Susanna Rissanen

Kyberresilienssin rooli tietojärjestelmien integroinnissa organisaation jatkuvuussuunnitteluun

[Subject]

Tuotantotalouden ja tietojärjestelmätieteen ohjelma
Tietojärjestelmätieteen kandidaatintutkielma
Kauppatieteiden kandidaatti

Vaasa 2026

VAASAN YLIOPISTO
Tekniikan ja innovaatiojohtamisen akateeminen yksikkö
Tekijä: Susanna Rissanen
Tutkielman nimi: Kyberresilienssin rooli tietojärjestelmien integroinnissa organisaation jatkuvuussuunnitteluun: [Subject]
Tutkinto: Kauppatieteiden kandidaatti
Koulutusohjelma: Tuotantotalouden ja tietojärjestelmätieteen ohjelma
Opintosuunta: Tietojärjestelmätiede
Työn ohjaaja: Laura Havinen
Valmistumisvuosi: 2026 **Sivumäärä:** **36**

TIIVISTELMÄ:
Organisaatioiden toiminta on entistä enemmän riippuvaista digitaalisista tietojärjestelmistä. Tietojärjestelmien avulla hallitaan, tallennetaan ja jaetaan liiketoiminnalle kriittistä tietoa sekä tuetaan päivittäisiä toimintoja. Digitalisaation edetessä kyberuhat ja tietojärjestelmähäiriöt ovat lisääntyneet organisaatioissa. Perinteiset kyberturvallisuusmenetelmät eivät enää riitä vastaamaan nykyaikaisiin kyberuhkiin. Tämän takia kyberturvallisuuden rinnalle on tullut kyberresilienssi. Kyberresilienssillä tarkoitetaan organisaation kykyä ennakoida, kestää, hallita ja palautua kyberuhkien aiheuttamista häiriötilanteista.

Tässä tutkielmassa tarkastellaan kyberresilienssin roolia tietojärjestelmien integroinnissa organisaation jatkuvuussuunnittelussa. Jatkuvuudensuunnittelulla tarkoitetaan yrityksen ennakointia, valmiutta, sopeutumista ja palautumista normaaliin arkeen erilaisten kriisien sattuessa mahdollisimman vähällä haitalla. Tutkielmassa pohditaan kyberresilienssin merkitystä ja tärkeyttä organisaatioiden jatkuvuussuunnittelussa yksilön ja organisaation näkökulmasta. Tutkielmassa tarkastellaan tietotekniikan ja liiketoiminnan välistä yhteistyötä ja sen vaikutusta organisaation kyberresilienssiin ja jatkuvuussuunnitteluun. Tutkielman tavoitteena on tarkastella, mikä on kyberresilienssin rooli tietojärjestelmien integroinnissa organisaation jatkuvuussuunnittelussa. Tulokset mahdollistavat teoreettisen pohjan organisaatioiden jatkuvuuden kehittämiselle ja IT:n paremmalle hyödyntämiselle kriisivalmiuden tukena.

Tutkimus toteutettiin narratiivisena kirjallisuuskatsauksena. Aineisto koostui tieteellisistä artikkeleista. Tutkimusaineisto haettiin tieteellisistä tietokannoista. Tutkimusaineistoa analysoitiin tutkimuskysymyksen näkökulmasta. Aineisto rajattiin viimeiselle seitsemälle vuodelle eli vuosille 2019–2026.

Tulosten perusteella kyberresilienssi on keskeinen osa organisaatioiden jatkuvuudenhallintaa, eikä sitä nykypäivänä voi tarkastella siitä erillisenä osa-alueena. Tietojärjestelmien tehokas integrointi osaksi jatkuvuussuunnittelua parantaa organisaatioiden kykyä varautua kyberuhkiin, ylläpitää toimintakykyään ja palautua häiriötilanteista. Keskeisenä havaintona on, että integrointi edellyttää sekä teknisten että organisatoristen tekijöiden huomioimista. Myös inhimillisillä tekijöillä, kuten koulutuksella ja avoimuudella, on merkittävä vaikutus kyberresilienssin toteutumiseen. Tulosten perusteella voidaan todeta, että tietojärjestelmien suunnitelmallinen integrointi on keskeinen edellytys organisaatioiden toimintakyvylle muuttuvassa digitaalisessa toimintaympäristössä. Tulosten pohjalta voidaan suositella seuraavia käytännön toimenpiteitä: kriittisten järjestelmien tunnistaminen, palautumissuunnitelmien säännöllinen testaus ja henkilöstön jatkuva kouluttaminen.

AVAINSANAT: kyberresilienssi, jatkuvuussuunnittelu, organisaation kyberturvallisuus, tietojärjestelmä

Sisällys

Taulukot

1 Johdanto

Liiketoiminnan jatkuvuussuunnittelun kehittäminen on välttämätöntä. Perinteiset varautumiskeinot, kuten manuaaliset suunnitelmat tai yksittäiset varmuuskopiot, eivät enää riitä vastaamaan nopeasti muuttuvan digitaalisen ympäristön uhkiin, kuten kyberhyökkäyksiin tai tietojärjestelmäkatkoksiin. Tietojärjestelmien integrointi osana jatkuvuudenhallintaa parantaa organisaation reagointikykyä, tiedonkulkua ja päätöksenteon laatua kriisitilanteissa. Awangin ja muiden (2023, s. 1–2) mukaan jatkuvuudenhallinnalla tarkoitetaan organisaatioiden strategisia johtamiskäytäntöjä. Niiden tehtävänä on reagoida erilaisiin kriiseihin ja lieventää odottamattomien tapahtumien vaikutuksia. Bladesin ja Doughtyn (2001, s. 27) mukaan jatkuvuussuunnittelulla tarkoitetaan organisaation toimia, joilla varmistetaan normaali toiminta ennen kyberuhan syntymistä, sen aikana ja tämän jälkeen mahdollisimman vähäisin haitoin muille toimijoille. Jatkuvuudenhallinta on laajempi yläkäsite. Jatkuvuussuunnittelu on jatkuvuudenhallinnan osa-alue, joka tapahtuu jatkuvuudenhallinnan sisällä ja toteuttaa nämä toimenpiteet.

Tässä tutkimuksessa tarkastellaan, mikä on kyberresilienssin rooli tietojärjestelmien integroinnissa organisaation jatkuvuussuunnittelussa. Aihe on tärkeä, koska organisaatioiden kasvava riippuvuus tietojärjestelmistä tekee niistä myös kohteen kyberuhille. Organisaatioiden toiminta on yhä riippuvaisempaa erilaisista tietojärjestelmistä. Näiden järjestelmien avulla organisaatiot hallitsevat, tallentavat ja jakavat liiketoiminnalle kriittistä tietoa sekä tukevat päivittäisiä toimintojaan.

Steenin ja muiden (2023, s. 7–9) mukaan digitalisaation edetessä organisaatioihin kohdistuvat kyberuhat ja tietojärjestelmähäiriöt lisääntyvät, jolloin tietojärjestelmien kyberturvallisuus korostuu entisestään. Tämän vuoksi tiedon turvallinen käsittely ja tietojärjestelmien toimintakyvyn turvaaminen ovat nousseet keskeisiksi kysymyksiksi organisaatioiden toiminnassa. Perinteisen kyberturvallisuuden rinnalle onkin noussut kyberresilienssi, joka korostaa organisaation kykyä ennakoida, kestää ja hallita erilaisia kyberuhkia sekä palautua niistä tehokkaasti. Steenin ja muiden (2023, s. 7–9) mukaan

yhdistämällä jatkuvuudenhallinnan organisaatioiden resilienssin kehitykseen voidaan parantaa kokonaisturvallisuutta organisaatioissa.

Kyberresilienssiä ja liiketoiminnan jatkuvuussuunnittelua on tutkittu aiemmin omina aiheina laajasti, mutta niiden välistä yhteyttä tietojärjestelmien näkökulmasta on käsitelty vähemmän. Saeed ja muut (2023, s. 1, 3 ja 14), tekivät PRISMA-katsauksen, jossa he tarkastelivat digitaalisen transformaation ja kyberturvallisuuden yhteyttä organisaatioiden resilienssiin. Tutkimuksessa todettiin, että nykyaikaisten teknologioiden käyttöönotto lisää tehokkuutta mutta kasvattaa erilaisia kyberriskejä. Heidän katsauksensa ei kuitenkaan käsitellyt liiketoiminnan jatkuvuussuunnittelua tai tietojärjestelmien roolia. Tämä aiheuttaa tutkimusaukon mihin tämä tutkielma pyrkii vastaamaan.

Ali, Hanafiah ja Mogindol, (2023, s. 1–2) tekivät kirjallisuuskatsauksen liiketoiminnan jatkuvuudenhallinnan käytännöistä pienissä tai keskisuurissa yrityksissä. He yhdistivät katsauksessaan organisaation resilienssin ja suorituskyvyn näkökulmat. Jättäen kuitenkin tietojärjestelmien ja kyberresilienssin yhdistelmän pois. Tämä tutkielma pyrkii täydentämään kyseistä tutkimusta tarkastelemalla tietojärjestelmien integroinnin ja kyberresilienssin yhteyttä liiketoiminnan jatkuvuussuunnitteluun.

Tulevaisuudessa on tarve syvällisemmälle ymmärrykselle siitä, mikä on kyberresilienssin rooli tietojärjestelmien integroinnissa organisaation jatkuvuussuunnittelussa. Pelkkä tekninen kyberturvallisuus ei riitä vastaamaan nykyaikaisiin kyberuhkiin, vaan organisaatioiden on kyettävä myös ylläpitämään toimintakykyään ja palautumaan häiriötilanteista tehokkaasti.

