksen tekijälle, jolta saat myös halutessasi lisätietoja aiheesta.

**Unfortunately, the survey is only in Finnish.
**Tyvärr finns frågeformuläret endast på finska.

Hanna Pikkusaari, YAMK-opiskelija, tutkimuksen tekijä
dhapi003@edu.xamk.fi
p. 050 310 4984

Pakollinen kysymys: Hyväksyn tietosuojakäytännöt ja vastaukseni tallentamisen tutkimuskäyttöön. Kyllä / Ei

---

Sivu 1/6

TAUSTATIEDOT

Yrityksenne / organisaationne toimiala? (Select your industry using 2-digit NACE rev 2.1 statistical classification for industries)?

- [NACE rev 2.1 tilastollisen toimialaluokituksen mukainen toimialalista]

Yrityksenne / organisaationne liikevaihto euroina?

- 1–99 999
- 100 000–199 999
- 200 000–399 999
- 400 000–999 999
- 1 000 000–1 999 999
- 2 000 000–4 999 999
- 5 000 000–9 999 999
- 10 000 000–19 999 999
- 20 000 000–49 999 999
- 50 000 000–99 999 999
- 100 000 000–249 999 999
- 250 000 000–499 999 999
- 500 000 000–

Valitse alla olevasta listasta yrityksenne / organisaationne rooli kiinteistö- ja rakentamisalalla. Voit valita useita vaihtoehtoja.

- Omistaja
- Käyttäjä
- Rahoittaja
- Rakennuttaja
- Vakuutusliike
- Suunnittelija
- Urakoitsija
- Konsultti
- Ylläpitäjä
- Laitetoimittaja
- Järjestelmätoimittaja
- Muu

Mikäli vastasit edelliseen "muu", kertoisitko mikä on yrityksenne / organisaationne rooli rakennettuun ympäristöön nähden?

Onko yrityksenne / organisaationne käytössä olevat rakennukset jonkin organisaationne sisäisen tahon vastuulla?

- Kyllä
- Rooli on olemassa, mutta tehtävää ei ole täytetty
- Ei

JÄRJESTELMÄYMPÄRISTÖÖN LIITTYVÄT VASTUUT

Mitkä yrityksenne / organisaationne käytössä olevien rakennusten toimintaa ohjaavat järjestelmät ovat yrityksenne / organisaationne vastuulla eli varmistatte päätösvaltaisena toimijana niiden lainmukaisuuden ja olemassaolon, sekä huolehditte niiden toimivuudesta ja kehittämisestä? Yrityksenne / organisaationne käytössä oleviksi rakennuksiksi lasketaan myös sellaiset rakennukset, jotka ovat välttämättömiä ydinliiketoiminnallenne (esimerkiksi käytössä olevat palvelinsalit konesalipalveluiden tarjoajalle tai ulkoistetut varastot logistiikkaoperaattorille).

Vastaa alla oleviin kohtiin valitsemalla yksi mielipidettäsi parhaiten kuvaava vaihtoehto. Mikäli vastausvaihtoehto ei sovi sinuun, jätä kysymys vastaamatta.

Matriisin sarakeotsikot

1. Täysin organisaatiomme vastuulla
2. Melko kattavasti organisaatiomme vastuulla
3. Jokseenkin kattavasti organisaatiomme vastuulla
4. Vain harvat organisaatiomme vastuulla
5. Ei organisaatiomme vastuulla

Matriisin riviotsikot

- Palotekniset järjestelmät (esim. paloilmoitinjärjestelmä, sprinklerijärjestelmä, savunpoistoluukkujen ohjausjärjestelmä, äänievakuointijärjestelmä, turvavalaistusjärjestelmä)
- Talotekniset järjestelmät (esim. rakennusautomaatiojärjestelmä, kylmäjärjestelmä ja valaistuksen ohjausjärjestelmä, LVIA, talotekniikkavalvomojärjestelmä, energiatehokkuusjärjestelmä, olosuhteidenseurantajärjestelmä)
- Turvallisuusjärjestelmät (esim. murtosuojajärjestelmä, kulunvalvonta- ja kameravalvontajärjestelmä, aluevalvontajärjestelmä, turvallisuusvalvomojärjestelmä)
- Hissien, liukuportaiden ja liukutasojen ohjausjärjestelmät
- Muut kulkemiseen liittyvät järjestelmät (esim. vierailijahallintajärjestelmä, kilpitunnistusjärjestelmä, porttipuhelinjärjestelmä, pysäköinninohjausjärjestelmä, sähköautojen, trukkien ym. latausjärjestelmät, ovien, porttien ja puomien ohjausjärjestelmät)
- Energiajärjestelmät (esim. sähkö, lämpö ja varavoima)
- Toiminnanohjausjärjestelmät (esim. jätehuollon ja kierrätyksen järjestelmät, puhtaanapidon järjestelmät, toimitilapalveluiden järjestelmät, AV-järjestelmät, ravintolapalveluiden järjestelmät, smart office -järjestelmät)

JÄRJESTELMÄYMPÄRISTÖÖN LIITTYVÄT PRIORITEETIT

Arvioi yrityksenne / organisaationne käytössä olevien rakennusten toimintaa ohjaavien järjestelmien kriittisyyttä. Arvioi järjestelmiä aihealuekohtaisesti. Yritykseni / organisaationne käytössä oleviksi rakennuksiksi lasketaan myös sellaiset rakennukset, jotka ovat välttämättömiä ydinliiketoiminnallenne (esimerkiksi käytössä olevat palvelinsalit konesalipalveluiden tarjoajalle tai ulkoistetut varastot logistiikkaoperaattorille).

