Leo-Pekka Arponen

RISKIENHALLINNAN SUUNNITTELU JA TOTEUTUS ICT-ALAN ORGANISAATIOISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Arponen, Leo-Pekka
Riskienhallinnan suunnittelu ja toteutus ICT-alan organisaatioissa
Jyväskylä: Jyväskylän yliopisto, 2023, 70 s.
Kyberturvallisuus, Pro gradu -tutkielma
Ohjaaja(t): Siponen, Mikko

Riskienhallinta on olennainen osa organisaatioiden toimintaa, jonka avulla pyritään kasvattamaan oman toiminnan onnistumisen todennäköisyyttä. Useimmiten organisaatioiden riskienhallintaa ohjaa ISO 31000:2018 riskienhallinnan ohjeet. Riskienhallinnan ohjeiden, standardien sekä muiden parhaiksi havaittujen käytänteiden tarkoituksena on luoda edellytykset riskienhallinnan toteuttamiseksi. Erilaiset ohjeet ja standardit lähestyvät riskienhallintaa useiden näkökulmien ja metodien kautta, mutta tavoite on silti yhteinen, tehokas riskienhallinta. Tämän tutkielman tavoitteena oli kerätä tietoa ja selvittää, miten ICT-organisaatioiden tulisi toteuttaa riskienhallintaa ja kannattaisiko yleisesti sovellettujen ISO 31000:2018 riskienhallinnan ohjeiden lisäksi hyödyntää NIST SP 800-37r2 riskienhallinnan viitekehystä. Tutkimuksen teoreettisessa viitekehyksessä perehdyttiin riskienhallinnan keskeisiin käsitteisiin, teoriaperusteisiin sekä tutkielmassa käsiteltyihin riskienhallintamalleihin ja niiden vertailuun. Tutkimuksen empiirinen osuus toteutettiin laadullisin menetelmin. Aineisto kerättiin puolistrukturoiduilla haastatteluilla, joissa haastateltiin erään suomalaisen ICT-organisaation turvallisuusjohtajia. Aineisto analysoitiin aineistolähtöisellä sisällönanalyysillä. Tutkimuksen avulla pääteltiin riskienhallinnan ohjeiden ja viitekehyksen yhdistäminen mahdolliseksi, mutta tehokkaan riskienhallinnan huomattiin olevan sidoksissa ihmisiin ohjeiden sijasta.

Asiasanat: riski, riskienhallinta, riskienhallinnan viitekehys, riskienhallinnan ohjeet, ICT-organisaatiot

ABSTRACT

Arponen, Leo-Pekka
Risk management planning and implementation in organizations in the ICT industry
Jyväskylä: University of Jyväskylä, 2023, 70 pp.
Cyber Security, Master's Thesis
Supervisor(s): Siponen, Mikko

Risk management is an essential part of a functioning organization's activities to increase the likelihood of success. Most organizations' risk management is guided by the ISO 31000:2018 risk management guidelines. The purpose of risk management guidelines, standards, and other best practices is to create the conditions for implementing risk management. The various guidelines and standards approach risk management through different perspectives and methodologies, but the goal is still the same, effective risk management. The aim of this thesis was to gather information and to find out how ICT organizations should implement risk management and whether it would be worthwhile to use the NIST SP 800-37r2 risk management framework in addition to the generally applied ISO 31000:2018 risk management guidelines. In the theoretical framework of the study, the main concepts of risk management, theoretical foundations, and risk management models and their comparison were examined. The empirical part of the study was carried out using qualitative methods. The data was collected through semi-structured interviews with the security managers of a Finnish ICT organization. The data was analyzed using content analysis. The study concluded that it is possible to combine risk management guidelines and a framework, but effective risk management was found to depend on people rather than guidelines.

Keywords: risk, risk management, risk management framework, risk management guidelines, ICT organizations

KUVIOT

TAULUKOT

SISÄLLYS

KÄSITEHAKEMISTO

Haavoittuvuus (engl. vulnerability): NIST SP 800-37r2 riskienhallinnan viitekehyksessä haavoittuvuus määritellään CNSSI 4009 Committee on National Security Systems Instruction 4009 -ohjeen mukaisesti tietojärjestelmän tai tietoturvamenettelyjen, kuten sisäisen valvonnan tai toteutuksen heikkoukseksi, jota uhka voi hyödyntää.

Hallintakeino (engl. control): Toimenpide, joka säilyttää tai muuttaa riskiä (SFS-ISO 31000:2018).

ISO: International Organisation for Standardization on valtiosta riippumaton kansainvälinen organisaatio, jonka tarkoituksena on kehittää ja julkaista kansainvälisiä standardeja (ISO, 2023).

Jäännösriski (engl. remaining risk): Hallintatoimenpiteen jälkeen voimaan jäänyt riski, johon ei haluta vai voida vaikuttaa (Valtionvarainministeriö, 2017).

NIST: National Institute of Standards and Technology toimii yhdysvaltalaisen kauppaministeriön alaisena virastona, ja sen tehtävät keskittyvät standardien, tekniikan sekä mittaustekniikoiden kehittämiseen (NIST, 2022).