1.1 Tutkimuksen tavoite ja menetelmä

Tutkimus toteutetaan kirjallisuuskatsauksena, jossa tarkastellaan aiempia tutkimuksia kyberturvallisuudesta, tiedonhallinnasta ja järjestelmäriippuvuuksista. Tutkimuksen tavoitteena on tarkastella, mikä on kyberresilienssin rooli tietojärjestelmien

integroinnissa jatkuvuussuunnittelussa. Tulokset tarjoavat pohjan organisaatioiden jatkuvuuden kehittämiselle ja IT:n paremmalle hyödyntämiselle kriisivalmiuden tukena. Tämän tutkimuksen tutkimuskysymys on: mikä on kyberresilienssin rooli tietojärjestelmien integroinnissa organisaation jatkuvuussuunnittelussa?

Tutkimus pyrkii tarkastelemaan, millä tavoin erilaiset tietojärjestelmät, digitaaliset ratkaisut ja tietohallinnan käytännöt voivat parantaa organisaation kykyä ylläpitää keskeisiä toimintojaan kriisitilanteiden aikana ja niiden jälkeen. Tutkimus rajataan erityisesti strategisen ja teknologisen tason integraatioon, jossa tarkastellaan tietojärjestelmien roolia jatkuvuudenhallinnan prosesseissa, kuten riskien arvioinnissa, tiedonhallinnassa, viestinnässä ja palautumissuunnitelmien toteutuksessa. Tutkimus tehdään narratiivisena kirjallisuuskatsauksena.

1.2 Työn rakenne

Luvussa kaksi määritellään tutkimuksen keskeiset käsitteet ja esitellään aikaisempia tutkimuksia aiheista ja vertaillaan tieteellisiä artikkeleita liittyen kyberresilienssiin. Luvussa kolme tarkastellaan tietojärjestelmiä ja niiden roolia liiketoiminnan jatkuvuussuunnittelussa. Luvut kaksi ja kolme toimivat tämän työn teoreettisena viitekehyksenä. Teoreettinen viitekehys luo tutkimukselle pohjaymmärryksen aiheesta. Tätä on hyödynnetty tutkimuksen aineiston analysoinnissa ja sen tulkitsemisessa.

Luvussa neljä syvennytään tämän työn tutkimusmenetelmään ja kerrotaan kirjallisuuskatsauksesta. Luvussa neljä kuvataan yksityiskohtaisesti aineiston hankinnasta, miten niitä on hyödynnetty ja miten työssä käytetyt artikkelit on seulottu, jotta niitä on päädytty käyttämään tässä työssä. Luvussa viisi syvennytään tämän kirjallisuuskatsauksen tuloksiin. Tutkimuksen lopussa käydään tarkasti läpi, mitä huomioita ja tuloksia on saatu tutkimusaineiston perusteella.

Johtopäätöksissä kootaan yhteen tutkimuksen keskeiset havainnot ja arvioidaan niiden merkitystä sekä teoreettisesta että käytännöllisestä näkökulmasta. Lisäksi pohditaan,

miten tietojärjestelmien integrointi osaksi liiketoiminnan jatkuvuussuunnittelua voi tukea organisaatioiden varautumista ja kriisinsietokykyä tulevaisuudessa. Lopuksi esitetään suosituksia jatkuvuussuunnittelun ja tietojärjestelmien hallinnan kehittämiseksi sekä nostetaan esiin jatkotutkimusaiheita.

2 Kyberresilienssi yritysten tietojärjestelmissä

Tämä kandidaatin tutkielma tarkastelee kyberresilienssin roolia tietojärjestelmien integroinnissa organisaation jatkuvuussuunnittelussa. Tässä luvussa käsitellään resilienssiä ja kyberresilienssiä käsitteenä ja niiden merkitystä tietojärjestelmissä. Luvussa 2.1 ensin avataan käsitteet ja tarkastellaan niiden taustoja ja kehitystä. Resilienssi käsitettä käytetään useilla eri tieteenaloilla ja sen merkitys vaihtelee kontekstin mukaan. Luvussa 2.2 pureudutaan organisaatioiden ja tietojärjestelmien kyberresilienssiin. Tutkimuksessa käydään läpi, miten kyberresilienssiä voidaan hyödyntää käytännön tasolla. Tutkimuksessa pohditaan millainen rooli kyberresilienssillä on tietojärjestelmien lisääntyessä ja miten kyberresilienssin tasoa voidaan vahvistaa.

2.1 Resilienssi ja kyberresilienssi käsitteinä

Poijula (2018, s. 16) kertoo, että resilienssi-käsite juontaa juurensa latinan kielen sanoista salire ja re-salire. Sana salire viittaa hyppäämiseen, kun taas re-salire viittaa takaisin hyppäämiseen. Hyppääminen viittaa tilanteeseen, josta lähdetään pois. Takaisinhyppääminen viittaa kykyyn palata takaisin tai sopeutua uuteen tilanteeseen tuon hyppäämisen jälkeen. Resilienssiä käytetään niin yksilöiden kuin organisaatioidenkin toimintakyvyn kuvaamiseen. Lipponen (2020, s. 20–21) muistuttaa, että resilienssiä on kaikkialla ja se muovautuu tilanteiden ja olosuhteiden mukaan.

Poijula (2018, s. 18, 123) toteaa, että yksilötason resilienssissä ei ole kyse ominaisuuksista tai yleisestä mielenterveydestä. Yksilöiden resilienssillä viitataan ihmisen sopeutumiskykyyn stressaavissa olosuhteissa tai tilanteissa. Lipposen (2020, s. 22, 26–28) mukaan resilienssi ei tarkoita pelkästään stressin vastustamista tai sen kestämistä, vaan myös kykyä sopeutua tilanteisiin ja oppia niistä. Resilienssi pyrkii jatkuvaan kehitykseen ja parempaan itsetietoisuuteen välttääkseen aiemmat kriisit. Lipponen (2020, s. 26–27) kertoo, että resilienssiä voidaan tarkastella sisäisenä ja ulkoisena ulottuvuutena. Sisäisellä resilienssillä viitataan yksilön psyykkisiin voimavaroihin, kuten hyvinvointiin ja selviytymiskeinoihin tilanteesta riippumatta.

Ulkoinen resilienssi puolestaan kuvaa yksilön kykyä selviytyä ja sopeutua osana ympäröivää sosiaalista ja yhteiskunnallista todellisuutta, hyödyntäen esimerkiksi sosiaalisia verkostoja ja saatavilla olevaa tukea. Lipponen (2020, s. 27) sanoo, että sisäinen ja ulkoinen resilienssi eivät riipu toisistaan. Sisäinen ja ulkoinen resilienssi voivat olla eri aikaan koetuksella.

Poijula (2018, s. 17) ja Lipponen (2020, s. 270) kertovat, että organisaatioiden resilienssillä viitataan organisaatioiden kykyyn palautua erilaisista muutoksista ja kriisitilanteista toimiakseen ennallaan. Poijulan (2018, s. 17) mukaan organisaatioiden resilienssillä tarkoitetaan dynaamisen järjestelmän kykyä sopeutua häiriöihin, jotka uhkaavat sen toimintaa, elinkelpoisuutta tai kehitystä. Poijula (2018, s. 17) toteaa, että ei ole yhtä selkeää määritelmää siitä, onko resilienssi prosessi, yksilöllinen ominaisuus, kehittyvä dynaaminen ilmiö, lopputulos vai näiden yhdistelmä. Resilienssi ei ole absoluuttista, vaan aina suhteellista. Organisaation resilienssiä käsitellään myöhemmin tässä ja seuraavassa luvussa.

Poijula (2018, s. 18) kertoo, että resilienssiä tutkitaan ja käytetään monilla eri tieteenaloilla. Resilienssin merkitys vaihtelee eri kontekstien mukaan. Esimerkiksi kehityspsykologiassa resilienssi nähdään taitona sopeutua erilaisiin vastoinkäymisiin. Joissain tapauksissa henkilön resilienssi voi jopa kasvaa stressaavien kokemusten seurauksena. Resilienssi käsitettä onkin sovellettu myös digitaaliseen ympäristöön kyberresilienssin muodossa, ja sitä käytetään tässä työssä. Petrenkon (2019, s. 109–111) mukaan kyberresilienssi tarkoittaa, kuinka hyvin kyberjärjestelmät kestävät, sopeutuvat ja palautuvat kyberuhan sattuessa.

Bagheri ja muut (2023, s. 4–5) toteavat, että organisaatioiden kyberresilienssi on monialainen käsite. Organisaatioiden kyberresilienssi ei keskity vain tekniseen kyberturvallisuuteen. Se keskittyy tekijöihin, jotka liittyvät sosiaalisiin ja käyttäytymiseen. Bagherin ja muiden (2023, s. 5) mukaan organisaatioiden kannattaisi hyödyntää kyberresilienssimatriisia käytännön tasolla parantaakseen kyberresilienssiään. Bagherin

ja muiden (2023, s. 5) mukaan kyberresilienssimatriisin keskeinen ajatus on, että organisaatio ei voi keskittyä vain ennakoivaan suunnitteluun. Organisaatioiden tulee huomioida kaikki vaiheet. Kyberresilienssimatriisissa on neljä vaihetta, jotka ovat suunnittelu, vastaanotto, palautuminen ja sopeutuminen. Kyberresilienssimatriisin keskeinen asia on suunnittelu- ja valmistautumisvaihe. Nämä vaiheet sisältävät jatkuvuussuunnittelun lisäksi myös henkilöstön kouluttamisen, viestintäprosessien kehittämisen ja selkeiden päätöksentekoprotokollien määrittämisen ennen mahdollisia häiriötilanteita. Kyberresilienssimatriisin tavoitteena ei kuitenkaan ole yksilöidä kyberresilienssiä edistäviä tekijöitä.