Vastaa alla oleviin kohtiin valitsemalla yksi mielipidettäsi parhaiten kuvaava vaihtoehto. Mikäli vastausvaihtoehto ei sovi sinuun, jätä kysymys vastaamatta.

Matriisin sarakeotsikot

1. Kriittinen
2. Tärkeä
3. Jokseenkin tärkeä
4. Ei kovin tärkeä
5. Ei lainkaan tärkeä

Matriisin riviotsikot

- Palotekniset järjestelmät (esim. paloilmoitinjärjestelmä, sprinklerijärjestelmä, savunpoistoluukkujen ohjausjärjestelmä, äänievakuointijärjestelmä, turvavalaistusjärjestelmä)
- Talotekniset järjestelmät (esim. rakennusautomaatiojärjestelmä, kylmäjärjestelmä ja valaistuksen ohjausjärjestelmä, LVIA, talotekniikkavalvomojärjestelmä, energiatehokkuusjärjestelmä, olosuhteidenseurantajärjestelmä)
- Turvallisuusjärjestelmät (esim. murtosuojajärjestelmä, kulunvalvonta- ja kameravalvontajärjestelmä, aluevalvontajärjestelmä, turvallisuusvalvomojärjestelmä)
- Hissien, liukuportaiden ja liukutasojen ohjausjärjestelmät
- Muut kulkemiseen liittyvät järjestelmät (esim. vierailijahallintajärjestelmä, kilpitunnistusjärjestelmä, porttipuhelinjärjestelmä, pysäköinninohjausjärjestelmä, sähköautojen, trukkien ym. latausjärjestelmät, ovien, porttien ja puomien ohjausjärjestelmät)
- Energiajärjestelmät (esim. sähkö, lämpö ja varavoima)
- Toiminnanohjausjärjestelmät (esim. jätehuollon ja kierrätyksen järjestelmät, puhtaanapidon järjestelmät, toimitilapalveluiden järjestelmät, AV-järjestelmät, ravintolapalveluiden järjestelmät, smart office -järjestelmät)

JÄRJESTELMÄYMPÄRISTÖN JATKUVUUDENHALLINNAN TOIMINTATAVAT

Arvioi seuraavien kohtien paikkaansapitävyyttä organisaationne käytössä olevien rakennusten ohjaavien järjestelmien osalta.

Vastaa alla oleviin kysymyksiin valitsemalla yksi mielipidettäsi parhaiten kuvaava vaihtoehto. Mikäli vastausvaihtoehto ei sovi sinuun, jätä kysymys vastaamatta.

Matriisin sarakeotsikot
Kyllä, täysin
Kyllä, osittain
Jokseenkin
Vain harvan osalta
Ei

Matriisin riviotsikot

Onko vastuu järjestelmien vaatimusmäärittelystä ulkoistettu?
Onko vastuu järjestelmien hankinnasta ulkoistettu?
Onko järjestelmien jatkuvuudenhallinnan prosessit kuvattu?
Onko jatkuvuudenhallinnan prosessit otettu käyttöön?
Onko järjestelmien väliset riippuvuudet kuvattu?
Onko järjestelmille määritelty vastuuhenkilöt / omistajat?
Toteutetaanko järjestelmille säännöllisesti kyberturvallisuusauditointi?
Toteutetaanko järjestelmille säännöllisesti tietoturva-auditointi?
Onko rakennusten järjestelmäympäristön kokonaisarkkitehtuuri kuvattu?

JÄRJESTELMÄYMPÄRISTÖN RESILIENSSIN NYKYTILA

Arvioi alla olevia väittämiä yrityksenne / organisaationne käytössä olevissa rakennuksissa olevan järjestelmäympäristön näkökulmasta.

Vastaa alla oleviin väittämiin valitsemalla yksi mielipidettäsi parhaiten kuvaava vaihtoehto. Mikäli vastausvaihtoehto ei sovi sinuun, jätä kysymys vastaamatta.

Matriisin sarakeotsikot
1. Täysin samaa mieltä
2. Lähes samaa mieltä
3. Jokseenkin samaa mieltä
4. Jokseenkin eri mieltä
5. Täysin eri mieltä

Matriisin riviotsikot

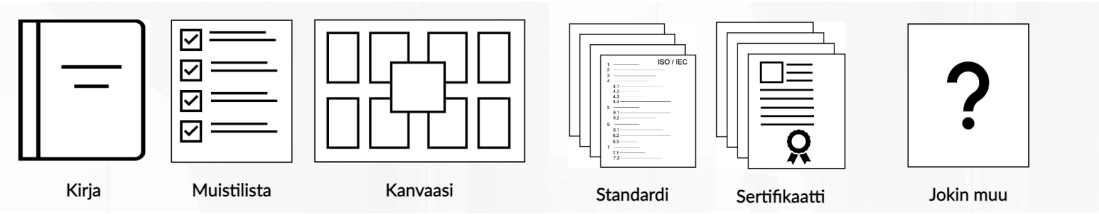
- Ydinliiketoiminta pystyy säilyttämään palvelutasonsa kyberhäiriöistä huolimatta.
- Liiketoimintalähtöinen resilienssianalyysi on osa järjestelmäympäristön jatkuvuudenhallinnan prosesseja.
- Tavoitteemme ei ole suojata järjestelmiä täysin kyberhäiriöiltä, vaan ympäristön sallitaan reagoida häiriötilanteisiin ja toipua niistä hallitusti.
- Resilienssi on sisäänrakennettu osa organisaatiota ja järjestelmiä.
- Järjestelmien ratkaisuarkkitehtuuri koostuu kerroksista, joista jokainen pystyy toipumaan erikseen yhden suojatun kerroksen sijasta.
- Liiketoimintaa ja järjestelmiä tarkastellaan yhteenliitettynä kokonaisuutena.
- Järjestelmien välisiä yhteyksiä käsitellään ennemminkin sekä vahvuutena että heikkoutena kuin vain uhkien lähteenä.

