Tampereen yliopisto

Siiri Piekkala

TIETOJÄRJESTELMÄRISKIT PERINTEISISSÄ JA SAAS-TIETOJÄRJESTELMISSÄ

Kandidaatintyö
Johtamisen ja talouden tiedekunta
Tarkastaja: Jussi Myllärinemi
12/2024

TIIVISTELMÄ

Siiri Piekkala: Tietojärjestelmäriskit perinteisissä ja SaaS-tietojärjestelmissä
Kandidaatintyö
Tampereen yliopisto
Tietojohtamisen tutkinto-ohjelma
Joulukuu 2024

Pilvipohjaiset tietojärjestelmät ovat yleistyneet nopeasti niiden tarjoamien hyötyjen ansiosta, ja yhä useampi organisaatio siirtää työkuormaansa pilveen. Pilvipohjaiset tietojärjestelmät tuovat kuitenkin mukanaan uusia riskejä, joiden tunnistaminen ja vertaaminen muihin vaihtoehtoihin on tärkeää ennen pilveen siirtymistä. Pilvipohjaiset tietojärjestelmät aiheuttavat esimerkiksi tiedon sijaintiin ja erillään pitoon liittyviä riskejä, minkä lisäksi pilvipohjaisten järjestelmien hyödyntämä jaettu teknologia voi altistaa järjestelmän hyökkäyksille. Tämän tutkimuksen tavoitteena on tunnistaa sekä perinteisten tietojärjestelmien että SaaS (Software as a Service) -tietojärjestelmien riskejä sekä tarkastella, miten näiden kahden järjestelmätyypin riskit eroavat toisistaan. Tutkimus keskittyy erityisesti tietojärjestelmän elinkaaren toimintavaiheeseen, sillä silloin tietojärjestelmä toteuttaa perimmäistä tarkoitustaan, eli tiedon keräämistä, käsittelyä, säilyttämistä ja jakamista organisaation toiminnan tehostamiseksi. Tutkimuksessa luokitellaan kirjallisuudesta löytyviä tietojärjestelmäriskejä eri riskikategorioihin ja vertaillaan näitä kategorioita järjestelmätyyppien välillä.

Tutkimus toteutettiin kirjallisuuskatsauksena, ja aineistona käytettiin artikkeleita, konferenssijulkaisuja ja raportteja, joista suurin osa oli vertaisarvioituja. Aineistoa haettiin kahdesta tietokannasta, ja hakutuloksia rajattiin muun muassa julkaisuvuoden ja -kielen perusteella. Lopulliset aineistot valittiin sen perusteella, vastaavatko tutkimuksen aiheeseen sekä vähintään yhteen alatutkimuskysymykseen.

Tulokset osoittavat, että SaaS-järjestelmiin liittyviä riskejä on tutkittu huomattavasti enemmän kuin perinteisiin tietojärjestelmiin liittyviä riskejä. Perinteisissä tietojärjestelmissä korostuvat sisäisistä tekijöistä aiheutuvat riskit, kun taas SaaS-järjestelmissä ulkoisista tekijöistä aiheutuvat riskit ovat merkittävämpiä. Teknologiariskit ovat keskeisempiä perinteisissä järjestelmissä, kun taas tietoon liittyvät riskit, liiketoimintaprosessiriskit ja tietoturvariskit korostuvat SaaS-järjestelmissä. Lisäksi SaaS-järjestelmissä suuri osa riskeistä kuuluu palveluntarjoajan vastuulle, mikä rajoittaa organisaation omia riskienhallintamahdollisuuksia. Tutkimus osoittaa, että kumpikin tietojärjestelmätyyppi tuo oman näkökulman riskienhallintaan. SaaS-järjestelmien käyttö edellyttää huolellista toimittajavalintaa ja luotettavaa palveluntarjoajaa, kun taas perinteisten järjestelmien käyttö edellyttää erityisesti toimivia sisäisiä riskienhallinnan prosesseja.

Avainsanat: pilvipohjainen tietojärjestelmä, SaaS-tietojärjestelmä, perinteinen tietojärjestelmä, tietojärjestelmäriskit, riskien vertailu

ABSTRACT

Siiri Piekkala: Information system risks in traditional and SaaS information systems
Bachelor's thesis
Tampere University
Degree Programme of Information and Knowledge Management
December 2024

Cloud-based information systems have rapidly gained popularity due to their advantages, prompting an increasing number of organizations to migrate workloads to the cloud. However, these systems also introduce new risks that must be identified and compared to alternative solutions before adoption. For instance, cloud-based systems pose risks related to data location and segregation, and the shared technology they utilize can expose systems to attacks. This study aims to identify the risks associated with both traditional information systems and SaaS (Software as a Service) systems, focusing on how the risks of these two system types differ. The research emphasizes the operational phase of the information system lifecycle and examines risks from the end-user's perspective. Risks identified in the literature are categorized and compared across the two system types.

The study was conducted as a literature review using articles, conference proceedings, and reports, most of which were peer-reviewed. Data were sourced from two databases, with results filtered based on publication year and language. The final materials were selected based on their relevance to the research topic and alignment with at least one sub-research question.

The findings indicate that risks related to SaaS systems have been studied significantly more than those of traditional systems. Traditional systems are primarily associated with internal risks, whereas SaaS systems are more exposed to external factors. Technological risks are more critical for traditional systems, while SaaS systems are dominated by data-related risks, business process risks, and cybersecurity risks. Additionally, many risks in SaaS systems fall under the responsibility of the service provider, limiting the organization's ability to manage these risks directly. The study highlights that both system types present unique perspectives on risk management. SaaS systems require careful vendor selection and a reliable service provider, whereas traditional systems demand robust internal risk management processes.

Keywords: cloud-based information system, SaaS information system, on-premises information system, information system risks, risk comparison

TEKOÄLYN KÄYTTÖ OPINNÄYTTEESSÄ

Opinnäytteessäni on käytetty tekoälysovelluksia:

☒ Ei
☐ Kyllä

Ilmoitukseni mukaan olen käyttänyt opinnäytteessäni tutkielmaprosessin aikana seuraavia tekoälysovelluksia:

Tekoälysovellusten nimet ja versiot:

Käyttötarkoitus:

Osiot, joissa tekoälyä on käytetty:

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

ALKUSANAT

Tämän kandidaatintyön tekeminen on ollut itselleni mieluinen prosessi, sillä olen päässyt perehtymään itseäni kiinnostavaan aiheeseen ja etenkin oppimaan uutta. Halusin liittää kandidaatintyöni jollain tavalla tietojärjestelmätutkimukseen, sillä olen ollut opintojeni aikana aiheesta hyvin kiinnostunut. Tietojärjestelmien riskit valikoituivat aiheekseni erityisesti kesätöiden kautta, jossa aihe oli paljon esillä. Haluan kiittää kandidaatintyön ohjaajaani Jussi Myllärniemeä avusta näkökulmien löytämisessä ja pohdinnassa sekä tuesta kirjoitustyön aikana.

Tampereella, 10.12.2024

Siiri Piekkala

SISÄLLYSLUETTELO

1. JOHDANTO

Pilvipalvelulla tarkoitetaan ohjelmaa tai järjestelmää, jossa tietoteknisiä palveluita, kuten tietokoneita, ohjelmia ja tallennustilaa käytetään verkon kautta (Sanastokeskus ry 2023). Pilvipohjaisella tietojärjestelmällä tarkoitetaan tietojärjestelmää, joka on toteutettu pilvipalveluna, eli järjestelmä hyödyntää ulkoista tallennustilaa ja laitteistokomponentteja. Pilviteknologiaan perustuvat tietojärjestelmät ovat yleistyneet IT-alalla nopeasti tuomalla uusia mahdollisuuksia niiden hyödyntäjille. Pilviympäristö mahdollistaa esimerkiksi tietojärjestelmän käytön verkon yli sijainnista riippumatta, resurssien keräämisen ja jakamisen laajassa verkostossa sekä nopeaa joustavuutta järjestelmän muokkaamiseen (Kofahi & Al-Rabadi 2018). Lisäksi pilvipohjainen tietojärjestelmä tarjoaa vaihtoehdon organisaation sisäiselle tietohallinnolle, sillä organisaatio pystyy käyttämään palveluntarjoajan infrastruktuuria, ohjelmistoresursseja sekä laitteistokomponentteja verkon yli (Henry & Ali 2017). Tällöin organisaation ei tarvitse omistaa tai hallinnoida näitä resursseja itse.

Pilvipohjaisten tietojärjestelmien edut ajavat organisaatioita siirtymään perinteisistä tietojärjestelmistä pilvipohjaisiin versioihin. Pericherlan (2023) mukaan organisaatiot ovat pilviteknologian kehittämisen jälkeen vähitellen siirtäneet työkuormitustansa pilveen säästääkseen omia resurssejaan. Pilviteknologia tuo kuitenkin mukanaan myös merkittävän määrän riskejä, kuten tiedon turvallisuuteen ja luotettavuuteen, tiedon sijaintiin, tiedon erillään pitämiseen sekä verkon turvallisuuteen liittyviä riskejä (Subashini & Kavitha 2011). Lisäksi pilvipohjaisten järjestelmien hyödyntämä jaettu teknologia altistaa pilvipohjaisia tietojärjestelmiä erilaisille hyökkäyksille ja tietovarkauksille (Chavan et al. 2022). Riskit, niiden tunnistaminen ja niiden hallinta ovat toistuva teema pilvipalveluita ja pilvipohjaisia tietojärjestelmiä koskevassa kirjallisuudessa, ja erityisesti tietoon ja sen turvallisuuteen liittyviä riskejä pohditaan kirjallisuudessa paljon (esim. Subashini & Kavitha 2011; Henry & Ali 2017; Kofahi & Al-Rabadi 2018). Organisaatiossa, jossa pohditaan pilveen siirtymistä, tulee punnita pilviteknologian tuomia hyötyjä ja sen aiheuttamia riskejä.

Tämän tutkimuksen tarkoituksena on tunnistaa ja vertailla riskejä perinteisissä eli organisaation sisäisissä tietojärjestelmissä ja pilviteknologiaan perustuvissa SaaS-tietojärjestelmissä. Tutkimuksen merkitystä voidaan perustella sillä, että organisaatioilla on motivaatio siirtyä perinteisestä tietojärjestelmästä pilvipohjaiseen versioon, mutta

ennen siirtymää tulisi punnita riskejä eri vaihtoehdoissa. Riskien vertailu perinteisten ja pilvipohjaisten tietojärjestelmien välillä on erityisen tarpeellista siksi, että kirjallisuuden mukaan pilviteknologia tuo mukanaan merkittävän määrän uusia riskejä. Lisäksi tutkimuksen merkitystä voidaan perustella sillä, että vaikka tutkimusta pilvipalveluiden riskeistä on olemassa paljon, niin vertailevaa tutkimusta perinteisen ja pilvipohjaisen tietojärjestelmien riskien välillä on melko vähän. Tässä tutkimuksessa tehtävä perinteisten ja pilvipohjaisten tietojärjestelmien riskien vertailu auttaa luomaan näkemyksen siitä, miten riskit eroavat perinteisen ja pilvipohjaisen tietojärjestelmän välillä. Tätä tietoa organisaatioiden on mahdollista hyödyntää päätöksenteossa, kun pohditaan tietojärjestelmän siirtämistä pilveen tai esimerkiksi tietojärjestelmän riskienhallinnan strategiaa.

1.1 Tutkimuksen keskeiset käsitteet ja näkökulman rajaus

Tietojärjestelmän käsite on laaja. Tietojärjestelmällä tarkoitetaan tiedoista ja tietoja käsittelevistä ihmisistä, tietojenkäsittelylaitteista, tiedonsiirtolaitteista, tietoja käsittelevistä ohjelmista ja tietojen käsittelysäännöistä koostuvaa järjestelmää, jonka tarkoitus on mahdollistaa jokin toiminta tai tehostaa ja helpottaa sitä (Finto 2024). Yhdysvaltain kauppaministeriön alainen instituutti *National Institute of Standards and Technology* NIST (2024a) määrittelee tietojärjestelmän erilliseksi tietoresurssien joukoksi, jonka tarkoituksena on kerätä, käsitellä, ylläpitää, käyttää ja jakaa tietoa. Myös Alter (2001) kuvaa tietojärjestelmiä itsenäisinä järjestelminä, jotka koostuvat ihmisistä ja koneista, ja jotka käyttävät tietoa, teknologiaa ja muita resursseja tuottaakseen palveluita sisäisille tai ulkoisille asiakkaille. Awatin (2024) mukaan tietojärjestelmän ydin koostuu laitteista, ohjelmista, tiedosta, ihmisistä ja prosesseista, jotka yhdessä luovat raakadatasta hyödyllistä tietoa. Tietojärjestelmä on siis erillinen kokonaisuus, joka koostuu muun muassa tiedosta, laitteistoista, ohjelmistoista, ihmisistä ja prosesseista. Tietojärjestelmä tarjoaa sen käyttäjälle palvelua, jonka tarkoituksena tehostaa organisaation toimintaa keräämällä, käsittelemällä, säilyttämällä ja jakamalla tietoa sekä luomalla näin myös uutta organisaatiolle hyödyllistä tietoa. Tässä työssä tietojärjestelmällä tarkoitetaan kaikkia järjestelmiä, jotka toteuttavat edellä esitetyn määritelmän vaatimukset. Tietojärjestelmä voi olla esimerkiksi organisaation asiakastietojärjestelmä tai toiminnanohjausjärjestelmä tai se voi olla organisaation sisäinen viestintäjärjestelmä, kuten Microsoft 365.

Perinteisellä tietojärjestelmällä tarkoitetaan tietojärjestelmää, jonka laitteisto- ja ohjelmistokomponentit ovat käyttäjäorganisaation omistuksessa ja kaikki tietojärjestelmän osa-alueet ovat käyttäjäorganisaation vastuulla. Perinteisestä

tietojärjestelmästä voidaan käyttää myös ilmausta paikallinen tietojärjestelmä. Pilvipohjainen tietojärjestelmä on nimensä mukaisesti pilviteknologian avulla toteutettu tietojärjestelmä. Se on siis laitteistosta, ohjelmistoista, tiedosta, ihmisistä ja prosesseista muodostuva erillinen kokonaisuus, jossa IT-infrastruktuuria eli laitteistoa ja ohjelmistoja hyödynnetään verkon yli. Pilvipohjaisissa tietojärjestelmissä tietojärjestelmän osa-alueet eivät ole yksin järjestelmää käyttävän tahon hallinnassa, vaan ne on jaettu tietojärjestelmää ylläpitävän tahon eli palveluntarjoajan kanssa. Pilvipalveluilla on erilaisia palvelumalleja. SaaS (*engl. Software as a Service*) viittaa palvelumuotoon, jossa käyttäjä hyödyntää palveluntarjoajan sovelluksia pilvi-infrastruktuurin kautta (Henry & Ali 2017). PaaS (*engl. Platform as a Service*) puolestaan antaa asiakkaalle mahdollisuuden hallita ja suojata omia sovelluksiaan palveluntarjoajan hallinnoidessa infrastruktuuria. IaaS (*engl. Infrastructure as a Service*) tarjoaa asiakkaalle vapauden rakentaa oman järjestelmän palveluntarjoajan antamien komponenttien avulla. (Henry & Ali 2017; Kofahi & Al-Rabadi 2018) SaaS-palvelumalli rakentuu muiden palvelumallien päälle (Henry & Ali 2017) ja se onkin yleisin käytetty palvelumalli (Itewiki.fi 2024). Kandidaatintyön laajuuden takia tarkastelun rajaaminen vain yhteen palvelumalliin on tarpeellista, ja aiheen rajaaminen palvelumalleista yleisimpään, eli SaaS-palvelumalliin, tulee luonnollisesti. Lisäksi SaaS-palvelumalli on hyvin toimittajariippuvainen, mikä tuo mielenkiintoisen näkökulman riskien tarkasteluun.

Tietojärjestelmä käy läpi vaiheita, joista käytetään nimitystä tietojärjestelmän elinkaari. Tietojärjestelmän elinkaaren vaiheet voidaan jakaa aloittamis-, kehittämis-, toiminta- ja lopetusvaiheeseen. (NIST 2024b) Tietojärjestelmäkehityksen näkökulmasta elinkaaren vaiheet voivat olla esimerkiksi suunnittelu, analyysi, muotoilu ja ylläpito (Nayan & Zaman 2009). Alter (2001) puolestaan esittää, että työ-ja tietojärjestelmien elinkaaren vaiheisiin kuuluvat aloitus-, kehitys-, implementointi- sekä toiminta- ja ylläpitovaihe. Vaiheet eroavat toisistaan hieman eri määritelmissä, mutta kaikista määritelmistä on tunnistettavissa tietojärjestelmän käytön vaihe eli toiminta- tai ylläpitovaihe. Riskien tunnistaminen ja hallinta on tärkeä osa kaikkia tietojärjestelmän elinkaaren vaiheita (GeeksForGeeks 2023), mutta tässä tutkimuksessa keskitytään erityisesti tietojärjestelmän toimintavaiheeseen, sillä silloin tietojärjestelmä toteuttaa perimmäistä tarkoitustaan eli organisaation toiminnan tehostamista. Tietojärjestelmän toimintavaiheessa tietojärjestelmä tukee aktiivisesti käyttäjäorganisaation toimintaa keräämällä, käsittelemällä, säilyttämällä ja jakamalla tietoa.