Chakrabortyn ja Biswassin (2019, s. 661–663) tekemässä tutkimuksessa tunnistettiin viisi eri osa-aluetta henkilöstösuunnittelussa. Nämä viisi eri henkilöstösuunnittelun osa-aluetta ovat: henkilöstösuunnitelma, työn analysointi ja suunnittelu, urasuunnittelu ja kehitys, seuraajasuunnittelu sekä kykyjen johtaminen. Chakrabortyn ja Biswassin (2019, s. 673) tekemässä henkilöstöjohtamisen tutkimuksessa todettiin, että kyseisistä osa-alueista merkittävin rooli oli seuraajasuunnittelulla, kun tavoiteltiin organisaatioiden strategisia tavoitteita.

Petrenko (2019, s. 42–44) ja Joinson (2023, s. 1–3) tarkastelevat kyberresilienssiä eri tasoilla organisaation ja yksilön näkökulmasta. Molemmat korostavat kohteen sopeutumiskykyä keskeisenä elementtinä. Joinson (2023, s. 1, 7, 9) kehitti tutkimuksessa nykypäivän ihmisen kyberresilienssiä mittaavan asteikon (human cyber-resilience scale). Tutkimuksen tavoitteena on ymmärtää paremmin yksilöiden kykyä selviytyä digitalisaation tuomista haasteista erityisesti työn ulkopuolisessa arjessa. Asteikossa on neljä osa-aluetta: itseluottamus, sosiaalinen tuki, oppiminen ja kasvu sekä avuttomuus. Osa-alueiden avulla pyritään hahmottamaan yksilöiden kokemaa kyberresilienssiä ja tunnistamaan tekijöitä, jotka tukevat tai heikentävät sitä.

Joinsonin (2023, s. 1, 7, 9) kehittämää asteikkoa voidaan käyttää yksilön kyberresilienssin arviointiin. Tämän lisäksi myös erilaisten väestöryhmien vertailuun esimerkiksi iän,

sukupuolen tai muiden demografisten tekijöiden perusteella. Lisäksi asteikko soveltuu interventioiden ja kampanjoiden vaikutusten arviointiin eri ajankohtina. Ala-asteikkojen avulla voidaan tunnistaa resilienssiä tukevia tai heikentäviä tekijöitä, mikä tarjoaa tietoa tulevien kyberturvallisuutta edistävien toimenpiteiden suunnitteluun.

2.2 Kyberresilienssi organisaatioissa ja tietojärjestelmissä

Digitaalinen resilienssi voidaan ymmärtää resilienssin yhdeksi osa-alueeksi, joka kuvaa organisaation kykyä sopeutua digitaalisen toimintaympäristön muutoksiin ja häiriöihin. Kyberresilienssi on tätä tarkempi käsite. Kyberresilienssi keskittyy nimenomaan kyberuhkiin ja tietojärjestelmiin liittyvään toimintakykyyn (Petrenko, 2019, s. 109–111).

Tsen ja muut (2023, s. 2–3) toteavat, että kyberresilienssin nykykäsitys on siirtynyt pois teknisestä tietoturvasta ja on menossa kohti kokonaisvaltaisempaa lähestymistapaa. Kokonaisvaltaisen lähestymistavan ideana on integroitua organisaation toimijoihin ja sen strategiaan. Tsenin ja muiden (2023, s. 10) tekemän tutkimuksen mukaan todettiin, että ne organisaatiot, joilla oli korkeampi kyberresilienssi koulutuksen tasolla ja strategisessa suunnittelussa, ne organisaatiot eivät joutuneet kyberhyökkäysten kohteeksi. Varsinkin koulutusten huomattiin vähentävän häiriötilanteita. Kweonin ja muiden (2019, s. 365, 369–370) tekemä tutkimus tukee Tsenin ja muiden (2023, s. 2–3) havaintoa. Kweonin ja muiden (2019, s. 365, 369–370) tutkimuksessa oli mukana 7089 organisaatiota. Tutkimuksessa käytettiin kolmea tekijää, joiden suhdetta analysoitiin Poissonin regressiomallilla. Nämä kolme tekijää olivat: koulutusaika, koulutuksen osallistujat ja koulutuksen ulkoistaminen. Näiden kolmen tekijän välistä suhdetta tutkittiin kyberturvallisuuspoikkeamien määrän kannalta. Tutkimuksen tuloksilla pystyttiin osoittamaan tilastollisesti merkitsevä negatiivinen yhteys tietoturvakoulutukseen käytetyn ajan ja tietoturvapoikkeamien määrän välillä.

Elliotin ja muiden (2010, s. 71–72) mukaan pelkkä teknologia ei riitä saavuttamaan laadukasta resilienssiä organisaatioissa. Se edellyttää jatkuvaa kehittämistä organisaation toimintatapojen ja rutiinien osalta. Organisaatioiden resilienssi rakentuu

ymmärryksestä käyttäytymiseen vaikuttavista tekijöistä sekä organisaation sisäisessä kuin ulkoisessa toimintaympäristössä. Tämä käyttäytymiseen liittyvien tekijöiden huomioiminen korostaa digitaalisen resilienssin merkitystä osana liiketoiminnan jatkuvuudenhallintaa. Digitaalinen resilienssi ei ole pelkästään tekninen kysymys, vaan siihen liittyy johtamisen lisäksi organisaation toimintatavat. Kun organisatorinen resilienssi yhdistetään toimiviin teknisiin turvatoimiin, organisaatiolla on paremmat edellytykset selviytyä kyberuhista. Steen ja muut (2023, s. 8) kertovat, että vahvistaakseen organisaatioiden resilienssiä ja parantaakseen organisaatioiden kyberturvaa on edellytyksenä protokollien ja jatkuvuussuunnitelmien säännöllinen päivittäminen ja testaaminen.

Petrenkon (2019, s. 10-11) mukaan kyberresilienssin kehittäminen edellyttää organisaatiolta toimivaa perustason kyberturvallisuutta, joka luo hyvän pohjan resilienssin rakentumiselle. Kyberturvallisuusalan osaajapula, teknologian nopea kehitys sekä koulutusohjelmien osittainen vanhentunut sisältö lisäävät tarvetta tulevaisuudessa tiiviimmälle yhteistyölle organisaatioiden ja koulutusta tarjoavien tahojen välillä. Tällainen yhteistyö on tärkeää, jotta ajantasainen osaaminen saadaan organisaatioiden käyttöön tehokkaasti. Petrenko (2019, s. 109–111) myös kuvaa kyberresilienssin yhdeksi päätavoitteeksi kyberjärjestelmien kehittämisen niin, että ne pystyvät jatkamaan toimintaansa ja mukautumaan erilaisiin häiriötilanteisiin myös silloin, kun järjestelmiin kohdistuu erilaisia merkittäviä haitallisia vaikutuksia.

Kyberresilienssin vahvistaminen edellyttää teknisten ratkaisujen lisäksi joustavaa ja kokonaisvaltaista lähestymistapaa kyberturvallisuuden johtamiseen. Organisaatioiden on kyettävä vastaamaan nopeasti muuttuviin uhkiin ja kehittämään toimintamallejaan jatkuvasti, mikä korostaa ketterän johtamisen merkitystä (Hausken, 2020, s. 4, 16).

Euroopan unioni on vastannut kasvaviin kyberuhkiin kyberkestävyyssäädöksellä (Cyber Resilience Act), joka tuli voimaan 10.12.2024. Säädöksen tarkoituksena on varmistaa, että digitaaliset tuotteet ja ohjelmistot suunnitellaan, päivitetään ja ylläpidetään niin,

että ne suojaavat käyttäjiä kyberuhilta läpi tuotteen elinkaaren (Euroopan komissio, 2026). Myös ISO 22301 – standardin (2019) mukaan liiketoiminnan jatkuvuus edellyttää, että organisaatio huomioi sekä henkilöstön toimintakyvyn että organisatoriset rakenteet osana resilienssin rakentamista.

3 Jatkuvuussuunnittelu ja varautuminen organisaatioissa

Tässä luvussa käsitellään jatkuvuussuunnittelua ja varautumista organisaatioissa sekä niiden yhteyttä tietojärjestelmiin. Luvussa 3.1 tarkastellaan jatkuvuussuunnittelun roolia organisaatiossa yleisellä tasolla. Luvussa käydään läpi, miksi jatkuvuussuunnittelusta on tullut yhä selkeämmin ylimmän johdon vastuulle kuuluva asia ja mitä tavoitteita sille asetetaan organisaation toiminnan erilaisissa häiriötilanteissa. Luvussa 3.2 käydään läpi tietojärjestelmien roolia jatkuvuussuunnittelussa ja miksi tietojärjestelmät muodostavat usein keskeisen osan jatkuvuussuunnittelussa. Millaisia vaatimuksia niiden toiminnan turvaamisella on. Miten tekninen, hallinnollinen ja inhimillinen näkökulma tukevat yhdessä tietojärjestelmien häiriönsietokykyä?

3.1 Jatkuvuussuunnittelun rooli organisaatiossa

Bladesin ja Doughtyn (2001, s. 27) mukaan jatkuvuussuunnittelulla organisaatioissa (*eng. business continuity planning*) tarkoitetaan toimenpiteitä, joilla mahdollistetaan organisaation normaali toiminta ennen kyberuhkaa, sen aikana ja sen jälkeen, kuitenkin mahdollisimman vähäisin vaikutuksin muihin toimijoihin. Kyseiset toimenpiteet ovat: ennaltaehkäisy, valmius, sopeutuminen ja palautuminen.