Sivu 4/6

JATKUVUUDENHALLINNAN TYÖKALUN DOKUMENTOINTITAPA

Millainen jatkuvuudenhallinnan työkalu auttaisi teidän organisaatiotanne parhaiten rakennusten järjestelmäympäristöön liittyvän prosessin kehittämisessä? Valitse alta sopivin kuva.

Vastaa kysymykseen valitsemalla mielipidettäsi parhaiten kuvaavat vaihtoehdot. Mikäli vastausvaihtoehto ei sovi sinuun, jätä kysymys vastaamatta.



Voisitko tarkentaa valintaasi omin sanoin?

OSAAMISEN KEHITTÄMISEN TAVAT

Mikä olisi mielestäsi paras osaamisen kehittämisen tapa rakennusten järjestelmien jatkuvuudenhallintaan liittyen? Valitse alta sopivin kuva.

Vastaa kysymykseen valitsemalla mielipidettäsi parhaiten kuvaavat vaihtoehdot. Mikäli vastausvaihtoehto ei sovi sinuun, jätä kysymys vastaamatta.

Mikäli vastasit "Jokin muu", voisitko kertoa mikä?

Sivu 5/6

KOKEMUS JÄRJESTELMÄYMPÄRISTÖN JATKUVUUDENHALLINNAN MATURITEETTITASOSTA

Arvioi organisaationne maturiteettitasoa huoltovarmuuden kannalta keskeisissä yrityksenne / organisaationne käytössä olevissa rakennuksissa olevan järjestelmäympäristön näkökulmasta.

Arvioi maturiteettitasoa valitsemalla yksi mielipidettäsi parhaiten kuvaava vaihtoehto. Mikäli vastausvaihtoehto ei sovi sinuun, jätä kysymys vastaamatta.

Matriisin sarakeotsikot

1. Edelläkävijä
2. Sitoutunut
3. Perustaso
4. Puutteellinen
5. Heikko

Matriisin riviotsikot

- Organisaation ja sen toimintaympäristön ymmärtäminen
- Sidosryhmien tarpeiden ja odotusten ymmärtäminen
- Liiketoiminnan jatkuvuudenhallinnan kattavuus ja soveltamisala
- Liiketoiminnan jatkuvuudenhallinnan toteuttaminen
- Ylimmän johdon sitoutuminen jatkuvuudenhallintaan
- Liiketoiminnan jatkuvuuden toimintaperiaatteet
- Organisaation roolit, vastuut ja valtuudet
- Jatkuvuudenhallintaan kohdistuvien riskien ja mahdollisuuksien käsittely
- Liiketoiminnan jatkuvuuden tavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu
- Toimitusketjujen hallinta
- Jatkuvuudenhallinnan resurssit
- Osaaminen ja pätevyys
- Tietoisuus jatkuvuudenhallinnan toimintaperiaatteista
- Viestintä

- Tiedonhallinta, dokumentoitu tieto
- Jatkuvuudenhallinnan suunnittelu ja ohjaus
- Liiketoiminnan vaikutusanalyysi
- Liiketoiminnan riskien arviointi
- Liiketoiminnan jatkuvuuden toteuttamislinjaukset
- Liiketoiminnan jatkuvuuden menettelyjen luominen ja toteuttaminen
- Harjoittelu ja testaus
- Seuranta, mittaus, analysointi ja arviointi
- Sisäinen auditointi
- Johdon katselmus
- Toiminta häiriötilanteessa
- Toipuminen ja palautuminen
- Jatkuva parantaminen
- Toimialan yhteinen varautuminen
- Alueellinen yhteinen varautuminen
- Varautuminen poikkeusoloihin

KOHDATUT HAASTEET JA MAHDOLLISUUDET

Millaisia onnistumisia olette kohdanneet omassa organisaatiossanne rakennusten järjestelmäympäristön jatkuvuudenhallintaan liittyen?

Millaisia mahdollisuuksia olette tunnistaneet rakennusten järjestelmäympäristön jatkuvuudenhallintaan liittyen?

Millaisia haasteita olette kohdanneet yleisesti rakennusten järjestelmäympäristön jatkuvuudenhallintaan liittyen?

TUTKIMUKSEN LOPPURAPORTTI

Mikäli haluat tutkimusraportin tutkimuksen valmistuttua, jätä sähköpostiosoitteesi tiedoksi.

Sähköpostiosoite:

Tietosuojailmoitus

Tietosuojalaki 2018/1050, EU:n yleinen tietosuoja-asetus 2016/679

Pyydän sinua osallistumaan Kaakkois-Suomen ammattikorkeakoulun (XAMK) opintoihin sisältyvään opinnäytetyöhön liittyvään tutkimukseen.

Opinnäytetyöhön osallistuminen on täysin vapaaehtoista ja voit keskeyttää osallistumisesi koska tahansa. Mikäli keskeytät tutkimuksen tai peruutat suostumuksen, keskeyttämiseen ja suostumuksen peruuttamiseen mennessä kerättyjä tietoja voidaan käyttää osana tutkimusaineistoa.

Tässä tietosuojaselosteessa kuvataan, miten henkilötietojasi käsitellään opinnäytetyössä, mitä oikeuksia sinulla on ja miten voit vaikuttaa tietojesi käsittelyyn.

