Atakan Ak

ISO/IEC 27001 -sertifioinnin oikeudellinen merkitys SaaS-ympäristön riskienhallinnassa

Laskentatoimen ja rahoituksen
akateeminen yksikkö
Talousoikeus
Kandidaatin tutkielma

Vaasa 2026

VAASAN YLIOPISTO
Laskentatoimen ja rahoituksen akateeminen yksikkö

Tekijä:	Atakan Ak
Tutkielman nimi:	ISO/IEC 27001 -sertifioinnin oikeudellinen merkitys SaaS-ympäristön riskienhallinnassa
Tutkinto:	Kauppatieteiden kandidaatti
Oppiaine:	Talousoikeus
Työn ohjaaja:	Mika Kärkkäinen
Valmistumisvuosi:	2026 **Sivumäärä:** 30

TIIVISTELMÄ:
Digitalisaation nopea kehitys on muuttanut yritysten toimintaa ja lisännyt pilvipohjaisten palveluiden, erityisesti SaaS-ratkaisujen, käyttöä. Näissä palveluissa käsitellään usein suuria määriä asiakas- ja henkilötietoja, mikä tekee tietoturvasta olennaisen osan yritysten riskienhallintaa. Yksi keskeisimmistä tietoturvan hallintaa ohjaavista standardeista on ISO/IEC 27001, joka tarjoaa rakenteen tietoturvan suunnittelulle, riskien tunnistamiselle ja jatkuvalle kehittämiselle.

Vaikka sertifiointi ei ole lakisääteinen vaatimus, se toimii tärkeänä osoituksena siitä, että organisaatio hoitaa tietoturvaansa systemaattisesti ja kansainvälisten käytäntöjen mukaisesti. SaaS-ympäristöissä ISO/IEC 27001 -sertifiointi tukee myös lakisääteisten velvoitteiden, kuten GDPR:n, noudattamista sekä helpottaa asiakkaiden kanssa käytäviä sopimusneuvotteluja ja due diligence -prosesseja. Sertifiointi tekee organisaation toimintatavoista läpinäkyvämpiä ja auttaa hallitsemaan myös alihankkijoihin ja muihin kolmansien osapuolten toimijoihin liittyviä riskejä.

Tutkielman perusteella ISO/IEC 27001 -sertifiointi on hyödyllinen työkalu SaaS-palveluiden oikeudellisessa riskienhallinnassa, mutta se ei yksin riitä täyttämään kaikkia tietosuojan ja sääntelyn vaatimuksia. Organisaation on täydennettävä sertifiointia omilla arvioillaan ja tilanteeseen sopivilla riskienhallintatoimilla.

AVAINSANAT: ISO/IEC 27001, SaaS, tietoturva, riskienhallinta

Sisällys

1 Johdanto

1.1 Tutkielman toteuttaminen

Digitalisaation kiihtymisen myötä yritysten liiketoimintarpeet ja mahdollisuudet ovat muuttuneet. Yhä useampi yritys siirtyy hyödyntämään erilaisia pilvipalveluita sekä ottaa käyttöönsä SaaS-ratkaisuja (Software as a Service) (Kim, Jang & Yang, 2017). SaaS-palvelut ovat pilvipohjaisia ohjelmistoratkaisuja, joita tarjotaan internetin kautta, ilman että tarvitsee asentaa niitä omalle tietokoneelleen. SaaS-palvelujen käyttöönottaminen on nopeaa, ne skaalautuvat hyvin erilaisten yritysten käyttöön, koska palveluntarjoaja pystyy konfiguroimaan näitä asiakkaan tarpeiden mukaiseksi, sekä palveluntarjoaja pystyy jatkuvasti päivittämään näitä ohjelmistoja. Ohjelmistoja pystyy käyttämään eri laitteilla ja ovat sijainnista riippumattomia. Yritykset, jotka ottavat käyttöön SaaS-palveluja, joutuvat yleensä luovuttamaan palveluntarjoajalle arkaluonteisia tietoja, tämän takia heidän tulee luottaa siihen, että tietoja käsitellään turvallisesti ja sääntelyvaatimusten mukaisesti.

Tämän kehityksen myötä tietoturvasta on tullut entistä keskeisempi osa yritysten liiketoimintaa. Tätä varten on kehitetty useita standardeja, joista tämän tutkimuksen kulmakivistä oleva ISO/IEC 27001 on yksi keskeisimmistä kansainvälisistä tietoturvan hallintajärjestelmästandardeista (Disterer, 2013). ISO 27001 standardi tarjoaa viitekehyksen, jolla yritykset voivat rakentaa ja ylläpitää heidän tietoturvan hallintajärjestelmää (ISMS). Vaikka sertifiointi ei ole lainsäädännöllinen vaatimus, se on kansainvälisesti tunnustettu työkalu yrityksille tietoturvan hallintaan ja kehittämiseen.

SaaS-palveluiden ympäristössä riskienhallinta ei rajoitu pelkästään yritysten sisäisiin tietoturvakontrolleihin, vaan ulottuu myös kolmansien osapuolten hallintaan. Palvelut hyödyntävät yleensä erilaisia toimittajia ja alihankkijoita, joten palveluntarjoajien on tiedettävä, että nämä kolmannet osapuolet sitoutuvat myös toimimaan tietoturvallisesti. Palveluntarjoajat, kolmannet osapuolet ja erilaiset tekniset alihankkijat muodostavat ekosysteemin, jossa yhdenkin toimijan virhe voi aiheuttaa merkittävän haavoittuvuuden

tietoturvaan (Culot et al., 2021). ISO 27001 -sertifioinnin avulla yritykset voivat hallita tästä ekosysteemistä muodostuneita riskejä. Tietoturvan hallintajärjestelmän kehittäminen vahvistaa yrityksen sisäisiä prosesseja. Sertifikaatti toimii samalla luottamuksen osoituksena asiakkaille ja yhteistyökumppaneille, siitä että yritys on sitoutunut noudattamaan korkeita tietoturvastandardeja ja jatkuvasti kehittämään omaa toimintaansa.

Koska sertifikaatti ei ole lain vaatima, sen merkitys riippuu siitä, miten yritykset voivat hyödyntää sitä operatiivisessa toiminnassaan. Erityisesti kiinnostavaa on tarkastella minkälainen vaikutus sertifikaatilla voi olla due diligence -prosessissa, kun asiakas tai yhteistyökumppani arvioi yrityksen tietoturvan tasoa ennen sopimuksen tekoa. Lisäksi sertifikaatilla voidaan täyttää ennakolta osa vaatimuksista, joka voi lyhentää sopimusneuvotteluprosessia. Tutkielmassani tulen tarkastelemaan miten ISO 27001 -sertifiointia voidaan hyödyntää SaaS-ympäristössä oikeudellisen riskienhallinnan välineenä.

1.2 Tutkielmakysymyksen tarkentaminen

Tietoturvan merkitys yrityksille jatkaa kasvamista digitalisaation edetessä. Sen alkuperäinen tarkoitus on ollut liiketoiminnan suojaaminen, mutta siitä on tullut myös kilpailuvaltti markkinoilla. Kyberuhkien määrä yrityksille on kasvanut, sekä samaan aikaan asiakkaiden turvavaatimukset ovat tiukentuneet, koska yritykset käsittelevät yhä enemmän asiakkaiden henkilötietoja ja muuta arkaluonteista dataa. Tämän vuoksi yritysten on kyettävä jatkuvasti kehittämään tietoturvaprosesseja.