Tietojärjestelmän toimintavaihe on erityisen tärkeä tietojärjestelmää hyödyntävälle taholle, minkä takia tutkimus toteutetaan tietojärjestelmän käyttäjän näkökulmasta. Tietojärjestelmän käyttäjäksi voidaan määritellä esimerkiksi henkilö, organisaatio tai muu

taho, joka pyytää pääsyä järjestelmän resursseihin ja käyttää niitä (NIST 2024c). Tässä tutkimuksessa tietojärjestelmän käyttäjällä tarkoitetaan organisaatiota, joka hyödyntää tietojärjestelmää toimintansa tehostamiseksi. Tietojärjestelmiin liittyy käyttäjän lisäksi kuitenkin muita sidosryhmiä, kuten palveluntarjoaja (engl. *Service provider*), joiden näkökulma jätetään tutkimuksen ulkopuolelle. Palveluntarjoajalla tarkoitetaan yleensä kaupallista organisaatiota, joka tarjoaa perus- tai lisäarvopalveluja jonkin verkoston toimintaa varten (NIST 2024d). Tietojärjestelmien kontekstissa palveluntarjoaja on organisaatio, joka tarjoaa palveluja tietojärjestelmän toimintaa varten. SaaS-tietojärjestelmien kohdalla palveluntarjoajalla tarkoitetaan organisaatiota, joka vastaa tietojärjestelmästä ja myy sitä palvelunaan. Palveluntarjoajan näkökulmasta tietojärjestelmän elinkaaren käyttövaihe näyttäytyy esimerkiksi järjestelmän ylläpitovaiheena.

1.2 Tutkimusongelma ja tutkimuksen tavoitteet

Tutkimusongelmaa ja tutkimuksen lähtökohtia alustetaan edellisissä luvuissa. Tutkimusongelmana on, että yhä yleistyvät SaaS-tietojärjestelmät tuovat esiin uusia riskejä, joita täytyy tunnistaa. Tässä tutkimuksessa tunnistetaan kirjallisuudessa esiintyviä riskejä SaaS-tietojärjestelmille sekä perinteisille tietojärjestelmille ja verrataan löydöksiä keskenään.

Tutkimuksen päätutkimuskysymys on seuraava: miten SaaS-tietojärjestelmien riskit eroavat perinteisten tietojärjestelmien riskeistä?

Tutkimuksen alatutkimuskysymykset ovat seuraavat:

- Mitä riskejä liittyy perinteisiin tietojärjestelmiin ja millaisia ne ovat?
- Mitä riskejä liittyy SaaS-tietojärjestelmiin ja millaisia ne ovat?
- Mitä ja millaisia riskejä esiintyy eniten kummassakin tutkittavassa tietojärjestelmätyypissä?
- Millaiset riskit korostuvat tutkittavissa tietojärjestelmätyypeissä?

Tutkimuksen tavoitteena on tunnistaa ja analysoida sekä perinteisten tietojärjestelmien että SaaS-tietojärjestelmien toimintavaiheeseen liittyviä riskejä. Tutkimuksen tavoitteena on, että lopputuloksena syntyy näkemys siitä, miten nämä tutkittavat tietojärjestelmätyypit eroavat toisistaan riskien näkökulmasta. Tutkimuksen tulokset voivat antaa pilvisiirtymää tai tietojärjestelmän riskienhallinnan strategioita pohtivalle organisaatiolle päätöksentekoa tukevaa tietoa siitä, miten tietojärjestelmän

toimintavaiheen riskit eroavat eri tietojärjestelmätyypeillä ja mitä tekijöitä tulee ottaa riskien osalta huomioon kummankin tietojärjestelmätyypin käytössä.

1.3 Työn rakenne

Tämä kandidaatintyö koostuu viidestä luvusta, joiden sisältö esitellään seuraavaksi. Ensimmäisessä luvussa esitellään tutkimuksen tausta ja lähtökohdat, tutkimuksen keskeiset käsitteet ja näkökulman rajaus sekä tutkimusongelma ja tutkimuksen tavoitteet. Johdantoluku muodostaa perustan koko tutkimukselle. Toisessa luvussa esitellään tutkimusmenetelmä vaiheittain. Luvussa 2 esitellään tutkimuksessa käytetyn aineiston hakulausekkeet, niiden muodostus sekä aineiston valinta- ja poissulkukriteerit.

Kolmas luku käsittelee tietojärjestelmäriskien luokittelua. Luvussa määritellään tietojärjestelmäriskien luokitteluun viitekehys, jonka avulla aineistoa analysoidaan tutkimuksessa. Aineiston analyysi viitekehyksen avulla esitetään luvussa 4, joka käsittelee tietojärjestelmäriskien tunnistamista kirjallisuudesta. Luvussa 4 esitellään ensin kirjallisuudesta löydettyjä riskejä perinteisille tietojärjestelmille ja SaaS-tietojärjestelmille, minkä jälkeen riskejä vertaillaan ja pohditaan, miten ne korostuvat eri tietojärjestelmätyypeissä. Luvussa 5 tehdään yhteenveto luvussa 4 esitetyn aineiston analyysin pohjalta ja vastataan tutkimuskysymyksiin. Lisäksi luvussa 5 arvioidaan tutkimusta ja esitetään jatkotutkimusehdotukset.

2. TUTKIMUSMENETELMÄ

Tutkimus toteutetaan systemaattisena kirjallisuuskatsauksena Finkin (2014) seitsenvaiheiseen kirjallisuuskatsauksen prosessiin perustuen. Kirjallisuuskatsauksen keskeisenä tavoitteena on määrittää, mitä riskejä kirjallisuudesta löytyy SaaS-tietojärjestelmille sekä perinteisille tietojärjestelmille. Tutkimusmenetelmäksi on valittu juuri systemaattinen kirjallisuuskatsaus, jotta riskien tunnistaminen kirjallisuuden pohjalta olisi mahdollisimman johdonmukaista ja yhdenvertaista kummallekin käsiteltävälle tietojärjestelmätyypille.

Fink (2014) esittelee systemaattisen kirjallisuuskatsauksen prosessin vaiheet seuraavasti:

1. Määritetään tutkimusaihe sekä keskeinen tutkimuskysymys ja siitä johdetut alatutkimuskysymykset.

2. Valitaan tiedonhakuun sopivat tietokannat.

3. Valitaan tiedonhaussa käytettävät hakutermit.

4. Tehdään hakutulosten käytännön seulominen.

5. Tehdään hakutulosten metodologinen seulominen.

6. Perehdytään löydettyyn aineistoon.

7. Luodaan synteesi.

Tässä luvussa esitellään tutkimuksen toteuttaminen Finkin (2014) prosessin avulla edeten prosessin mukaisessa järjestyksessä.

Kirjallisuuskatsaus aloitetaan määrittelemällä tutkimuksen aihe, tutkimusongelma sekä tutkimuskysymykset, jotka esitellään johdantoluvussa (ks. luku 1). Tämän jälkeen valitaan sopivat tietokannat tiedonhakua varten. Tietokannoiksi on valittu Tampereen Yliopiston tietokanta Andor sekä yleinen tieteellisen kirjallisuuden tietokanta Google Scholar, joka sisältää suuren määrän erilaista aineistoa. Näiden kahden tietokannan yhdistelmällä saadaan haettua aineistoa kandityötä varten riittävän kattavasti, sillä yhteensä nämä tietokannat sisältävät kattavasti erilaista aineistoa, eikä muista tietokannoista, kuten Scopuksesta tai IEEE Xploresta, löytynyt ensimmäisten hakujen perusteella aineistoa, jota kaksi valittua tietokantaa eivät olisi jo sisältäneet.

Tiedonhaku aloitetaan määrittelemällä hakulausekkeita tutkimusaiheen avainsanojen perusteella. Tutkimuksen aiheesta kertovassa kirjallisuudessa esiintyvät usein muun muassa avainsanat ”information system”, ”information system risk”, ”cloud computing”, ”cloud computing threats” sekä ”on-premises computing”, joiden pohjalta muodostetaan ensimmäiset hakulausekkeet. Avainsanoja on kartoitettu perinteisiä tietojärjestelmiä, pilvipohjaisia tietojärjestelmiä, sekä tietojärjestelmien riskejä käsittelevän kirjallisuuden pohjalta. Aikaisemmasta kirjallisuudesta löydettyjä avainsanoja hyödyntämällä pyritään saamaan hakulausekkeisiin tutkimuksen aiheen keskeiset termit, jotta tutkimuksen aiheen kannalta keskeinen aineisto saataisiin kirjallisuuskatsauksessa käsiteltyä mahdollisimman hyvin. Hakulausekkeiden muotoilussa käytettiin apuna avainsanojen lisäksi niiden synonyymejä sekä johdantoluvussa esiteltyjä alatutkimuskysymyksiä. Hakulausekkeet muodostettiin sen pohjalta, että tarkoituksena on ensin kartoittaa yleisesti tietojärjestelmiin liittyviä riskejä, minkä jälkeen tarkemmin perinteisiin tietojärjestelmiin sekä pilvipohjaisiin tietojärjestelmiin liittyviä riskejä. Hakuja tehtiin useilla eri hakulausekkeilla ja hakulausekkeiden versioilla, jotta pystyttiin valitsemaan ne, jotka tuottavat osuvimmat tulokset.

Tutkimus aloitettiin tekemällä laajoja hakuja esimerkiksi hakulausekkeilla ”Information system” AND risk tai ”Cloud computing” AND risk, jotka tuottivat kymmeniätuhansia hakutuloksia. Suurin osa näistä hakutuloksista osoittautui kuitenkin tutkimuksen aiheen kannalta epärelevanteiksi, sillä ne eivät käsitelleet suoraan tietojärjestelmien riskejä. Tämän jälkeen hakulausekkeita muokattiin, jotta hakutuloksia saatiin rajattua ja tarkennettua tämän tutkimuksen kannalta oleellisiin hakutuloksiin. Tarkennusta tehtiin muotoilemalla hakulausekkeita uudestaan, ja esimerkiksi hakulauseke ”Information system” AND risk muokattiin lopulta muotoon ”Information system risks” OR ”Information system threats”. Tämän lisäksi joitakin hakulausekkeita haettiin ainoastaan teosten otsikoista, jotta saataisiin rajattua pois epärelevantit hakutulokset. Kaikille hakulausekkeille otsikosta hakeminen ei kuitenkaan toiminut, sillä se laski hakutulosten määrän nollaan. Lopulliset hakulausekkeet, joita hyödynnettiin kirjallisuuskatsauksessa, on esitetty taulukossa 1.

Taulukko 1. *Lopulliset kirjallisuuskatsauksessa hyödynnetyt hakulausekkeet sekä hakutulosten lukumäärä eri tietokannoissa ilman rajauksia.*

	Mistä haetaan?	Andor	Google Scholar	Yhteensä
”Information system risks” OR ”Information system threats”	Otsikko	136	32	168
”Cloud computing risks” OR ”Cloud computing threats”	Otsikko	124	172	296
"Cloud-based information system” AND (risk OR threat)	Kaikki kentät	1 138	37 400	38 538
”On-premises computing” AND (risk OR threat)	Kaikki kentät	12	321	333
In-house AND ”information system” AND (risk OR threat)	Kaikki kentät	687	80 100	80 787

Kun hakulausekkeet on määritelty, tehdään hakutulosten seulominen. Finkin (2014) mukaan hakutuloksille tehdään ensin käytännön seulominen esimerkiksi julkaisuvuoden ja -kielen perusteella, minkä jälkeen tehdään metodologinen seulominen esimerkiksi teoksen otsikon ja abstraktin avulla. Tässä tutkimuksessa käytännön seulomisen kriteereiksi valittiin, että teos on julkaistu vuosina 2014-2024 ja että se on englanninkielinen. Lisäksi Andorissa hakutulokset rajattiin artikkeleihin, aikakausilehden artikkeleihin, katsausartikkeleihin, kirjan lukuihin ja konferenssijulkaisuihin, sillä muut julkaisutyypit, kuten patentit, tuottivat tutkimuksen kannalta epärelevantteja tuloksia. Julkaisuvuodet 2014-2024 valittiin sillä perusteella, että IT-ala kehittyy nopeasti ja tutkimukseen halutaan mahdollisimman hyvä kuva tietojärjestelmien nykytilanteesta. Hakutuloksia ei kuitenkaan löytynyt niin paljoa, että olisi ollut mielekästä rajata tulokset esimerkiksi vain viimeiseen viiteen vuoteen. Englannin kieli puolestaan valikoitui aineiston valintakriteeriksi siksi, että suomenkielistä tutkimusta aiheesta ei ollut saatavilla.

Metodologinen seulominen toteutettiin lukemalla hakutulosartikkeleiden otsikot ja abstraktit ja päättelemällä, liittyvätkö ne tutkimuksen aiheeseen. Kriteereinä metodologisessa seulomisessa oli, että aineisto sopii tutkimuksen aiheeseen sekä tehtyihin rajauksiin ja että se vastaa ainakin yhteen alatutkimuskysymykseen. Käytännössä tämä tarkoitti sitä, että aineistossa käsiteltiin tietojärjestelmien riskejä tietojärjestelmän elinkaaren toimintavaiheessa ja tietojärjestelmän käyttäjän näkökulmasta. Aineisto sai käsitellä tietojärjestelmien riskejä sekä yleisellä tasolla että keskittyen joko perinteisiin tai pilvipohjaisiin tietojärjestelmiin, mutta aineistosta tuli käydä

selkeästi ilmi, mitä riskejä sen mukaan tietojärjestelmiin kohdistuu. Tämä rajasi pois esimerkiksi paljon riskienhallintaa käsittelevää aineistoa. Lopullisiksi aineistonvalintakriteereiksi muodostuivat:

- Tampereen Yliopiston opiskelijalla on ilmainen pääsy aineistoon ja koko teksti on saatavilla.
- Aineisto on englanninkielinen.
- Aineisto on vuosilta 2014-2024.
- Aineisto kuuluu (Andorissa) artikkeleihin, aikakausilehden artikkeleihin, katsausartikkeleihin, kirjan lukuihin tai konferenssijulkaisuihin.
- Aineisto sopii tutkimuksen aiheeseen sekä tehtyihin rajauksiin.
- Aineisto vastaa vähintään yhteen alatutkimuskysymykseen.

Aineiston poissulkukriteeriksi puolestaan muodostui se, että aineisto ei selkeästi esittele tietojärjestelmiin liittyviä riskejä.

Vaikka useat hakulausekkeet tuottavat taulukon 1 mukaan lukuisia hakutuloksia, lopulliseen kirjallisuuskatsaukseen valikoitui kuitenkin melko vähän aineistoa. Tämä johtuu siitä, että edellä esitetyt aineistonvalintakriteerit täyttävää kirjallisuutta löytyy etenkin perinteisten tietojärjestelmien kohdalla vähän. Esimerkiksi hakulausekkeen ”Information system risks” OR ”information system threats” hakutulosten joukossa on paljon riskienhallinnan prosesseista tai riskien arviointiin hyödynnettävistä tekniikoista kertovaa kirjallisuutta, joka ei suoraan esittele tietojärjestelmiin kohdistuvia riskejä tai vastaa tämän tutkimuksen tutkimuskysymyksiin. Toisaalta esimerkiksi hakulauseke ”Cloud computing risks” OR ”Cloud computing threats” tuottaa tuloksia, joissa esitellään tarkasti jonkun tietyn organisaation pilvisiirtymään liittyviä haasteita ja jotka eivät myöskään suoraan esittele tietojärjestelmiin liittyviä riskejä. Kaikki käytännön seulonnan läpäisseet hakutulokset on kuitenkin käyty yksitellen läpi, minkä takia ei ole todennäköistä, että olennaista tietoa jäisi kirjallisuuskatsauksen ulkopuolelle aineiston suppeudesta huolimatta. Kirjallisuuskatsaukseen valittujen artikkelien lukumäärä hakulausekkeittain eri tietokannoissa esitetään taulukossa 2. Lisäksi tutkimukseen valittu aineisto esitellään liitteessä 1.

Taulukko 2. *Kirjallisuuskatsaukseen valittujen artikkeleiden lukumäärä hakulausekkeittain eri tietokannoissa.*

	Mistä haetaan?	Andor	Google Scholar	Yhteensä
”Information system risks” OR ”Information system threats”	Otsikko	1	0	1
”Cloud computing risks” OR ”Cloud computing threats”	Otsikko	2	3	5
"Cloud-based information system” AND (risk OR threat)	Kaikki kentät	0	1	1
”On-premises computing” AND (risk OR threat)	Kaikki kentät	0	3	3
In-house AND ”information system” AND (risk OR threat)	Kaikki kentät	0	0	0

Kirjallisuuskatsauksen viimeiset vaiheet ovat aineistoon perehtyminen ja synteesi (Fink 2014). Tässä tutkimuksessa aineistoon perehtymisen vaiheessa pyritään tunnistamaan aineistosta perinteisiin tietojärjestelmiin ja SaaS-tietojärjestelmiin kohdistuvia riskejä sekä luokittelemaan niitä ja vertaamaan niitä tietojärjestelmätyyppien välillä. Aineistoa tullaan analysoimaan esimerkiksi luokittelemalla tunnistettuja riskejä kategorioihin viitekehyksen avulla. Riskien luokitteluun käytettävä viitekehys esitellään seuraavassa luvussa, minkä jälkeen tunnistetaan riskejä viitekehyksen avulla kirjallisuuskatsauksen aineiston pohjalta. Synteesin muodostamiseksi kirjallisuudesta tunnistettuja riskejä vertaillaan perinteisten ja SaaS-tietojärjestelmien välillä, ja pohditaan, miten eri riskit korostuvat kummassakin tietojärjestelmätyypissä.

3. TIETOJÄRJESTELMÄRISKIEN LUOKITTELU

Tässä luvussa perehdytään riskin määritelmään sekä siihen, miten tietojärjestelmiin kohdistuvia riskejä voidaan luokitella. Luvussa 3.1 perehdytään ensin kirjallisuudessa esiintyviin määritelmiin riskeistä, minkä jälkeen tutustutaan kirjallisuudessa esitettyihin tapoihin jakaa tietojärjestelmäriskejä kategorioihin. Luvussa 3.2 määritellään kirjallisuuden pohjalta tässä tutkimuksessa hyödynnettävä viitekehys tietojärjestelmäriskien luokitteluun. Tässä luvussa muodostettava viitekehys perustuu kirjallisuuskatsauksen aineistoon, mutta luvussa käytetään apuna myös kirjallisuuskatsauksen ulkopuolisia lähteitä.