1. Opinnäytetyön rekisterinpitäjä ja tietojen käsittelijä

   Tämän opinnäytetyön rekisterinpitäjä sekä tietojen käsittelijä on
   Hanna Pikkusaari
   dhapi003@edu.xamk.fi
   050 310 4984

2. Opinnäytetyön suorittaja

   Hanna Pikkusaari

3. Mihin tarkoitukseen henkilötietojani kerätään ja käsitellään?

   Henkilötietoja (sähköpostiosoite) tarvitaan haastattelututkimuksen kokouskutsun tapauskohtaista lähettämistä varten. Näistä tiedoista ei muodostu henkilörekisteriä. Sekä haastateltavan että organisaation tunnistetiedot anonymisoidaan eikä sähköpostiosoitetta tallenneta erilliseen rekisteriin tai tiedostoon.

   Kyselytutkimukseen vastaavat henkilöt saavat jättää sähköpostiosoitteensa, mikäli haluavat saada tutkimusraportin tiedoksi sen valmistumisen jälkeen. Tästä muodostuu henkilörekisteri, jonka tiedot poistetaan lähetyksen jälkeen.

4. Millä perusteella henkilötietojani käsitellään opinnäytetyössä?

   Henkilötietoja käsitellään seuraavalla yleisen tietosuoja-asetuksen (EU 679/2016 6.1 a) mukaisella perusteella:

   ☒ tutkittavan suostumus

   ☐ rekisterinpitäjän lakisääteisen velvoitteen noudattaminen

☐ yleistä etua koskevan tehtävän suorittaminen (tieteellinen tai historiallinen tutkimus tai tilastointi tai aineiston arkistointi) rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen

☐ rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttaminen.

5. Opinnäytetyön aihe ja kesto

Opinnäytetyön aihe: Rakennuksen OT-ympäristön digitaalisen resilienssin lisääminen jatkuvuudenhallintaa kehittämällä

Opinnäytetyön kesto: 30.6.2023 saakka (tavoite)

6. Mitä tietoja minusta käsitellään?

- sähköpostiosoite

Opinnäytetyössä ei käsitellä arkaluonteisia henkilötietoja

7. Mistä lähteistä tietoni kerätään?

Sähköpostiosoite kerätään haastattelututkimukseen liittyvän tapaamisen sopimisen yhteydessä tapaamiskutsua varten.

Kyselyyn vastaaja voi jättää sähköpostiosoitteensa kyselytutkimuksen tekijälle, mikäli haluaa saada tutkimusraportin tiedoksi sen valmistumisen jälkeen.

8. Luovutetaanko henkilötietojani kolmansille osapuolille?

Tietoja ei luovuteta kolmansille osapuolille.

9. Käsitelläänkö tietojani EU:n tai ETA:n ulkopuolella?

XAMKissa käytetään tallennustilana pilvipalvelua (Microsoft OneDrive). Microsoft saattaa siirtää näihin palveluihin tallennettua tietoa tai niiden varmuuskopioita EU:n tai ETA-alueen ulkopuolelle. Microsoftin tietosuojalauseke on luettavissa osoitteesta: https://privacy.microsoft.com/fi-FI/privacystatement

10. Kuinka kauan henkilötietojani säilytetään?

Opinnäytetyöprosessin ajan

11. Miten henkilötietoni säilytetään ja suojataan?

Kalenterikutsua varten kerätty sähköpostiosoite tallentuu kalenterikutsuun sekä mahdollisiin sähköpostikeskusteluihin XAMKin Microsoft 365-ympäristöön.

Kyselytutkimukseen vastanneiden sähköpostiosoite tallentuu XAMKin lisenssillä olevaan tutkimuksen tekijän henkilökohtaisilla tunnuksilla toimivaan Webropol-ympäristöön.

12. Miten voin käyttää tietosuoja-asetuksen mukaisia oikeuksiani?

Yhteyshenkilö tutkittavan oikeuksiin liittyvissä asioissa, johon voi ottaa yhteyttä on:

Hanna Pikkusaari, 050 310 4984, dhapi003@edu.xamk.fi

(a) Suostumuksen peruuttaminen (tietosuoja-asetuksen 7 artikla)

Sinulla on oikeus peruuttaa antamasi suostumus, mikäli henkilötietojen käsittely perustuu suostumukseen. Suostumuksen peruuttaminen ei vaikuta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen.

(b) Oikeus saada pääsy tietoihin (tietosuoja-asetuksen 15 artikla)

Sinulla on oikeus saada tieto siitä, käsitelläänkö henkilötietojasi ja mitä henkilötietojasi käsitellään. Voit myös halutessasi pyytää jäljennöksen käsiteltävistä henkilötiedoista.

(c) Oikeus tietojen oikaisemiseen (tietosuoja-asetuksen 16 artikla)

Jos käsiteltävissä henkilötiedoissasi on epätarkkuuksia tai virheitä, sinulla on oikeus pyytää niiden oikaisua tai täydennystä.

(d) Oikeus tietojen poistamiseen (tietosuoja-asetuksen 17 artikla)

Sinulla on oikeus vaatia henkilötietojesi poistamista tietyissä tapauksissa.

(e) Oikeus käsittelyn rajoittamiseen (tietosuoja-asetuksen 18 artikla)

Sinulla on oikeus henkilötietojesi käsittelyn rajoittamiseen tietyissä tilanteissa kuten, jos kiistät henkilötietojesi paikkansapitävyyden.

(f) Vastustamisoikeus (tietosuoja-asetuksen 21 artikla)

Sinulla on oikeus vastustaa henkilötietojesi käsittelyä, jos käsittely perustuu yleiseen etuun tai oikeutettuun etuun. Tällöin ammattikorkeakoulu ei voi käsitellä henkilötietojasi, paitsi jos se voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää oikeutesi.