Riski (engl. risk): Epävarmuuden vaikutus tavoitteisiin (SFS-ISO 31000:2018, 2018).

Riskianalyysi (engl. risk analysis): Toimenpide, jonka tarkoituksena on ymmärtää riskin luonne, sen ominaisuudet ja tarvittaessa riskin taso (SFS-ISO 31000:2018, 2018).

Riskienhallinta (engl. risk management): Koordinoitua toimintaa, jolla organisaatiota johdetaan ja ohjataan riskien osalta (SFS-ISO 31000:2018, 2018).

Riskienhallintapolitiikka (engl. risk management policy): Koostuu organisaation päättämistä, kuvaamista ja dokumentoimista riskienhallinnan periaatteista ja tavoitteista (Valtionvarainministeriö, 2017).

Riskin lähde (engl. risk source): Tekijä, jolla on kyky joko yksinään tai muihin tekijöihin yhdistettynä aiheuttaa riski. (SFS-ISO 31000:2018, 2018).

Riskinottohalu (engl. risk appetite): Organisaation kyvykkyys, jonka se on valmis ottamaan pyrkiessään tavoitteisiinsa (Valtionvarainministeriö, 2017).

Riskinsietokyky (engl. risk tolerance): Organisaation sitoutuman riskin suuruus, johon se on valmis sitoutumaan riskien määrittelyn jälkeen (Valtionvarainministeriö, 2017).

SFS: Suomen Standardisoimisliitto (engl. Finnish Standards Association).

Sidosryhmä (engl. stakeholder): Henkilö tai organisaatio, joka voi vaikuttaa päätökseen tai toimintoon, tai johon jokin päätös tai toiminto voi vaikuttaa tai joku, joka kokee olevansa jonkin päätöksen tai toiminnon vaikutuksen kohteena (SFS-ISO 31000:2018).

Standardi (engl. standard): Julkaisu tai ohje, johon on kirjattu yhteisesti sovittuja vaatimuksia, suosituksia tai palvelukohtaisia ominaisuuksia (SFS, 2022).

Uhka (engl. threat): NIST SP 800-37r2 riskienhallinnan viitekehyksessä uhka määritellään NIST SP 800-30 mukaisesti miksi tahansa olosuhteeksi tai tapahtumaksi, joka voi vaikuttaa haitallisesti organisaation toimintaan, sen omaisuuteen, yksilöihin tai muihin organisaatioihin.

Vaikutustaso (engl. impact level): NIST SP 800-37r2 riskienhallinnan viitekehyksessä vaikutustaso määritellään FIPS 199 mukaisesti, pahimmaksi arvioiduksi tapauksen mahdolliseksi vaikutukseksi.

1 JOHDANTO

Organisaatioille riskienhallinta voi olla monimutkainen prosessi. Osa organisaatioista käsittelee riskienhallintaa pelkkänä pakollisena kulueränä, kun taas osa tunnistaa sen vahvuudeksi, joka tukee tietoperusteista päätöksentekoa tuottaen arvoa organisaatiolle. Avenin (2011) mukaan riskienhallinnan avulla organisaatioiden on mahdollista kartoittaa riskeistä koituvat mahdolliset hyödyt ja uhkat. Almeidan, Teixeiran, Mira da Silvan ja Faroleiron (2019) mukaan riskienhallintaa varten on kehitetty erilaisia standardeja ja riskienhallinnan viitekehyksiä riskien tehokkaan tunnistamisen, arvioinnin ja hallinnan suorittamiseksi. Useimmiten riskienhallinnan suunnittelua ja toteutusta ohjaa ISO 31000:2018 riskienhallinnan ohjeet, sillä niiden esitetään soveltuvan jokaisen organisaation käyttöön riippumatta organisaation koosta, toimintamallista, sijainnista ja tyypistä (SFS-ISO 31000:2018, 2018).

Jotta riskienhallinta olisi tehokasta, organisaatioiden on tunnistettava toimivansa monimutkaisissa ja toisiinsa yhteydessä olevissa tietotekniikkaympäristöissä, joissa käytetyt teknologiat ja järjestelmät voivat olla hyvinkin erilaisilla tasoilla (Pöyhönen, 2020). Standardit itsessään eivät johda onnistuneeseen riskienhallintaan ja Siposen (2006) mukaan akateeminen kirjallisuus onkin kritisoinut standardien olemassaolon vaikuttavan tärkeämmältä kuin niiden soveltamiselle käytössä olevat työkalut ja niiden saatavuus. Riskienhallinnan osalta johdon sitoutuminen ja riskienhallinnan sisällyttäminen osaksi kaikkia organisaation toimintoja koetaan erityisen tärkeäksi (SFS-ISO 31000:2018, 2018).