Tutkielmani pääkysymys on, voidaanko ISO 27001 -sertifiointia pitää osana oikeudellista riskienhallintaa ja kolmansien osapuolten hallintaa SaaS-toimialalla. Alakysymyksinä tutkielmassa selvitän, mitkä ovat standardin keskeiset elementit tietoturvan hallinnan kannalta, millä tavoin sertifiointi tukee tietosuoja- ja sääntelyvaatimuksia. Tämän lisäksi

tutkin, miten sertifiointia voidaan hyödyntää osana due diligence -prosessia asiakas- ja alihankkijasuhteiden riskienhallinnassa.

1.3 Tutkielman rakenne

Tutkielmani tulee koostumaan edellä esittämästäni johdannosta, tietoturvan hallintajärjestelmien ja ISO 27001 -standardin esittelystä, oikeudellisesta viitekehyksestä, jossa käsittelen SaaS-yritysten sopimusoikeudellisia vastuita sekä keskeisiä sääntelykehyksiä, kuten GDPR. Aloitan tutkielmani teoreettisella taustalla, jossa käyn läpi ISO 27001 -standardin pääpiirteitä sekä SaaS-ympäristön keskeisiä elementtejä.

Tämän pohjustuksen jälkeen toteutan analyysin, missä yhdistän aikaisemmin mainitsemani teemat tutkimuskysymykseen. Tulen tarkastelemaan ISO 27001 -sertifioinnin merkitystä SaaS-yritysten käytännön riskienhallinnassa. Erityisesti tutkielmassani tarkastelen SaaS-yritysten ongelmaa, miten he voivat hyödyntää kyseistä sertifikaattia, voiko tämä toimia osoituskeinona GDPR:n noudattamisesta ja miten tämä toimii työkaluna kolmansien osapuolten hallinnassa.

Tutkimukseni rajautuu käsittelemään pääosin EU- ja Suomen oikeuslähteisiin, jotta tutkielmasta ei tulisi liian laaja-alainen. Tutkielmani rakentuu lainopillisesta näkökulmasta, jossa hyödynnän voimassa olevaa lainsäädäntöä, oikeuskirjallisuutta ja standardiin liittyviä julkaisuja. Näin muodostan kattavan kokonaiskuvan siitä, minkälainen ISO 27001 -sertifioinnin oikeudellinen merkitys on SaaS-yritysten riskienhallinnassa.

2 ISO/IEC 27001 -standardin merkitys SaaS-ympäristöissä

2.1 Tietoturvan hallintajärjestelmien kehitys

Tietoturvaa torjuttiin aikaisemmin yrityksissä ainoastaan teknisin keinoin, kuten palomuureilla, virustorjunnalla ja erilaisilla salauksilla. Näiden avulla pystyttiin torjumaan tietokoneisiin liittyviä tietoturvauhkia. Digitalisaation edistyessä on tajuttu, ettei tietoturva koske pelkästään teknisiä järjestelmiä, vaan se ulottuu yritysten jokaiseen eri osa-alueeseen, kuten prosesseihin, henkilöstöön ja johtamiseen. Tämä ei tarkoita, ettei teknisillä torjuntakeinoilla ole edelleen merkittävä vaikutus. Lisääntyneet tietoturvauhat ovat luoneet tarpeen tietoturvan hallintajärjestelmälle, joka toimii koko yrityksen johtamisjärjestelmänä (Disterer, 2013).

Yksi varhaisista yleisesti tunnetuista tietoturvastandardeista oli 1990-luvulla syntynyt BS 7799 -standardi (von Solms, 2005) ja se jakautui kahteen ohjeistavaan osaan. Ensimmäinen osa sisältää parhaat käytännöt tieturvan hallintaan (code of practice) ja toinen osa sisälsi vaatimuksia hallintajärjestelmälle rakentamisella ja kuinka sitä tulee ylläpitää. Erityisesti toisen osan uudistukset toimivat pohjana nykyiselle hallintajärjestelmälle, koska siinä tuotiin esille, että koko organisaatio kuuluu tietoturvan soveltamisalaan. BS 7799 -standardin kansainvälistymisen myötä alkoi rakentumaan pohja ISO/IEC 27001 -standardille. Näin syntyi myös uusi normi tietoturvan hallintajärjestelmä ISMS (Information Security Management System) (Disterer, 2013). Standardia on täydennetty myöhemmin ISO/IEC 27002 -kontrollioppaalla sekä ISO/IEC 27005 -standardille, joka keskittyy riskienhallintaan. Näistä standardeista muodostuu kansainvälisesti tunnustettu standardiperhe, mikä toimii viitekehyksenä tieturvan hallinnalle.

ISO/IEC 27001 on laajasti käytetty tietoturvastandardi. Standardin vahvuutena pidetään sen joustavuutta, kuinka se soveltuu eri kokoisille yrityksille, sekä useille toimialoille. Erityisesti toimialoilla, joissa sääntelyvaatimukset ovat erityisen tiukkoja hyödyntävät tätä sertifikaattia. Näitä ovat esimerkiksi finanssisektori ja julkishallinto. ISO 27001 -

standardi on myös merkittävä SaaS-toimialla, koska näihin ohjelmistoihin viedään jatkuvasti enemmän arkaluonteista dataa. Sääntely- ja sopimusvelvoitteiden tiukentuessa ISO 27001 -sertifikaatti toimii hyvänä osoituksena sidosryhmille sitoutumisesta turvallisuuteen (Culot et al., 2021).

2.2 ISO/IEC 27001 -standardin merkitys

Tässä osiossa käydään läpi yleisesti standardin merkitystä, tavoitteita ja hyötyjä. Lisäksi tarkastellaan sen asemaa osana ISO/IEC 27000 -sarjaa. ISO-standardiin on lisätty päivityksiä vuosina 2013 ja 2022, jotka ovat vahvistaneet standardin asemaa kansainvälisenä viitekehyksenä. Standardi päivittyy jatkuvasti vastaamaan uusia toimintaympäristön vaatimuksia. Tämän luvun tarkoituksen on luoda pohja tulevalle pohdinnalle, jossa käydään läpi miten ISO/IEC 27001 -standardi toimii SaaS-toimialalla osana riskienhallintaa.

2.2.1 Tavoitteet ja hyödyt

Distererin (2013) mukaan standardin päätavoite on luoda kansainvälisesti tunnustettu viitekehys, jonka avulla organisaatiot voivat tunnistaa, arvioida ja hallita tietoturvariskejä. Lisäksi standardin tavoitteena on ohjata organisaatioita implementoimaan tietoturvan hallinta osaksi yrityksen liiketoimintastrategiaa ja hallintajärjestelmää. Tietoturvan merkitys on kasvanut ja siitä koituvat uhat eivät ainoastaan kohdistu teknisiin toimintoihin, vaan koko organisaation osa-alueisiin. Standardi muokkaa organisaatioiden riskienhallintaa ja arjen prosesseja, eikä tietoturvaa nähdä vain teknisenä tukitoimintana

Kamilin, Lundin ja Islamin (2023) tutkimuksessa tarkasteltiin, miten ulkoiset sidosryhmät kokevat sertifikaatin omaavien organisaatioiden toiminnan. Tutkimuksessa tuli esille kahdeksan eri tavoitetta, joilla organisaatiot vastaavat kumppaneiden odotuksiin ja vahvistavat heidän luottamustaan. ISO 27001 -sertifikaatin omaavat yritykset nähdään

vastuullisina toimijoina, ja samalla heidän kilpailuasemansa vahvistuu, koska sertifiointi helpottaa sopimusvelvoitteiden ja sääntelyn noudattamisen osoittamista.