Cedergrenin ja Hasselin (2025, s. 1) mukaan, jatkuvuudenhallinta ja suunnittelu on alkujaan ollut käytössä yksityisellä sektorilla. Myöhemmin jatkuvuudenhallinta ja suunnitelmat on tullut käyttöön myös julkiselle puolelle. Cedergrenin ja Hasselin (2025, s. 2) mukaan, jatkuvuussuunnittelun merkitys on julkisella puolella kriittinen, koska julkinen puoli kohdistuu koko yhteiskunnan kriittisiin toimintoihin esimerkiksi terveydenhuolto ja turvallisuuspalvelut. Näillä on suora vaikutus kansalaisten terveyteen ja yleiseen turvallisuuteen. Cedergrenin ja Hasselin (2025, s. 8) tutkimus toteaa että, julkisen sektorin jatkuvuudenhallinta on jäljessä ja suunnitelmat pinnallisia. Tutkimus myös toteaa että, julkisella sektorilla jatkuvuudenhallinta on haastavampaa lakisääteisten velvoitteiden ja laajan vastuualueen vuoksi. Julkisen sektorin rajalliset

resurssit ovat myös esteenä. Näistä syistä yksityisellä sektorilla pystytään olemaan edelläkävijöitä jatkuvuudenhallinnan ja suunnitelmien osalta.

Bladesin ja Doughtyn (2001, s. 26–29) mukaan liiketoiminnan jatkuvuuden turvaaminen, hallinta ja aloittamisprosessi ovat nousseet organisaatioissa yhä selkeämmin ylimmän johdon vastuulle, eikä niitä enää nähdä pelkästään kyberturvallisuus- tai IT-organisaation vastuualueena. Ylimmän johdon pitää ymmärtää entistä paremmin erilaiset riskit sekä henkilökohtainen vastuu katastrofin sattuessa. Blades ja Doughty (2001, s. 28–29) puhuvat myös taloudellisesta näkökulmasta. Mitä paremmin organisaatiot osaavat arvioida tilannetta ja selvittää omat riskialueensa, sitä paremmin ne ovat turvassa suurilta katastrofeilta. Suuret katastrofit ja niistä palautuminen ovat organisaatioille erittäin kalliita prosesseja. Iivarin ja Laaksosen (2009, s. 100) mukaan riskienhallintaa lisätään jatkuvuussuunnitteluun nykypäivänä entistä enemmän osana organisaatioiden jatkuvuussuunnittelua. Siitä huolimatta jatkuvuussuunnittelussa on edelleen nähtävissä kehittämistarpeita.

Iivarin ja Laaksosen (2009, s. 18) mukaan jatkuvuussuunnittelun avulla pyritään varmistamaan organisaation toiminta normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Jatkuvuussuunnittelu ei valmistu yhdellä kertaa, vaan se on jatkuva prosessi. Iivari ja Laaksonen (2009, s. 18) kertovat, että jatkuvuussuunnittelun keskeisenä tavoitteena on ennakoida ja hallita erilaisia toimintaa häiritseviä tilanteita. Toiminnan jatkuvuutta uhkaavia tekijöitä voivat olla esimerkiksi tietojärjestelmähäiriöt, inhimilliset virheet, tahallinen väärinkäyttö, tietoliikenne- tai sähkökatkokset, tulipalot sekä vesivahingot. Iivari ja Laaksonen (2009, s. 22–24) kertovat, että jatkuvuussuunnittelulla on merkitys myös organisaatioiden riskienhallinnassa. Näihin mahdollisiin riskeihin voidaan varautua jatkuvuussuunnitteluun kuuluvien toipumissuunnitelmien sekä normaalioloissa toteutettavien liiketoiminnan tukiprosessien avulla.

Groenendaalin ja Helslootin (2020, s. 102, 104–105) mukaan organisaation resilienssi koostuu kahdesta toisiaan täydentävästä strategiasta: jatkuvuudenhallinnasta

ennakoitavia uhkia vastaan ja ennakoidusta improvisaatiosta yllättäviä suuronnettomuuksia varten. Jatkuvuussunnittelu on todettu tehokkaaksi keinoksi hallita tietojärjestelmähäiriöitä, mutta se ei yksin riitä kattamaan odottamattomia niin kutsuttuja ”musta joutsen” (*eng. black swan*) tapahtumia. Näille niin sanotuille ”musta joutsen” tapahtumille on ominaista niiden yllätyksellisyys ja niiden mittavat vaikutukset. Groenendaalin ja Helslootin (2020, s. 105–106) tutkimus toteaa, että jatkuvuussuunnittelun liiallinen byrokratisoituminen ja kasvavat vaatimukset voivat lisätä organisaatioiden kuormitusta. Tämä heikentää organisaation ketteryyttä ja sopeutumiskykyä.

Groenendaalin ja Helslootin (2020, s. 105, 108) mukaan resilienssin toteuttaminen organisaation arjessa vaatii tasapainoa suunnitelmien noudattamisen ja asiantuntijoiden improvisaatiokyvyn välillä. Suunnitelman tarkoituksena tulisi olla sellaisen rakenteen luominen, joka mahdollistaa nopean päätöksenteon ja tiedonkulun jopa silloin, kun kohdataan tilanteita, joihin valmiit protokollat eivät vastaa.

Jenningsin (2025) mukaan ISO 22301-standardi korostaa tietojärjestelmien keskeistä roolia organisaation toiminnan jatkuvuuden turvaamisessa. Nykyaikainen liiketoiminta on vahvasti riippuvainen digitaalisista järjestelmistä ja tiedonkäsittelystä. Standardin mukainen jatkuvuudenhallintajärjestelmä edellyttää, että organisaatio tunnistaa kriittiset tietojärjestelmät, arvioi niihin kohdistuvat riskit ja määrittelee toimintamallit, joilla järjestelmien toiminta voidaan turvata häiriötilanteissa. Kuten luvussa 2.2 todettiin ISO 22301 korostaa ennakoivaa varautumista, selkeitä vastuita sekä testattuja palautumis- ja toipumissuunnitelmia, joiden avulla organisaatio kykenee vastaamaan esimerkiksi kyberhyökkäyksiin, järjestelmäkatkoksiin tai tietomurtoihin hallitusti. Näin standardi tukee kyberresilienssin rakentamista varmistamalla, että tietojärjestelmät eivät ainoastaan pyri estämään häiriöitä, vaan kykenevät myös sietämään niitä ja palautumaan nopeasti ilman merkittäviä vaikutuksia liiketoiminnan jatkuvuuteen.

3.2 Tietojärjestelmät osana jatkuvuussuunnittelua

Berkeley School of Informationin (2022) mukaan tietojärjestelmä on kokonaisuus, jonka pääideana on auttaa keräämään, analysoimaan, ylläpitämään ja jakamaan tietoa. Tyypillisesti tietojärjestelmiin kuuluu laitteisto, ohjelmisto, tietokanta, verkko sekä järjestelmiä käyttävä ja ylläpitävä henkilöstö. Kyberturvallisuussanasto (2026) määrittelee samansuuntaisesti, että tietojärjestelmä koostuu digitaalisesta tiedosta, tietoa käsittelevistä ohjelmista, käsittelysäännöistä, laiteresursseista sekä erilaisista toimintaohjeista. Nämä osa-alueet muodostavat kokonaisuuden, jota voidaan kutsua tietojärjestelmäksi. Määritelmään liittyy myös huomautus, että tietojärjestelmän osaksi voidaan jossain yhteyksissä sisällyttää tietojärjestelmien käyttäjiä ja heidän toimintakäytäntöjään. Teknologiariippuvaisessa toimintaympäristössä tietojärjestelmät perustuvat ihmisten ja tietoteknisten ratkaisujen yhteistyöhön. Tietojärjestelmät eivät ainoastaan tallenna ja analysoi dataa, vaan ne myös muokkaavat datan käyttökelpoiseksi tiedoksi, joka tukee organisaatioiden päätöksentekoa. Tietojärjestelmien toiminta on monimutkaista, mutta loppujen lopuksi edellyttää aina näiden kolmen tekijän yhteispeliä: ihmisten, teknologian ja prosessien.

Plevnikin (2026, s. 1, 2) mukaan viestintä- ja tietojärjestelmät muodostavat nykyaikaisen digitaalisen hallinnon keskeisen perustan. Niiden merkitys ulottuu teknisen toiminnan ylläpitämistä pidemmälle. Nämä vaikuttavat suoraan organisaation jatkuvuuteen, vastuullisuuteen ja toimintakykyyn. Organisaatioissa, joissa on korkea turvataso, jatkuvuudenhallinta nousee strategiseen rooliin, koska järjestelmähäiriöt voivat heikentää organisaation kykyä reagoida turvallisuushaasteisiin.

Bladesin ja Doughtyn (2001, s. 28–29) mukaan organisaatioiden suuri huolenaihe pitäisi olla tietokoneresurssit. Suurin osa organisaatioista luottaa reaaliaikaiseen tietojenkäsittelyyn. Tilastojen mukaan, jos organisaatioiden koneet ovat käyttökelvottomia viiden työpäivän ajan, yli 90 % organisaatioista lopettaa toimintansa seuraavan vuoden aikana. Jatkuvuussuunnittelu kytkeytyy tiiviisti organisaation

riskienhallintaan, koska molempien tavoitteena on tunnistaa toimintaa uhkaavat tekijät ja varautua niihin ennakoivasti.

Valtiovarainministeriön (2016, s. 7) mukaan jatkuvuussuunnittelun tavoitteena on turvata organisaation ydintoimintojen häiritsemätön ja yhtenäinen toiminta. Keskeistä on, että jatkuvuudensuunnittelu integroidaan osaksi organisaatioiden päivittäistä toimintaa ja sitä tuetaan dokumentoidulla jatkuvuudensuunnittelujärjestelmällä. Järjestelmällisen jatkuvuussuunnittelun avulla organisaatiot pystyvät ennakoivasti suojautumaan häiriöiltä, vähentää niiden todennäköisyyttä sekä varautua häiriöiden korjaamiseen ja niistä palautumiseen.

Jatkuvuudensuunnittelua tarkasteltaessa on tärkeää huomioida myös sektorikohtaiset erot. Iivarin ja Laaksosen (2009, s. 21–22) mukaan on tärkeää muistaa eroavaisuudet julkishallinnon ja yrityshallinnon välillä. Erityisesti varautumiseen ja varautumissuunnitteluun liittyvässä terminologiassa on eroja. On hyvä erottaa toisistaan normaaliolot, normaaliolojen häiriötilanteet sekä poikkeusolot. Näihin liittyvät vaatimukset ja toimintamallit eroavat toisistaan.