Tämän tutkielman aiheena oli riskienhallinnan suunnittelu ja toteutus ICT-alan organisaatioissa. Tutkielmassa käsitellyt ISO 31000:2018 riskienhallinnan ohjeet on valmisteltu riskienhallintaan keskittyvän Technical Committee ISO/TC 262, Risk management -teknisen komitean toimesta (ISO 31000:2018, 2018). Ohjeiden lisäksi tutkielmassa käsiteltiin NIST SP 800-37r2 riskienhallinnan viitekehystä, joka soveltuu erityisesti ICT-organisaatioiden ja tietojärjestelmien käyttöön. NIST (National Institute of Standards and Technology) on yhdysvaltalainen kauppaministeriön alainen virasto, jonka tehtävät keskittyvät standardien, tekniikan sekä mittaustekniikoiden kehittämiseen (NIST, 2022).

Tutkielman tavoitteena oli kerätä tietoa ja selvittää, miten ICT-organisaatioiden tulisi toteuttaa riskienhallintaa ja kannattaisiko yleisesti sovellettujen ISO 31000:2018 riskienhallinnan ohjeiden lisäksi hyödyntää NIST SP 800-37r2 riskienhallinnan viitekehystä. Tämä tutkielma antaa vastaukset seuraaviin kysymyksiin:

- *Miten riskienhallinta tulisi toteuttaa ICT-alan organisaatiossa?*
- *Miten ISO 31000:2018 riskienhallintamallin ohjeet ja NIST SP 800-37r2 riskienhallinnan viitekehys vertautuvat toisiinsa?*
- *Voiko ISO 31000:2018 riskienhallintamallin ohjeiden ja NIST SP 800-37r2 riskienhallinnan viitekehyksen yhdistäminen tehostaa riskienhallinnan suunnittelua ja toteutusta ICT-organisaatiossa?*

Tutkimus toteutettiin laadullisin menetelmin. Aineisto kerättiin puolistrukturoiduilla haastatteluilla ja analysoitiin hyödyntäen aineistolähtöistä sisällönanalyysiä. Haastatteluun valikoidut henkilöt olivat erään suomalaisen ICT-organisaation turvallisuusjohtajia. Tutkielma jakautui teoria ja empiria osioihin, joiden avulla pyrittiin vastaamaan tutkimusongelmaan.

Riskienhallinta itsessään on laajasti tutkittu aihealue. Aihealueen tutkimus käsittelee riskienhallintaa useiden näkökulmien kautta, kuten sen onnistumiseen vaikuttavia tekijöitä (Rampini, Takia & Berssaneti, 2019; Lalonde & Boiral, 2012; Kelly, 2022), riskienhallinnan uusia menetelmiä (Almeida, ym., 2019; Hardjomidjojo, Pranata & Baigorria, 2022) tai riskienhallinnan standardien ja muiden työkalujen ongelmia ja mahdollisuuksia (Aven, 2011; Björnsdóttir, Jensson, Boer & Thorsteinsson, 2022). Tässä tutkielmassa käsiteltiin kahden riskienhallinnan standardin yhdistämisen tuomia mahdollisuuksia. Vastaavan kaltaista aihetta ISO 27005 ja NIST SP 800-30r1 -standardien osalta ovat tutkineet Al-Fikri, Putra, Suryanto ja Ramli (2019).

Tutkielman ensimmäisessä sisältöluvussa aloitettiin teoreettisen viitekehyksen käsitteleminen. Luvussa tarkastellaan riskejä, riskienhallinnan standardeja sekä sitä, mistä standardit ylipäätään tulevat. Tämän lisäksi luvussa käsitellään riskienhallinnan roolia ICT-organisaatiossa ja sitä, kuka riskienhallinnasta on organisaatiossa vastuussa. Luvun loppuun on kirjoitettu lyhyt yhteenveto, jossa käsitellyt asiat sidotaan yhteen.

Tutkielman kolmannessa ja neljännessä luvussa jatkettiin teoreettisen viitekehyksen käsittelyä. Luvun kolme aikana esiteltiin tutkielmalle oleelliset ISO 31000:2018 riskienhallinnan ohjeet sekä NIST SP 800-37r2 riskienhallinnan viitekehys. Tämä pyrittiin tekemään kattavasti, jotta luvun neljä aikana oli mahdollista vertailla ISO 31000:2018 riskienhallintaprosessia ja NIST SP 800-37r2 riskienhallinnan viitekehystä. Vertailun keskeisimmät havainnot esitettiin taulukossa, jonka jälkeen esitettiin pohdintaa mallien samanaikaisen käytön mahdollisuuksista.

Viides luku käsitteli tutkimuksen toteutusta. Luvussa käsiteltiin tutkimuksen tavoitteet ja tutkimusmenetelmä. Luvussa esitettiin tutkimuksen aineis-

tonkeruumenetelmä sekä tutkimuksessa käytetty aineistolähtöinen sisällönanalyysin menetelmä. Luvun lopussa pohdittiin tutkimuksen luotettavuutta ja arviotiin sen eettisyyttä.

Kuudennessa luvussa avattiin tutkimuksen tulokset. Tulokset jaettiin kolmeen alalukuun, jotka vastasivat tutkielman yksittäisiin tutkimuskysymyksiin. Tutkimuksen tulokset muodostuivat sekä teorian että kerätyn aineiston pohjalta.