2.2.2 Minkälainen asema standardilla on osana ISO/IEC 27000 -perhettä

ISO/IEC 27001 on osa laajempaa standardiperhettä, mikä tunnetaan nimellä ISO/IEC 27000-sarja. Sarjassa jokaisella on oma roolinsa tietoturvan takaamiseen. ISO/IEC 27000 luo yleisesti alalla tunnetut käsitteet ja terminologian. Tunnetuin perheen standardeista on ISO/IEC 27001, joka asettaa vaatimukset tietoturvan hallintajärjestelmälle. Muita tunnettuja standardeja perheessä on ISO/IEC 27002 ja ISO/IEC 27005, joiden tehtävä on tarjota käytännön ohjeita tietoturvan hallitsemiseen ja riskienhallintaa (ISO/IEC 27000, 2018).

Tietoturvan hallinnan käytännön ohjeet ja suositukset tulevat ISO/IEC 27002:sta. Sen ohjeita organisaatiot voivat soveltaa täydentääkseen ISO/IEC 27001:n vaatimuksia. Erityisesti tämän standardi kattaa ohjeita esimerkiksi seuraavista organisaatioiden osa-alueista: tietoturvapolitiikan hallinta, henkilöstöön liittyvät toimenpiteet, fyysinen työympäristö ja pääsynhallintapolitiikan hallinta. Kyseinen standardi on päivitetty vuonna 2022, jonka myötä toimenpiteet jaettiin neljään kontrolliin: organisatoriset kontrollit, henkilöstöön liittyvät kontrollit, fyysiset kontrollit ja tekniset kontrollit. Puolestaan ISO/IEC 27005 tuo esille riskiperusteisen lähestymistavan tietoturvan hallinnalle. Organisaatioille tämä tarjoaa joustavan prosessin tietoturvan riskienhallinnalle. Joustavuudella tarkoitetaan tässä kontekstissa, sitä kuinka yritykset voivat itse määritellä heidän riskinsä ja kuinka näitä käsitellään. Standardi ei luo tarkkoja ohjeita, kuinka paljon yritykset saisivat kantaa riskejä, vaan yritykset päättävät tästä itse omien liiketoimintatarpeiden näkökulmasta. Standardi tarjoaa ainoastaan prosessin tietoturvariskien tunnistamiseen, arviointiin ja käsittelyyn (Taherdoost, 2021).

ISO/IEC 27001 on sarjan keskeisin sertifioitava hallintajärjestelmästandardi, ja yleensä organisaatioiden sertifiointi kohdistuu siihen. Muiden standardien tehtävä on tukea tätä, ja organisaatiot toteuttavat tietämättään muita standardeja, koska ne luodaan osaksi

organisaation hallintajärjestelmää, kun lähdetään sertifiointia hakemaan. Voidaan todeta, että ISO/IEC 27001:n asema standardiperheessä on toimia ydinstandardina, jota muut täydentävät.

2.3 Standardin rakenne ja keskeiset elementit

Jotta ISO/IEC 27001-standardin merkitys osana riskienhallintaa, tulee ymmärtää standardin rakenne. Standardin keskeisimpänä elementtinä pidetään riskienhallintaprosessia, jatkuvaa parantamista sekä kontrolleja ja liitteitä. Näiden avulla organisaatiot voivat muokata tieturvatoimenpiteensä vastaamaan omia liiketoimintatarpeitaan sekä osoittaa sääntelyvaatimusten noudattamista (ISO/IEC 27001, 2022).

2.3.1 Riskienhallintaprosessi

ISO/IEC 27001 -standardi edellyttää organisaatioiden integroimaan riskienhallintaprosessit osaksi liiketoiminnan ydinprosesseja. Organisaatioiden tulee tunnistaa, arvioida ja käsitellä tietoturvariskejä, joita toimintaympäristössä ilmenee ja suhteuttaa nämä liiketoimintatavoitteisiinsa. Riskienhallintaprosessi on jatkuva sykli, jonka tehtävänä on tehostaa toimenpiteitä ja kehittää riskien hallinta keinoja vastaamaan toimintaympäristöä. Käytännössä monet yritykset hyödyntävät esimerkiksi vuosikelloa, joka ohjaa riskien arviointia, auditointeja ja kehitystoimia osaksi organisaation vuosisuunnittelua. Tämä tukee standardin vaatimaa jatkuvan parantamisen periaatetta (Taherdoost, 2021).

Prosessi alkaa riskien tunnistamisella. Organisaatiot tunnistavat minkälaisia riskejä sen tietoihin, palveluihin, omaisuuksiin ja palveluihin kohdistuu. Seuraavaksi näille riskeille määritellään todennäköisyys, vaikutus ja jonkinlainen mittari miten se on tällä hetkellä käsitelty. Esimerkiksi jokin prosenttiasteikko voidaan asettaa riskeille ja tätä voidaan päivitellä vuosikellon asettamassa tahdissa. Organisaatiot saavat itse määritellä

riskinsietotasonsa ISO/IEC 27001 -standardin mukaan. Tämän takia standardi soveltuu eri toimialoille ja toimii kaiken kokoisissa organisaatioissa (Alberts & Dorofee, 2002).

Tøndelin, Linen ja Jaatunin (2014) artikkelin mukaan riskienhallinta on strateginen väline, jolla organisaatiot arvioivat, miten resursseja kohdennetaan tietoturvan hallintaa varten. Vaikka organisaatiolle olisi myönnetty ISO 27001-sertifikaatti jää vastuu silti organisaation johdolle, miten tietoturvan kehittämistä priorisoidaan ja minkälaiset resurssit sille varataan. Riskienhallintaprosessi tukee siten organisaation johdon päätöksentekoa ja auttaa varmistamaan, että tietoturvatoimet ovat linjassa yrityksen liiketoimintatavoitteiden kanssa.

2.3.2 Jatkuva parantaminen ja PDCA-malli

Harva yritys toimii stabiilissa toimintaympäristössä. Digitalisaation vauhdikas kehitys mullistaa organisaatioiden toimintaympäristöä ja tässä kehityksessä tietoturvan hallintajärjestelmän tulee pysyä mukana. ISO 27001 -standardi varmistaa, että hallintajärjestelmän kehittyy muutosten mukana. Standardiin sisältyy prosessi nimeltään PDCA-malli (Plan-Do-Check-Act). Mallin tarkoituksena on varmistaa, ettei tietoturvan hallinta jää ainoastaan yhden kerran projektiksi vaan siihen sitoudutaan ja sitä kehitetään jatkuvasti.

PDCA-malli jakautuu neljään vaiheeseen. Ensimmäinen vaihe (Plan) ohjaa organisaatioita suunnittelemaan tietoturvan hallintakeinot aikaisemmin tunnistettujen riskien perusteella. Toisessa vaiheessa (Do) suunnitelmat toteutetaan ja otetaan käyttöön. Kolmannessa vaiheessa (Check) arvioidaan, miten tietoturvan hallinnan toimenpiteet toimivat käytännössä. Viimeisessä vaiheessa (Act) organisaatio toteuttaa muutokset ja parannukset edellisessä vaiheessa ilmenneisiin havaintoihin. PDCA-malli on todettu tehokkaaksi työvälineeksi, koska se sitouttaa organisaation kehittämään tietoturvan hallintaa ja se auttaa integroimaan tietoturvan osaksi organisaation jokapäiväistä toimintaa (Hsu, Wang & Lu, 2016).