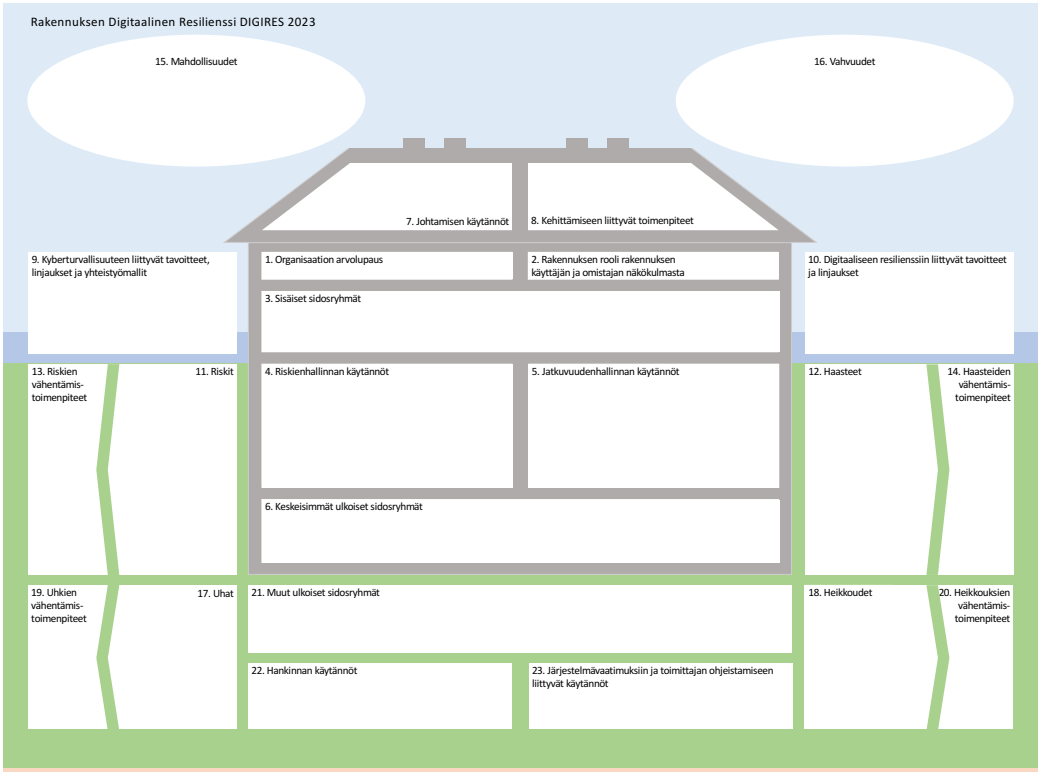
Oikeuksista poikkeaminen
Tässä kuvatuista oikeuksista saatetaan tietyissä yksittäistapauksissa poiketa tietosuoja-asetuksessa ja Suomen tietosuojalaissa säädetyillä perusteilla siltä osin, kuin oikeudet estävät tieteellisen tai historiallisen tutkimustarkoituksen tai tilastollisen tarkoituksen saavuttamisen tai vaikeuttavat sitä suuresti. Tarvetta poiketa oikeuksista arvioidaan aina tapauskohtaisesti.

Valitusoikeus
Sinulla on oikeus tehdä valitus erityisesti vakinaisen asuin- tai työpaikkasi sijainnin mukaiselle valvontaviranomaiselle, mikäli katsot, että henkilötietojen käsittelyssä rikotaan EU:n yleistä tietosuoja-asetusta (EU) 2016/679. Suomessa valvontaviranomainen on tietosuojavaltuutettu.

13. Tietosuojavastaavan yhteystiedot

XAMKin tietosuojavastaava on Markus Häkkinen. Häneen saa yhteyden sähköpostiosoitteesta tietosuojavastaava@xamk.fi

DIGIRES-kanvaasi



24. Järjestelmät*	Paloturvallisuustekniikka	Turvallisuustekniikka	Hissit, liukutasot, liukuportaat	Muut liikkumisen järjestelmät	Energiajärjestelmät	Muu talotekniikka (LVIA)	Toiminnanohjaus-järjestelmät
Järjestelmä							
Kriittisyys							
Käyttöönottovuosi ja elinkaari vuosina							
Tuki loppuu (vuosi)							
Vastuuhenkilö / omistaja							
Valmistaja(t)							
Järjestelmän-toimittaja, jakelija							
Palveluntoimittaja, ylläpitäjä + vasteaika							
Viimeisin auditointi (teema+vuosi)							

* Esimerkiksi paloturvallisuustekniset järjestelmät (esim. paloturvalaitteet, paloilmoitinjärjestelmä, sprinklerijärjestelmä, savunpoistoluukkujen ohjausjärjestelmä, äänievakuointijärjestelmä, turvavalaistusjärjestelmä), turvallisuusjärjestelmät (esim. murtosuojajärjestelmä, kulunvalvonta- ja kameravalvontajärjestelmä, aluevalvontajärjestelmä, turvallisuusvalvomojärjestelmä), hissien, liukuportaiden ja liukutasojen ohjausjärjestelmät, muut kulkemiseen liittyvät järjestelmät (esim. vierailijahallintajärjestelmä, kilpitunnistusjärjestelmä, porttipuhelinjärjestelmä, pysäköinninohjausjärjestelmä, sähköautojen, trukkien ym. latausjärjestelmät, ovien, porttien ja puomien ohjausjärjestelmät), energiajärjestelmät (esim. sähkö, lämpö ja varavoima) , muut talotekniset järjestelmät (esim. rakennusautomaatiojärjestelmä, kylmäjärjestelmä ja valaistuksen ohjausjärjestelmä, LVIA, talotekniikkavalvomojärjestelmä, energiatehokkuusjärjestelmä, olosuhteidenseurantajärjestelmä), toiminnanohjausjärjestelmät (esim. jätehuollon ja kierrätyksen järjestelmät, puhtaanapidon järjestelmät, toimitilapalveluiden järjestelmät, AV-järjestelmät, ravintolapalveluiden järjestelmät, smart office -järjestelmät)