Tutkielman viimeisessä luvussa tehtiin tutkimuksen tuloksista yhteenveto. Tämän lisäksi esiteltiin mahdollisia jatkotutkimusaiheita ja tutkimukseen liittyviä rajoitteita. Tutkielmassa saavutetuista tuloksista pyrittiin muodostamaan selkeä kokonaiskuva.

2 RISKIENHALLINTA JA SEN STANDARDIT

Tässä luvussa tarkastellaan mitä riskienhallinta on ja mitä se merkitsee ICT-organisaatiossa. Luvussa myös esitellään erilaisia riskienhallinnan standardeja sekä standardien merkitystä. Luvun tarkoituksena on vastata tutkimuksen ensimmäiseen tutkimuskysymykseen *"Miten riskienhallinta tulisi toteuttaa ICT-alan organisaatiossa?"*. Tutkielmassa ICT-alan organisaatiolla tarkoitetaan tieto- ja viestintätekniikkaa tuottaviksi organisaatioiksi.

2.1 Riski

Jotta riskienhallintaa ja sen merkitystä on mahdollista käsitellä, on ensin määriteltävä, mitä riski itsessään tarkoittaa. Riski voidaan määritellä epävarmuuden vaikutukseksi tavoitteisiin, joka voidaan huomata esimerkiksi poikkeamana odotetusta (SFS-ISO 31000:2018). Epävarmuuden rooli on riskienhallinnan kannalta suuri, sillä se voi lisätä riskin potentiaalia sekä vaikuttaa päätöksiin ja toimenpiteisiin (Popov & Popov, 2022). Organisaatioiden näkökulmasta riskejä voidaan käsitellä tapahtumina, jotka voivat aiheuttaa tappioita organisaatiolle (Ghita, Sokolov & Bakhshi, 2021). Vastaavasti, myös riski, jota organisaatio ei kykene tunnistamaan, voi aiheuttaa organisaatiolle vakavia seurauksia (Gorzen-Mitka, 2013).

Riskille tyypillisesti myös poikkeamalla on kaksi puolta. Poikkeama voi olla sekä myönteinen että kielteinen, mahdollisesti myös molempia, sillä poikkeamat voivat avata uusia mahdollisuuksia ja uhkia (SFS-ISO 31000:2018). Koska riskeillä on kaksi puolta, organisaatiot joutuvatkin usein pohtimaan, kannattaisiko heidän ottaa riski, pyrkiessään tavoitteisiinsa. Valtionvarainministeriön (2017) mukaan, tällainen kyvykkyys määritellään riskinottohaluksi. Organisaatiot tai ihmiset yleisesti eivät välttämättä halua ottaa riskejä, mutta joissakin tapauksissa riski on otettava tavoiteltaessa uutta mahdollisuutta tai pyrittäessä suoritustavoitteeseen (Bruce, Lyon, Kadampi & Popov, 2022). Ostromin ja Wilhelmsenin (2019) mukaan ISO 31000:2018 mukaisen riskienhallintamallin im-

plementointi tukee organisaatiota erityisesti riskin mahdollisuuksien ja negatiivisten vaikutusten punnitsemisessa.

Mahdollisia tapoja riskin ilmaisemiseksi on useita, ja riskienhallinnan alalla termi saa useimmiten kvantitatiivisen merkityksen (Boholm, Möller & Hansson, 2016). Walker (2013) esittää riskin olevan tulo tapahtumien todennäköisyydestä ja niiden lopputuloksesta, mutta Covertin ja Nielsenin (2005) mukaan riskejä voidaan laskea myös asteikolla korkea, keskitasoinen tai matala. SFS-ISO 31000:2018 (2018) tarjoaa kattavamman näkökulman, jonka mukaan tavallisesti riskit ilmaistaan riskin lähteiden, mahdollisten tapahtumien, niiden seurausten sekä näiden todennäköisyyksien yhdistelmänä. Myös NIST SP 800-37r2 käytetty määritelmä esittää riskin olevan mitta, joka tarkastelee riskin olosuhteiden tai tapahtumien sattuessa syntyvien haitallisten vaikutusten ja tapahtumien todennäköisyyttä (Ross ym., 2018).

Riskin lähteenä tarkoitetaan tekijää, jolla on yksin tai muihin tekijöihin yhdistettynä kyky aiheuttaa riski. Tapahtumalla tarkoitetaan tiettyjen olosuhteiden esiintymistä tai muutosta, ja se voi itsessään olla riskin lähde. (SFS-ISO 31000:2018 2018.) Tällaisia muutoksia ovat esimerkiksi kilpailusta, globalisaatiosta tai sääntelystä johtuvat olosuhteiden muutokset (Choo & Goh, 2015).

Seurauksella tarkoitetaan tavoitteisiin vaikuttavan tapahtuman tulosta, joka voi olla esimerkiksi varmuus tai epävarmuus. Seuraukset ovat laadullisesti ja määrällisesti ilmaistavia ja niiden vaikutukset voivat kasvaa. Todennäköisyys kuvaa jonkin tapahtuman toteutumismahdollisuutta ja se voidaan määritellä, mitata tai määrittää laadullisesti, määrällisesti, objektiivisesti, tai subjektiivisesti. Tämän lisäksi se voidaan kuvata yleisellä tasolla tai matemaattisesti, esimerkiksi tietyn ajanjakson ajalta. (SFS-ISO 31000:2018 2018.)