Osa ISO 27001 -sertifiointiprosessia on jatkuva parantaminen, jota seurataan säännöllisissä auditoinneissa. Näissä tarkastellaan, miten organisaatio ylläpitää ja kehittää hallintajärjestelmää vuosittain. PDCA-malli luo rakenteen, joka helpottaa organisaatioita prosessin seurannassa, ja sen avulla voidaan osoittaa sitoutuminen standardin luomiin vaatimuksiin sekä tietoturvan jatkuvaan kehittämiseen (ISO/IEC 27001, 2022).

2.3.3 Kontrollit ja liitteet (Annex A)

ISO/IEC 27001 -standardi sisältää liitteen A, joka kokoaa eri kontrollit, joilla hallitaan tietoturvaa. Liitettä voidaan pitää eräänlaisena ohjeistuksena organisaatioille, miten tietoturvaa sekä riskejä tulisi hallita konkreettisesti. Kontrollien tarkoitus on tukea organisaatioita integroimaan tietoturva osaksi päivittäistä toimintaa. Kuten aikaisemmin todettu kontrollit jaetaan neljään pääluokkaan: organisatoriset, henkilöstöön liittyvät, fyysiset ja tekniset kontrollit. Tämä jaottelu kattaa koko organisaation toiminnan eri osa-alueet (ISO/IEC 27001:2022, liite A). Alle on listattuna esimerkkejä kontrolleista:

- Organisatoriset kontrollit:
    - Tietoturvapolitiikan laatiminen
    - Riskien tunnistaminen ja hallinta
    - Tietoturvapoikkeamien käsittely
- Henkilöstöön liittyvät kontrollit:
    - Henkilöstön kouluttaminen
    - Käyttöoikeuksien ja roolien hallinta
- Fyysiset kontrollit:
    - Toimitilat ja niiden turvallisuus
    - Pääsynhallinta
- Tekniset kontrollit:
    - Järjestelmien valvonta
    - Tietojen salaus

Nämä ovat yleisesti sovellettuja kontrolleja, joita organisaatiot käyttävät tietoturvan hallinnan perustana (Tahir & Razali, 2018).

Tahir ja Razali (2018) painottavat artikkelissaan, että organisaatioiden tulee pystyä soveltamaan tietoturvaan liittyviä toimenpiteitä suhteessa liiketoimintaansa sekä kontrollien tehtävä on ohjata organisaatioita arvioimaan oman liiketoiminnan riskejä. Kontrollit eivät ole täysin velvoittavia vaan niiden soveltaminen määräytyy organisaation riskien ja liiketoiminnan perusteella. Kontrollit kytkeytyvät suoraan riskienhallintaprosessiin, PDCA-malliin ja organisaatioiden tulee pystyä osoittamaan mitä kontrolleja on valittu suhteessa riskeihin.

3 Oikeudellinen viitekehys SaaS-ympäristössä

Tässä luvussa tarkastellaan SaaS-toimintaympäristöä ja siihen liittyviä oikeudellisia velvoitteita, joita toimialan organisaatioilla on tietoturvan näkökulmasta. Lisäksi luvussa käsitellään miten ISO/IEC 27001 -sertifiointi toimii osana oikeudellista riskienhallintaa.

SaaS-palvelumallissa tietoturva kytkeytyy suoraan oikeudellisiin velvoitteisiin, koska palveluntarjoaja käsittelee tyypillisesti asiakkaan puolesta henkilötietoja ja muuta luottamuksellista aineistoa. Tällöin vastuu ei rajoitu teknisiin suojausratkaisuihin, vaan ulottuu myös sopimusjärjestelyihin sekä tietosuojalainsäädännön vaatimuksiin. Subashinin ja Kavithan (2011) mukaan SaaS-palveluihin liittyviä keskeisiä riskejä ovat erityisesti vastuunjako ja sopimusvelvoitteiden täyttämisen epäselvyydet palveluntarjoajan ja asiakkaan välillä. ISO/IEC 27001 -standardin mukainen sertifiointi voi toimia palveluntarjoajalle osoituskeinona siitä, että tietoturvan hallinta on järjestelmällistä ja auditoitua.

3.1 SaaS-ympäristön oikeudellinen perusta ja vastuut

Lyhyesti selitetty SaaS-palveluiden toimintamalli perustuu siihen, että palveluntarjoajat hallitsevat asiakkaidensa dataa pilvipalveluun rakennetussa ohjelmistossa. Palveluntarjoajat rakentavat ja ylläpitävät infrastruktuurin, jota he kehittävät vastaamaan asiakkaittensa tarpeita. Palveluiden konfiguroitavuus ja muokattavuus asiakkaiden tarpeiden mukaiseksi ovat merkittäviä syitä, miksi SaaS-palveluiden määrä on kasvanut merkittävästi digitalisaation myötä. Vastuu asiakkaiden datan hallinnasta on siirtynyt tämän myötä palveluntarjoajille (Subashini & Kavitha, 2011). Tämän seurauksena tietoturvan merkitys on muuttunut oikeudelliseksi ja sopimukselliseksi velvoitteeksi, jota hallitaan tietoturvan hallitsemisjärjestelmien avulla.

Pilvipalveluissa käsitellään usein monenlaista asiakasdataa, mutta erityisesti silloin, kun palveluun on syötetty asiakkaiden arkaluonteisia tietoja tai henkilötietoja, tietoturvan merkitys korostuu. Tikkinen-Piri, Rohunen ja Markkula (2018) korostavat

tutkimuksessaan, kuinka GDPR on muokannut tietoturvan merkitystä liiketoiminnassa. Osoitusvelvollisuus on kasvanut EU:n yleisen tietosuoja-asetuksen myötä, kun palveluntarjoajien on kyettävä osoittamaan, että asiakkaiden tiedot on suojattu asianmukaisesti. Asiakkaiden datahallinta luo palveluntarjoajille myös uudenlaisia riskejä, joita on kyettävä hallitsemaan vähintään asiakkaan vaatimusten mukaisesti. Osoitusvelvollisuuden korostumisen myötä ISO/IEC 27001 -sertifioinnilla pystytään osoittamaan, että tietoturvaa hallitaan asianmukaisin keinoin sekä riskienhallinta on otettu osaksi liiketoimintaa. Sertifikaatti luo asiakkaille luottamusta ja toimii kilpailuetuna markkinoilla

3.1.1 Vastuunjako ja tietoturvan oikeudellinen vastuu

Vastuunjako tietoturvasta SaaS-ympäristössä voi olla vaikea määritellä, jos sitä ei ole palvelusopimuksessa määritetty. Usein palvelusopimuksissa määritellään, että asiakas toimii rekisterinpitäjänä ja palveluntarjoaja rekisterinkäsittelijänä, jolloin saadaan jaettua vastuuta tietosuojalainsäädännön näkökulmasta. Vastuunjako pohjautuu shared responsibility -malliin, jolloin palveluntarjoajien vastuulla on palvelun tekninen turvallisuus, infrastruktuuri sekä käyttäjien kouluttaminen. Asiakkaalle jää puolestaan vastuu käyttöoikeuksien hallinnasta, sekä tietojen eheydestä ja luotettavuudesta (Cloud Security Alliance, 2023).