3.1 Tietojärjestelmäriskien luokittelu kirjallisuudessa

Riskillä tarkoitetaan muun muassa epävarmuutta ja epäonnistumisen mahdollisuutta tarkasteltaessa jonkin toiminnan seurauksia (Tieteen termipankki 2024). Lisäksi riskillä voidaan tarkoittaa esimerkiksi kielteisiä lopputuloksia ja menetyksiä aiheuttavia tekijöitä (Sherer & Alter 2004). Menetys voi olla taloudellinen, kuten suora rahallinen menetys tai organisaation toiminnan keskeytyminen, tai se voi olla muunlainen menetys, kuten mainehaitta tai henkilön yksityisyyden loukkaaminen. Tietojärjestelmäriski (engl. *Information system risk)* löytyy esimerkiksi joidenkin tietojärjestelmien riskejä käsittelevien artikkelien avainsanoista (esim. Sherer & Alter 2004), mutta se ei esiinny käsitteenä hakemistoissa tai sanakirjoissa, kuten Computer Security Resource Center Glossary, Oxford English Dictionary tai Tieteen Termipankki. Tämän perusteella tietojärjestelmäriskiä voidaan käyttää käsitteenä kuvaamaan tietojärjestelmiin kohdistuvia riskejä, mutta sille ei ole vakiintunutta tai tarkkaa määritelmää. Tässä tutkimuksessa tietojärjestelmäriskillä tarkoitetaan johonkin tietojärjestelmän osa-alueeseen eli laitteistoon, ohjelmistoihin, tietoon, ihmisiin tai prosesseihin kohdistuvaa epävarmuutta tai menetyksiä aiheuttavaa tekijää.

Tietojärjestelmiä koskevassa kirjallisuudessa puhutaan usein riskien lisäksi myös uhista ja haavoittuvuuksista. Uhalla tarkoitetaan mahdollisesti toteutuvaa haitallista tapahtumaa tai kehityskulkua (Valtioneuvosto 2023) ja haavoittuvuudella mitä tahansa heikkoutta, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa (Sanastokeskus ry 2018). Riski ja uhka vastaavat määritelmiltään toisiaan, sillä molemmilla tarkoitetaan mahdollisesti tapahtuvaa epäonnistumista. Haavoittuvuus puolestaan voidaan nähdä riskin tai uhan aiheuttajana. Tutkimuksessa

riskiä ja uhkaa pidetään toisiaan vastaavina käsitteinä ja haavoittuvuuksia riskien ja uhkien aiheuttajina.

Tietojärjestelmien riskejä luokitellaan kirjallisuudessa eri tavoin. Esimerkiksi Sherer ja Alter (2004) esittävät, että riskejä voidaan jakaa kategorioihin erityyppisten kielteisten tulosten perusteella, ja näitä kategorioita voivat olla esimerkiksi projektiriskit, poliittiset riskit tai turvallisuusriskit. Ohjelmisto- ja tietojärjestelmäriskejä käsittelevässä kirjallisuudessa riskejä jaetaan usein karkeasti sisäisiin ja ulkoisiin riskeihin (esim. Hoodat & Rashidi 2009) sekä pienempiin kategorioihin, kuten kustannuksiin, teknologiaan, turvallisuuteen, tietoon, ihmisiin, liiketoimintaprosesseihin ja organisaation menestymiseen liittyviin riskeihin (esim. Smith et al. 2001). Nämä esitetyt luokitteluperusteet ovat melko vanhoja, mutta niitä käytetään edelleen tietojärjestelmätutkimuksessa. Esimerkiksi Whitaker ja Thekdi (2024) hyödyntävät tutkimuksessaan tietojärjestelmäriskien jaotteluun nelikenttää, joka on jaettu sisäisiin ja ulkoisiin riskeihin sekä teknologia- ja liiketoimintariskeihin.

3.2 Tietojärjestelmäriskien luokittelu tässä tutkimuksessa

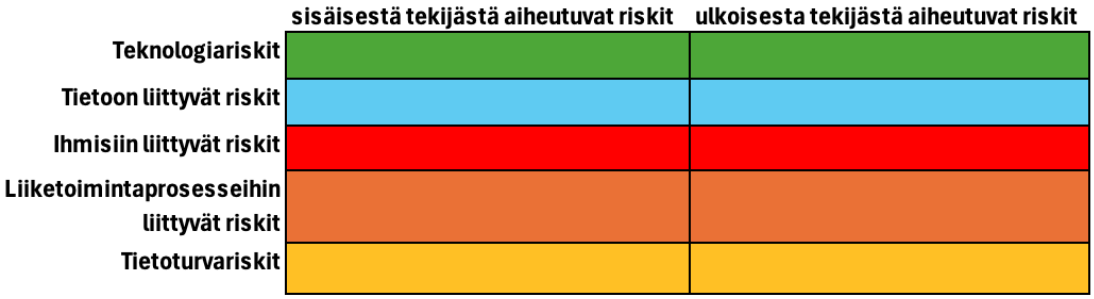
Tietojärjestelmien riskejä voidaan kirjallisuuden perusteella jakaa muun muassa turvallisuuteen, kustannuksiin, teknologiaan, tietoon, ihmisiin, sekä liiketoimintaprosesseihin liittyviin riskeihin. Tässä tutkimuksessa tarkastellaan erityisesti tietojärjestelmän osa-alueisiin ja sen toimintavaiheeseen liittyviä riskejä. Tietojärjestelmä on laitteistosta, ohjelmistoista, tiedosta, ihmisistä ja prosesseista muodostuva itsenäinen kokonaisuus, jolloin teknologiaan, tietoon sekä ihmisiin liittyvät riskikategoriat on aiheellista ottaa tarkasteluun. Tietojärjestelmän tarkoituksena on sen elinkaaren toimintavaiheessa tehostaa organisaation toimintaa, minkä takia myös liiketoimintaprosessiriskit otetaan tarkasteluun. Lisäksi turvallisuusriskit on aiheellista ottaa tarkasteluun, sillä ne esiintyvät tietojärjestelmäriskejä luokittelevassa kirjallisuudessa usein (esim. Smith et al. 2001; Sherer & Alter 2004; Hoodat & Rashidi 2009). Tässä tutkimuksessa tietojärjestelmien riskejä luokitellaan Whitakerin ja Thekdin (2024) nelikenttäluokittelua laajentaen sisäisiin ja ulkoisiin riskeihin sekä teknologiaan, tietoon, ihmisiin, liiketoimintaprosesseihin sekä turvallisuuteen liittyviin riskeihin. Whitakerin ja Thekdin (2024) nelikenttäluokittelua laajennetaan, jotta voidaan huomioida kaikki tietojärjestelmän määritelmässä esiintyvät osa-alueet sekä tietojärjestelmän elinkaaren toimintavaihe. Viitekehyksen riskikategorioiden merkittävyyttä tutkimuksessa perustellaan seuraavaksi.

Teknologiaan, tietoon, ihmisiin ja liiketoimintaprosesseihin liittyvät riskit ovat tutkimuksen kannalta merkittäviä riskikategorioita, sillä ne edustavat tietojärjestelmän eri osa-alueita.

Näitä riskejä voidaan luonnehtia esimerkiksi operatiivisiksi riskeiksi, joilla tarkoitetaan seurausta tapahtumasta, joka häiritsee organisaation toimintaa (Morgan 2024) ja joka aiheutuu riittämättömistä tai toimimattomista sisäisistä prosesseista, järjestelmistä tai ihmisistä (Suomen riskienhallintayhdistys 2024).Tietojärjestelmän tarkoituksena on sen elinkaaren toimintavaiheessa tehostaa organisaation toimintaa keräämällä, käsittelemällä, säilyttämällä ja jakamalla tietoa, jolloin tietojärjestelmän operatiiviseksi riskiksi voidaan luonnehtia epäonnistumisen mahdollisuus, että riittämättömistä sisäisistä prosesseista, järjestelmistä tai ihmisistä aiheutuu haittaa tiedon keräämiselle, käsittelemiselle, säilyttämiselle ja jakamiselle. Operatiivinen riski on kuitenkin käsitteenä laaja ja moniulotteinen, minkä takia riskit jaotellaan tutkimuksessa pienempiin kategorioihin.

Tietojärjestelmistä puhuttaessa turvallisuusriski kohdistuu järjestelmän sisältämään tietoon, minkä takia turvallisuusriskejä voidaan tässä tutkimuksessa nimittää tietoturvariskeiksi. Tietoturvariskit ovat tämän tutkimuksen kannalta olennainen luokitteluperuste, sillä pilviteknologiaa koskevassa kirjallisuudessa tietoturvariskit ovat hyvin usein esillä. Tietoturvallisuuden perustana pidetään tiedon luottamuksellisuutta, eheyttä sekä käytettävyyttä (Nguyen & Khorev 2019) ja tietoturvariskiksi voidaankin määritellä tapahtuma, joka voi johtaa tiedon luottamuksellisuuden, eheyden ja käytettävyyden loukkauksiin (Geric & Hutinski 2007). Lisäksi tietoturvariskiksi voidaan määritellä mahdollisuus, että olemassa olevaa tietotekniikan haavoittuvuutta käytetään luomaan jokin organisaation omaisuuteen kohdistuva uhka, joka aiheuttaa vahinkoa organisaatiolle (Nguyen & Khorev 2019). Tässä tutkimuksessa tietoturvariskiksi määritellään jokin sellainen tapahtuma, joka uhkaa tietojärjestelmän sisältämän tiedon luottamuksellisuutta, eheyttä tai käytettävyyttä tai sellainen tapahtuma, jossa tietojärjestelmän haavoittuvuutta käytetään aiheuttamaan sen sisältämään tietoon kohdistuva uhka.

Kirjallisuuden sekä edellä esitetyn pohdinnan perusteella tässä tutkimuksessa tietojärjestelmiin liittyvät riskit luokitellaan nelikentän avulla laajentaen Whitakerin ja Thekdin (2024) esittelemää viitekehystä. Tässä tutkimuksessa tietojärjestelmäriskit jaetaan sisäisiin ja ulkoisiin riskeihin, sekä teknologiaan, tietoon, ihmisiin, liiketoimintaprosesseihin ja tietoturvaan liittyviin riskeihin kuvan 1 mukaisesti.



Kuva 1. *Tutkimuksessa hyödynnettävä viitekehys tietojärjestelmäriskien luokitteluun (Mukaillen Whitaker & Tehkdi 2024)*

Riskien luokittelu eri kategorioihin ei ole täysin yksikäsitteistä, ja on mahdollista, että yksi riski kuuluu useampaan kategoriaan. Voi myös olla, että kaikkien riskien kohdalla ei ole täysin selvää, aiheutuuko se sisäisestä vai ulkoisesta tekijästä. Tässä tutkimuksessa riskikategorioiden avulla pyritään karkeasti luokittelemaan riskejä, jotta voidaan arvioida, minkä tyyppiset riskit korostuvat eri tietojärjestelmätyypeissä. Tutkimuksessa pyritään luokittelemaan kukin riski aina yhteen riskikategoriaan ja luokittelut tehdään mahdollisimman yhdenmukaisesti perinteisten ja SaaS-tietojärjestelmien välillä.

4. TIETOJÄRJESTELMÄRISKIEN TUNNISTAMINEN

Tässä luvussa tunnistetaan riskejä tutkimusaineiston pohjalta. Luvussa 4.1 esitellään perinteisiin tietojärjestelmiin liittyvät riskit, minkä jälkeen luvussa 4.2 esitellään SaaS-tietojärjestelmiin liittyvät riskit. Luvussa 4.3 tunnistettuja riskejä ja niiden merkitystä kummassakin tietojärjestelmätyypissä vertaillaan. Lopuksi esitetään tärkeitä huomioita tietojärjestelmäriskien vertailusta tässä tutkimuksessa.

4.1 Riskit perinteisissä tietojärjestelmissä

Kirjallisuuden perusteella perinteisissä tietojärjestelmissä riskit jakautuvat melko tasaisesti eri riskikategorioiden sekä ulkoisten ja sisäisten riskien välillä. Riskikategorioista korostuvat kuitenkin hieman muita enemmän teknologia- ja tietoturvariskit, minkä lisäksi sisäisistä tekijöistä aiheutuvia riskejä löytyy hieman ulkoisista tekijöistä aiheutuvia riskejä enemmän. On huomautettava, että nimenomaan perinteisten tietojärjestelmien riskeistä kertovaa kirjallisuutta löydettiin kirjallisuuskatsauksessa vain vähän, jolloin perinteisten tietojärjestelmien riskien lista jäi pieneksi. Lisäksi monet perinteisiin tietojärjestelmiin liittyvistä riskeistä ovat sellaisia, jotka liittyvät yleisesti tietojärjestelmiin eli koskevat kumpaakin tutkittavaa tietojärjestelmätyyppiä. Seuraavaksi esitellään kirjallisuuden pohjalta tunnistettuja riskejä perinteisissä tietojärjestelmissä. Kaikki löydetyt perinteisiin tietojärjestelmiin kohdistuvat riskit lähteineen esitetään liitteessä 2.

Teknologiariskit liittyvät tietojärjestelmän hyödyntämään teknologiaan, ja näitä riskejä perinteisissä tietojärjestelmissä ovat järjestelmän rajoitettu käytettävyys ja skaalautuvuus, ohjelmiston tai laitteiston kaatuminen, uudet teknologiat sekä luonnonkatastrofien tai terrorismin aiheuttamat vahingot (Sen et al. 2023; Whitaker & Thekdi 2024). Perinteisen tietojärjestelmän rajoitettu käytettävyys aiheutuu siitä, että sitä ei voi pilvijärjestelmän tavoin hyödyntää mistä tahansa, eikä kenellä tahansa ole välttämättä pääsyä kaikkiin järjestelmän osiin (Sen et al. 2023). Rajoitettu käytettävyys on perinteisiin tietojärjestelmiin kohdistuva ainutlaatuinen riski, sillä käytettävyys ei ole pilvipohjaisessa tietojärjestelmässä yhtä rajattua. Rajoitettu skaalautuvuus puolestaan on riskinä silloin, kun järjestelmä ei enää vastaa sille asetettuja tarpeita ja sitä tarvitsee uudistaa (Sen et al. 2023). Perinteisen tietojärjestelmän uudistaminen voi siis olla jäykkää ja kallista, sillä organisaatio on hankkinut laitteisto- ja ohjelmistokomponentit omistukseensa juuri tiettyä järjestelmää varten. Nämä kaksi esitettyä riskiä, sekä

Whitakerin ja Thekdin (2024) mainitsema järjestelmän kaatuminen, luokitellaan sisäisistä tekijöistä johtuviksi, sillä ne liittyvät suoraan organisaation hyödyntämään tietojärjestelmään ja sen teknologiaan, joista perinteisten tietojärjestelmien tapauksessa organisaatio on itse vastuussa. Ulkoisista tekijöistä johtuviksi riskeiksi luokitellaan luonnonkatastrofit tai terrorismi, jotka voivat vahingoittaa teknisiä järjestelmiä, sekä uudet teknologiat, jotka ajavat organisaatiota uudistamaan olemassa olevaa järjestelmää (Whitaker & Thekdi 2024). Teknisten järjestelmien uudistaminen vahinkojen tai uuden teknologian takia on organisaatiolle riski, sillä perinteisen tietojärjestelmän korjaaminen tai uudistaminen voi olla kallista, hidasta ja jäykkää.

Tietoon ja ihmisiin liittyviä riskejä löytyi kirjallisuudesta perinteisille tietojärjestelmille hyvin vähän. Yleisesti tietojärjestelmien hyödyntämiseen liittyy riski, että organisaatio ei välttämättä kykene noudattamaan tietosuojaan ja tietojen siirtoon liittyviä lakeja, kuten Euroopan Unionin GDPR-asetusta (Whitaker & Thekdi 2024). Tämä riski luokitellaan ulkoisesta tekijästä aiheutuvaksi tietoon kohdistuvaksi riskiksi, sillä se aiheutuu organisaation ulkopuolisesta lainsäädännöstä, joka kohdistuu organisaation tietoresursseihin. Lisäksi yleisesti tietojärjestelmiin liittyy riski, että tietojärjestelmän kompleksisuus rasittaa organisaation IT-henkilöstöä (Morrow et al. 2019). Tämä riski luokitellaan sisäisestä tekijästä aiheutuvaksi, ihmisiin liittyväksi riskiksi. Lisäksi on huomioitava, että näistä esitellyistä riskeistä kummatkin ovat sellaisia, jotka voivat esiintyä myös pilvipohjaisessa tietojärjestelmässä.

Organisaation liiketoimintaprosesseihin liittyväksi, sisäisistä tekijöistä aiheutuvaksi riskiksi luokitellaan perinteisten tietojärjestelmien kohdalla se, että organisaatio on itse vastuussa järjestelmän hallinnasta, ylläpidosta ja prosesseista (Madaan et al. 2023; Sen et al. 2023). Tällöin myös esimerkiksi tietojärjestelmän virheet ja haavoittuvuudet sekä niiden korjaaminen ovat organisaation itsensä vastuulla. Riskinä on esimerkiksi se, että organisaatiolla ei ole riittävästi resursseja tai osaamista järjestelmän huolelliseen hallintaan, mikä taas voi johtaa esimerkiksi tietoturvan rikkoutumiseen tai rahallisiin menetyksiin. Tätä riskiä ei esiinny lainkaan SaaS-tietojärjestelmillä, jossa tietojärjestelmän ylläpito on palveluntarjoajan vastuulla. Ulkoisista tekijöistä aiheutuvia liiketoimintaprosessiriskejä perinteisissä tietojärjestelmissä ovat järjestelmän toimitusketjun vaarantuminen sekä toimittajariippuvuus (Morrow et al. 2019). Nämä riskit perustuvat siihen, että vaikka perinteinen tietojärjestelmä on organisaation omistuksessa, se on usein ostettu ulkoiselta palveluntarjoajalta, minkä takia palveluntarjoajasta aiheutuvat riskit on myös hyvä ottaa huomioon. Nämä riskit kuitenkin korostuvat erityisesti SaaS-tietojärjestelmissä, eikä niiden merkitys perinteisissä järjestelmissä ole yhtä suuri.