2.2 Riskienhallinta

Dionnen (2019) mukaan riskienhallinnan tutkimus alkoi toisen maailmansodan jälkeen ja nykyaikaisen riskienhallinnan alkuperä sijoittuu vuosien 1955–1964 välille. Kaksi ensimmäistä riskienhallintaa käsittelevää teosta ovat Mehrin ja Hedgesin (1963) sekä Williamsin ja Hemsin (1964) kirjoittamat teokset. Teokset käsittelevät puhtaasti riskienhallintaa, eivätkä sisällä esimerkiksi taloudellisia riskejä. Teosten myötä insinöörit aloittivat riskienhallintamallien kehittämisen. (Dionne, 2019) Gordonin ja Loebin (2002) mukaan useita ylemmän tason riskienhallinnan ja tietoturvallisuuden malleja on kehitetty myös resurssien kohdentamista varten. Resurssien kohdentaminen tähtää tulojen lisäämiseen tai kustannusten vähentämiseen, ja ne perustuvatkin riski- ja kustannusnäkökohdilta odotettuihin voittoihin (Menon & Siponen, 2020).

Nykyaikaiset määritelmät riskienhallinnalle ovat varsin laajoja ja niihin sisältyykin ajatus järjestelmällisestä toiminnasta, joka perustuu kehitettyjen mallien noudattamiseen. SFS-ISO 31000:2018 (2018) määrittelee riskienhallinnan koordinoiduksi toiminnaksi, jolla organisaatiota johdetaan ja ohjataan riskien osalta. Valtiovarainministeriön (2021) mukaan riskienhallinta tarkoittaa koordi-

noitua, systemaattista ja jatkuvaa toimintaa, jonka avulla riskejä voidaan tunnistaa, analysoida, arvioida, käsitellä ja seurata. Valtionvarainministeriön käyttämän määritelmän lisäksi Pöyhönen (2020) lisää korjaavat toimenpiteet riskienhallintaan kuuluvaksi toimenpiteeksi.

Määritelmien eroavaisuuksista huolimatta riskienhallinta on pohjimmiltaan kokonaisuus toimenpiteitä, jolla pyritään lisäämään oman onnistumisen todennäköisyyttä. Riskienhallinnan toimenpiteet luovat siis suotuisat lähtöasetelmat, jonka perusteella voidaan tehdä päätös riskin ottamisesta tai sen ottamatta jättämisestä. Valtionvarainministeriö (2017) esittää riskienhallinnan tarkoituksen olevan mahdollistava tekijä organisaation menestymiselle, toiminnan jatkuvuuden takaamiselle ja tavoitteiden saavuttamiselle. Riskienhallinnantoimenpiteiden hyödyt tapahtuvat useimmiten pitkällä aikavälillä. Tämä voi myös vaikuttaa negatiivisesti riskienhallinnan priorisointiin, sillä se vääristää päättäjien kannustimia tehdä tulevaisuuteen kohdistuvia riskienhallintainvestointeja, varsinkin niiden korkeiden ennakkokustannusten takia. (Hallegatte & Rentschler, 2014.)

2.2.1 Standardit

Riskienhallinnassa, kuten myös yleisestikin, standardit ovat julkaisuja tai ohjeita, joihin on kirjattu yhteisesti sovittuja vaatimuksia, suosituksia tai palvelukohtaisia ominaisuuksia (SFS, 2022). Tämän perusteella standardien voidaan ajatella olevan käytäntöjä, jotka ovat yhteisesti sovittuja ja hyväksyttyjä. Myös TEPA-termipankki (2022) määrittelee standardin toistuvien ongelmien ratkaisuja esittäväksi asiakirjaksi.

Pohjimmiltaan standardien tarkoituksena on siis helpottaa ja yhdenmukaistaa suoritettavia toimenpiteitä standardille sovellettavassa toimintaympäristössä. SFS:n (2022) mukaan standardien käyttö on vapaaehtoista, mutta useimmiten suositeltavaa. Organisaatiot voivat myös edellyttää yhteistyökumppaneiltaan jonkin standardin käyttöä, jotta he voivat osoittaa toimivansa yhteisesti sovittujen periaatteiden mukaisesti (von Solms, 1999). Vaatimusten lisäksi standardien käyttöä perustellaan usein niiden hyödyllä, sillä standardit parantavat yhteensopivuutta ja turvallisuutta, jolloin myös riskit vähenevät (SFS, 2022).