Teknisten ja hallinnollisten näkökulmien lisäksi jatkuvuussuunnittelussa korostuu yhä enemmän inhimillinen ulottuvuus. Siirtolan (2024) mukaan kyberuhka ei ole vain teknologinen ongelma eikä sitä aina korjata vain digitaalisilla ohjelmilla. Ihmisten osaamisella ja kouluttamisella on suuri vastuu. Virheistä ei tulisi rangaista yksilöä, vaan niitä tulisi käsitellä avoimesti yhteisönä. Virheistä opittua työympäristöön syntyy avoimuuden lisäksi psykologista turvallisuutta. Avoin ja kannustava ilmapiiri tukee kyberresilienssiä, joka on osa organisaation kokonaisturvallisuutta.

4 Narratiivinen kirjallisuuskatsaus

Tässä luvussa käydään läpi tutkielman tutkimusmenetelmää ja perustellaan, miksi valittu menetelmä soveltuu parhaiten juuri tähän tutkielmaan. Tutkimus on tehty narratiivisena kirjallisuuskatsauksena. Toteutustavan myötä on tärkeää käydä läpi, mitä kirjallisuuskatsaustyyppejä on olemassa ja mikä niistä soveltuu parhaiten tähän työhön. Luvussa 4.1 vertaillaan erilaisia tutkimusmenetelmiä. Tutkimuksessa käydään läpi narratiivisen kirjallisuuskatsauksen tyylejä. Miksi juuri tähän menetelmään on päädytty. Tutkimuksessa käytettyä narratiivista kirjallisuuskatsausta verrataan myös muihin kirjallisuuskatsaustyyppeihin. Luvussa 4.2 kuvataan tutkielman aineiston hakuprosessia konkreettisesti. Mistä tutkimusaineisto on haettu. Millaisia kriteereitä tutkimusaineiston rajaamisessa ja seulonnassa on ollut.

4.1 Kirjallisuuskatsauksia

Salmisen (2023, s. 3) mukaan kirjallisuuskatsauksen ideana on löytää uusia kehityskohteita, joiden avulla voidaan luoda uutta teoriaa vanhan lisäksi sekä samalla kehittää ja arvioida vanhoja teorioita. Kirjallisuuskatsausten avulla voidaan tiivistää suuria aineistoja ja löytää niiden avulla uutta tietoa käsiteltävästä aiheesta. Löydetyn tiedon avulla tutkijat pystyvät syventämään omaa tietämystään ja vahvistamaan asemaansa eri yhteisöissä.

Kuvaileva kirjallisuuskatsaus on yksi suosituimmista kirjallisuuskatsauksista. Salmisen (2023, s. 7–8) mukaan kuvaileva kirjallisuuskatsaus on eri kirjallisuuskatsauksista luovin. Sillä ei ole täysin rajattuja sääntöjä ja sitä kutsutaankin yleiskatsaukseksi. Kuvailevassa kirjallisuuskatsauksessa tutkimusaineistot ovat hyvin laajoja ja tutkimusaineistoa käsitellään tutkimuksissa laajasti. Kuvaileva kirjallisuuskatsaus voidaan jakaa kolmeen eri tarkoituksen mukaiseen katsaukseen, joita ovat: narratiivinen, kartoittava ja integroiva.

Salminen (2023, s. 8–11) toteaa, että narratiivinen kirjallisuuskatsaus on kirjallisuuskatsauksista niin sanotusti kevyin katsaustyyppi. Narratiivisen katsauksen

tavoitteena on antaa laaja, helppolukuinen yleiskuva aiheesta ja sen kehityskulusta. Aineistossa ei käytetä systemaattista seulaa, vaan analyysi on enemmän kuvailevaa synteesiä. Kartoittava katsaus on näistä uusin, jonka suosio on kasvussa. Kartoittava katsaus muistuttaa osin narratiivista katsausta. Kartoittava katsaus perustuu narratiivisen katsauksen tavoin aineistolähteisiin ja etenee saman vaiheen toistamisen kautta. Integroivassa kirjallisuuskatsauksessa puolestaan keskitytään mahdollisimman laajaan kuvaamiseen ja tuotetaan uutta tietoa jo tutkitusta aiheesta kriittisen arvioinnin pohjalta. Integroivassa katsauksessa on narratiivisen katsauksen joustavuutta, mutta myös systemaattisen katsauksen kriittistä analyysiä ja vaiheittain etenemistä.

Tutkielmaan valittiin narratiivinen katsaus ja tarkemmin vielä narratiivinen yleiskatsaus. Kyberresilienssi ja jatkuvuussuunnittelu ovat molemmat laajoja aihealueita. Niitä on käsitelty esimerkiksi tietojärjestelmätieteen-, johtamisen- ja riskienhallinnan näkökulmista. Aihealueiden laajuuden takia tiukasti rajattua katsausta ei pidetty järkevänä. Työn tavoitteena on antaa lukijalle laaja ja helppolukuinen yleiskuva kyberresilienssistä ja jatkuvuussuunnittelusta ja niiden välisestä yhteydestä. Salminen (2023, s. 8) kertoo, kuinka narratiivisella yleiskatsauksella pystytään antamaan lukijalle kirjallisuuskatsauksista laajin mahdollinen kuva tarkastellusta aiheesta, mikä tukee tutkielman tavoitetta.

4.2 Aineiston hankinta

Tutkielmassa käytetty aineisto haettiin tieteellisistä tietokannoista: Scopus, ACM Digital Library, IEEE Xplore ja Web of science. Tietokannoissa käytettiin hakutermejä *resilience, cyber resilience, business continuity planning, organization, information systems* ja näiden yhdistelmiä käyttäen boolen operaattoreita. Hakua tehtäessä valittiin hakusanan esiintyvän otsikossa. Tämä rajasi monia olemassa olevia aineistoja. Tietoa hain viimeiseltä seitsemältä vuodelta, eli vuosilta 2019–2026. Lähteitä etsittiin aina jonkinlainen kysymys edellä esimerkiksi ”mitä tarkoittaa kyberresilienssi” tai ”vaikuttaako ihmiset organisaation kyberresilienssiin”. Tämä helpotti tutkimusaineiston valintaa. Jos aineisto ei vastannut kysymykseeni sitä ei hyödynnetty.

4.3 Aineiston analyysi

Työssä käytettyjen artikkeleiden analyysiä on tehty koko ajan työn edetessä. Salminen (2023, s. 8) toteaa, että narratiivisessa katsauksessa analyysi on kuvailevaa eikä systemaattista, minkä vuoksi aineiston keruun ja tekstin kirjoittamisen pystyi tekemään samanaikaisesti. Artikkeleihin tutustuin aluksi lukemalla niiden tiivistelmät. Tiivistelmää lukiessa pohdin, käsitteleekö kyseinen artikkeli kyberresilienssiä, jatkuvuudenhallintaa tai tietojärjestelmiä yksin tai erikseen. Kun artikkeli oli vaaditulta aikaväliltä ja tiivistelmä vaikutti tutkielman kannalta relevantilta, siirryin lukemaan koko tekstin yksityiskohtaisemmin. Näiden avulla huomasi nopeasti epäoleelliset artikkelit, jotka pystyivät jättämään pois. Jos aineisto ei vastannut aiemmassa kohdassa mainitsemiini kysymyksiin, mutta oli sisällöltään hyvä, otin artikkelin tiedot itselleni ylös tulevaa varten. Valituista artikkeleista kirjoitin itselle keskeiset muistiinpanot ylös. Tämän jälkeen pohdin, mihin kohtaan tutkielmaa kyseistä artikkelia voisi hyödyntää. Samalla jaoin artikkeleita aihepiirien mukaan, esimerkiksi kyberresilienssin määrittely, yksilön ja organisaation resilienssi, tietojärjestelmät ja jatkuvuudenhallinta. Tämä helpotti työn tekemistä ja tulosluvun kirjoittamista lopussa.

5 Tulokset

Tämän kandidaatintutkimuksen tarkoituksena oli selvittää kyberresilienssin roolia tietojärjestelmien integroinnissa organisaation jatkuvuussuunnittelussa. Tässä luvussa käsitellään tämän kirjallisuuskatsauksen keskeisiä tuloksia ja vastataan alussa mainittuun tutkimuskysymykseen aineiston perusteella. Luvussa 5.1 käydään tarkemmin läpi tutkimuksessa käytettyä aineistoa. Luvussa 5.2 käydään tutkimuksen tulokset läpi kyberresilienssin integrointiin vaikuttavien tekijöiden kautta. Vaikuttavat tekijät on jaettu teknisiin ja organisatoriin tekijöihin sekä inhimillisiin tekijöihin. Luvussa 5.3 käydään tutkimuksen tulosten yhteenveto tarkemmin läpi ja arvioidaan, miten ne vastaavat tutkimuksen tutkimuskysymykseen ja tavoitteeseen.

5.1 Tutkimusaineisto

Alla olevaan taulukkoon 1 on koottu tässä tulosluvussa hyödynnetyt kymmennen artikkelia. Taulukossa esitetään jokaisen artikkelin tunniste, nimi, tekijät, julkaisuvuosi ja julkaisupaikka.

Taulukko 1. Tutkimuksessa käytetty aineisto.