Tietoturvariskit ovat suurin riskikategoria perinteisissä tietojärjestelmissä. Tietoturvariskejä perinteisissä tietojärjestelmissä ovat kirjallisuuden perusteella tietojärjestelmän sisäinen uhka, huolimattomuus järjestelmän käytössä, datan menettäminen muusta syystä kuin hyökkäyksen takia, käyttäjän tekemät virheet, ulkopuolisen pääsy järjestelmään sekä tietomurrot (Morrow et al. 2019; Whitaker & Thekdi 2024). Näistä riskeistä neljä ensimmäistä luokitellaan sisäisestä tekijästä aiheutuvaksi ja kaksi viimeistä riskiä ulkoisesta tekijästä aiheutuviksi. Tietojärjestelmän sisäisellä uhalla (*Malicious insider threat*) tarkoitetaan luvallisen järjestelmäkäyttäjän aiheuttamaa tahallista vahinkoa, kuten järjestelmän tietojen vuotamista tai järjestelmän vahingoittamista (Morrow et al. 2019), minkä takia se luokitellaan sisäisestä tekijästä aiheutuvaksi riskiksi. Huolimattomuus järjestelmän käytössä sekä käyttäjän virhe ovat myös sisäisistä tekijöistä aiheutuvia riskejä, sillä ne aiheutuvat nimenomaan järjestelmää käyttävästä tahosta (Morrow et al. 2019; Whitaker & Thekdi 2024). Myös datan menettäminen luetaan tässä tapauksessa sisäisestä tekijästä aiheutuvaksi riskiksi, sillä perinteisen järjestelmän tapauksessa organisaatio on itse vastuussa järjestelmän sisältämästä tiedosta. Ulkoisen hyökkääjän pääsy järjestelmään luokitellaan puolestaan ulkoisesta tekijästä aiheutuvaksi riskiksi (Whitaker & Thekdi 2024). Kaikki tietoturvariskeiksi luokitellut riskit ovat sellaisia, jotka esiintyvät myös SaaS-tietojärjestelmissä, eikä kirjallisuuden perusteella tietoturvariskien joukosta löydy lainkaan sellaista riskiä, joka kohdistuisi ainoastaan perinteiseen tietojärjestelmään.

Perinteiset tietojärjestelmät

	Sisäisistä tekijöistä aiheutuvat riskit	Ulkoisista tekijöistä aiheutuvat riskit
Teknologiariskit	• Järjestelmän käytettävyys rajattua (*1 maininta*) • Järjestelmän skaalautuvuus haasteena, jos järjestelmää tarvitsee uudistaa (*1 maininta*) • Järjestelmän kaatuminen (*1 maininta*)	• Luonnonkatastrofit tai terrorismi voivat vahingoittaa teknisiä järjestelmiä (*1 maininta*) • Uudet teknologiat, jotka ajavat organisaatioita uudistamaan järjestelmää (*1 maininta*)
Tietoon liittyvät riskit		• Organisaatio ei ehkä pysty noudattamaan täysin tietosuojaan ja tietojen siirtoon liittyviä lakeja (*1 maininta*)
Ihmisiin liittyvät riskit	• Järjestelmän kompleksisuus rasittaa IT henkilöstöä (*1 maininta*)	
Liiketoiminta-prosessiriskit	• Järjestelmän jatkuva hallinnointi ja ylläpito vaatii resursseja, joiden toteutumisesta organisaatio on itse vastuussa (*2 mainintaa*)	• Järjestelmän toimitusketjun vaarantuminen palveluntarjoajan hyödyntämien kolmansien osapuolien takia (*1 maininta*) • Toimittajariippuvuus: haastava vaihtaa palveluntarjoajaa. (*1 maininta*)
Tietoturvariskit	• Sisäinen uhka eli "malicious insider threat" (*1 maininta*) • Datan menettäminen muusta syystä, kuin hyökkäyksen takia (*1 maininta*) • Huolimattomuus järjestelmän käytössä lisää kyberturvallisuusriskejä (*1 maininta*) • Käyttäjän virheet (*1 maininta*)	• Varastetut tunnukset: ulkoinen hyökkääjä pääsee käsiksi järjestelmään (*2 mainintaa*) • Tietomurrot (*1 maininta*)

Kuva 2. *Perinteisiin tietojärjestelmiin kohdistuvat riskit riskikategorioittain ja niiden kirjallisuudessa saamien mainintojen lukumäärä.*

Kuvaan 2 on tiivistetty kirjallisuudesta löytyneet perinteisten tietojärjestelmien riskit. Riskit on järjestetty kunkin kategorian kohdalla eniten mainintoja saaneesta riskistä vähiten mainintoja saaneeseen. Kuitenkin kuvasta 2 voidaan havaita, että mikään riski ei ole saanut enempää kuin 2 mainintaa, mikä kertoo siitä, että kirjallisuutta on ollut niukasti. Kuvan 2 perusteella voidaan todeta, että perinteisten tietojärjestelmien kohdalla kirjallisuudessa painottuvat hieman enemmän sisäisistä tekijöistä aiheutuvat riskit sekä riskikategorioista liiketoimintaprosessi- ja tietoturvariskit. Kokonaisuudessaan tietoa juuri perinteisten tietojärjestelmien riskeistä löydettiin vähän.

4.2 Riskit SaaS-tietojärjestelmissä

SaaS-tietojärjestelmiin liittyviä riskejä löytyy kirjallisuudesta enemmän, kuin perinteisiin tietojärjestelmiin liittyviä riskejä. Erityisesti tietoturvariskejä esitetään kirjallisuudessa suuri määrä. SaaS-tietojärjestelmien kohdalla kirjallisuudesta löydetyt riskit painottuvat enemmän ulkoisista tekijöistä aiheutuviin riskeihin, mutta riskikategorioista korostuu perinteisten tietojärjestelmien tavoin erityisesti tietoturvariskit. Seuraavaksi esitellään kirjallisuuden pohjalta tunnistettuja SaaS-tietojärjestelmiin liittyviä riskejä. Kaikki löydetyt SaaS-tietojärjestelmiin kohdistuvat riskit lähteineen esitetään liitteessä 3.

Vähiten riskejä löytyi kirjallisuuden perusteella teknologiariskien ja ihmisiin liittyviin riskien kategorioihin. Sisäisestä tekijästä aiheutuvana teknologiariskinä SaaS-järjestelmissä on se, että järjestelmä ei vastaa sille asetettuja tarpeita ja se täytyy uudistaa (Sen et al. 2023). Tämä riski koskee kaikkia tietojärjestelmätyyppejä, eikä se ole SaaS-tietojärjestelmän kohdalla yhtä merkittävä kuin perinteisen tietojärjestelmän kohdalla pilviteknologian tuoman joustavuuden ja skaalautuvuuden ansiosta. Lisäksi perinteisten tietojärjestelmien tavoin myös uudet teknologiat ajavat organisaatiota uudistamaan tietojärjestelmää (Whitaker & Thekdi 2024), mutta tämäkään riski ei ole SaaS-tietojärjestelmillä niin merkittävä pilviteknologian joustavuuden ja skaalautuvuuden ansiosta. Kolmas teknologiariski SaaS-tietojärjestelmissä on se, että hyödyntämänsä teknologian takia järjestelmä on täysin riippuvainen internetyhteydestä (Singh & Parminder 2017). Tämä riski aiheutuu puhtaasti pilviteknologiasta, minkä takia se luokitellaan ulkoisesta tekijästä aiheutuvaksi riskiksi. Ihmisiin liittyviin riskeihin luokitellaan se, että järjestelmän kompleksisuus rasittaa IT henkilöstöä (Morrow et al. 2019). Vaikka tämä riski on olemassa myös perinteisten tietojärjestelmien kohdalla, korostuu sen merkittävyys SaaS-järjestelmissä pilviteknologian kompleksisuuden takia. Tämä riski luokitellaan sisäisestä tekijästä aiheutuvaksi, sillä ajatellaan sen liittyvän pelkistään organisaation henkilöstöön. Toisaalta tämä riski voidaan luokitella myös

ulkoisesta tekijästä aiheutuvaksi, sillä pilvijärjestelmän toimittajan tulisi antaa käyttäjäorganisaatiolle riittävän hyvät valmiudet järjestelmän käyttöön.

Tietoon liittyvien riskien kohdalla kirjallisuudesta löydettiin ainoastaan ulkoisista tekijöistä aiheutuvia riskejä, mihin vaikuttaa se, että tiedon hallinta on SaaS-tietojärjestelmässä palveluntarjoajan vastuulla. Hallinnan menettäminen datasta onkin yksi SaaS-tietojärjestelmiin kohdistuva riski (Morrow et al. 2019; Sen et al. 2023). Tämän myötä myös tietojen todellisen sijainnin hallinta siirtyy palveluntarjoajalle, mikä aiheuttaa käyttäjäorganisaatiolle riskin. Monissa maissa tietojärjestelmän sisältämän datan todellista sijaintia on rajoitettu säädöksillä, joiden rikkomisesta voi aiheutua seuraamuksia (Ahmad et al. 2017; Nguyen & Khorev 2019; Patel & Alabishi 2019). Näitä esitettyjä riskejä ei esiinny perinteisissä tietojärjestelmissä, joissa tietoresurssit ovat ainoastaan järjestelmän käyttäjäorganisaation hallinnassa. Myös tietojärjestelmän sisältämän datan epäjohdonmukaisuus ja yhteensopimattomuus muun organisaation datan kanssa on tietoon liittyvä riski SaaS.-tietojärjestelmissä (Ahmad et al. 2017). SaaS-järjestelmissä datan yhteensopimattomuus ja epäjohdonmukaisuus aiheutuvat esimerkiksi standardoinnin puutteesta tai epäjohdonmukaisuuksista sovellusrajapinnoissa (Ahmad et al. 2017), minkä takia riski luokitellaan ulkoisesta tekijästä, tässä tapauksessa palveluntarjoajasta, aiheutuvaksi. Lisäksi, kuten perinteisten tietojärjestelmien kohdalla, tietosuojaan ja tiedonsiirtoon liittyvien lakien noudattaminen luokitellaan tietoon liittyväksi ulkoisesta tekijästä johtuvaksi riskiksi (Whitaker & Thekdi 2024).

Myös liiketoimintaprosessiriskien kohdalla kirjallisuudesta löytyy ainoastaan ulkoisista tekijöistä johtuvia riskejä. SaaS-tietojärjestelmille täysin uniikki liiketoimintaprosessiriski on kontrollin menettäminen joistakin järjestelmän operaatioista, joista palveluntarjoaja vastaa (Morrow et al. 2019). Tämä voi olla riski organisaation toiminnan jatkuvuudelle, sillä organisaatio ei pysty itse hallinnoimaan joitakin tietojärjestelmään kohdistuvia liiketoimintaprosesseja eikä turvaamaan niiden jatkuvuutta. SaaS-tietojärjestelmiin kohdistuu osittain myös samoja liiketoimintaprosessiriskejä kuin perinteisiin tietojärjestelmiin, jotka kuitenkin korostuvat erityisesti SaaS-tietojärjestelmillä. Näitä riskejä ovat toimittajariippuvuus sekä järjestelmän toimitusketjun vaarantuminen palveluntarjoajan hyödyntämien kolmansien osapuolien takia (Morrow et al. 2019) ja ne korostuvat SaaS-tietojärjestelmillä, joiden toiminta on hyvin riippuvaista palveluntarjoajasta. Lisäksi tietojärjestelmätoimittajan konkurssi tai muusta syystä johtuva liiketoiminnan loppuminen, riittämätön käyttötuki palveluntarjoajalta, käyttökatkot järjestelmässä sekä haasteet kolmannen osapuolen auditoinneissa ovat liiketoimintaprosessiriskejä SaaS-tietojärjestelmissä (Ahmad et al. 2017; Nguyen &

Khorev 2019). Nämä riskit luokitellaan liiketoimintaprosessiriskeiksi, sillä ne uhkaavat esimerkiksi tietojärjestelmän käytettävyyttä ja näin organisaation liiketoimintaprosessien jatkuvuutta.

Selvästi eniten SaaS-tietojärjestelmien riskejä kirjallisuudesta löytyi tietoturvariskien kategoriaan, ja sekä sisäisistä että ulkoisista tekijöistä aiheutuvia riskejä löydettiin. Sisäisistä tekijöistä aiheutuvien riskien kohdalla eniten mainintoja kirjallisuudessa saivat sisäinen hyökkäys (*engl. malicious insider threat*), datan menettäminen sekä huolimattomuus järjestelmän käytössä (*engl. insufficient due diligence*) (Ahmad et al. 2017; Kofahi & Al-Rabadi 2018; Morrow et al. 2019; Pericherla 2023). Nämä riskit esiintyivät myös perinteisiä tietojärjestelmiä koskevassa kirjallisuudessa, mutta ne korostuvat enemmän SaaS-tietojärjestelmillä. Esimerkiksi sisäisen hyökkäyksen riski on SaaS-tietojärjestelmässä perinteistä tietojärjestelmää suurempi sen takia, että järjestelmään pääsee käsiksi mistä tahansa ja joillakin toimittajapuolen henkilöillä voi olla myös pääsy järjestelmään. Morrow et al. (2019) esittävät, että SaaS-järjestelmät lisäävät myös ilman IT-osaston tukea tapahtuvaa ohjelmistojen käyttöä eli varjojärjestelmiä, jotka voivat altistaa haittaohjelmille tai tietojen luvattomalle siirrolle. Muita kirjallisuudessa mainittuja sisäisistä tekijöistä aiheutuvia tietoturvariskejä ovat tietojen salausavaimen menettäminen (Nguyen & Khorev 2019), kyvyttömyys arvioida palveluntarjoajan luotettavuutta (Singh & Parminder 2017), sekä Pericherlan (2023) mainitsemat riittämättömät välineet ja menetelmät turvallisuuden varmistamiseen, riittämätön vastuun ottaminen järjestelmän turvallisuudesta ja inhimilliset virheet.

Ulkoisista tekijöistä aiheutuvat tietoturvariskit SaaS-tietojärjestelmissä ovat kaikista suurin riskikategoria tässä tutkimuksessa. Näistä riskeistä eniten mainintoja ovat saaneet ulkoisen hyökkääjän pääsy järjestelmään, haavoittuvuudet sovellusrajapinnoissa, tietomurrot, jaetusta teknologiasta aiheutuvat haavoittuvuudet sekä heikko tunnistuksen ja pääsyoikeuksien hallinta (ks. liite 3). Ulkoinen hyökkääjä voi päästä käsiksi tietojärjestelmään esimerkiksi kalastelemalla tunnuksia phishing-hyökkäyksen kautta tai manipuloimalla ihmisiä (Ahmad et al. 2017). Ulkoisen hyökkääjän pääsy järjestelmään on riski yleisesti kaikissa tietojärjestelmissä (Whitaker & Thekdi 2024), mutta riski korostuu SaaS-järjestelmissä, sillä niihin pääsee perinteisiä järjestelmiä helpommin käsiksi. Haavoittuvuudet sovellusrajapinnoissa on puolestaan SaaS-järjestelmille uniikki riski. Heikot rajapinnat ja API:t (*engl. Application Programming Interface*) altistavat tietojärjestelmän esimerkiksi palvelunestohyökkäyksille tai datan menettämiselle, ja niiden suojaaminen on palveluntarjoajan vastuulla (Kofahi & Al-Rabadi 2018). Tätä riskiä korostaa SaaS-tietojärjestelmissä se, että toisin kuin perinteisissä tietojärjestelmissä, SaaS-järjestelmien sovellusrajapinnat ovat

käytettävissä internetin kautta, mikä altistaa ne hyväksikäytölle (Morrow et al. 2019). Myös pilvipohjaisten sovellusten hyödyntämästä jaetusta teknologiasta aiheutuvat riskit, kuten side-channel hyökkäykset sekä haasteet pitää eri organisaatioiden data erillään ovat SaaS-järjestelmille uniikkeja riskejä (Ahmad et al. 2017; Singh & Parminder 2017; Kofahi & Al-Rabadi 2018; Pericherla 2023).

Ulkoisesta tekijästä aiheutuvia tietoturvariskejä löytyi vielä edellä mainittujen lisäksi lukuisia. Pääosin riskit liittyvät järjestelmässä, sovelluksissa sekä verkossa oleviin haavoittuvuuksiin ja niistä aiheutuviin riskeihin, kuten erilaisiin hyökkäyksiin. Näitä riskejä ovat esimerkiksi palvelunestohyökkäykset (Kofahi & Al-Rabadi 2018; Pericherla 2023) sekä lunnasohjelmat (Pericherla 2023), jotka voivat aiheutua esimerkiksi järjestelmän haavoittuvuuksista. Lisäksi suoraan tietoon ja sen luottamuksellisuuteen, eheyteen ja saatavuuteen liittyviä tietoturvariskejä löytyi kirjallisuudesta paljon. Näitä ovat esimerkiksi palveluntarjoajan vastuulla oleva tietojen eheyden säilyttäminen ja eri asiakkaiden tietojen pitäminen erillään (Nguyen & Khorev 2019) sekä se, että pääsy tietojärjestelmän dataan rajoittuu turvallisuusmenettelyjen takia (Patel & Alabishi 2019). Kirjallisuuden perusteella voidaan todeta, että ulkoisista tekijöistä, ja tarkemmin palveluntarjoajasta aiheutuvia riskejä on paljon. Tämän takia SaaS-tietojärjestelmiä hyödyntävän organisaation sisäiseksi riskiksi muodostuu, ettei se osaa arvioida palveluntarjoajan turvallisuutta riittävästi (Singh & Parminder 2017). Pericherla (2023) kuitenkin muistuttaa, että organisaation sisäiseksi tietoturvariskiksi voi SaaS-tietojärjestelmien kohdalla muodostua se, ettei järjestelmää käyttävä taho ota lainkaan vastuuta tietoturvamenettelyistä.