Rakennuksen Digitaalinen Resilienssi DIGIRES 2023

24. Järjestelmät*	Paloturvallisuustekniikka	Turvallisuustekniikka	Hissit, liukutasot, liukuportaat	Muut liikkumisen järjestelmät	Energiajärjestelmät	Muu talotekniikka (LVIA)	Toiminnanohjaus-järjestelmät
Järjestelmä							
Kriittisyys							
Käyttöönottovuosi ja elinkaari vuosina							
Tuki loppuu (vuosi)							
Vastuuhenkilö / omistaja							
Valmistaja(t)							
Järjestelmän-toimittaja, jakelija							
Palveluntoimittaja, ylläpitäjä + vasteaika							
Viimeisin auditointi (teema+vuosi)							

24. Järjestelmät*	Paloturvallisuustekniikka	Turvallisuustekniikka	Hissit, liukutasot, liukuportaat	Muut liikkumisen järjestelmät	Energiajärjestelmät	Muu talotekniikka (LVIA)	Toiminnanohjaus-järjestelmät
Järjestelmä							
Kriittisyys							
Käyttöönottovuosi ja elinkaari vuosina							
Tuki loppuu (vuosi)							
Vastuuhenkilö / omistaja							
Valmistaja(t)							
Järjestelmän-toimittaja, jakelija							
Palveluntoimittaja, ylläpitäjä + vasteaika							
Viimeisin auditointi (teema+vuosi)							

24. Järjestelmät*	Paloturvallisuustekniikka	Turvallisuustekniikka	Hissit, liukutasot, liukuportaat	Muut liikkumisen järjestelmät	Energiajärjestelmät	Muu talotekniikka (LVIA)	Toiminnanohjaus-järjestelmät
Järjestelmä							
Kriittisyys							
Käyttöönottovuosi ja elinkaari vuosina							
Tuki loppuu (vuosi)							
Vastuuhenkilö / omistaja							
Valmistaja(t)							
Järjestelmän-toimittaja, jakelija							
Palveluntoimittaja, ylläpitäjä + vasteaika							
Viimeisin auditointi (teema+vuosi)							

* Esimerkiksi paloturvallisuustekniset järjestelmät (esim. paloturvalaitteet, paloilmoitinjärjestelmä, sprinklerijärjestelmä, savunpoistoluukkujen ohjausjärjestelmä, äänievakuointijärjestelmä, turvavalaistusjärjestelmä), turvallisuusjärjestelmät (esim. murtosuojajärjestelmä, kulunvalvonta- ja kameravalvontajärjestelmä, aluevalvontajärjestelmä, turvallisuusvalvomojärjestelmä), hissien, liukuportaiden ja liukutasojen ohjausjärjestelmät, muut kulkemiseen liittyvät järjestelmät (esim. vierailijahallintajärjestelmä, kilpitunnistusjärjestelmä, porttipuhelinjärjestelmä, pysäköinninohjausjärjestelmä, sähköautojen, trukkien ym. latausjärjestelmät, ovien, porttien ja puomien ohjausjärjestelmät), energiajärjestelmät (esim. sähkö, lämpö ja varavoima) , muut talotekniset järjestelmät (esim. rakennusautomaatiojärjestelmä, kylmäjärjestelmä ja valaistuksen ohjausjärjestelmä, LVIA, talotekniikkavalvomojärjestelmä, energiatehokkuusjärjestelmä, olosuhteidenseurantajärjestelmä), toiminnanohjausjärjestelmät (esim. jätehuollon ja kierrätyksen järjestelmät, puhtaanapidon järjestelmät, toimitilapalveluiden järjestelmät, AV-järjestelmät, ravintolapalveluiden järjestelmät, smart office -järjestelmät)

Rakennuksen Digitaalinen Resilienssi DIGIRES 2023

Organisaation järjestelmäympäristön kyvykkyyttä sopeutua vallitsevaan tilanteeseen kutsutaan digitaaliseksi resilienssiksi. Digitaalinen resilienssi on sitä parempi, mitä tarkemmin järjestelmäympäristö ja siihen liittyvät sisäiset ja ulkoiset riippuvuudet tunnetaan. Digitaalista resilienssiä tehostaa tarkoituksenmukaiset järjestelmäympäristöön liittyvät sopimukset, vastuut ja velvollisuudet sekä selkeät johtamisen, riskienhallinnan ja jatkuvuudenhallinnan käytännöt. Koska kyberturvallisuutta kehittämällä ei voi varautua kaikkiin mahdollisiin häiriötilanteisiin, on digitaalisen resilienssin lisääminen käytännössä välttämätöntä kaikissa kaikille teknisille ympäristöille.

DIGIRES-kanvaasi havainnollistaa rakennuksen digitaalisen resilienssin tilan sekä siihen liittyvät haasteet ja mahdollisuudet. Täytä DIGIRES-kanvaasin kentät huolellisesti ja rehellisesti alla olevia ohjeita soveltaen. Kiinnitä erityisesti huomiota kokonaisuuteen eli arvioi myös rakennuksen järjestelmäympäristöön liittyviä epäsuoria vaikutuksia, prosesseja ja sidosryhmiä. Koska kokonaisuus koskee useita eri organisaation toimintoja, kannattaa kanvaasi täyttää yhdessä eri vastuutahojen kanssa. Näin varmistat samalla tiedon siirtymisen organisaation sisällä ja näin ollen myös nopeamman kehittämisen prosessin koko toimintaympäristöön liittyen.