Id	Nimi	Tekijä	Vuosi	Julkaisupaikka
A1	Organizational Cyber Resilience	Bagheri, S., Ridley, G. & Williams, B.	2023	Australasian Journal of Information Systems
A2	Business continuity management in public sector organizations: Development, challenges, and ways forward	Cedergren, A. & Hassel, H	2025	Journal of contingencies and crisis management
A3	Evaluating the impact of human resource planning programs in addressing the	Chakraborty, D. & Biswas, W.	2019	Journal of advances in management research

Id	Nimi	Tekijä	Vuosi	Julkaisupaikka
	strategic goal of the firm an organizational perspective.			
A4	Organisational resilience: Shifting from planning-driven business continuity management to anticipated improvisation	Groenendaal, J. & Helsloot, I.	2020	Journal of business continuity & emergency planning
A5	Cyber resilience in firms, organizations and societies	Hausken, K.	2020	Internet of Things
A6	Development of a new 'human cyber-resilience scale'	Joinson, A.	2023	Journal of Cybersecurity
A7	The Utility Information Security Training and Education on cybersecurity Incidents: An empirical evidence	Kweon, E., Lee, H., Chai, S. & Yoo, K	2019	Information Systems Frontiers
A8	Communication and information systems user support as a governance mechanism in a high-security public organization	Plevnik, M	2026	Multidisciplinary digital publishing institute (MDPI)
A9	Business continuity and resilience management: A conceptual framework.	Steen R., Haug J. & Patriarca R.	2023	Journal of Contingencies and Crisis Management
A10	The effect of organizational cyber	Tsen, E., K L Ko, R. & Slapnicar, S.	2023	Journal of Cybersecurity

Id	Nimi	Tekijä	Vuosi	Julkaisupaikka
	resilience on cyber incident outcomes.			

Taulukosta 1 ilmenee, että artikkelit ovat julkaistu vuosina 2019–2026. Julkaisuvuodeltaan uusin artikkeli (Plevnik, 2026) keskittyy tietojärjestelmien rooliin julkisen puolen turvallisuudessa. Muut artikkelit keskittyvät tarkastelemaan kyberresilienssiä ja jatkuvuudenhallintaa yksilön tai organisaation näkökulmasta. Tämä mahdollistaa aiheen tutkimisen useasta eri suunnasta. Suurin osa artikkeleista onkin julkaistu kyberturvallisuuden ja kriisijohtamisen tieteellisissä aikakausilehdissä, kuten Journal of Cybersecurity ja Journal of Contingencies and Crisis Management.

5.2 Kyberresilienssin integrointiin vaikuttavat tekijät

Tutkimuksen tulokset osoittavat, että tietojärjestelmät voidaan kyberresilienssin näkökulmasta integroida osaksi organisaation liiketoiminnan jatkuvuussuunnittelua neljän eri päätekijän kautta. Nämä neljä eri tekijää ovat toisiaan täydentäviä tekijöitä ja ne ovat: joustava johtaminen (A), suunnitelmien jatkuva päivittäminen ja testaaminen (B), tietojärjestelmien tekninen rooli (C) sekä henkilöstön osaaminen (D). Tekijät A, B ja C liittyvät teknisiin ja organisatorisiin ratkaisuihin, joita käsitellään tulosluvussa 5.2.1. Tekijä D puolestaan liittyy inhimillisiin tekijöihin, jota käsitellään tulosluvussa 5.2.2.

5.2.1 Tekniset ja organisatoriset tekijät

Kirjallisuuskatsaus osoittaa, että kyberresilienssi näyttäytyy huomattavasti laajempana kokonaisuutena kuin pelkkä perinteinen kyberturvallisuus. Tutkimuksesta voidaan todeta, ettei organisaatioiden tavoitteena ole ainoastaan estää kyberhyökkäyksiä, vaan myös ylläpitää toimintakykyä ja palautua nopeasti häiriötilanteista. Katsauksen perusteella tekniset ratkaisut ja organisatoriset toimintatavat muodostavat yhdessä perustan kyberresilienssin integroimiselle osaksi organisaation jatkuvuussuunnittelua.

Tutkimusaineisto osoittaa, että pelkkä tekninen varautuminen ei riitä, vaan kyberresilienssi edellyttää myös joustavaa johtamista, jatkuvaa suunnitelmien päivittämistä sekä henkilöstön osaamista.

Organisaation resilienssi rakentuu kahdesta toisiaan täydentävästä strategiasta: ennakoitavia riskejä vastaan toimivasta jatkuvuudenhallinnasta ja yllättäviä suuronnettomuuksia varten suunnitellusta ennakoidusta improvisaatiosta (Groenendaal ja Helsloot, 2020, s. 102, 104–105). Tämän tutkimuksen edetessä hyvin keskeiseksi tekijäksi nousi joustava johtaminen. Liian tiukat säännöt ja protokollat voivat heikentää organisaation kykyä reagoida odottamattomiin tilanteisiin. Hyvän jatkuvuussuunnittelun tulisi mahdollistaa nopea päätöksenteko myös tilanteissa, joihin valmiit säännöt tai protokollat eivät sovellu (Groenendaal ja Helsloot, 2020, s.105–106). Samaan johtopäätökseen päätyi myös Hausken (2020, s. 4, 16). Hauskenin (2020, s. 4, 16) toteaa, että kyberresilienssin vahvistaminen edellyttää teknisten ratkaisujen lisäksi ketterää ja kokonaisvaltaista lähestymistapaa, jotta organisaatiot kykevät vastaamaan nopeallakin aikataululla muuttuviin tilanteisiin. Molempien tutkimusten (Groenendaal ja Helsloot, 2020, s.105–106 ja Hausken, 2020, s. 4, 16) tukevat siis toisiaan siinä, että tiukka ja yksityiskohtainen suunnittelu voi heikentää organisaation kykyä reagoida odottamattomiin tilanteisiin. Bagherin ja muiden (2023, s. 9) tekemä tutkimus tukee edellisiä havaintoja siitä, että onnistuneen kyberresilienssin saavuttamiseksi edellytetään IT-johdon ja liiketoimintajohdon välistä ymmärrystä toisistaan. Joustava johtaminen ei toteudu yksittäisten johtajien tasolla, vaan vaatii yhteistyötä eri tahojen välillä.

Eri organisaatioiden lähtökohdat jatkuvuudenhallinnalle eivät ole aina tasavertaisia. Cedergenin ja Hasselin (2025, s.1–2, 8) mukaan jatkuvuudenhallinta on kehittynyt alun perin yksityisellä sektorilla. Julkinen sektori tulee jäljessä, kun verrataan sitä yksityiseen sektoriin. Julkisella sektorilla lakisääteiset velvoitteet ja laaja vastuu kriittisistä yhteiskunnallisista toiminnoista, kuten terveydenhuollosta ja turvallisuuspalveluista, tekevät jatkuvuudenhallinnasta erityisen haastavaa. Julkisen sektorin rajalliset resurssit

tekevät jatkuvuudenhallinnasta julkisella sektorilla haastavampaa ja suunnitelmista usein pinnallisempia. Cedergrenin ja Hasselin (2025, s. 1–2, 8) tutkimus osoittaa, että joustavan johtamisen ja jatkuvan päivittämisen (tekijä B) toteuttaminen käytännössä riippuu myös organisaation toimialasta ja käytettävissä olevista resursseista. Pelkkä tieto hyvistä käytännöistä ei riitä ilman niiden edellyttämää kapasiteettia.

Organisaation resilienssin ja kyberturvan vahvistaminen edellyttää erilaisten protokollien ja jatkuvuussuunnitelmien jatkuvaa päivittämistä sekä niiden testaamista. Järjestelmien on pysyttävä ajan tasalla jatkuvasti. Pelkkien suunnitelmien olemassaolo ei riitä (Steen ja muut, 2023, s. 8). Tätä tukien Tsenin ja muiden (2023, s. 10) tekemä tutkimus osoittaa, että organisaatiot, joilla oli korkeampi kyberresilienssi erityisesti koulutuksen tasossa ja strategian suunnittelussa, joutuivat harvemmin kyberhyökkäysten kohteeksi. Nämä tutkimukset osoittavat yhdessä sen, että organisatoriset toimintatavat ja tekninen valmius täydentävät toisiaan. Pelkkä tekninen järjestelmä ei riitä, jos sitä ei tueta jatkuvalla ylläpidolla ja osaamisella.

Viestintä- ja tietojärjestelmät muodostavat nykyaikaisen digitaalisen hallinnon keskeisen perustan, jonka merkitys ulottuu pelkän teknisen toiminnan ylläpitoa pidemmälle (Plevnik 2026, s. 1–2). Järjestelmähäiriöt voivat heikentää organisaation kykyä reagoida turvallisuushaasteisiin. Tämän vuoksi jatkuvuudenhallinta nousee korkean turvatason organisaatioissa strategiseen rooliin. Tietojärjestelmien avulla voidaan toteuttaa esimerkiksi järjestelmien jatkuvaa valvontaa, varmuuskopiointia ja muita teknisiä ratkaisuja, jotka mahdollistavat liiketoiminnan jatkumisen myös häiriötilanteissa (Plevnik, 2026, s. 1–2). Tietojärjestelmien tekninen rooli muodostaa keskeisen osan organisaation jatkuvuudenhallinnasta. Sillä pystytään mahdollistamaan kriittisten toimintojen ylläpitäminen myös häiriötilanteissa.

Yhteenvetona voidaan todeta, että tekijät joustava johtaminen, suunnitelmien jatkuva päivittäminen ja testaaminen sekä tietojärjestelmien tekninen rooli osoittavat, että tietojärjestelmien integrointi jatkuvuussuunnitteluun ei ole pelkkä tekninen kysymys.

Onnistunut tietojärjestelmien integrointi edellyttää teknisten ratkaisujen lisäksi ketterää ja joustavaa johtamista, jatkuvaa kehittämistä sekä organisaation kykyä mukautua muuttuviin kyberuhkiin. Kyberresilienssi rakentuu teknologian ja organisatoristen toimintatapojen yhteisvaikutuksesta, ei kummastakaan yksinään. Seuraavaksi tarkastellaan, miten inhimilliset tekijät täydentävät tätä kokonaisuutta.