SaaS-tietojärjestelmät

	Sisäisistä tekijöistä aiheutuvat riskit	Ulkoisista tekijöistä aiheutuvat riskit
Teknologiariskit	• Järjestelmä ei enää vastaa tarpeita ja sitä täytyy uudistaa (*1 mainintaa*)	• Järjestelmä täysin riippuvainen internetyhteydestä (*1 mainintaa*) • Uudet teknologiat, jotka ajavat organisaatioita uudistamaan järjestelmää. (*1 mainintaa*)
Tietoon liittyvät riskit		• Organisaatio ei voi olla varma tietojen todellisesta sijainnista (*3 mainintaa*) • Organisaatio menettää kontrollin datasta. (*2 mainintaa*) • Datan epäjohdonmukaisuus ja yhteensopimattomuus muun organisaation datan kanssa (*1 mainintaa*) • Organisaatio ei ehkä pysty noudattamaan täysin tietosuojaan ja tietojen siirtoon liittyviä lakeja (*1 mainintaa*)
Ihmisiin liittyvät riskit	• Järjestelmän kompleksisuus rasittaa IT henkilöstöä (*1 mainintaa*)	
Liiketoiminta-prosessiriskit		• Tietojärjestelmätoimittajan konkurssi tai muusta syystä johtuva liiketoiminnan loppuminen (*2 mainintaa*) • Organisaatio menettää kontrollia joistakin järjestelmän operaatiosta (*1 mainintaa*) • Riittämätön tuki järjestelmän käyttöön palveluntarjoajalta (*1 mainintaa*) • Järjestelmän toimitusketjun vaarantuminen palveluntarjoajan hyödyntämien kolmansien osapuolien takia (*1 mainintaa*) • Haasteet kolmannen osapuolen auditoinneissa, koska datakeskukset sijaitsevat maantieteellisesti eri paikoissa (*1 mainintaa*) • Toimittajaosapuolesta aiheutuvat käyttökatkot järjestelmässä (*1 mainintaa*) • Toimittajariippuvuus (*1 mainintaa*)
Tietoturvariskit	• Sisäinen uhka eli "malicious insider threat" (*4 mainintaa*) • Datan menettäminen muusta syystä, kuin hyökkäyksen takia. (*4 mainintaa*) • Huolimattomuus järjestelmän käytössä lisää tietoturvariskejä. (*4 mainintaa*) • inhimilliset virheet uhkaavat järjestelmän tietoturvallisuutta (*2 mainintaa*) • Salausavaimen menettäminen (*1 mainintaa*) • Luvattomien pilvipalvelujen käyttö (*1 mainintaa*) • Riittämättömät välineet ja menetelmät turvallisuuden varmistamiseen. (*1 mainintaa*) • Järjestelmän käyttäjä ei ota itse riittävästi vastuuta järjestelmän turvaamisesta (*1 mainintaa*) • Organisaatiolla ei ole kykyä arvioida palveluntarjoajan luotettavuutta. (*1 mainintaa*)	• Varastetut tunnukset: ulkoinen hyökkääjä pääsee käsiksi järjestelmään. (*6 mainintaa*) • Heikko tunnistautumisen ja pääsyoikeuksien hallinta (*5 mainintaa*) • Tietomurrot (*5 mainintaa*) • Haavoittuvuudet sovellusrajapinnoissa aiheuttavat tietoturvariskejä (*4 mainintaa*) • Jaetusta teknologiasta aiheutuvat riskit (*4 mainintaa*) • Haavoittuvuudet järjestelmässä ja sovelluksissa altistavat hyökkäyksille (*3 mainintaa*) • Haavoittuvuudet verkossa altistavat hyökkäyksille (*3 mainintaa*) • Heikentynyt kyky varmistaa datan turvallinen poistaminen (*2 mainintaa*) • Eri asiakkaiden tietojen pitäminen erillään toimittajan vastuulla (*2 mainintaa*) • Palvelunestohyökkäys (*2 mainintaa*) • Eristysvirhe eli hyökkääjä pääsee käsiksi organisaation tietoihin toisen organisaation järjestelmän kautta (*1 mainintaa*) • Tiedon eheyden valvonta palveluntarjoajan vastuulla (*1 mainintaa*) • Tietovuodot (*1 mainintaa*) • Salakuuntelu (*1 mainintaa*) • ...

Kuva 3. *SaaS-tietojärjestelmiin kohdistuvat riskit riskikategorioittain ja niiden kirjallisuudessa saamien mainintojen lukumäärä.*

Kuvaan 3 on tiivistetty kirjallisuudesta löytyneet SaaS-tietojärjestelmien riskit. Riskit on järjestetty kunkin kategorian kohdalla eniten mainintoja saaneesta riskistä vähiten mainintoja saaneeseen. Kuvan 3 perusteella on helppo havaita, kuinka suuri tietoturvariskien kategoria on muihin riskikategorioihin verrattuna. Lisäksi kuva 3 havainnollistaa, kuinka paljon enemmän riskit painottuvat ulkoisista tekijöistä aiheutuviin riskeihin.

4.3 Tietojärjestelmäriskien vertailu ja niiden korostuminen eri tietojärjestelmätyypeissä

Kirjallisuuden perusteella perinteisten tietojärjestelmien ja SaaS-tietojärjestelmien riskit eroavat toisistaan jonkin verran, mutta riskeissä on myös yhtäläisyyksiä. Suurin ero kirjallisuuden perusteella on se, että SaaS-tietojärjestelmiin kohdistuvia riskejä löytyy runsaasti enemmän, kuin perinteisiin tietojärjestelmiin kohdistuvia riskejä. On huomautettava, että SaaS-tietojärjestelmien riskejä koskevassa kirjallisuudessa esitetään useita riskejä, joita ei voida poissulkea perinteisten tietojärjestelmien kohdalla, kuten järjestelmähaavoittuvuuksista johtuvat hyökkäykset tai riittämättömät välineet turvallisuuden varmistamiseen. Näitä riskejä ei kuitenkaan suoraan esitetä perinteisten

tietojärjestelmien riskejä koskevassa kirjallisuudessa, minkä takia niitä ei ole listattu perinteisten tietojärjestelmien riskeiksi. Seuraavaksi vertaillaan perinteisille tietojärjestelmille sekä SaaS-tietojärjestelmille löydettyjen riskien eroja ja yhtäläisyyksiä riskikategorioittain sekä pohditaan, kummalla järjestelmätyypillä kukin riskikategoria mahdollisesti korostuu enemmän.

Teknologiariskien kategoriassa molempien tietojärjestelmätyyppien kohdalla riskinä on, että tietojärjestelmä ei enää vastaa organisaation muuttuviin tarpeisiin ja vaatii uudistamista. Tämä riski on merkittävämpi perinteisissä järjestelmissä, joissa uudistaminen on usein kallista ja jäykkää, kun taas SaaS-järjestelmät hyötyvät pilviteknologian tuomasta joustavuudesta ja skaalautuvuudesta. Perinteisillä tietojärjestelmillä on lisäksi rajoittuneempi käytettävyys, mikä tekee niistä riippuvaisempia fyysisestä sijainnista. (Sen et al. 2023) Luonnonkatastrofit, kuten tulvat tai maanjäristykset, muodostavat erityisen ulkoisen riskin perinteisille järjestelmille (Whitaker & Thekdi 2024). Perinteisten tietojärjestelmien tekninen infrastruktuuri on keskittynyt tiettyihin fyysisiin tiloihin, ja sen tuhoutuminen on riski tietojärjestelmän toiminnan jatkuvuudelle. Pericherlan (2023) mukaan tämä riski ei ole merkittävä SaaS-tietojärjestelmillä, sillä järjestelmä hyödyntää muualla sijaitsevaa laitteistoa verkon yli. Toisaalta SaaS-järjestelmät ovat riippuvaisia internetyhteydestä, mikä puolestaan tuo riskin niiden käyttövarmuuteen (Singh & Parminder 2017). SaaS-järjestelmät siis hyötyvät pilviteknologian joustavuudesta ja skaalautuvuudesta, mutta ovat riippuvaisia internetyhteydestä, kun taas perinteisissä tietojärjestelmissä teknologiariskit liittyvät järjestelmän uudistamisen jäykkyyteen, rajoitettuun käytettävyyteen sekä fyysisen infrastruktuurin tuhoutumiseen. Voidaan sanoa, että teknologiariskit korostuvat erityisesti perinteisten tietojärjestelmien kohdalla, sillä kirjallisuuden mukaan perinteisiin tietojärjestelmiin kohdistuu SaaS-tietojärjestelmiä enemmän teknologiariskejä esimerkiksi perinteisten tietojärjestelmien jäykkyyden ja rajoitetun käytettävyyden takia, sekä siksi, että ne ovat riippuvaisia fyysisestä infrastruktuurista.

Tietoon liittyvät riskit eroavat perinteisissä tietojärjestelmissä ja SaaS-tietojärjestelmissä erityisesti siltä osin, kuka tietoa viimekädessä hallinnoi. Kumpaankin tietojärjestelmätyyppiin liittyy riski siitä, pystytäänkö tietosuojaan ja tietojen siirtoon liittyviä lakeja noudattamaan (Whitaker & Thekdi 2024), mutta perinteisissä tietojärjestelmissä tämä riski kohdistuu järjestelmän käyttäjäorganisaatioon suoraan, sillä tietoresurssit ovat organisaation omassa hallinnassa. SaaS-järjestelmissä puolestaan tietoresurssien hallinnointi on palveluntarjoajan vastuulla. Tällöin järjestelmän käyttäjäorganisaatio menettää hallinnan tietoresursseista, mikä aiheuttaa esimerkiksi epäselvyyksiä siitä, missä tiedot fyysisesti sijaitsevat (Ahmad et al. 2017;

Nguyen & Khorev 2019; Patel & Alabishi 2019). Tiedon hallinnan riskien lisäksi SaaS-tietojärjestelmillä esiintyy riski siitä, että tietojärjestelmän tieto on epäjohdonmukaista tai yhteensopimatonta muun organisaation datan kanssa, mikä johtuu esimerkiksi standardoinnin puutteesta tai epäjohdonmukaisuuksista sovellusrajapinnoissa (Ahmad et al. 2017). Perinteisissä tietojärjestelmissä tietoon liittyvät riskit ovat siis suoraan käyttäjäorganisaation vastuulla, kun taas SaaS-tietojärjestelmissä riskit ovat palveluntarjoajan vastuulla. Tietoon liittyvien riskien voidaan sanoa olevan merkittävämpiä SaaS-tietojärjestelmissä, sillä niihin kohdistuu pilviteknologian ja toimittajariippuvuuden takia enemmän tietoon liittyviä riskejä, eikä organisaatio ei pysty itse lainkaan vaikuttamaan näiden riskien minimoimiseen tai hallintaan.

Liiketoimintaprosessiriskien kategoriassa perinteistä tietojärjestelmää käyttävä organisaatio on vastuussa järjestelmän hallinnasta ja ylläpidosta, mikä voi aiheuttaa riskejä, jos resurssit tai osaaminen eivät riitä järjestelmän ylläpitoon tai virheiden ja haavoittuvuuksien hallintaan (Madaan et al. 2023; Sen et al. 2023). SaaS-järjestelmissä tätä riskiä ei esiinny, sillä tietojärjestelmän ylläpito on palveluntarjoajan vastuulla. SaaS-järjestelmissä riskinä on kuitenkin se, ettei organisaatio pysty itse hallinnoimaan kaikkia tietojärjestelmän prosesseja (Morrow et al. 2019). Molemmissa järjestelmissä esiintyviä riskejä ovat toimittajariippuvuus sekä toimitusketjun vaarantuminen kolmansien osapuolien takia (Morrow et al. 2019), mutta nämä riskit korostuvat erityisesti SaaS-tietojärjestelmissä, jotka ovat palveluntarjoajan hallinnoimia. Lisäksi kirjallisuudessa esitettyjä SaaS-tietojärjestelmien riskejä ovat myös toimittajan liiketoiminnan päättyminen, järjestelmän käyttökatkot sekä riittämättömät tukipalvelut (Ahmad et al. 2017; Nguyen & Khorev 2019). Näitä riskejä ei voida sulkea pois myöskään perinteisiltä tietojärjestelmiltä, mutta niitä ei suoraan mainita perinteisiä tietojärjestelmiä koskevassa kirjallisuudessa. Perinteisissä tietojärjestelmissä liiketoimintaprosessiriskit liittyvät siihen, että organisaatio vastaa itse järjestelmän ylläpidosta, kun taas SaaS-tietojärjestelmässä liiketoimintariskit liittyvät palveluntarjoajan toimintaan. Liiketoimintaprosessiriskien katsotaan korostuvan hieman enemmän SaaS-tietojärjestelmillä, sillä sen lisäksi, että kirjallisuudesta löydettiin enemmän liiketoimintaprosessiriskejä SaaS-tietojärjestelmille, myös tietojärjestelmätyypeille yhteiset riskit korostuvat entisestään SaaS-tietojärjestelmillä niiden toimittajariippuvuuden takia.

Tietoturvariskit ovat kummallakin järjestelmätyypillä suurin riskikategoria, mutta kirjallisuudesta on löydettävissä huomattavasti enemmän SaaS-tietojärjestelmien turvallisuusriskejä. Kumpaakin järjestelmätyyppiä koskee kuitenkin riski järjestelmän sisäisestä uhasta, kuten luvallisen järjestelmäkäyttäjän tahallisesta vahingonteosta

(Morrow et al. 2019). Samoin ulkopuolisen hyökkääjän pääsy järjestelmään varastettujen tunnusten avulla on yleinen riski kummassakin järjestelmätyypissä (Morrow et al. 2019; Whitaker & Thekdi 2024). Nämä riskit ovat hieman merkittävämpiä SaaS-järjestelmillä, joihin pääsee perinteisiä järjestelmiä helpommin käsiksi. Lisäksi ulkoinen hyökkääjä voi pahimmassa tapauksessa päästä yhden SaaS-tietojärjestelmän kautta kaikkiin samaa pilvijärjestelmää hyödyntäviin tietojärjestelmään käsiksi (Morrow et al. 2019; Pericherla 2023). Myös käyttäjän virheet sekä huolimattomuus järjestelmän käytössä nousevat esiin kummankin tietojärjestelmätyypin kohdalla (esim. Kofahi & Al-Rabadi 2018; Morrow et al. 2019). SaaS-järjestelmät kuitenkin tuovat mukanaan myös erityisiä riskejä, joita ei perinteisissä järjestelmissä ilmene. Esimerkiksi jaetusta teknologiasta aiheutuvat riskit, kuten side-channel hyökkäykset tai vaikeudet pitää tietoja erillään (esim. Ahmad et al. 2017; Pericherla 2023) tai hyökkäyksille altistavat heikot sovellusrajapinnat (Kofahi & Al-Rabadi 2018) ovat SaaS-järjestelmille ominaisia eikä niitä esiinny lainkaan perinteisissä tietojärjestelmissä.

Kuten on todettu muidenkin riskikategorioiden kohdalla, perinteisissä tietojärjestelmissä organisaatio vastaa itse kaikesta tietoturvasta ja datan hallinnasta, kun taas SaaS-järjestelmissä tämä vastuu siirtyy palveluntarjoajalle. Tietoturvallisuusriskit ovat merkittävämpiä SaaS-tietojärjestelmissä perinteisiin tietojärjestelmiin verrattuna, sillä esimerkiksi pilviteknologia ja toimittajariippuvuus tuovat SaaS-tietojärjestelmille paljon uniikkeja riskejä, minkä lisäksi joidenkin yleisten tietojärjestelmäriskien merkittävyys korostuu SaaS-tietojärjestelmien kohdalla. Se, että SaaS-tietojärjestelmien ja yleisesti pilviteknologian turvallisuusriskeistä löytyi kirjallisuuskatsauksessa huomattavasti enemmän tuloksia, kertoo myös siitä, että turvallisuusriskit ovat nousseet pilviteknologian yleistyttyä enemmän esille. On kuitenkin huomautettava, että tietoturvariskit olivat myös perinteisissä tietojärjestelmissä suurin riskikategoria, minkä takia ei voida sanoa, etteivätkö tietoturvariskit olisi merkittäviä myös periteisissä tietojärjestelmissä. Niiden merkitys kuitenkin korostuu entisestään SaaS-tietojärjestelmissä, minkä takia niiden sanotaan olevan merkittävämpiä SaaS-tietojärjestelmissä.

Tässä luvussa tehtyjen päätelmien perusteella voidaan sanoa, että perinteisiin tietojärjestelmiin kohdistuvissa riskeissä korostuvat SaaS-järjestelmiä enemmän teknologiariskit. SaaS-järjestelmiin kohdistuvissa riskeissä sen sijaan korostuvat perinteisiä järjestelmiä enemmän tietoon liittyvät riskit, liiketoimintaprosessiriskit sekä tietoturvariskit. Ihmisiin liittyvät riskit eivät ole tutkimuksen perusteella merkittävä riskikategoria kummassakaan tietojärjestelmätyypissä, sillä tähän kategoriaan löydettiin

vain yksi riski kummankin järjestelmätyypin kohdalla. Kuvassa 4 havainnollistetaan, kummassa tietojärjestelmätyypissä riskikategoriat painottuvat enemmän.