DIGIRES-kanvaasin voi tulostaa (optimoitu koko A0) tai sitä voi hyödyntää eri kollaboraatiotyökaluissa työskentelyn pohjana. Kirjoita vastaukset tarralapuille ja siirrä ne kanvaasissa oikeaan kohtaan. Merkitse kriittiset asiat korostusvärillä tai tarralla. Kirjoita aina yksi asia yhdelle lapulle, jotta tiedon siirtäminen paikasta toiseen on mahdollisimman sujuvaa. Huomaa, että esimerkiksi riskit, haasteet, uhat ja heikkoudet voivat sisältää samoja asioita hieman eri näkökulmista.

DIGIRES-kanvaasin kohdat on numeroitu ja ne suositellaan täytettäväksi numerojärjestyksessä. Tämä ei kuitenkaan ole välttämätöntä.

Koska rakennuksen järjestelmäympäristö todennäköisesti kehittyy jatkuvasti tavalla tai toisella ja sidosryhmät sekä vastuuhenkilöt vaihtuvat, kannattaa DIGIRES-kanvaasin täyttäminen ja tietojen tarkistaminen ottaa osaksi riskienhallinnan sekä jatkuvuudenhallinnan jatkuvia prosesseja. Näin varmistat tietojen oikeellisuuden myös poikkeusoloissa.

Huom! Yksi jatkuvuudenhallinnan kannalta keskeisin asia on riippuvuuksien kuvaaminen. Sitä ei kuitenkaan ole sisällytetty DIGIRES-kanvaasiin, sillä arkkitehtuurin mallinnustyökaluja on saatavissa markkinoilta useita eri näkökulmiin sopivia. Järjestelmien välisiä riippuvuuksia voi kuvata myös esimerkiksi toimisto-ohjelmistoilla.

Huom! Koska huolellisesti täytetty kanvaasi sisältää rakennuksen digitaalisen resilienssin sekä toiminnan kannalta kriittistä tietoa, ylläpidä ja säilytä sitä turvallisessa paikassa. Huolehdi myös asianmukaisesta käyttöoikeuksien ja pääsyn hallinnasta.

1. Organisaation arvolupaus

Kirjoita tähän rakennusta käyttävän organisaation arvolupaus. Organisaatio noudattaa arvolupaustaan kaikessa toiminnassaan, joten se koskee myös käytössä olevia rakennuksia ja sen järjestelmiä.

2. Rakennuksen rooli

Kuvaa tähän rakennuksen rooli osana organisaation toimintaa rakennuksen käyttäjän näkökulmasta. Kuvaile myös rakennuksen rooli rakennuksen omistajan näkökulmasta, mikäli omistaja on eri kuin käyttäjä.

3. Sisäiset sidosryhmät

Luettele tässä ne sisäiset sidosryhmät, jotka liittyvät rakennuksen ja koko kiinteistön järjestelmäympäristöön.

4. Riskienhallinnan käytännöt

Luettele tässä ne riskienhallinnan käytännöt, jotka liittyvät suoraan tai epäsuorasti rakennuksen järjestelmäympäristöön.

5. Jatkuvuudenhallinnan käytännöt

Kuvaa tähän sellaiset liiketoiminnan ja teknisen ympäristön (sisältäen ICT) jatkuvuudenhallintaan liittyvät käytännöt, jotka koskevat rakennuksen järjestelmäympäristöä.

6. Keskeisimmät ulkoiset sidosryhmät

Kuvaa tähän keskeisimmät ulkoiset sidosryhmät rakennuksen järjestelmäympäristöön, sen johtamiseen ja siihen liittyviin muihin prosesseihin liittyen.

7. Johtamisen käytännöt

Kerro tässä, miten rakennuksen järjestelmäympäristöön liittyviä prosesseja johdetaan normaali- ja poikkeusoloissa. Onko näillä eroavaisuuksia ja jos on, niin miksi? Kuka kokonaisuudesta vastaa? Minkälainen on päätöksentekomalli? Entä, jos päätöksenteko koskee useita eri organisaation toiminta-alueita?

8. Kehittämiseen liittyvät toimenpiteet

Kerro tässä, miten rakennuksen järjestelmäympäristöön liittyviä prosesseja kehitetään? Miten johtamista kehitetään? Miten varmistetaan ajantasainen osaaminen ja miten sitä kehitetään?

9. Kyberturvallisuuteen liittyvät tavoitteet, linjaukset ja yhteistyömallit

Kuvaa tähän rakennuksen järjestelmäympäristön kyberturvallisuuteen liittyvät tavoitteet, linjaukset ja yhteistyömallit. Varmista, että saat näkökulman aiheeseen eri turvallisuuden osa-alueista vastaavilta tahoilta (kyberturvallisuus, tietoturva, fyysinen turvallisuus).

10. Digitaaliseen resilienssiin liittyvät tavoitteet ja linjaukset

Kuvaa tähän rakennuksen digitaaliseen resilienssiin liittyvät tavoitteet ja linjaukset. Ota huomioon myös sellaiset liiketoiminnan ja ICT:n digitaaliseen resilienssiin liittyvät tavoitteet ja linjaukset, jotka koskevat suoraan tai epäsuorasti rakennuksia ja kiinteistöjä.

11. Riskit

Luettele tähän riskejä, jotka kohdistuvat rakennuksen ja koko kiinteistön järjestelmäympäristöön. Riskit voivat olla joko suoria tai epäsuoria.