Palvelusopimuksissa vastuunjako jää usein epäselväksi, minkä vuoksi saattaa tulla oikeudellisia ristiriitoja erityisesti epäselvissä tilanteissa toteaa Järvinen ja Ruohonen (2020). Tietoturvaloukkausten ja palvelukatkosten yhteydessä saattaa syntyä sopimuksellinen epäselvyys siitä, miten vastuut palvelusopimuksessa on määritelty ja kenellä on vastuu vahingosta aiheutuneista seurauksista.

Tietoturvasta syntyvät oikeudelliset vastuut ulottuvat sopimusvelvoitteista laajemmalle. Organisaatioiden johdolla on huolellisuusvelvoite, jonka mukaan johdon tulee varmistaa, että sen toiminta täyttää oikeudelliset velvoitteet, tätä kutsutaan due diligence -periaatteeksi. Tämä velvoittaa johtoa tunnistamaan toimintaympäristössä olevia riskejä

ja hallitsemaan näitä asianmukaisesti. Tämä koskee myös tietoturvaan liittyviä riskejä. Humphreys (2008) toteaa, että organisaatioiden hallituksilla ja johdolla on vastuu tietoturvan hallitsemisessa. ISO/IEC 27001 -standardin mukainen hallintajärjestelmä auttaa johtoa seuraamaan ja kehittämään tietoturvaa ja se tukee myös tätä huolellisuusperiaatetta. Tietoturvaan liittyvissä oikeudellisissa ja sopimuksellisissa epäselvyyksissä standardilla pystytään osoittamaan huolellisuus tietoturvan hallinnassa.

3.1.2 Sopimusvelvoitteet ja ISO/IEC 27001:n rooli niiden tukena

SaaS-palvelusopimuksissa on olennaista määritellä tietoturvan taso sekä palvelutasot ja vastuut. Sopimusneuvotteluiden aikana arvioidaan palvelun kriittisyys asiakkaan liiketoiminnalle ja se, minkälaisia tietoja palvelussa käsitellään. Esimerkiksi toiminnanohjausjärjestelmä, joka on asiakkaalle liiketoimintakriittinen, edellyttää korkeaa palvelutasoa, koska järjestelmän häiriöt vaikuttavat välittömästi asiakkaan päivittäiseen toimintaan. Vastaavasti tietoturvan ja tietosuojan taso määritellään korkeaksi silloin, kun palvelussa käsitellään arkaluonteista dataa tai henkilötietoja.

Palvelusopimuksiin kirjataan tyypillisesti vahingonkorvausvastuut, tietoturvavaatimukset, palvelutasot (SLA) sekä tietosuojavelvoitteet, jotka yhdessä muodostavat sopimuksellisen viitekehyksen palveluntarjoajan ja asiakkaan vastuille. Tietoturvavaatimukset toimivat asiakkaalle keinona varmistua siitä, että palveluntarjoaja hallitsee tietoturvariskejä järjestelmällisesti. Pearsonin Yee'n (2013) korostavat, että pilvipalveluiden käyttäjät edellyttävät jatkuvasti enemmän läpinäkyvyyttä palveluntarjoajilta tietoturvan hallinnasta ja konkreettisia todisteita riskienhallinnasta.

Sopimusvelvoitteiden näkökulmasta ISO/IEC 27001 -sertifiointi tekee palveluntarjoajan tietoturvan ja riskienhallinnan rakenteen näkyväksi ja helpommin arvioitavaksi. Sertifiointi perustuu säännöllisiin ulkopuolisiin auditointeihin sekä dokumentoituihin kontrollikäytäntöihin, mikä voi vahvistaa asiakkaan luottamusta siihen, että tietoturvaan liittyviä vastuita hoidetaan johdonmukaisesti. Tämä on merkityksellistä erityisesti

tilanteissa, joissa joudutaan arvioimaan palveluntarjoajan huolellisuutta mahdollisten tietoturvaloukkausten tai sopimusvastuiden yhteydessä.

On kuitenkin tärkeää korostaa, ettei ISO/IEC 27001 -sertifiointi poista palveluntarjoajan oikeudellista vastuuta, vaan toimii osoituksena siitä, että organisaatio on ryhtynyt asianmukaisiin toimenpiteisiin riskien hallitsemiseksi ja integroinut tietoturvan osaksi ydintoimintaansa (Culot et al., 2021). Sertifiointi voi siten tukea palveluntarjoajan uskottavuutta sopimusneuvotteluissa ja due diligence -arvioinneissa sekä vähentää neuvottelujen transaktiokustannuksia, kun tietoturvan perustaso on jo lähtökohtaisesti todennettavissa (Monk & Munns, 2019).

3.2 Tietoturvaan liittyvät sääntelyvelvoitteet SaaS-ympäristössä

SaaS-palveluiden määrä on kasvanut pilvipohjaisten ratkaisujen yleistymisen myötä (Kim, Jang & Yang, 2017). Pilvipohja-alustoilla yritykset pystyvät säilyttämään suuria määriä liiketoimintakriittistä dataa kustannustehokkaasti, mikä on kasvattanut SaaS-palveluiden suosita. Kasvavan datamäärän myötä tietoturvan merkitys on korostunut ja se on kytkeytynyt yhä tiiviimmin lainsäädännön ja sääntelyn asettamiin vaatimuksiin. Teknisen turvallisuuden lisäksi SaaS-palveluntarjoajien tulee osoittaa, että palvelussa hallinnoitu data on suojattu asianmukaisesti ja että riskejä hallitaan järjestelmällisesti. Palveluissa käsitellään usein henkilötietoja, minkä vuoksi EU:n tietosuoja-asetus on keskeinen lainsäädännöllinen velvoite. Henkilötietojen käsittelyn ohella sääntely ulottuu myös tiedonsiirtoon, palvelun jatkuvuuteen ja sopimusvastuisiin. Tässä luvussa käsitellään keskeisiä sääntelyvelvoitteita ja sitä, miten ne muokkaavat SaaS-palveluntarjoajien tietoturvan hallintaa.

3.2.1 GDPR ja henkilötietojen käsittely SaaS-ympäristössä

Valtaosa SaaS-palveluista käsittelee henkilötietoja, minkä vuoksi GDPR muodostaa keskeisen sääntelykehyksen SaaS-ympäristössä. Tyypillisesti asiakas toimii rekisterinpitäjänä ja palveluntarjoaja henkilötietojen käsittelijänä, mikä korostaa GDPR:n 28 artiklan mukaista velvollisuutta varmistua käsittelijän riittävistä teknisistä ja

organisatorisista toimenpiteistä. Walden ja Michels (2022) korostavat, että GDPR:n osoitusvelvollisuus lisää vaatimuksia dokumentaatiolle ja läpinäkyvyydelle, mikä näkyy erityisesti pilvipohjaisissa palveluketjuissa. Tällöin ISO/IEC 27001 -sertifiointi voi toimia yhtenä yleisesti tunnistettuna osoituskeinona tietoturvan hallintajärjestelmän olemassaolosta.