	Perinteiset tietojärjestelmät	SaaS-tietojärjestelmät
Teknologiariskit	✕	
Tietoon liittyvät riskit		✕
Ihmisiin liittyvät riskit		
Liiketoimintaprosessi-riskit		✕
Tietoturvariskit		✕

Kuva 4. *Riskikategorioiden korostuminen perinteisissä ja SaaS-tietojärjestelmissä*

On hyvä kuitenkin muistaa, että vaikka riskit korostuvat enemmän yhdessä tietojärjestelmätyypissä, ei se tarkoita, että niiden merkitys on toisessa tietojärjestelmätyypissä mitätön. Riskien korostumisen pohdinnalla halutaan tuoda ilmi, miten riskit eroavat tietojärjestelmätyyppien välillä, ja mihin riskikategorioihin kannattaa kummankin tietojärjestelmätyypin kohdalla kiinnittää erityistä huomiota.

4.4 Tietojärjestelmäriskien merkittävyyden arvioinnista

Kun halutaan arvioida jonkin riskin merkittävyyttä organisaation toiminnassa, täytyy ensin tunnistaa riskin todennäköisyys ja sen vaikutus. Yksittäisen riskin merkitys määräytyy näiden kahden tekijän tulona. Esimerkiksi riski, joka toteutuu todennäköisesti ja jolla on suuri kielteinen vaikutus, määritellään korkeaksi eli merkittäväksi riskiksi. Toisaalta riski, jonka vaikutukset ovat pienet ja toteutumisen todennäköisyys keskisuuri tai pieni, määritellään pieneksi riskiksi. (Patel & Alabishi 2019) Tässä tutkimuksessa tarkastellaan tietojärjestelmien riskejä yleisesti, eikä siksi pystytä suoraan kartoittamaan riskien todennäköisyyksiä tai tarkkoja vaikutuksia jollekin organisaatiolle. Tästä syystä tässä tutkimuksessa ei oteta kantaa eri riskien merkittävyyteen, vaan pohditaan sitä, mitä riskejä kirjallisuudessa esiintyy eniten, ja minkälaiset riskikategoriat korostuvat eri tietojärjestelmätyypeissä.

Eri riskikategorioiden korostumisen arviointi tutkittavissa tietojärjestelmätyypeissä luvussa 4.3 perustuu siihen, miten löydetyt riskit mahdollisesti korostuvat perinteisten tietojärjestelmien tai SaaS-tietojärjestelmien käytössä. Lisäksi korostumisen arvioinnissa otetaan huomioon riskien määrä, mutta se ei ole arvioinnissa ainoa tekijä tutkimusaineiston suppeuden vuoksi. Todellisuudessa eri riskikategorioiden merkittävyys voi vaihdella organisaatioittain, riippuen siitä, minkälainen organisaatio on kyseessä. Riskikategorioiden korostumisen arvioinnilla pyritään tässä tutkimuksessa määrittämään sitä, minkä tyyppiset riskit korostuvat perinteisissä ja SaaS-tietojärjestelmissä järjestelmän käyttövaiheessa, ja löytyykö tässä eroja tietojärjestelmätyyppien välillä. Riskikategorioiden korostuminen toisessa tietojärjestelmätyypissä merkitsee sitä, että kyseisiin riskeihin kannattaa kiinnittää erityistä huomiota tietojärjestelmää käyttävässä organisaatiossa kuitenkaan laiminlyömättä muita riskikategorioita.

5. YHTEENVETO

Yhteenvetoluvussa esitellään tutkimuksen keskeiset tulokset ja niiden pohjalta muodostetut päätelmät. Tulokset esitellään vastaamalla tutkimuskysymyksiin. Lisäksi luvussa pohditaan valitun aineiston merkitystä tutkimuksen tuloksiin. Luvun lopussa esitetään vielä tutkimuksen arviointi ja jatkotutkimusehdotukset.

5.1 Tulokset ja päätelmät

Tässä kandidaatintyössä tutkittiin perinteisiin tietojärjestelmiin ja SaaS-tietojärjestelmiin liittyviä riskejä. Aihetta tutkittiin järjestelmän käyttäjän näkökulmasta keskittyen erityisesti tietojärjestelmän käyttövaiheen riskeihin. Tutkimusta tehdessä havaittiin, että kirjallisuutta pilviteknologiaan ja pilvipohjaisiin tietojärjestelmiin liittyvistä riskeistä löytyy paljon, kun taas perinteisiin tietojärjestelmiin liittyvistä riskeistä kertovaa kirjallisuutta löytyy vähemmän. Tästä voidaan päätellä, että pilvipohjaiset tietojärjestelmät korostavat riskien tarkastelun merkittävyyttä.

Tutkimuksen päätutkimuskysymys oli ”Miten SaaS-tietojärjestelmien riskit eroavat perinteisten tietojärjestelmien riskeistä?”. Tutkimuksessa pyrittiin vastaamaan tähän kysymykseen alatutkimuskysymysten avulla, jotka olivat seuraavat: ”Mitä riskejä liittyy perinteisiin tietojärjestelmiin ja millaisia ne ovat?”, ”Mitä riskejä liittyy SaaS-tietojärjestelmiin ja millaisia ne ovat?”, ” Mitä ja millaisia riskejä esiintyy eniten kummassakin tutkittavassa tietojärjestelmätyypissä?” sekä ”Millaiset riskit korostuvat tutkittavissa tietojärjestelmätyypeissä?”. Näihin kysymyksiin muodostettiin vastaukset kirjallisuuskatsauksen pohjalta. Kirjallisuuskatsauksen toteutus esitellään luvussa 2.

Kahden ensimmäisen alatutkimuskysymyksen avulla haluttiin selvittää, mitä riskejä kirjallisuudesta löytyy kummallekin tietojärjestelmätyypille ja millaisia nämä löydetyt riskit ovat. Tutkimusaineistosta löydetyt tietojärjestelmiin kohdistuvat riskit esitellään luvuissa 4.1 ja 4.2, minkä lisäksi ne ovat listattuna lähteineen liitteissä 2 ja 3. Luvussa 3 määriteltiin tietojärjestelmäriskien luokitteluun viitekehys, jonka avulla pyrittiin tunnistamaan, millaisia riskejä kirjallisuudesta löytyy. Riskit jaettiin viiteen kategoriaan, jotka ovat teknologiaan, tietoon, ihmisiin, liiketoimintaprosesseihin sekä tietoturvaan liittyvät riskit. Nämä kategoriat jaetaan vielä sisäisistä ja ulkoisista tekijöistä aiheutuviin riskeihin. Tämä viitekehys esitellään kuvassa 1. Tutkimustulosten perusteella perinteisillä tietojärjestelmillä esiintyy kokonaisuudessaan vähemmän riskejä kuin SaaS-tietojärjestelmillä. Perinteisten tietojärjestelmien kohdalla korostuvat hieman enemmän

sisäisistä tekijöistä aiheutuvat riskit, kun taas SaaS-tietojärjestelmillä painottuvat huomattavasti ulkoisista tekijöistä aiheutuvat riskit. Tutkimusaineiston perusteella eniten riskejä kummallekin järjestelmätyypille on tietoturvariskien kategoriassa, ja vähiten riskejä on ihmisiin liittyvien riskien kategoriassa.

Kolmannen alatutkimuskysymyksen avulla haluttiin selvittää, mitä ja millaisia riskejä esiintyy tutkimusaineiston perusteella eniten kummassakin tietojärjestelmätyypissä. Tätä tutkittiin laskemalla riskien saamat maininnat eri lähteissä. Jokaisen riskin saamat maininnat on listattu liitteisiin 2 ja 3, minkä lisäksi mainintojen lukumäärät on kirjattu kuviin 2 ja 3. Tutkimuksen mukaan perinteisissä tietojärjestelmissä eniten mainintoja saivat seuraavat riskit: *järjestelmän hallinnointi ja ylläpito organisaation vastuulla* sekä *ulkoisen hyökkääjän pääsy järjestelmään*. Näistä riskeistä ensimmäinen kuuluu liiketoimintaprosessiriskeihin ja jälkimmäinen tietoturvariskeihin, ja kummatkin riskit ovat saaneet kirjallisuudessa kaksi mainintaa. Täytyy huomioida, että perinteisiin tietojärjestelmiin liittyviä riskejä löytyi kirjallisuudesta niin vähän, ettei riskien yleisyyden arviointi ole välttämättä tarpeellista. SaaS-tietojärjestelmiin liittyvistä riskeistä eniten mainintoja saivat *ulkoisen hyökkääjän pääsy tietojärjestelmään* sekä *heikko tunnistautumisen ja pääsyoikeuksien hallinta.* Molemmat riskit ovat tietoturvariskejä, ja ensimmäinen riski sai 6 mainintaa jälkimmäisen saadessa 5. SaaS-tietojärjestelmien kohdalla riskien yleisyyden arviointi on jo mielekkäämpää, sillä riskejä löytyi perinteisiin tietojärjestelmiin verrattuna moninkertainen määrä.

Viimeisen alatutkimuksen avulla haluttiin selvittää, millaiset riskit korostuvat tutkittavissa tietojärjestelmätyypeissä. Tätä pohdintaa on esitetty riskikategorioittain luvussa 4.3. Kirjallisuuden perusteella teknologiariskit korostuvat hieman enemmän perinteisillä tietojärjestelmillä, kun taas tietoon liittyvät riskit, liiketoimintaprosessiriskit sekä tietoturvariskit korostuvat enemmän SaaS-tietojärjestelmillä. Ihmisiin liittyviä riskejä löytyi vain yksi, joka pätee kumpaankin tutkittavaan järjestelmätyyppiin, minkä takia tätä riskikategoriaa ei pidetä tämän tutkimuksen perusteella merkittävänä. On kuitenkin hyvä tunnistaa, että esimerkiksi tietoturvariskien kategoriasta löytyy ihmisistä aiheutuvia riskejä, kuten inhimilliset virheet, mutta tässä tutkimuksessa niitä ei ole asetettu ihmisiin liittyviin riskeihin, sillä ne ovat sopivampia tietoturvariskien kategoriaan.

Alatutkimuskysymyksiin saatujen vastausten avulla muodostetaan synteesi ja vastaus päätutkimuskysymykseen. Tutkimuksen tulosten mukaan SaaS-tietojärjestelmillä korostuu useampi riskikategoria, kuin perinteisillä tietojärjestelmillä. Tämä johtuu siitä, että SaaS-tietojärjestelmiin kohdistuu tutkimuksen mukaan enemmän riskejä, minkä lisäksi useat kumpaankin tietojärjestelmätyyppiin sopivat riskit korostuvat enemmän SaaS-tietojärjestelmillä. Useat SaaS-tietojärjestelmien riskit aiheutuvat

palveluntarjoajasta tai ovat palveluntarjoajan vastuulla, minkä takia SaaS-tietojärjestelmää käyttävän osapuolen on vaikea itse hallita riskejä. Tämä lisää myös riskien merkittävyyttä SaaS-tietojärjestelmissä. Tutkimuksen tulosten perusteella SaaS-tietojärjestelmillä korostuvat erityisesti tietoon, liiketoimintaprosesseihin ja tietoturvaan liittyvät riskit, kun taas perinteisillä tietojärjestelmillä korostuvat teknologiariskit. Kuvassa 5 pyritään havainnollistamaan tätä synteesiä ja vastausta päätutkimuskysymykseen. Kuvassa 5 listataan yleisimmät riskit riskikategorioittain kummallekin tietojärjestelmätyypille, sekä havainnollistetaan, mikä riskikategoria painottuu missäkin tietojärjestelmätyypissä.

Riskikategoria	Perinteiset tietojärjestelmät	SaaS-tietojärjestelmät
Teknologiariskit	• Järjestelmän käytettävyys rajattua • Järjestelmän skaalautuvuus haasteena, jos järjestelmää tarvitsee uudistaa • Järjestelmän kaatuminen • Luonnonkatastrofit tai terrorismi voivat vahingoittaa teknisiä järjestelmiä • Uudet teknologiat, jotka ajavat organisaatioita uudistamaan järjestelmää	• Järjestelmä ei enää vastaa tarpeita ja sitä täytyy uudistaa • Järjestelmä täysin riippuvainen internetyhteydestä • Uudet teknologiat, jotka ajavat organisaatioita uudistamaan järjestelmää.
Tietoon liittyvät riskit	• Organisaatio ei ehkä pysty noudattamaan täysin tietosuojaan ja tietojen siirtoon liittyviä lakeja	• Organisaatio ei voi olla varma tietojen todellisesta sijainnista • Organisaatio menettää kontrollin datasta. • Datan epäjohdonmukaisuus ja yhteensopimattomuus muun organisaation datan kanssa • Organisaatio ei ehkä pysty noudattamaan täysin tietosuojaan ja tietojen siirtoon liittyviä lakeja
Ihmisiin liittyvät riskit	• Järjestelmän kompleksisuus rasittaa IT henkilöstöä	• Järjestelmän kompleksisuus rasittaa IT henkilöstöä
Liiketoiminta-prosessiriskit	• Järjestelmän jatkuva hallinnointi ja ylläpito vaatii resursseja, joiden toteutumisesta organisaatio on itse vastuussa • Järjestelmän toimitusketjun vaarantuminen palveluntarjoajan hyödyntämien kolmansien osapuolien takia • Toimittajariippuvuus: haastava vaihtaa palveluntarjoajaa.	• Tietojärjestelmätoimittajan konkurssi tai muusta syystä johtuva liiketoiminnan loppuminen • Organisaatio menettää kontrollia joistakin järjestelmän operaatiosta • Riittämätön tuki järjestelmän käyttöön palveluntarjoajalta • Järjestelmän toimitusketjun vaarantuminen palveluntarjoajan hyödyntämien kolmansien osapuolien takia • Haasteet kolmannen osapuolen auditoinneissa, koska datakeskukset sijaitsevat maantieteellisesti eri paikoissa • Toimittajaosapuolesta aiheutuvat käyttökatkot järjestelmässä • Toimittajariippuvuus: haastava vaihtaa palveluntarjoajaa
Tietoturvariskit	• Varastetut tunnukset: ulkoinen hyökkääjä pääsee käsiksi järjestelmään • Tietomurrot • Sisäinen uhka eli "malicious insider threat" • Datan menettäminen muusta syystä, kuin hyökkäyksen takia • Huolimattomuus järjestelmän käytössä lisää kyberturvallisuusriskejä • Käyttäjän virheet	• Varastetut tunnukset: ulkoinen hyökkääjä pääsee käsiksi järjestelmään. • Heikko tunnistautumisen ja pääsyoikeuksien hallinta • Tietomurrot • Haavoittuvuudet sovellusrajapinnoissa aiheuttavat tietoturvariskejä • Jaetusta teknologiasta aiheutuvat riskit • Sisäinen uhka eli "malicious insider threat" • Datan menettäminen muusta syystä, kuin hyökkäyksen takia. • Huolimattomuus järjestelmän käytössä lisää kyberturvallisuusriskejä.

Selite:
- Sisäisistä tekijöistä aiheutuvat riskit kirjattu punaisella
- Ulkoisista tekijöistä aiheutuvat riskit kirjattu mustalla
- Riskikategorian painottuminen tietojärjestelmätyypissä merkitty harmaalla pohjalla

Kuva 5. *Yleisimmät tietojärjestelmäriskit riskikategorioittain perinteisillä ja SaaS-tietojärjestelmillä.*

Tutkimuksen tuloksiin voi vaikuttaa se, että lähdeaineistoa löydettiin kirjallisuuskatsaukseen melko vähän. Kuten liitteessä 1 kerrotaan, kuusi lähdettä käsittelee pilvipohjaisiin tietojärjestelmiin tai pilviteknologiaan liittyviä riskejä, kolme lähdettä käsittelee sekä perinteisten, että pilvipohjaisten tietojärjestelmien riskejä, ja yksi lähde käsittelee tietojärjestelmien riskejä yleisesti. Se, että suurempi osa lähdeaineistosta käsittelee pilvipohjaisia tietojärjestelmiä, näkyy tutkimuksen tuloksissa siinä, että SaaS-tietojärjestelmiin kohdistuvia riskejä on löydetty enemmän. Tämän takia

tutkimuksen tuloksia tai päätelmiä ei voida perustella pelkästään sillä, että toiselle tietojärjestelmätyypille löydettiin määrällisesti enemmän riskejä. Lähdeaineiston painottuminen SaaS-tietojärjestelmiä koskeviin riskeihin kertoo siitä, että SaaS-tietojärjestelmät ovat nostaneet esille lisääntynyttä tarvetta riskien tunnistamiselle perinteisiin tietojärjestelmiin verrattuna. Lisäksi se, että SaaS-tietojärjestelmien riskejä käsittelevästä aineistosta löydettiin myös riskejä, joita ei voida poissulkea perinteisten tietojärjestelmien kohdalla kertoo siitä, että SaaS-tietojärjestelmät ovat nostaneet esiin myös sellaisia riskejä, mitä ei perinteisten tietojärjestelmien kohdalla ole osattu välttämättä huomioida.

Tutkimuksen perusteella voidaan todeta, että perinteisillä tietojärjestelmillä painottuvat sisäisistä tekijöistä aiheutuvat riskit, kun taas SaaS-järjestelmillä ulkoisista tekijöistä aiheutuvat riskit. SaaS-tietojärjestelmillä iso osa riskeistä aiheutuu palveluntarjoajasta tai tämän vastuulla olevista tekijöistä, mikä voi vaikeuttaa riskienhallintaa. Tämä tarkoittaa sitä, että SaaS-tietojärjestelmän kohdalla organisaatiolle erityisen tärkeää on luotettava palveluntarjoaja. Perinteisillä tietojärjestelmillä iso osa riskeistä aiheutuu tekijöistä, johon järjestelmän käyttäjäorganisaatio voi itse vaikuttaa, minkä takia organisaation sisäisten riskienhallintaprosessien toimivuus on perinteisten tietojärjestelmien kohdalla erityisen tärkeää.