5.2.2 Inhimilliset tekijät

Teknisten ja organisatoristen ratkaisujen lisäksi tutkimusaineistosta nousee esiin myös inhimillinen ulottuvuus, joka koskee henkilöstöä ja yksilöitä. Tämä osoittautuu yhtä keskeiseksi kyberresilienssin kannalta kuin tekniset ja organisatoriset tekijät. Luvussa 5.2.1 käsiteltiin johtamista, prosesseja ja järjestelmiä. Tässä luvussa 5.2.2 tarkastellaan, miten henkilöstön osaaminen ja yksilön kyberresilienssi vaikuttavat tietojärjestelmien integroimiseen jatkuvuussuunnittelussa.

Tsenin ja muiden (2023, s. 10) mukaan organisaatiot, joissa henkilöstön osaaminen ja henkilöstön koulutustaso oli korkeampi, joutuivat harvemmin kyberhyökkäysten kohteeksi. Myös Bagherin ja muiden (2023, s. 5) tekemä kyberresilienssimatriisi nostaa henkilöstön kouluttamisen yhdeksi suunnittelu- ja valmistautumisvaiheen keskeiseksi osaksi jatkuvuussuunnittelun rinnalla. Nämä havainnot yhdessä osoittavat, että koulutus ei ole pelkkä tukitoimenpide vaan suoraan mitattavissa oleva tekijä organisaation kyberresilienssin tasossa.

Koulutuksen merkitystä tukee myös Kweonin ja muiden (2019, s. 368–369) tekemä kvantitatiivinen tutkimus. Se tutkimus perustui 7089 organisaation aineistoihin, joka esiteltiin luvussa 2.2. Heidän tutkimuksensa tulokset vahvistavat, että koulutukseen käytetty aika on yhteydessä tietoturvapoikkeamien vähenemiseen. Varsinkin silloin, kun koulutus oli järjestetty organisaation ylimmälle johdolle.

Henkilöstösuunnittelun tutkimus tukee myös tämän tutkielman tulosta henkilöstön osaamisen merkityksestä. Seuraajasuunnittelu turvaa organisaation osaamispääoman

jatkuvuuden myös johtajavaihdosten yhteydessä. Tämä tekee siitä keskeisen tekijän pitkän aikavälin toimintakyvyn kannalta (Chakraborty ja Biswas, 2019, s. 673). Heidän havaintonsa tukee tämän tutkielman tulosta siitä, että henkilöstön osaaminen (tekijä D) on keskeinen osa kyberresilienssin rakentumista. Pelkkä hetkellinen koulutus ei riitä. Tarvitaan myös pitkäjänteistä suunnittelua siitä, kuka osaa mitäkin ja kuka voi tarvittaessa astua toisen tilalle. Nämä vahvistavat organisaation kykyä toimia erilaisissa häiriötilanteissa.

Yksilön näkökulmasta kyberresilienssiä on tutkinut erityisesti Joinson (2023, s. 1, 7, 9). Joinson kehitti tekemässään tutkimuksessa asteikon (*human cyber-resilience scale*). Kyseinen asteikko mittaa ihmisen kykyä selviytyä digitalisaation aiheuttamista haasteista. Tämä asteikko koostuu neljästä eri osa-alueesta. Nämä neljä osa-aluetta ovat: itseluottamus, sosiaalinen tuki, oppiminen ja kasvu sekä avuttomuus. Näiden eri osa-alueiden avulla pyritään löytämään piirteitä, jotka heikentävät tai vahvistavat yksilön resilienssiä. Asteikkoa voidaan käyttää myös eri väestöryhmien vertailuun sekä koulutushankkeisiin (Joinson, 2023, s. 1, 7, 9). Tämä asteikko tarjoaa apuvälineen, jota täydentää myös Tsenin ja muiden (2023, s. 10) havainto. Tsen ja muut (2023, s. 10) osoittaa, että korkeampi koulutustaso vähentää organisaatioihin kohdistuvia hyökkäyksiä, Joinsonin (2023, s. 1, 7, 9) tekemä asteikko mahdollistaa keinon selvittää, mitä yksilön kyberresilienssissä tulisi kehittää ja mitata.

5.3 Yhteenveto tuloksista

Tämän tutkimuksen tavoitteena oli tarkastella kyberresilienssin roolia tietojärjestelmien integroinnissa organisaation jatkuvuussuunnittelussa. Tutkimuksen tulokset vastaavat tähän tavoitteeseen osoittamalla, että kyberresilienssin rooli ei rajoitu yksittäiseen tekniseen toimenpiteeseen vaan muodostuu useista toisiaan täydentävistä tekijöistä. Nämä yhdessä määrittävät, miten tietojärjestelmät voidaan integroida onnistuneesti osaksi jatkuvuussuunnittelua.

Tulokset keskittyivät kahden pääteeman ympärille. Ensimmäinen teema on tekniset ja organisatoriset tekijät. Tämä teema sisälsi vielä kolme alateemaa, jotka olivat: joustava johtaminen (A), suunnitelmien jatkuva päivittäminen ja testaaminen (B) ja tietojärjestelmien tekninen rooli (C). Kyseiset tekijät osoittivat, että kyberresilienssin rooli tietojärjestelmien integroinnissa rakentuu teknologian ja organisatoristen toimintatapojen yhteiskuntavaikutuksesta. Pelkkä tekninen varautuminen ei riitä ilman joustavaa johtamista ja jatkuvaa ylläpitoa. Toisena pääteemana toimi inhimilliset tekijät jonka alateemana oli henkilöstön osaaminen ja koulutus (D). Tämä teema täydensi ensimmäistä osoittamalla, että henkilöstön kouluttaminen, pitkäjänteinen henkilöstösuunnittelu ja yksilön kyky sopeutua digitaalisen ympäristön haasteisiin ovat yhtä keskeisiä kuin tekniset ja organisatoriset ratkaisut sillon kun tietojärjestelmiä integroidaan osaksi jatkuvuussuunnttelua.

Useiden tutkimusten perusteella jatkuvuussuunnittelun tulisi perustua kykyyn toimia joustavasti odottamattomissa tilanteissa (Groenendaali ja Helsloot, 2020, Steen ja muut, 2023). Lisäksi tutkimusten pohjalta havaittiin, että suunnitelmien säännöllinen päivittäminen, testaaminen ja henkilöstön osaamisen kehittäminen vahvistavat organisaation kyberresilienssiä (Tsen ja muut, 2023). Tämän lisäksi tulokset osoittavat, että suunnitelmien säännöllinen päivittäminen, testaaminen ja henkilöstön osaamisen kehittäminen vahvistavat käsitystä siitä, että kyberresilienssi ei ole pelkkä tekninen ominaisuus. Se on monialainen ilmiö, joka edellyttää teknisten ratkaisujen, organisatoristen toimintatapojen ja inhimillisten tekijöiden yhteensovittamista. Tämä näkökulma tarjoaa perustan seuraavassa luvussa esitettäville johtopäätöksille ja käytännön suosituksille.

6 Johtopäätökset ja pohdinta

Tämän tutkimuksen tavoitteena oli tarkastella kyberresilienssin roolia tietojärjestelmien integroinnissa organisaation jatkuvuussuunnittelussa. Tämän kirjallisuuskatsauksen perusteella voidaan todeta, että kyberresilienssi ja jatkuvuussuunnittelu ovat vahvasti toisiinsa liittyviä kokonaisuuksia. Niitä ei voi nykypäivänä tutkia erillisinä osa-alueina. Organisaatioiden digitalisoituessa tietojärjestelmien merkitys liiketoiminnan jatkuvuuden turvaamisessa on kasvanut huomattavasti, jonka takia niiden toimintakykyyn kohdistuvat riskit on huomioitava yhtenä osana jatkuvuudenhallintaa.

Yhtenä keskeisenä havaintona tutkimuksessa havaittiin, että tietojärjestelmien integrointi osaksi jatkuvuudensuunnittelua edellyttää sekä teknisten että organisaatioiden tekijöiden huomioimista. Pelkkä tekninen kyberturvallisuus ei riitä takaamaan organisaation toimintakykyä häiriötilanteissa. Tarvitaan myös selkeät toimintamallit, henkilöstön osaaminen, johtaminen ja jatkuva kouluttautuminen. Nämä tulokset ovat linjassa Elliotin ja muiden (2010, s. 71–72) tekemien havaintojen kanssa. Resilienssiä ei voida saavuttaa teknologian avulla yksin. Se edellyttää organisaation toimintatapojen jatkuvaa kehittämistä. Samansuuntaisesti Groenendaal ja Helsloot (2020, s. 105–106) sekä Hausken (2020, s. 4, 16) korostavat joustavan johtamisen merkitystä ennalta määrättyjen ja tiukkojen suunnitelmien sijaan. Tämä on havainto, joka toistui myös tämän tutkielman tuloksissa erityisesti joustavan johtamisen (tekija A) osalta.

Katsauksen perusteella huomataan myös, että inhimillisillä tekijöillä on merkittävä vaikutus kyberresilienssin toteutumiseen. Organisaatioiden henkilöiden osaaminen, koulutus sekä avoimuus vaikuttavat siihen, kuinka tehokkaasti organisaatio kykenee tunnistamaan uhkia ja miten he toimivat häiriötilanteissa. Tätä havaintoa tukevat Tsenin ja muiden (2023, s. 10) sekä Kweonin ja muiden (2019, s. 365, 369–370) tutkimusten tulokset koulutuksen ja tietoturvapoikkeamien vähenemisen välisestä yhteydestä. Chakrabortyn ja Biswasin (2019, s. 673) tekemä laajempi henkilöstöjohtamisen näkökulma, jonka mukaan pitkäjänteinen henkilöstösuunnittelu, vahvistaa organisaation

kykyä toimia häiriötilanteissa. Myös Joinsonin (2023, s. 1, 7, 9) kehittämä yksilön kyberresilienssiä mittaava asteikko tukee tätä havaintoa nostamalla esiin, että kyberresilienssissä ei ole kyse pelkästään teknologisesta ominaisuudesta, vaan myös sosiaalisista taidoista ja yksilön kyvystä sopeutua.