Standardien käyttö ei kuitenkaan ole täysin ongelmatonta. Akateemisessa kirjallisuudessa standardeja on kritisoitu esimerkiksi siksi, että standardien olemassaolo vaikuttaa tärkeämmältä, kuin itse standardin soveltamiselle käytössä olevien työkalujen käyttö ja saatavuus (Siponen, 2006). Björnsdóttir, Jensson, Thorsteinsson, Dokas ja Boer (2022b) osoittavat kritiikkiä ISO 31000:2018 standardia kohtaan myös siksi, että standardissa ei viitata tieteelliseen kirjallisuuteen, vaan muihin ISO-standardeihin, parhaisiin käytänteisiin sekä harvoin myös riskienhallinnan tekniikoihin ja käsikirjoihin. Organisaatiot voivat myös kohdata institutionaalisia paineita omaksua standardien ja parhaat käytänteet hallitakseen riskejä (Niemimaa & Niemimaa, 2019).

Myös Björnsdóttir, ym. (2022a) esittävät, että organisaation sertifioituessa riskienhallintastandardin käyttöön, ne ovat täysin riippuvaisia standardin laa-

dusta, jotta riskienhallintaa voidaan suorittaa tehokkaasti. ISO 31000:2018 riskienhallinnan standardi on kuitenkin tarkoitettu yleiseksi ohjeeksi riskienhallintaa varten, eikä sen tarkoituksena ole johtaa organisaation sertifiointiin (Björnsdóttir, ym., 2022b).

2.2.2 Riskienhallinnan standardit ja ohjeistukset

Aihealueena riskienhallinta on erittäin laaja. Siksi onkin loogista, että riskienhallinnalle on aihe- ja toimialuekohtaisia standardeja ja ohjeistuksia. Esimerkiksi SFS-ISO 27005:2013 (2013) sekä NIST SP 800-39 ovat standardeja, joiden soveltamisalat keskittyvät tietoturvariskien hallintaan. Toinen esimerkki toimialakohtaisesta standardista on ISO 14971:2019 (2019) standardi, joka käsittelee lääkinnällisten laitteiden terminologiaa, periaatteita ja niiden riskienhallintaa. Esimerkkinä riskienhallinnan ohjeistuksesta toimii julkisen hallinnon digitaalisen turvallisuuden johtoryhmän tuottama riskienhallintaohje, joka on suunnattu erityisesti ministeriöiden, virastojen sekä muiden julkisenhallinnon laitosten käyttöön (Valtionvarainministeriö, 2017).

Yksityiskohtaisten ja aihealueelle spesifien standardien lisäksi on olemassa standardeja, joiden vaatimusten täyttämiseksi ei ole vain yhtä oikeaa tapaa toimia. Esimerkiksi SFS-ISO 31000:2018 (2018) standardi riskienhallinnan ohjeista on organisaation sovellettavissa ja sen esitetäänkin olevan hyödynnettävissä kaikilla toimialoilla.

Almeidan ym. (2019) sekä Jennexin ja Durcikovan (2020) mukaan riskienhallinnan standardit sekä viitekehykset ovat kehitetty tehostamaan riskien tunnistamista, arvioimista ja niiden hallintaa. Organisaation tehtäväksi kuitenkin jää standardissa esitettyjen ohjeiden hyödyntäminen ja muokkaaminen sen omille käyttötavoille sopivaksi. On myös mahdollista, että organisaatiot hyödyntävät riskienhallinnassaan muitakin standardeja tai ohjeita, joiden tarkoituksena on antaa konkreettisia esimerkkejä riskienhallinnan suorittamisesta.

2.2.3 Organisaatiot standardointien takana

Standardisoinnista vastaavia organisaatioita on useita ja ne voivat toimia sekä kansallisesti että kansainvälisesti. Euroopassa yksi tunnetuimmista standardisointiorganisaatioista on ISO, International Organization for Standardization. ISO on valtiosta riippumaton kansainvälinen organisaatio. Organisaatioon kuuluu 168 standardointielintä ja sen tavoitteena on kehittää kansainvälisiä standardeja, jotka tukevat innovaatioita ja tarjoavat ratkaisuja globaaleihin haasteisiin. (ISO, 2022.) ISO-standardien valmistelutyö tapahtuu yleensä teknisten komiteoiden kautta, mutta työhön osallistuvat myös valtiolliset ja valtiosta riippumattomat järjestöt sekä kansainväliset järjestöt.

Suomessa SFS, eli Suomen Standardisoimisliitto toimii standardisoinnin keskusjärjestönä ja käytännön standardointityö tehdään yhteistyössä toimialoja edustavien organisaatioiden kanssa standardisointiryhmissä. Standardisointiryhmien esitetään seuraavan alansa eurooppalaista ja maailmanlaajuista standardisointia ja osallistuvan standardien kommentointiin ja laadintaan. Suomes-

sa voimassa olevista standardeista 97 % on kansainvälistä alkuperää, ja suomalaiset standardit tehdäänkin usein kansainvälisten standardien tueksi tai tarpeen mukaan vain Suomessa käytettäviksi. (SFS, 2022.)