12. Haasteet

Luettele haasteita, jotka kohdistuvat rakennuksen ja koko kiinteistön järjestelmäympäristöön ja siihen liittyviin prosesseihin.

13. Riskien vähentämistoimenpiteet

Listaa tähän sellaiset toimenpiteet, joilla tunnistettuja riskejä voi vähentää. Lisää myös aikataulu ja vastuuhenkilö.

14. Haasteiden vähentämistoimenpiteet

Listaa tähän sellaiset toimenpiteet, joilla tunnistettuja haasteita voi vähentää. Lisää myös aikataulu ja vastuuhenkilö.

15. Mahdollisuudet

Kuvaa tähän sellaisia mahdollisuuksia, joita rakennuksen järjestelmäympäristö voi tuottaa organisaation toiminnalle. Mahdollisuudet voivat olla esimerkiksi toiminnan tehostamiseen, toimenpiteiden oikea-aikaisuuteen tai uusiin datatuotteisiin liittyviä.

16. Vahvuudet

Kuvaa tähän erityisiä vahvuuksia, joita olet tunnistanut rakennuksen järjestelmäympäristöön liittyen. Vahvuudet voivat liittyä esimerkiksi sopimuksiin, kustannusten ennustettavuuteen tai tasalaatuiseen palveluun.

17. Uhat

Luettele tähän ulkopuolelta rakennuksen järjestelmäympäristöön tai sen kautta organisaation toimintaan koskevia uhkia.

18. Heikkoudet

Luettele tähän heikkouksia, joita rakennuksen järjestelmäympäristöön liittyy.

19. Uhkien vähentämistoimenpiteet

Listaa tähän sellaiset toimenpiteet, joilla tunnistettuja uhkia voi vähentää. Lisää myös aikataulu ja vastuuhenkilö.

20. Heikkouksien vähentämistoimenpiteet

Listaa tähän sellaiset toimenpiteet, joilla tunnistettuja heikkouksia voi vähentää. Lisää myös aikataulu ja vastuuhenkilö.

21. Muut ulkoiset sidosryhmät

Kuvaa tähän muut ulkoiset sidosryhmät, joita et ole maininnut kohdassa 6.

22. Hankinnan käytännöt

Kuvaa tähän käytännöt, joiden mukaisesti rakennuksen järjestelmiin liittyviä hankintoja tehdään. Hankinnat voivat liittyä järjestelmien lisäksi esimerkiksi laitteisiin, suunnittelu-, korjaus- ja asennustöihin, lisensseihin ja ylläpitopalveluun. Kirjaa tähän myös kaikki sopimiseen liittyvät käytännöt. Näihin voi liittyä esimerkiksi hankinta-, huolto-, ylläpito-, palvelutaso- ja lisenssisopimukset.

23. Järjestelmävaatimuksiin ja toimittajan ohjeistukseen liittyvät käytännöt

Kuvaa tähän sellaiset käytännöt, joiden mukaan toimittajia ja muita sidosryhmiä ohjeistetaan esimerkiksi tarjous-, toteutus-, asennus- ja ylläpitovaiheessa. Kirjaa myös eskalointikäytännöt poikkeusoloja varten.

24. Järjestelmät*

Listaa tähän järjestelmät sisältäen laitteet, ohjelmat, tiedonsiirtotavat ja yhteydet sekä niihin liittyvät tiedot teemakohtaisesti. Lisää tietoja tarvittaessa. Yhteen teemaan (esimerkiksi paloturvallisuus) voi sisältyä useita järjestelmiä. Käy taulukko kohta kohdalta läpi, sillä eri tiedot voivat erota merkittävästi eri järjestelmien välillä. Vasteajat löydät esimerkiksi ylläpito-, palvelu- tai palvelutasosopimuksista.

* Esimerkiksi paloturvallisuustekniset järjestelmät (esim. paloturvalaitteet, paloilmoitinjärjestelmä, sprinklerijärjestelmä, savunpoistoluukkujen ohjausjärjestelmä, äänievakuointijärjestelmä, turvavalaistusjärjestelmä), turvallisuusjärjestelmät (esim. murtosuojajärjestelmä, kulunvalvonta- ja kameravalvontajärjestelmä, aluevalvontajärjestelmä, turvallisuusvalvomojärjestelmä), hissien, liukuportaiden ja liukutasojen ohjausjärjestelmät, muut kulkemiseen liittyvät järjestelmät (esim. vierailijahallintajärjestelmä, kilpitunnistusjärjestelmä, porttipuhelinjärjestelmä, pysäköinninohjausjärjestelmä, sähköautojen, trukkien ym. latausjärjestelmät, ovien, porttien ja puomien ohjausjärjestelmät), energiajärjestelmät (esim. sähkö, lämpö ja varavoima) , muut talotekniset järjestelmät (esim. rakennusautomaatiojärjestelmä, kylmäjärjestelmä ja valaistuksen ohjausjärjestelmä, LVIA, talotekniikkavalvomojärjestelmä, energiatehokkuusjärjestelmä, olosuhteidenseurantajärjestelmä), toiminnanohjausjärjestelmät (esim. jätehuollon ja kierrätyksen järjestelmät, puhtaanapidon järjestelmät, toimitilapalveluiden järjestelmät, AV-järjestelmät, ravintolapalveluiden järjestelmät, smart office -järjestelmät)

DIGIRES-kanvaasi on toteutettu Huoltovarmuusorganisaation Yksityisen turva-alan poolin tilauksesta osana Kaakkois-Suomen ammattikorkeakoululle (XAMK) tehtävää opinnäytetyötä.