Tutkimukseen liittyy aina rajoitteita. Tämä aineisto koostui kymmenestä artikkelista. Tutkimuksen tarkoituksena ei ollut kattaa koko aihepiiriä koskevaa tutkimusta. Tämän seurauksena jotkut näkökulmat ovat saattaneet jäädä tutkimuksen ulkopuolelle. Kyberresilienssi on nopeasti kehittyvä ala. Tämän seurauksena osa tulokista voi vanhetua nopeasti kun teknologia muuttuu.

Aihe on suhteellisen uusi ja jatkuvasti kehittyvä tutkimusalue. Tutkimukset voi siis muuttua nopeastikin teknologian kehittyessä. Voidaan siis todeta, että tietojärjestelmien merkityksen kasvaessa myös niiden rooli liiketoiminnan jatkuvuuden turvaamisessa korostuu. Tietojärjestelmien suunnitelmallinen integrointi osaksi jatkuvuussuunnittelua on siten keskeinen edellytys organisaatioiden toimintakyvyn ja kilpailukyvyn säilymiselle muuttuvassa digitaalisessa toimintaympäristössä.

Jatkotutkimuksissa voisi vertaille eri toimialoja ja eri kokoisia organisaatioita keskenään. Cedergrenin ja Hasselin (2025, s. 2) tutkimuksen avulla voidaan huomata, että julkisen- ja yksityisen sektorin välillä on eroja jatkuvuudenhallinnan tasossa ja sen osaamisessa. Jatkotutkimuksissa voitaisiin myös tutkia miten organisaatioiden kyberresilienssi ja jatkuvuussuunnittelu kehittyvät häiriötilanteiden myötä ja kun aikaa kuluu. Se auttaisi ymmärtämään paremmin, onko kyberresilienssi oppimiseen perustuva, joka kehittyy jatkuvasti vai onko se enemmän pysyvä tila, joka vain reagoi häiriötilanteisiin.

Jatkotutkimuksissa olisi myös hyödyllistä tarkastella käytännön esimerkkejä, miten organisaatiot ovat onnistuneet yhdistämään kyberresilienssin ja jatkuvuussuunnittelun osaksi päivittäistä toimintaansa sekä millaisia vaikutuksia tällä yhdistämisellä on ollut niiden toimintakykyyn kesken häiriötilanteiden. Erilaiset tapauskohtaiset- ja laadulliset tutkimukset antaisivat tutkielman teoreettiseen viitekehykseen käytännön syvyyttä ja mahdollistaisivat laajempaa kriittistä arviointia. Esim. toteutuvatko katsauksessa

tunnistetut menestystekijät, IT-johdon ja liiketoimintajohdon yhteistyö, henkilöstön koulutus sekä ennakoidun improvisaation ja muodollisen suunnittelun tasapaino aidoissakin kriisitilanteissa.

Lähteet

Awang Ali, Q. S., Hanafiah, M. H., & Mogindol, S. H. (2023). Systematic literature review of Business Continuity Management (BCM) practices: Integrating organisational resilience and performance in Small and medium enterprises (SMEs) BCM framework. *International journal of disaster risk reduction,* 99, 104135. https://doi.org/10.1016/j.ijdrr.2023.104135

Bagheri, S., Ridley, G. & Williams, B. (2023), Organizational Cyber Resilience, Management perspectives. *Australasian journal of information systems.* 27, 10.3127/ajis.v27i0.4183

Berkeley School. (2022), What is an information system? Noudettu 13.1.2026. osoitteesta https://ischoolonline.berkeley.edu/blog/what-is-information-systems/

Blades & Doughty, K. (2000), *Business continuity planning: Protecting your organization's Life*, Auerbach publishers, Incorporated. Noudettu 15.6.2026 osoitteesta https://tritonia.finna.fi/Record/nelli07.1000000000020615?sid=5373267412

Cedergren, A. & Hassel, H. (2020). Business continuity management in public sector organizations: Development, challenges, and ways forward. *Journal of contingencies and crisis management ,*33*,* 06329, https://doi.org/10.1111/1468-5973.70055

Chakraborty, D. & Biswas, W. (2019). Evaluating the impact of human resource planning programs in addressing the strategic goal of the firm an organizational perspective. *Journal of advances in management research.* 16, https://doi.org/10.1108/JAMR-01-2019-0007

Elliot, D., Herbane, B. & Swartz, E. (2010), *Business continuity management, second edition, a crisis management approach.* Taylor & Francis group

Euroopan keskuspankki. (2026), *Cyber Resilience.* Noudettu 9.1.2026. osoitteesta https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html

European comission, (2026) *Cyber resilience act*, Noudettu 31.5.2026 osoitteesta https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

Groenendaal, J. & Helsloot, I. (2020), Organisational resilience: Shifting from planning-driven business continuity management to anticipated improvisation. *Journal of business continuity & emergency* planning. 14, https://doi.org/10.69554/SEYT2614

Hausken, K. (2020), Cyber resilience in firms, organizations and societis. *Internet of things.* 11, 100204. https://doi.org/10.1016/j.iot.2020.100204

Iivari, M., & Laaksonen, M. (2009). *Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen*. Tietosanoma.

Jennings, M. (2026), ISO 22301 – The business continuity management standard, simplified. Noudettu 22.1.2026. osoitteesta https://www.isms.online/iso-22301/#what-is-iso-22301-and-why-do-you-need-it

Joinson, A. (2023). Development of a new 'human cyber-resilience scale', *Journal of cybersecurity.* 9. https://doi.org/10.1093/cybsec/tyad007

Kweon, E., Lee, H., Chai, S. & Yoo, K. (2019). The Utility Information Security Training and Education on cybersecurity Incidents: An empirical evidence. *Information Systems Frontiers.* 23, 361–373 https://doi.org/10.1007/s10796-019-09977-z

Lipponen, K. (2020). *Resilienssi arjessa.* Duodecim

OpenAI. (2025). *ChatGPT* (12.12.2025) [ChatGPT-5.1 & ChatGPT-5.6. Noudettu 10.8.2026. osoitteesta https://chat.openai.com/chat

Petrenko, S. (2019). *Cyber Resilience*. River publisher. Noudettu 12.1.2026. osoitteesta https://tritonia.finna.fi/Record/nelli07.4100000009669757?sid=5224349801&imgid=1

Plevnik, M. (2026). Communication and information systems user support as a governance mechanism in a high-security public organization. *Multidisciplinary digital publishing institute*. 14, 20798954. https://doi.org/10.3390/systems14030288

Poijula, S. (2018). *Resilienssi, Muutosten kohtaamisen taito.* Kirjapaja

Saeed, S., Altamimi, S., Alkayyal, N., Alshehri, E. & Alabbad, D. (2023). Digital transformation and cybersecurity challenges for business resilience: Issues and

recommendations. *Multidisciplinary digital publishing institute,* 23, 6666. https://doi.org/10.3390/s23156666

Salminen, A. (2023). *Mikä kirjallisuuskatsaus?* Noudettu 5.6.2026. osoitteesta https://osuva.uwasa.fi/server/api/core/bitstreams/12594b89-5f96-4a7d-932f-04215239659f/content

Siirtola, S. (2024). Hyvä johtaminen on avain resilientille kulttuurille kyberuhkien aikana. Noudettu 31.5.2026. osoitteesta https://tekir.fi/ajankohtaista/hyva-johtaminen-on-avain-resilientille-kulttuurille-kyberuhkien-aikana/

Steen R., Haug J. & Patriarca R. (2023). Business continuity and resilience management: A conceptual framework. *Journal of contingencies and crisis management*, https://doi.org/10.1111/1468-5973.12501

Tsen, E., K L Ko, R. & Slapnicar, S. (2023). The effect of organizational cyber resilience on cyber incident outcomes. *Journal of cybersecurity*, 11. https://doi.org/10.1093/cybsec/tyaf040

Valtion kyberturvallisuusjohtajan toimisto, Liikenne- ja viestintäministeriö. (2026). Kyberturvallisuussanasto. Noudettu 29.6.2026. osoitteesta https://valtioneuvosto.fi/-/1410829/paivitetty-kyberturvallisuussanasto-selkeyttamaan-kyberturvallisuustermien-kayttoa

Valtiovarainministeriö, (2016). VAHTI 2/2016, Toiminnan jatkuvuuden hallinta, Noudettu 12.1.2026. osoitteesta https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/f17b8657-f234-4fca-9f80-14c4462eb326/content

Liitteet

Liite 1. Tekoälyn käytön raportointilomake

Tekoälyn käyttö kandidaatin tutkielmassa.

Kandidaatin tutkielmassa on käytetty tekoälysovelluksia:
Kyllä

Ilmoitukseni mukaan olen käyttänyt kandidaatin tutkielmaprosessin aikana seuraavia tekoälysovelluksia:
Tekoälysovellusten nimet ja versiot: ChatGPT-5.1, ChatGPT-5.6.

Käyttötarkoitus:
Käytin ChatGPT-5.1 työn alkuvaiheessa ideointiin ja aiheen tarkempaan rajaamiseen.
Työn lopussa käytin ChatGPT-5.6 työn tarkistamiseen kirjoitusvirheiden osalta.

Osoiot, joissa tekoälyä on käytetty:
Olen tarkistanut koko työn kirjoitusvirheiden osalta ChatGPT-5.6 avulla.

Olen tietoinen siitä, että olen täysin vastuussa koko kandidaatin tutkielman sisällöstä, mukaan lukien osat, joissa on hyödynnetty tekoälyä, ja hyväksyn vastuun mahdollisista eettisten ohjeiden rikkomuksista.