ISO standardisointiorganisaation lisäksi toinen laajasti vaikuttava organisaatio on Yhdysvaltain kauppaministeriön alainen NIST, The National Institute of Standards and Technology. Yhdysvaltain kongressi perusti NIST:in alun perin kehittämään maan teollisuuden kilpailukykyä, mutta nykyisin NIST:in tietotaito tukee kehitystä lähes kaikilla teknologian tasoilla. (NIST, 2022.) Nykyisin NIST:in visio onkin toimia maailman johtavana kriittisten mittausratkaisujen luojana ja standardien edistäjänä, johon he pyrkivät innovaatioita ja kilpailukykyä edistämällä.

2.3 Riskienhallinta ICT-organisaatiossa

Organisaatioiden näkökulmasta onnistunutta riskienhallintaa voidaan pitää yhtenä menestystekijänä. On kuitenkin todettava, että onnistunut riskienhallinta ei tapahdu itsestään tai vain sokeasti standardeja sekä parhaita käytänteitä seuraamalla. Farrelin ja Gallagherin (2014) organisaatioiden riskienhallinta koostuu riskien tarkkailemisesta, analysoinnista ja niiden hallinnasta sekä samalla riskien mahdollisista suhteista, jotta organisaation riskinottohalua on mahdollista optimoida. Organisaation riskienhallinta on täynnä haasteita ja organisaatioissa kohdatut riskit ovat riippuvaisia sen sosiaalisesta kontekstista (Schiller & Prpich, 2014). Tsohoun, Karydan, Kokolakiksen ja Kiountouziksen (2006) mukaan riskien tunnistaminen ja arviointi on sekä inhimillistä että sosiaalista toimintaa. Nykyinen vahva uskomus on kuitenkin se, että riskienhallinta tarjoaa riittävän työkalun mahdollisuuksien kartoittamiseen, sekä tappioiden ja katastrofien välttämiseen (Aven, 2011).

Organisaatioiden riskienhallinnan tavoitteena on luoda viitekehys, jonka avulla riskejä ja epävarmuutta on mahdollista käsitellä. Riskien tunnistamis-, arviointi– ja hallintaprosessin on myös oltava osa organisaation strategiaa ja kehitystä. (Dionne 2019, s. 7.) SFS-ISO 31000:2018 (2018) mukaan ylimmän johdon ja hallituksen tulisikin varmistaa, että riskienhallinta sisällytetään kaikkiin organisaation toimintoihin. Toisaalta organisaation riskienhallinnassa tarkoituksena on toimia päätöksenteon tukena ja näin lisätä toiminnallisten ja strategisten tavoitteiden saavuttamisen todennäköisyyttä (McShane, 2017).

Myös Valtionvarainministeriö (2021) yhtyy näkemykseen, jossa riskienhallinta kuvataan osaksi johtamisen ja toiminnan prosesseja sekä suunnittelua ja seurantaa. Johtamisen ohella riskienhallinnan kuitenkin muistutetaan koskettavan organisaation jokaista työntekijää, joka yksinkertaisimmillaan voi tarkoittaa esimerkiksi sitä, että työntekijä havaitsee poikkeaman ja ilmoittaa tästä omalle esimiehelleen (Valtionvarainministeriö, 2017). Jotta työntekijätkin osaisivat noudattaa riskienhallinnan kannalta toivottuja periaatteita organisaatiot pyrkivät luomaan sisäisiä riskienhallintapolitiikkoja ja ohjeita, joissa kuvataan toimintatavat esimerkiksi riskin välttämiseksi.

Organisaation asettamaa riskienhallinnan toimintamallia tulee myös soveltaa sitä käyttävän organisaation toimintamallin mukaisesti, sillä riskienhallinnan keskeinen tavoite on tukea tietoperusteista päätöksentekoa tuottamalla tietoa ja analyysiä epävarmuuden vaikutuksesta organisaation tavoitteisiin. Riskienhallinnan tarjoama tuki päätöksenteossa ulottuukin aina yksittäisestä hankkeesta, koko organisaation strategiaan liittyvään päätöksentekoon. (Valtionvarainministeriö, 2021.)

Riskienhallinnan tavoitteiden saavuttamiseksi päätöksentekoa tukevan tiedon tulee olla sekä relevanttia että monipuolista, mutta myös oikea-aikaisesti saatavilla. (Valtionvarainministeriö, 2021). Tiedot on mahdollista saada riskianalyysin avulla, jonka tarkoituksena on selvittää ne tasapainotetut toimet, joilla uhkia ja mahdollisuuksia hallitaan. Toimintakulttuuri, prosessit sekä rakenteet, jotka edesauttavat mahdollisuuksien toteutumista ja joiden avuilla hallitaan haitallisia tapahtumia sisältyvät kaikki osaksi riskienhallintaa (Valtionvarainministeriö, 2017).

Riskienhallinnalle oleellista on myös sen avoimuus sekä kattavuus, sillä tämä mahdollistaa riskien tunnistamisen ja tiedostamisen sekä huolehtimisen siitä, että organisaation eri tasoilla olevat päätöksentekijät, asiantuntijat sekä sidosryhmät tietävät riskeistä (Valtionvarainministeriö, 2017). Riskienhallinnalle oleellista on myös sisäinen valvonta, jonka tarkoituksena on varmistaa organisaation talouden ja toiminnan laillisuus, tuloksellisuus, varojen ja maisuuden turvamaminen sekä oikeat tiedot organisaation taloudesta ja toiminnasta. Esitettyä toimintaa voidaan valvoa sisäisten tarkastusten avulla, joiden tehtävänä on selvittää johdolle sisäisen valvonnan riittävyys ja asianmukaisuus. (Valtionvarainministeriö, 2017.)