Teknisen toteutuksen osalta GDPR luo myös vaatimuksia. Asetuksen 32 artiklan mukaan rekisterinpitäjän, että henkilötietojen käsittelijän tulee toteuttaa riittävät tekniset ja organisatoriset toimenpiteet, joilla suojataan henkilötietoja. Näihin kuuluvat esimerkiksi, pääsynhallinnan valvonta, lokitietojen kerääminen sekä salaukset tiedonsiirrossa. Pääsynhallinnan avulla varmistetaan, että henkilöt, joilla ei ole perusteltua tarvetta tarkastella henkilötietoja eivät pääse, näihin tietoihin käsiksi. Lokitietojen kerääminen on myös keskeistä, jotta voidaan jälkikäteen todentaa ketkä ovat tarkastelleet tai muokanneet henkilötietoja. Asetus luo rekisterinpitäjälle vastuun varmistaa, että käsittelijä täyttää edellyttämät vaatimukset, joka luo heille oikeuden auditoida palvelutarjoajan toimintaa. Tyypillisesti SaaS-palvelusopimuksissa on erikseen sovittu rekisterinpitäjän auditointioikeudesta. Tikkinen-Piri, Rohunen & Markkula (2018) korostavat tutkimuksessaan, että GDPR on kasvattanut osoitusvelvollisuus merkitystä, joka on lisännyt palveluntarjoajille painetta dokumentoida ja todentaa tietoturvatoimia entistä kattavammin, mikä on muodostunut yhdeksi keskeisistä haasteista SaaS-ympäristöissä.

SaaS-ympäristöissä riskien tunnistaminen ja hallinta ovat keskeisessä roolissa, koska palveluntarjoajat käsittelevät usein useiden asiakkaiden dataa samaan aikaan. Tämä lisää sekä teknisiä että organisatorisia vaatimuksia, ja siksi riskienhallinnan täytyy olla jatkuvaa ja huolellisesti suunniteltua. Merkittäviä riskejä SaaS-palveluntarjoajilla ovat tietoturvaloukkaukset -ja poikkeamat, jotka käsittelevät asiakkaiden dataa. GDPR:n artiklat 33 ja 34 käsittelevät henkilötietojen tietoturvaloukkauksia ja niiden ilmoittamisvelvollisuutta. Artiklojen mukaan käsittelijän tulee ilmoittaa viipymättä tietoturvaloukkauksesta rekisterinpitäjälle ja heillä tulee olla selkeät ja dokumentoidut

prosessit poikkeamien havaitsemisesta ja raportoinnista. Artikla 28 luo palveluntarjoajalle velvollisuuden tukea rekisterinpitäjää lakisääteisten velvollisuuksien täyttämisessä. Kun rekisterinpitäjä on saanut ilmoituksen tietoturvaloukkauksesta käynnistyvät heillä sisäiset prosessit, joita ovat esimerkiksi vaikutustenarviointi sekä mahdollisten rekisteröityjen tietopyyntöjen käsittely. Tämä tarkoittaa käytännössä sitä, että palveluntarjoajan vastuut ulottuvat teknisestä suojauksesta laajemmalle. Yhdessä nämä säännökset korostavat sitä, että teknisten toimenpiteiden lisäksi tarvitaan lisäksi organisatorisia toimenpiteitä ja nämä muodostavat perustan palveluntarjoajan tietoturvavelvoitteille.

4 ISO/IEC 27001 -sertifiointi SaaS-yritysten riskienhallinnan välineenä

Luvussa 4 tarkastellaan miten ISO/IEC 27001 -sertifiointi toimii käytännössä oikeudellisen riskienhallinnan välineenä SaaS-toimialalla. Aikaisemmin olen kuvannut standardin rakennetta sekä käynyt läpi SaaS-toimialan yleisiä käytänteitä läpi ja sääntely-ympäristöä. Tässä luvussa huomio kohdistuu erityisesti siihen, miten sertifiointi vaikuttaa sopimusneuvotteluihin ja niihin liittyviin due diligence -arviointeihin sekä siihen, miten sertifiointi tukee kolmansien osapuolien hallintaa. Samalla arvioidaan tilanteita joissa, sertifiointi voi olla riittävä keino täyttää sopimus- ja sääntelyvaatimukset, sekä niitä tilanteita, joissa se ei yksin riitä.

4.1 ISO/IEC 27001 due diligence -prosessissa

Due diligence -arviointi on olennainen osa riskienhallintaa ja sopimusneuvotteluja erityisesti SaaS-palveluissa, joissa asiakkaat arvioivat palveluntarjoajan tietoturvavalmiuksia ennen sopimusten allekirjoittamista. Olennaisimmat asiat, mitä arvioinneissa tarkastellaan, on se, miten palveluntarjoaja tunnistaa, hallitsee ja raportoi tietoturvariskejä sekä täyttääkö se sääntely- ja sopimusvelvoitteet. Sertifiointi edellyttää jatkuvia seuranta-auditointeja ja tieturvan hallintajärjestelmän kehittämistä, mikä tukee due diligence -prosessia ja mahdollistaa ulkopuolisen arvioinnin tietoturvan tasosta (Kiwa, n.d.). Suomessa ISO/IEC 27001 nähdään kilpailuetuna ja luotettavuuden osoituksena, mikä vahvistaa palveluntarjoajan asemaa sopimusneuvotteluissa ja arviointiprosessissa.

4.1.1 ISO/IEC 27001 osoituskeinona due diligence -arvioinnissa

Seuraavaksi tarkastelen tarkemmin, millä tavoin ISO/IEC 27001 -sertifiointi toimii konkreettisena osoituskeinona due diligence -arvioinnissa ja miten se vaikuttaa arviointiprosessin sisältöön. Due diligence -arvioinnin tarkoituksen on lisätä tietoisuutta

yrityksen sisäisistä prosesseista ja arvioida palveluntarjoajan kyvykkyyttä täyttää sille asetetut vaatimukset. SaaS-ympäristön näkökulmasta arviointi keskittyy siihen, miten se hallitsee asiakkaiden dataa, tunnistaa riskejä ja reagoi tietoturvapoikkeamiin.

ISO/IEC 27001 -sertifiointi toimii standardoituna osoituskeinona siitä, että palveluntarjoajan tietoturvan hallintajärjestelmän täyttää kansainväliset vaatimukset, hallintatoimenpiteet ovat dokumentoitu ja organisaatio on sitoutunut jatkuvaan parantamiseen. Sertifiointi vähentää tarvetta tehdä laajoja erillisiä selvityksiä due diligence -prosessin aikana ja tekee palveluntarjoajan tietoturvan arvioinnista systemaattisempaa ja selkeämpää (Behl & Behl, 2017).

Tutkimusten mukaan standardipohjaiset sertifioinnit lisäävät luottamusta erityisesti silloin, kun asiakas ei pysty itse arvioimaan palveluntarjoajan sisäisiä prosesseja kattavasti. Sertifiointi toimii tällöin signaalina organisaation kyvykkyydestä ja vastuullisuudesta tietoturvan hallinnassa (Spence, 1973). Tämä korostuu SaaS-ympäristössä, joissa asiakkaan näkyvyys palveluntarjoajan teknisiin ja organisatorisiin ratkaisuihin on rajallinen. Sertifioinnin ansiosta asiakkaat voivat keskittyä due diligence -arvioinnissa erityisriskeihin, kuten tietojen sijaintiin, alihankkijoihin ja poikkeamien hallintaan. Näin sertifiointi tehostaa due diligence -prosessia, kuitenkaan korvaamatta osapuolten omaa vastuunarviointia (Culot et al., 2021).