Tutkimuksen perusteella tietoturvariskit ovat isoin riskikategoria kummassakin tietojärjestelmätyypissä, mutta erityisesti se painottuu SaaS-tietojärjestelmissä. Ulkoisista tekijöistä aiheutuvat SaaS-tietojärjestelmiin kohdistuvat tietoturvariskit ovat tutkimuksen mukaan kaikkein suurin riskikategoria. Tietoturvariskien merkittävyyttä perustelee myös se, että kummankin tietojärjestelmätyypin kohdalla eniten mainintoja keränneiden riskien joukossa oli tietoturvariskejä. Tämän perusteella voidaan todeta, että tietoturvariskit ovat erityisen tärkeä riskitekijä kummassakin tietojärjestelmätyypissä, minkä lisäksi SaaS-tietojärjestelmien kohdalla niihin tulisi kiinnittää vielä erityistä huomiota. Siispä, esimerkiksi organisaation, jossa säilytetään paljon hyvin arkaluontoista tietoa, kannattaa harkita pilveen siirtymistä tarkkaan, sillä tietoturvariskit korostuvat SaaS-tietojärjestelmissä.

Tutkimuksen perusteella SaaS-tietojärjestelmissä korostuu useampi riskikategoria, kuin perinteisissä tietojärjestelmissä. Jos organisaatio kuitenkin löytäisi täysin luotettavan ja yhteistyöhaluisen SaaS-tietojärjestelmän palveluntarjoajan, pienentyisi iso osa järjestelmään kohdistuvista riskeistä, mikä saattaisi tehdä siitä perinteistä tietojärjestelmää riskittömämmän vaihtoehdon. Tutkimuksesta havaitaan, että kumpaankin järjestelmätyyppiin kohdistuu ainutlaatuisia riskejä, jotka täytyy ottaa huomioon tietojärjestelmätyypin valinnassa. Organisaatiossa täytyy tunnistaa,

minkälaiset riskit ovat juuri heille merkittävimpiä, ja sen perusteella valita itselleen sopiva tietojärjestelmätyyppi.

5.2 Tutkimuksen arviointi

Tutkimusta voidaan arvioida usealla tavalla. Koska tässä työssä tutkimusmenetelmänä on systemaattinen kirjallisuuskatsaus, tutkimusta Ketchenin ja Craigheadin (2023) esittelemien erinomaisen kirjallisuuskatsauksen piirteiden avulla, jotka ovat tiivistäminen, yhdistäminen, käsitteellistäminen sekä innostaminen. Tässä luvussa arvioidaan tutkimusta ensin erinomaisen kirjallisuuskatsauksen piirteiden avulla ja lopuksi vielä yleisesti laadukkaan tutkimuksen kriteerien perusteella.

Tiivistämisessä tavoitteena on kartoittaa ja esittää tutkimusalueen nykytila. Tiivistäminen sisältää olemassa olevan kirjallisuuden jäsentämisen ja aiempien tutkimusten keskeisten löydösten esittelyn. (Ketchen & Craighead 2023) Tässä tutkimuksessa tiivistäminen näkyy erityisesti luvuissa 4.1 ja 4.2, jossa esitellään tutkimusaineistosta löydetyt riskit. Tiivistäminen näkyy lisäksi liitteissä 2 ja 3, joissa esitellään kaikki tutkimusaineistosta löydetyt tietojärjestelmäriskit. Tutkimusaineiston valinnassa on hyödynnetty systemaattisia hakuja, mikä on Ketchenin ja Craigheadin (2023) mukaan hyvä käytäntö kartoittaa aiheesta tehtyä tutkimusta. Tiivistämisen näkökulmasta työtä voisi kuitenkin vielä parantaa esittelemällä entistä laajemmin aiheen tutkimuksen nykytilaa.

Yhdistäminen eli synteesi tarkoittaa loogisen kokonaisuuden muodostamista kirjallisuudesta, ja sen tavoitteena on löytää yhteiset linjat, ristiriidat ja aukot olemassa olevassa tutkimuksessa (Ketchen & Craighead 2023). Tässä tutkimuksessa yhdistäminen näkyy erityisesti luvuissa 4.3 ja 5.1. Luvussa 4.3 pyritään löytämään eroja ja yhtäläisyyksiä luvuissa 4.1 ja 4.2 esitettyjen riskien välillä ja tekemään löydöksistä johtopäätöksiä. Luvussa 5.1 pyritään yhdistämään kaikki luvun 4 löydökset yhdeksi synteesiksi, joka esitetään tutkimuksen tuloksena. Lisäksi yhdistäminen näkyy tutkimuksessa siinä, että tutkimusaineistosta löydettyjä riskejä taulukoidaan ja ryhmitellään riskikategorioiden mukaan ja pyritään näin muodostamaan kokonaiskuva tietojärjestelmäriskeistä eri tietojärjestelmätyypeissä. Kandidaatintyön laajuuden vuoksi kaikkein syvin analyysi jää tutkimuksesta kuitenkin puuttumaan. Syvempää analyysia ja synteesiä voisi tehdä esimerkiksi siitä, miten eri riskikategorioiden riskit liittyvät toisiinsa ja mitä mahdollisia yhteyksiä eri riskikategorioiden välillä on.

Käsitteellistämisellä tarkoitetaan kirjallisuuskatsauksen tulosten järjestämistä ja esittämistä siten, että ne muodostavat selkeän kokonaisuuden, mikä voi tapahtua esimerkiksi mallien tai viitekehysten avulla (Ketchen & Craighead 2023).

Käsitteellistäminen näkyy erityisesti luvussa 3, jossa määritellään kirjallisuuden avulla viitekehys tietojärjestelmäriskein luokittelulle. Kirjallisuuskatsaus rakentuu tämän viitekehyksen päälle, sillä tutkimusaineistosta löydetyt riskit luokitellaan tämän viitekehyksen avulla. Myös tutkimustuloksia analysoidaan tämän viitekehyksen avulla. Käsitteellistämistä voisi parantaa esimerkiksi kehittämällä viitekehystä näyttämään eri riskiluokkien suhteita ja yhteyksiä, mutta kandidaatintyön laajuus rajoittaa näin syvällisen analyysin tekemistä tässä tutkimuksessa.

Innostamisella tarkoitetaan esimerkiksi uusien tutkimuskysymysten esittämistä, sillä erinomaisen kirjallisuuskatsauksen on tarkoitus herättää kiinnostusta ja luo pohjaa tulevalle tutkimukselle (Ketchen & Craighead 2023). Innostaminen näkyy tässä tutkimuksessa erityisesti jatkotutkimusehdotuksissa, jotka esitellään luvussa 5.3. Kokonaisuudessaan tämä tutkimus pyrkii innostamaan tuomalla esiin näkemyksiä tietojärjestelmäriskien eroista eri tietojärjestelmätyyppien välillä, mikä luo pohjaa uusille näkökulmille ja tulevalle tutkimukselle.

Tutkimuksesta on löydettävissä kaikki erinomaisen kirjallisuuskatsauksen piirteet, mutta parannettavaakin löytyy. Tämän perusteella voidaan sanoa, että kirjallisuuskatsaus on laadullisesti hyvä, mutta aiheeseen voitaisiin vielä syventyä lisää esimerkiksi jossakin toisessa tutkimuksessa. Tutkimuksen laatua voidaan lisäksi perustella sillä, että siinä käytetyt kirjallisuuslähteet ovat pääosin vertaisarvioituja tieteellisiä artikkeleita tai konferenssijulkaisuja, jotka ovat melko tuoreita. Tutkimus perustuu siis luotettavaan tietoon, joka ei ole vanhentunutta. Lisäksi tutkimus on toistettava, sillä tutkimusmenetelmä on kuvattu selkeästi, ja hakulausekkeet sekä tutkimukseen valitut artikkelit esitellään työssä selkeästi. On huomautettava, että tutkimuksen luotettavuuteen voi vaikuttaa se, että perinteisten tietojärjestelmien riskeistä kirjallisuutta on löydetty vain vähän. Tämä on kuitenkin pyritty ottamaan huomioon tutkimuksen tuloksissa (ks. luku 5.1), minkä takia aisaa ei nähdä merkittävänä puutteena. Edellä esitettyjen perusteluiden nojalla voidaan sanoa, että tutkimus on luotettava ja se on kokonaisuudessaan toteutettu laadukkaasti.

5.3 Jatkotutkimusehdotukset

Tässä kandidaatintyössä keskityttiin tietojärjestelmäriskien tunnistamiseen ja vertailuun perinteisillä tietojärjestelmillä ja SaaS-tietojärjestelmillä. Koska tässä kandidaatintyössä tutkimus toteutettiin kirjallisuuskatsauksena, voi seuraava askel olla empiirisen tutkimuksen toteuttaminen kirjallisuuskatsauksen rinnalle. Empiirisessä tutkimuksessa voidaan tutkia esimerkiksi sitä, mitkä riskit realisoituvat yleisimmin organisaatioiden

arjessa, mikä toisi lisää näkökulmia erityisesti riskikategorioiden merkittävyyden tarkasteluun.

Myös jonkun tietyn tutkimuksessa esitellyn riskikategorian voi ottaa jatkotutkimuksen kohteeksi. Esimerkiksi tietoturvariskien syvällisempi tarkastelu on merkityksellistä, sillä se on tämän tutkimuksen perusteella suurin tietojärjestelmiä koskeva riskikategoria. Riskien vertailu yksityiskohtaisemmin ja syvällisemmin keskittyen ainoastaan yhteen riskikategoriaan voi tuottaa tuloksia, joihin tässä tutkimuksessa ei ylletty. Lisäksi yhteyksien löytäminen eri riskikategorioiden tai yksittäisten riskien välillä on arvokas aihe tutkimukselle, sillä näillä suhteilla voi olla vaikutusta esimerkiksi riskien merkittävyyden arvioinnissa.

Tässä tutkimuksessa keskityttiin erityisesti SaaS-palvelumallin tarkasteluun, joten jatkotutkimusta voidaan tehdä myös muiden palvelumallien osalta. SaaS-, PaaS-, ja IaaS-palvelumallien keskinäinen riskien vertailu on hyödyllistä esimerkiksi silloin, kun halutaan selvittää, mikä vaihtoehdoista on riskittömin. Tämän tutkimuksen avulla voidaan myös tarjota vielä kattavampi näkemys juuri pilvipohjaisten tietojärjestelmien riskeistä.

Tässä tutkimuksessa keskityttiin tietojärjestelmän toimintavaiheeseen liittyviin riskeihin, mutta myös muita tietojärjestelmän elinkaaren vaiheita on aiheellista tutkia. Esimerkiksi tietojärjestelmän käyttöönotto ja päivitykset voivat sisältää merkittäviä riskejä, joita ei tässä tutkimuksessa ole käsitelty. Riskejä elinkaaren eri vaiheissa voidaan tutkia niin perinteisillä tietojärjestelmillä kuin pilvipohjaisillakin tietojärjestelmillä. Myös riskien tarkastelu muiden sidosryhmien, kuten järjestelmätoimittajan näkökulmasta on aiheellista erityisesti SaaS-tietojärjestelmien kohdalla. Jatkotutkimuksissa voitaisiin tarkastella esimerkiksi sitä, miten toimittajat hallitsevat omia riskejään ja miten tämä vaikuttaa asiakasorganisaatioihin.

Riskienhallinta on jatkotutkimusaihe, joka täydentäisi tämän tutkimuksen tuloksia. Tässä tutkimuksessa tunnistettiin ja analysoitiin tietojärjestelmiin liittyviä riskejä, jolloin jatkotutkimuksessa voidaan tutkia keinoja näiden riskien hallitsemiseksi. Riskienhallintaa voidaan tutkia kirjallisuuskatsauksena, jolloin voidaan esimerkiksi etsiä erilaisia riskienhallintamalleja ja määrittää niistä sopivimmat perinteisille tietojärjestelmille ja SaaS-tietojärjestelmille löydettyjen riskien valossa. Lisäksi riskienhallintaa voidaan tutkia empiirisesti esimerkiksi kyselemällä organisaatioilta heidän riskienhallintastrategioistaan ja vertaamalla niitä kirjallisuudessa esiintyviin riskeihin.

LÄHTEET

Ahmad, I., Bakht, H. & Mohan, U. (2017). Cloud Computing–Threats and Challenges. Journal of computing and management studies. Vol.1(1)

Alter, S. (2001). Which Life Cycle – Work System, Information System, or Software? Communications of the Association for Information Systems. Vol.7(17). DOI: 10.17705/1CAIS.00717

Awati, R. (2024). What is an information system (IS). TechTarget. Available at (6.12.2024): https://www.techtarget.com/whatis/definition/IS-information-system-or-information-services

Chavan, J., Patil, R., Patil, S., Gutte, V. & Karande, S. (2022). A Survey on Security Threats in Cloud Computing Service Models. 6th International Conference on Intelligent Computing and Control Systems (ICICCS). Madurai, India. pp. 574–580. DOI: 10.1109/ICICCS53718.2022.9788148

Fink, A. (2014). Conducting Research Literature Reviews: From the Internet to Paper. 4. ed. Sage, Thousand Oaks.

Finto. (2024). Tietojärjestelmä. Hakemistossa Tietotermit. Saatavissa (25.10.2024): http://urn.fi/URN:NBN:fi:au:tt:t79

GeeksForGeeks. (2023). Information System Life Cycle – Software Engineering. Geeksforgeeks.org. Available at (9.12.2024): https://www.geeksforgeeks.org/software-engineering-information-system-life-cycle/

Geric, Z & Hutinski, Ž. (2007). Information systems security threats classifications. Journal of Information and organizational sciences. Vol.31(1). pp. 51–61.

Henry, S. & Ali, L. (2017). Cloud Computing Security Threats and Solutions. I-manager's Journal on Cloud Computing. Vol.4(2). pp. 1–8.

Hoodat, H. & Rashidi, H. (2009). Classification and Analysis of Risks in Software Engineering. World Academy of Science, Engineering and Technology. Vol.56.

Itewiki.fi. (2024). Mikä on pilvipalvelu. Itewiki.fi bloggaus. Saatavissa (10.12.2024): https://www.itewiki.fi/p/mika-on-pilvipalvelu

Ketchen, D.J. & Craighead, C.W. (2023). What constitutes an excellent literature review? Summarize, synthesize, conceptualize, and energize. Journal of Business Logistics. Vol.44(2). pp. 164–169. DOI: 10.1111/jbl.12339

Kofahi, N. & Al-Rabadi, A. (2018). Identifying the Top Threats in Cloud Computing and Its Suggested Solutions: A Survey. Advances in Networks. Vol.6(1). DOI: 10.11648/j.net.20180601.11.

Madaan, S., Arora, A.B. & Kaur, R. (2023). Cloud Computing Services Versus on-Premise Computing. In: Dhiman, V. & Dhand, P. (eds.) Emerging Trends in Engineering and Management. pp. 141–149. DOI: 10.56155/978-81-955020-3-5-16

Morgan, L. (2024). What is operational risk. TechTarget. Available at (25.11.2024): https://www.techtarget.com/searchsecurity/definition/operational-risk

Morrow, T., Pender, K., Lee, C., Faatz, D. & Richmond, N. (2019). Overview of Risks, Threats, and Vulnerabilities Faced in Moving to the Cloud. Technical report CMU/SEI-2019-TR-004. Software Engineering Institute, Carnegie Mellon University.

National Institute of Standards and Technology NIST. (2024a). Information System. Hakemistossa Computer Security Resource Center– Glossary. Available at (6.12.2024): https://csrc.nist.gov/glossary/term/information_system

National Institute of Standards and Technology NIST. (2024b). Information System Life Cycle. Hakemistossa Computer Security Resource Center– Glossary. Available at (6.12.2024): https://csrc.nist.gov/glossary/term/information_system_life_cycle

National Institute of Standards and Technology NIST. (2024c). Information System User. Hakemistossa Computer Security Resource Center– Glossary. Available at (6.12.2024): https://csrc.nist.gov/glossary/term/information_system_user

National Institute of Standards and Technology NIST. (2024d). Service Provider. Hakemistossa Computer Security Resource Center– Glossary. Available at (6.12.2024): https://csrc.nist.gov/glossary/term/service_provider

Nayan, N. M. & Zaman, H. B. (2009) Information System Development Model: Theories Analysis and Guidelines. First International Visual Informatics Conference IVIC. Kuala Lumpur, Malaysia. pp. 894–904.

Nguyen, M.T. & Khorev, P.B. (2019). Information risks in the cloud environment and cloud-based secure information system model. 2019 International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE). Moscow, Russia. pp. 1–6. DOI: 10.1109/REEPE.2019.8708845

Patel, K. & Alabisi, A. (2019). Cloud computing security risks: Identification and assessment. The Journal of New Business Ideas & Trends, Vol.17(2). pp. 11–19.

Pericherla, S. (2023). Cloud Computing Threats Vulnerabilities and Countermeasures: A State-of-the-Art. The ISC International Journal of Information Security. Vol.15(1). pp. 1–15. DOI: 10.22042/isecure.2022.312328.718

Sanastokeskus ry. (2018). Haavoittuvuus. Hakemistossa Tietotekniikan Termitalkoot. Saatavissa (6.11.2024): https://sanastokeskus.fi/tsk/fi/termitalkoot/haku-266.html

Sanastokeskus ry. (2023). Pilvipalvelu. Hakemistossa Tietotekniikan termitalkoot. Saatavissa (1.10.2024): https://sanastokeskus.fi/tsk/fi/termitalkoot/hakemistot-267.html?page=get_id&id=ID141&vocabulary_code=TSKTT

Sen, V.V., Hussein, S., Sumaru, M., Ali, S. & Ali, F. (2023). Cloud-Based Service versus On-Premise Services: A Comparative Study at a Local Organization in Fiji. 2023 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE). Nadi, Fiji. pp. 1-5. DOI: 10.1109/CSDE59766.2023.10487723

Sherer, S. & Alter, S. (2004). Information Systems Risks and Risk Factors: Are They Mostly About Information Systems. Communications of the Association for Information Systems. Vol.14. DOI: 10.17705/1CAIS.01402

Singh, G. & Parminder, P. (2017). Cloud Computing Risks and Benefits. nternational Journal of Advanced Research in Computer Science. Vol. 8(4).