4.1.2 Sertifioinnin rajat due diligence -arvoinnissa

Vaikka ISO/IEC 27001 -sertifiointi toimii vahvana osoituskeinona palveluntarjoajan tietoturvan hallinnan tasosta, se ei kuitenkaan yksinään kata kaikkia due diligence -arvioinnissa tarkistettavia riskejä. Sertifiointi toimii osoituksena kattavasta kokonaisuudesta, mutta ei ota yksityiskohtaisesti kantaa palvelukohtaisiin tietosuojariskeihin (Culot et al., 2021). Esimerkiksi henkilötietoja käsittelevät korkean riskin asiakkaat edellyttävät tietosuojaa koskevaa vaikutustenarviointia (Data Protection Impact Assessment, DPIA). GDPR:n 35 artikla vaatii tätä arviointia, kun henkilötietojen käsittely aiheuttaa merkittävän riskin rekisteröityjen oikeuksille ja vapauksille (EU

2016/679, art. 35). DPIA arvio käsittelyn vaikutuksia yksilötasolla, kun taas ISO/IEC 27001 tarkastelee tietoturvaa organisatorisesta ja prosessilähtöisestä näkökulmasta. Tämän vuoksi sertifiointi ei korvaa DPIA:a, vaan toimii täydentävänä tekijänä due diligence -arvioinnissa (Walden & Michels, 2022).

Euroopan unionin kyberturvallisuusvirasto ENISA on todennut, että sertifioinnit ja standardit tukevat riskienhallintaa, mutta eivät poista tapauskohtaisten arviointien tarvetta, erityisesti pilvipalveluissa ja monimutkaisissa tietojenkäsittelyketjuissa (ENISA, 2021). ISO/IEC 27001 -sertifiointi helpottaa due diligence -prosessia, koska sen avulla ei tarvitse arvioida tietoturvan perusrakenteita alusta asti. Silti asiakkaiden on arvioitava palvelukohtaiset riskit ja sääntelyvaatimukset erikseen. Sertifiointi siis tukee arviointia tehokkaasti, mutta sen rajat tulevat esiin erityisesti silloin, kun käsitellään arkaluonteisia henkilötietoja tai toimintaan liittyy kohonnut tietosuojariski.

4.2 ISO/IEC 27001 kolmansien osapuolten ja alihankkijoiden hallinnassa

SaaS-ympäristössä tietoturvariskien hallinta ei ulotu ainoastaan yrityksen omiin prosesseihin, vaan ne ulottuvat paljon laajempaan kokonaisuuteen. Tämä laaja kokonaisuus koostuu kolmansista osapuolista ja alihankkijoista. Näitä ovat esimerkiksi pilvipohjaiset infrastruktuuripalvelut, ylläpitopalvelut ja integraatiokumppanit. Riippuvuus näistä kumppanuuksista tekee tietoturvariskien hallinnasta monimutkaista ja vaatii selvää vastuunjakoa.

Kolmansien osapuolten ja alihankkijoiden käyttäminen palvelun tuottamiseen muodostavat organisaatioille yhden merkittävimmistä haasteista, etenkin silloin kun palvelu rakentuu pilvipalvelualustalle ja sisältää monimutkaisia palveluketjuja kuten Arora, Buckley & Seitz, (2021) osoittavat. Riskit eivät kuitenkaan liity pelkästään teknisiin haavoittuvuuksiin, vaan ne voivat syntyä myös esimerkiksi puutteellisesta toimittajavalvonnasta, epäselvistä sopimuksista tai heikosta näkyvyydestä alihankintaketjuun. Tämä korostuu erityisesti SaaS-ympäristöissä, joissa palveluntarjoaja vaikuttaa usein asiakkaan näkökulmasta yhdeltä selkeältä toimijalta, vaikka taustalla

palvelua tuottaa joukko eri kumppaneita ja alihankkijoita. ISO/IEC 27001 -standardi tukee tällaisten riskien hallintaa edellyttämällä, että organisaatiot tunnistavat ulkoisiin toimijoihin liittyvät tietoturvariskit ja käsittelevät niitä osana omaa riskienhallintaprosessiaan. Käytännössä standardi ohjaa arvioimaan, miten toimittajat vaikuttavat organisaation tietoturvatavoitteisiin, ja valitsemaan sopivat kontrollit riskien vähentämiseksi. Tämä voi tarkoittaa esimerkiksi toimittajien riskiluokittelua, tietoturvavaatimusten kirjaamista sopimuksiin sekä toimittajien jatkuvaa seurantaa koko yhteistyösuhteen ajan.

Kaikkia toimittajia ei ole järkevää arvioida samalla tarkkuudella, vaan arvioinnin tulisi riippua esimerkiksi käsiteltävän datan luonteesta, palvelun kriittisyydestä ja mahdollisista sääntelyvaatimuksista (Torkura, Cheng & Meinel, 2019). Suurten pilvipalvelutoimittajien, kuten Microsoftin ja Amazon AWS:n, osalta arviointi perustuu usein laajasti saatavilla olevaan dokumentaatioon ja sertifiointeihin. ISO/IEC 27001 -standardi tarjoaa tähän selkeän viitekehyksen, jonka avulla SaaS-yritykset voivat rakentaa järjestelmällisen toimittajamallin ja osoittaa asiakkailleen, että ulkoisiin toimijoihin liittyvät riskit on tunnistettu ja otettu huomioon.

Suomessa kolmansien osapuolten hallinnan merkitystä on korostanut myös Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus, jonka mukaan organisaatioiden tulee kiinnittää huomiota toimittajavalintaan, selkeisiin sopimusehtoihin ja jatkuvan valvontaan (Kyberturvallisuuskeskus, 2023). Erityisesti tulisi kiinnittää huomiota siihen, ketkä alihankkijat osallistuvat palveluun, missä tietoja säilytetään ja miten poikkeamat tai häiriöt käsitellään. Näiden tekijöiden kautta ISO/IEC 27001 -sertifiointi toimii SaaS-yrityksille tärkeänä tukena, koska se auttaa rakentamaan dokumentoidun ja johdonmukaisen tavan hallita toimittajiin liittyviä riskejä ja vahvistaa samalla asiakkaiden luottamusta palvelun turvallisuuteen.

4.3 ISO/IEC 27001 -sertifioinnin rajat SaaS-yritysten riskienhallinnassa

Kuten on todettu, ISO/IEC 27001 -sertifiointi tarjoaa SaaS-palveluntarjoajille vahvan ja järjestelmällisen rakenteen tietoturvariskien hallintaan sekä tehostaa asiakkaiden kanssa käytäviä sopimusneuvotteluita, due diligence -arviointeja ja kolmansien osapuolten hallintaa. Organisaatio, jolla on kyseinen sertifiointi, pystyy osoittamaan, että tietoturvaan liittyvät riskit on arvioitu, keskeiset prosessit dokumentoitu ja toimintaa arvioidaan säännöllisesti ulkopuolisten auditointien avulla.

Sertifiointi ei kuitenkaan poista palveluntarjoajan vastuuta arvioida jatkuvasti omaa toimintaansa suhteessa muuttuvaan sääntely- ja uhkaympäristöön. Organisaatioiden onkin tunnistettava sertifioinnin rajat, erityisesti tilanteissa, joissa palvelussa käsitellään korkean riskin henkilötietoja, toimintaan sisältyy kansainvälisiä tiedonsiirtoja tai asiakkaan toimialasta johtuvia erityisiä sääntelyvaatimuksia, kuten finanssisektorilla. Tällaisissa tilanteissa pelkkä sertifiointi ei ole riittävä, vaan sitä on täydennettävä tapauskohtaisilla arvioinneilla, kuten tietosuojaa koskevalla vaikutustenarvioinnilla GDPR:n 35 artiklan mukaisesti (EU 2016/679, art. 35), kansainvälisiä tiedonsiirtoja koskevalla TIA-arvioinnilla tai asiakkaan suorittamilla lisäauditoinneilla.

Kokonaisuutena ISO/IEC 27001 tarjoaa SaaS-yrityksille tärkeän perustan riskienhallintaan, mutta sitä ei voi silti pitää kaikenkattavana ratkaisuna. Sertifioinnista on eniten hyötyä silloin, kun se liitetään osaksi laajempaa riskienhallinnan ja vaatimustenmukaisuuden kokonaisuutta, jossa huomioidaan sekä palvelukohtaiset erityispiirteet, asiakkaiden omat odotukset, että toimialaan liittyvät sääntelyvaatimukset. Aiempi tutkimus tukee tätä näkemystä ja korostaa, että standardit ja sertifioinnit toimivat hyvänä rakenteellisena tukena pilvipalveluissa, mutta eivät korvaa jatkuvaa, tapauskohtaista arviointia tai palvelun ympäristöön perustuvaa päätöksentekoa (Casola et al., 2019). Toisin sanoen standardi auttaa luomaan toimivan pohjan, mutta yrityksen täytyy silti tarkastella riskejä omassa kontekstissaan ja täydentää sertifiointia muilla arviointimenetelmillä.

5 Johtopäätökset

ISO/IEC 27001 -sertifioinnin merkitys SaaS-ympäristön riskienhallinnassa on moniulotteinen, joka ei ainoastaan rajaudu teknisiin toimenpiteisiin, vaan kytkeytyy myös oikeudelliseen toimintaympäristöön. SaaS-palveluissa käsitellään usein suuria määriä asiakkaiden dataa mukaan lukien henkilötietoja, ja palvelut ovat riippuvaisia laajoista toimittajaketjuista. Näistä syistä standardin rooli korostuu riskienhallinnan välineenä, sillä sen avulla organisaatiot voivat tunnistaa, arvioida ja hallita toimintaansa liittyviä riskejä järjestelmällisesti.

Tutkielman perusteella voidaan todeta, että ISO/IEC 27001 -sertifiointi toimii ennen kaikkea osoituskeinona siitä, että organisaatio huolehtii tietoturvastaan järjestelmällisesti. Vaikka sertifikaatti ei ole lainsäädännön edellyttämä, sen merkitys korostuu käytännössä erityisesti sopimusneuvotteluissa ja due diligence -prosesseissa. Sertifiointi helpottaa ja nopeuttaa sopimusneuvotteluita, erityisesti, kun asiakkaalle ei ole mahdollisuutta perehtyä syvällisesti yrityksen sisäisiin prosesseihin. Sertifiointi antaa sidosryhmille selkeän viestin siitä, että yritys noudattaa kansainvälisesti hyväksyttyjä tietoturvakäytäntöjä ja että sen toimintaa tarkastellaan säännöllisesti ulkopuolisten auditointien kautta.

GDPR on lisännyt palveluntarjoajien osoitusvelvollisuutta, sillä niiden on pystyttävä näyttämään toteen riittävät tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi. ISO/IEC 27001 -sertifiointi voi toimia tähän osoituskeinona, mutta ei yksin riitä täyttämään kaikkia sääntelyvaatimuksia eikä korvaa rekisterinpitäjän tai käsittelijän omia vastuita, kuten korkean riskin käsittelytilanteissa vaadittavaa vaikutustenarviointia. Siksi sertifiointi toimii täydentävänä työkaluna osana laajempaa oikeudellista riskienhallintaa, sopimusvastuiden hallintaa ja sääntelyn noudattamista. Digitalisaation ja pilvipalveluiden merkityksen kasvaessa tietoturvan rooli korostuu entisestään, minkä vuoksi ISO/IEC 27001 -sertifiointi tarjoaa organisaatioille rakenteellisen ja systemaattisen perustan riskien hallintaan.

Lähteet

Alberts, C., & Dorofee, A. (2002). Managing information security risks: The OCTAVE approach. Addison-Wesley.

Arora, A., Buckley, J., & Seitz, J. (2021). Third-party risk management in cloud ecosystems. Journal of Cybersecurity and Privacy, 1(2), 215–232.

Behl, A., & Behl, K. (2017). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

Casola, V., De Benedictis, A., Rak, M., & Villano, U. (2019). Security policy enforcement in cloud environments. Future Generation Computer Systems, 93, 290–306.

Cloud Security Alliance. (2023). Shared responsibility model. https://cloudsecurityalliance.org (Noudettu 3.10.2025)

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. The TQM Journal, 33(1), 76–105.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 4(2), 92–100.

ENISA. (2021). Cloud security certification and assurance. European Union Agency for Cybersecurity. https://www.enisa.europa.eu (Noudettu 18.10.2025)

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. Information Security Technical Report, 13(4), 247–255.

Hsu, C., Wang, T., & Lu, A. (2016). The impact of ISO 27001 certification on firm performance. Total Quality Management & Business Excellence, 27(9–10), 1085–1101.

International Organization for Standardization. (2018). ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. https://www.iso.org (Noudettu 18.12.2025)

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org (Noudettu 7.1.2026)

Järvinen, J., & Ruohonen, J. (2020). Pilvipalveluiden tietoturva ja vastuunjako. Informaatiotutkimus, 39(4), 1–18.

Kamil, M., Lundqvist, K., & Islam, S. (2023). Stakeholder trust and ISO 27001 certification. Computers & Security, 124, 102974.

Kim, G., Jang, S., & Yang, K. (2017). Analysis of SaaS adoption factors. Information Systems Management, 34(4), 1–12.

Kiwa. (n.d.). ISO/IEC 27001 certification and audits. https://www.kiwa.com (Noudettu 20.11.2025)

Kyberturvallisuuskeskus. (2023). Toimittajaturvallisuus ja alihankintariskien hallinta. Liikenne- ja viestintävirasto Traficom. https://www.kyberturvallisuuskeskus.fi (Noudettu 5.12.2025)

Monk, A., & Munns, A. (2019). Due diligence in information security management. Information & Computer Security, 27(5), 667–683.

Pearson, S., & Yee, G. (2013). Privacy and security for cloud computing. Springer.

Spence, M. (1973). Job market signaling. Quarterly Journal of Economics, 87(3), 355–374.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1–11.

Taherdoost, H. (2021). Understanding ISO 27001 risk management processes. International Journal of Information Security Science, 10(1), 1–12.

Tahir, M., & Razali, R. (2018). Information security controls implementation. International Journal of Advanced Computer Science and Applications, 9(9), 280–287.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134–153.

Tøndel, I., Line, M., & Jaatun, M. (2014). Information security incident management. Computers & Security, 45, 42–57.

Torkura, K., Cheng, F., & Meinel, C. (2019). Third-party risk management in cloud computing. Future Generation Computer Systems, 97, 1–15.

von Solms, R. (2005). Information security governance: COBIT or ISO 17799 or both? Computers & Security, 24(2), 99–104.

Walden, I., & Michels, J. (2022). Cloud computing and data protection. Oxford University Press.

Säädökset

European Parliament and the Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation).* https://eur-lex.europa.eu