Smith, H. A., McKeen, J. D. & Staples, S. (2001). New Developments in Practice I: Risk Management in Information Systems: Problems and Potential. Communications of the Association for Information Systems. Vol 7. DOI: 10.17705/1CAIS.00713

Subashini, S. & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications. Vol. 34 no 1. pp. 1-11. DOI: 10.1016/j.jnca.2010.07.006

Suomen riskienhallintayhdistys. (2024). Riskien luokittelu: Operatiivinen riski. Saatavissa (25.11.2024): https://pk-rh.fi/riskien-luokittelu/operatiiviset-riskit.html

Tieteen termipankki. (2024). Riski. Hakemistossa Tieteen termipankki. Saatavissa (25.11.2024): https://tieteentermipankki.fi/wiki/Kasvatustieteet:riski

Valtioneuvosto. (2023). Uhka. Hakemistossa Sisäisen turvallisuuden sanasto. Saatavissa (6.11.2024): https://valtioneuvosto.fi/documents/1410869/4024872/Sisaisen_turvallisuuden_sanasto.pdf/

Whitaker, J. & Thekdi, D. (2024). You cannot spell risk without “I-S”: The disclosure of information systems risks by Fortune 1000 firms. Risk Analysis. pp. 1–17. DOI: 10.1111/risa.17644

LIITTEET

Liite 1: Kirjallisuuskatsaukseen valitut artikkelit

Hakusana	Otsikko val kaikki kentät	Tietokanta	Lehti/julkaisu	Teos	Kirjoittaja(t)	Vuosi	Merkitsevyys tutkimuksen kannalta
"Information system risks" OR "Information system threats"	Otsikko	Andor	Risk Analysis – an international journal	You cannot spell risk without "I-S"	Whitaker & Thekdi	2024	Listaa tietojärjestelmiin liittyviä riskejä ja määrittelee viitekehyksen
"Cloud computing risks" OR "Cloud computing threats"	Otsikko	Andor	International Journal of Advanced Research in Computer Science	Cloud computing risks and benefits	Singh & Parminder	2017	Esittelee pilvipalveluiden riskejä sekä hyötyjä. Ei koske ainoastaan pilvipohjaisia tietojärjestelmiä, vaan pilvitekniologiaa yleisesti.
"Cloud computing risks" OR "Cloud computing threats"	Otsikko	Andor	The ISC International Journal of Information Security	Cloud Computing Threats, Vulnerabilities and Countermeasures: A State-of-the-Art	Pericherla	2023	Listaa pilvipalveluihin liittyviä uhkia ja haavoittuvuuksia. Määrittelee myös, mikä ero on uhalla ja haavoittuvuudella.
"Cloud computing risks" OR "Cloud computing threats"	Otsikko	Google Scholar	Journal of computing and management studies	Cloud Computing – Threats and Challenges	Ahmad et al.	2017	Listaa pilvipalveluiden tietoturvallisuusriskejä. Listauksessa on esitetty myös, mihin palvelumallin esitetty riski kuuluu sekä mihin turvallisuusattribuuttiin se liittyy.
"Cloud computing risks" OR "Cloud computing threats"	Otsikko	Google Scholar	Journal of New Business Ideas & Trends	Cloud Computing Security Risks: Identification and Assessment	Patel & Alabisi	2019	Esittelee turvallisuusriskejä pilvipalveluiden toimittajille, asiakkaille sekä valtionhallinnolle. Esittelee lisäksi eri palvelumalleihin kohdistuvia riskejä. Keskittyy
"Cloud computing risks" OR "Cloud computing threats"	Otsikko	Google Scholar	Advances in Networks	Identifying the Top Threats in Cloud Computing and Its Suggested Solutions: A Survey	Kofahi & Al-Rabadi	2018	Listaa suurimpia riskitekijöitä pilvipalveluissa ja esittelee muun muassa, mihin palvelumallin mikäkin riski kuuluvat ja mitä tietoturvallisuuden osa-aluetta ne uhkaavat.
"on-premises computing" AND (risk OR threat)	Kaikki kentät	Google Scholar	Emerging Trends in Engineering and Management (Kirja)	Cloud Computing Services Versus On-Premise Computing	Madaan et al.	2023	Vertailee pilvijärjestelmien ja paikallisten järjestelmien hyviä ja huonoja puolia. Pyrkii tarjoamaan näkemyksen siitä, kannattaako jonkin organisaation siirtyä pilveen.
"on-premises computing" AND (risk OR threat)	Kaikki kentät	Google Scholar	2023 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)	Cloud-based service versus On-Premise Services: A comparative study at a local organization in Fiji	Sen et al.	2023	Vertailee pilvijärjestelmiä ja paikallisia järjestelmiä Fijiläisessä organisaatiossa. Esittää sekä perinteisiin järjestelmiin liittyviä haasteita että pilvijärjestelmien tuomia riskejä.
"on-premises computing" AND (risk OR threat)	Kaikki kentät	Google Scholar	Teknінen raportti nro CMU/SEI-2019-TR-004. Carnegie Mellon University	Overview of Risks, Threats, and Vulnerabilities Faced in Moving to the Cloud	Morrow et al.	2019	Listaa pilvipohjaisele tietojärjestelmälle uniikkeja riskejä sekä kumpaankin tietojärjestelmätyyppiin kuuluvia riskejä. Esittelee yleisestä tasolta, miten riskit muuttuvat siirryttaessä perinteisestä tietojärjestelmästä pilvipohjaiseen tietojärjestelmään.
"Cloud-based information system" AND (risk OR threat)	Kaikki kentät	Google Scholar	2019 International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE).	Information risks in the cloud environment and cloud-based secure information system model	Nguyen & Khorev	2019	Esittelee mallin tietoturvalliselle pilvijärjestelmälle esitellen samalla tietoturvariskejä pilvipohjaisissa tietojärjestelmissä.

Liite 2: Kirjallisuudesta löydetyt perinteisiin tietojärjestelmiin kohdistuvat riskit

	sisäisestä tekijästä aiheutuvat riskit	Lähde	ulkoisesta tekijästä aiheutuvat riskit	Lähde
Teknologiariskit	Järjestelmällä voi olla rajoitettu käytettävyys/saatavuus, eli	Sen et al 2023	Luonnonkatastrofit tai terrorismi voi vahingoittaa teknologiaa	Whitaker & Thekdi 2024
	järjestelmään pääsee sisälle rajoitetusti			
	Järjestelmää ei enää vastaa tarpeita ja sitä täytyy uudistaa:	Sen et al 2023	Uudet teknologiat, jotka ajavat uudistamaan järjestelmää	Whitaker & Thekdi 2024
	perinteinen järjestelmä ei niin skaalautuva			
	Järjestelmän kaatuminen	Whitaker & Thekdi 2024		
Tietoon liittyvät riskit			yritykset eivät ehkä pysty noudattamaan täysin tietosuojaan ja	Whitaker & Thekdi 2024
			tietojen siirtoon liittyviä lakeja	
Ihmisiin liittyvät riskit	Järjestelmän kompleksisuus rasittaa IT henkilöstöä	Morrow et al. 2019		
Liiketoimintaprosesseihin liittyvät riskit	jatkuva kunnossapitovaatii resursseja, organisaatio itse	Sen et al. 2023	Järjestelmän toimitusketjun vaarantuminen palveluntarjoajan	Morrow et al. 2019
	vastuussa näiden toteutumisesta		hyödyntämien kolmansien osapuolien takia	
	Resursseja ja prosesseja organisaation vastuulla	Shaina et al. 2023	Toimittajariippuvuus: haastava vaihtaa palveluntarjoajaa	Morrow et al. 2019
Tietoturvariskit	Sisäinen uhka eli "malicious insider threat"	Morrow et al. 2019	Varastetut tunnukset: ulkoinen hyökkääjä pääsee käsiksi	Morrow et al. 2019; Whitaker
			järjestelmään	& Thekdi 2024
	Datan menettäminen muusta syystä, kuin hyökkäyksen takia	Morrow et al. 2019	Tietomurrot	Whitaker & Thekdi 2024
	Huolimattomuus järjestelmän käytössä lisää	Morrow et al. 2019		
	kyberturvallisuusriskejä			
	Käyttäjän virhe	Whitaker & Thekdi 2024		

punaisella on merkitty ne riskit, jotka ovat riskejä myös SaaS-järjestelmissä, mutta korostuvat perinteisissä järjestelmissä

sinisellä on merkitty riskit, jotka eivät esiinny SaaS-teitojärjestelmissä vaan ainoastaan perinteisissä tietojärjestelmissä

Liite 3: Kirjallisuudesta löydetyt SaaS-tietojärjestelmiin kohdistuvat riskit

	sisäisestä tekijästä aiheutuvat riskit	Lähde	ulkoisesta tekijästä aiheutuvat riskit	Lähde
Teknologiariskit	Järjestelmä ei enää vastaa tarpeita ja sitä täytyy uudistaa	Sen et al. 2023	Järjestelmä täysin riippuvainen internetyhteydestä	Singh & Parminder 2017
			Uudet teknologiat, jotka ajavat uudistamaan järjestelmää	Whitaker & Thekdi 2024
Tietoon liittyvät riskit			Järjestelmän data ei ole yhteensopivaa muun organisaation datan kanssa	Ahmad et al. 2017
			Tietojen todellinen sijainti: Monissa maissa säädöksiä sille, missä data saa todellisuudessa sijaita	Ahmad et al. 2017; Nguyen & Khorev 2019; Patel & Alabishi 2019
			Datan epäjohdonmukaisuus	Ahmad et al. 2017
			Organisaatio menettää kontrollin datasta	Morrow et al. 2019; Sen et al. 2023
			yritykset eivät ehkä pysty noudattamaan täysin tietosuojaan ja tietojen siirtoon liittyviä lakeja	Whitaker & Thekdi 2024
Ihmisiin liittyvät riskit	Järjestelmän kompleksisuus rasittaa IT henkilöstöä	Morrow et al. 2019		
Liiketoimintaprosesseihin liittyvät riskit			Organisaatio menettää kontrollia joistakin järjestelmän operaatioista	Morrow et al. 2019
			Tietojärjestelmätoimittajan konkurssi tai muusta syystä johtuva liiketoiminnan loppuminen (voi johtaa myös datan menettämiseen pahimmassa tapauksessa)	Ahmad et al. 2017; Nguyen & Khorev 2019
			Riittämätön tuki järjestelmän käyttöön palveluntarjoajalta	Nguyen & Khorev 2019
			Järjestelmän toimitusketjun vaarantuminen palveluntarjoajan hyödyntämien kolmansien osapuolien takia	Morrow et al. 2019
			Haasteet kolmannen osapuolen auditoinneissa, koska datakeskukset sijaitsevat maantieteellisesti eri paikoissa	Ahmad et al. 2017
			Käyttökatkot järjestelmässä (uhkaavat myös datan käytettävyyttä)	Ahmad et al. 2017
			Toimittajariippuvuus: haastava vaihtaa palveluntarjoajaa	Morrow et al. 2019
Tietoturvariskit	Sisäinen uhka eli "malicious insider threat"	Ahmad et al. 2017; Kofahi & Al-Rabadi 2018; Morrow et al. 2019; Pericherla 2023	Varastetut tunnukset: ulkoinen hyökkääjä pääsee käsiksi järjestelmään. Tunnuksien varastaminen tapahtuu usein esim. phishing- tai social engineering hyökkäyksellä. Tähän riskiin liittyy myös identiteettivarkaus.	Ahmad et al. 2017; Kofahi & Al-Rabadi 2018; Morrow et al. 2019; Pericherla 2023; Sen et al. 2023; Whitaker & Thekdi 2024
	Datan menettäminen: Erityisesti jostakin muusta syystä, kuin hyökkäyksen takia	Ahmad et al. 2017; Kofahi & Al-Rabadi 2018; Morrow et al. 2019; Pericherla 2023	Haavoittuvuudet sovellusrajapinnoissa (API) aiheuttavat tietoturvariskejä, sillä ne ovat julkisesti saatavilla	Ahmad et al. 2017; Kofahi & Al-Rabadi 2018; Morrow et al. 2019; Pericherla 2023
	Salausavaimen menettäminen	Nguyen & Khorev 2019	Eristysvirhe (isolation failure) eli hyökkääjä pääsee käsiksi organisaation tietoihin toisen organisaation järjestelmän kautta	Morrow et al. 2019
	Huolimattomuus järjestelmän käytössä lisää kyberturvallisuusriskejä (insufficient Due Diligence)	Ahmad et al. 2017; Kofahi & Al-Rabadi 2018; Morrow et al. 2019; Pericherla 2023	Heikentynyt kyky varmistaa datan turvallinen poistaminen (Morrow et al. 2019). Hyökkääjän on mahdollista palauttaa sensitiivistä poistettua tietoa (Ahmad et al. 2017).	Ahmad et al. 2017; Morrow et al. 2019
	Luvattomien pilvipalvelujen käyttö: voi johtaa lisääntyneisiin haittaohjelmatartuntoihin tai tietojen poissuodattamiseen (exfiltration?)	Morrow et al. 2019	Tietomurrot	Ahmad et al. 2017; Kofahi & Al-Rabadi 2018; Pericherla 2023; Sen et al. 2023; Whitaker & Thekdi 2024
	Riittämättömät välineet ja menetelmät turvallisuuden varmistamiseen	Pericherla 2023	Tietojen pitäminen erillään: toimittajan vastuulla on säilyttää eri asiakasorganisaatioiden data erillään toisistaan	Nguyen & Khorev 2019; Patel & Alabishi 2019
	Järjestelmän käyttäjä ei ota itse riittävästi vastuuta järjestelmän turvaamisesta	Pericherla 2023	Tiedon eheyden valvonta palvelunntarjoajan vastuulla, sillä asiakasorganisaatio ei pysty hallinnoimaan dataansa	Nguyen & Khorev 2019
	Käyttäjän virheet / Inhimilliset virheet uhkaavat järjestelmän tietoturvallisuutta	Pericherla 2023; Whitaker & Thekdi 2024		
	Organisaatiolla ei ole kykyä arvioida palveluntarjoajan luotettavuutta.	Singh & Parminder 2017	Palvelunestohyökkäys	Kofahi & Al-Rabadi 2018; Pericherla 2023
			Pilvijärjestelmän hyödyntämästä **"jaetusta teknologiasta"** johtuvat haavoittuvuudet, kuten esimerkiksi side-channel hyökkäykset	Ahmad et al. 2017; Singh & Parminder 2017; Kofahi & Al-Rabadi 2018; Pericherla 2023
			Heikko tunnistautumisen ja pääsyoikeuksien hallinta, hallinta toimittajan vastuulla	Ahmad et al. 2017; Kofahi & Al-Rabadi 2018; Nguyen & Khorev 2019; Patel & Alabishi 2019; Pericherla 2023
			Haavoittuvuudet järjestelmässä tai sovelluksissa altistavat hyökkäyksille (Kofahi & Al-Rabadi 2018). Esimerkiksi bugeja vaikea tunnistaa, sillä järjestelmät niin suuria kokonaisuuksia (Ahmad et al. 2017). Esim Botnet-isännöinti eli bot-haittaohjelmien pääsy koneille johtuu usein haavoittuvuuksista ohjelmistoissa (Singh & Parminder 2017)	Ahmad et al. 2017; Singh & Parminder 2017; Kofahi & Al-Rabadi 2018
			Haavoittuvuudet verkossa altistavat hyökkäyksille (Patel & Alabishi 2019) Esim. Advanced Persistent Threats (APTs) eli verkon kautta tapahtuvat hyökkäykset (Kofahi & Al-Rabadi 2018; Pericherla 2023)	Kofahi & Al-Rabadi 2018; Patel & Alabishi 2019; Pericherla 2023
			Tietovuodot	Ahmad et al. 2017
			Salakuuntelu: ulkoinen taho pääsee käsiksi dataan verkon kautta tapahtuvan siirron aikana	Ahmad et al. 2017
			Virtuaalikoneiden haavoittuvuudet altistavat haittaohjelmille, kuten VM-pohjaisille rootkiteille	Singh & Parminder 2017
			Epäluotettava palveluntarjoaja voivat rikkoa asiakkaan tietojen turvallisuutta (esim hyödyntämällä niitä markkinointiin tai jälleenmyyntiin)	Singh & Parminder 2017
			Tietoturvariskit riippuvat pitkälti toimittajan määrittelemistä käyttöehdoista ja tietosuojakäytännöistä	Singh & Parminder 2017
			Lunnasohjelmat	Pericherla 2023
			Laitteistotason haavoittuvuudet, joiden avulla hyökkääjät voivat päästä käsiksi samassa asuvien käyttäjien tietoihin	Pericherla 2023
			Pääsy dataan rajoittuu lukuisien turvallisuusmenettelyiden takia	Patel & Alabishi 2019

punaisella on merkitty ne riskit, jotka ovat riskejä myös perinteisissä järjestelmissä, mutta korostuvat entisestään SaaS-järjestelmissä

sinisellä on merkitty riskit, jotka eivät esiinny perinteisissä järjestelmissä, vaan ainoastaan SaaS-järjestelmissä