Usein riskienhallinnan ajatellaan vain aiheuttavan kuluja organisaatiolle, vaikka sen toiminta onkin täysin päinvastaista, esimerkiksi tunnistamalla riskeihin sisältyviä mahdollisuuksia. Rampini, ym. (2019) myös esittävät, että riskienhallinnan tarkoitus ei ole jokaisen organisaation havaitseman riskin eliminoiminen. Käsiteltäessä riskienhallintaa on myös huomioitava, että riskienhallinnasta muodostuu dataa ja informaatiota, jota organisaatioiden tulisi hyödyntää tiedolla johtamisessa. Riskienhallinnan tuottaman lisäarvon on kuitenkin oltava havaittavissa organisaatiolle ja tämän vuoksi riskienhallinnan toteuttamisen kustannusten ja vaikutusten tuleekin olla mitattavissa (Valtionvarainministeriö, 2017).

2.4 Riskienhallintapolitiikka

Riskienhallintapolitiikka on organisaation sisäinen dokumentti. Riskienhallintapolitiikassa esitetään organisaation riskienhallinnan toimintamalli, suunnitelma tai toimintatapa. Toimintamallin laatimalla organisaation ylin johto ja hallitus osoittavat sitoutuneisuutensa riskienhallintaan. Riskienhallintaan sitoutumisesta tulee viestiä organisaation sisäisesti, mutta myös soveltuvin osin sidosryhmille. (SFS-ISO 31000:2018, 2018)

Useimmiten riskienhallintapolitiikkaa ohjaavat myös muut organisaation sisäiset turvallisuuden ohjeet. Vaikka organisaation muut ohjeet voivat vaikuttaa riskienhallintapolitiikan sisältöön, sen ydinajatuksena on silti tarkasti kuvastaa organisaation riskienhallinnan tavoitteita ja vastuita (Stefanova-Stoyanova & Danov, 2022). Onnistunut riskienhallintapolitiikka vaatii myös kommunikointia ylimmältä johdolta, jonka tulee asettaa selkeät tavoitteet ja standardit riskienhallintapolitiikan rakenteelle ja sisällölle (Okonofua & Rakhman, 2018). SFS-ISO 31000:2018 (2018) mukaan riskienhallintapolitiikan tulisi sisällyttää ainakin seuraavat asiat:

- Organisaation riskienhallinnan tarkoitus ja yhteydet organisaation tavoitteisiin sekä muihin toimintaperiaatteisiin.
- Korostaminen riskienhallinnan sisällyttämisestä organisaation kulttuuriin.
- Johtavan roolin ottaminen riskienhallinnan sisällyttämisessä keskeisiin toimintoihin ja päätöksentekoon.
- Vastuut ja valtuudet.
- Tarvittavien resurssien asettaminen saataville.
- Tapa, jolla voidaan käsitellä keskenään ristiriidassa olevia tavoitteita.
- Organisaation suorituskykymittareihin liittyvät riskienhallinnan mittarit ja niiden raportointi.
- Katselmointi ja kehittäminen.

Siponen ja Willison (2009) esittävät turvallisuuden ohjeiden noudattamisen välttämättömäksi. Käyttämällä virallisia ohjeita organisaatiot osoittavat sitoutumisensa turvallisen liiketoiminnan käytäntöihin (Siponen & Willison, 2009). Björnsdóttir ym. (2022a) esittävät, että standardien sekä muiden politiikkojen käytön tulee osoittautua hyödylliseksi todellisten, haastavien riskienhallintatilanteiden kautta, jolloin ne eivät myöskään anna ihmisille väärää turvallisuuden tunnetta.

Riskienhallintapolitiikan, kuten myös turvallisuuspolitiikkojen osalta, organisaatioiden tulee kuitenkin ymmärtää, että pelkkä politiikan olemassaolo ei automaattisesti johda sen noudattamiseen organisaation sisällä tai sen sidosryhmien keskuudessa. Hyungjinin ja Hanin (2019) mukaan vastuun tunteminen organisaatiosta rohkaisee työntekijöitä esimerkiksi tietoturvapolitiikkojen noudattamiseen. Yksittäisen työntekijän tietoturvapolitiikan noudattaminen voi toimia kannustimena myös muille työntekijöille tietoturvapolitiikan noudattamiseksi, vaikkeivat he olisi sitä lukeneetkaan (Hyungjin & Han, 2019). Ehkäpä tässä olisikin hyvä tunnustaa organisaation ja sen ympäristön vaikutus yksilöihin, sillä hyvä ympäristö voi ohjata yksilöitä toimimaan turvallisella tavalla.

2.5 Vastuu riskienhallinnasta

Valtionvarainministeriön (2017) mukaan riskienhallinta on osa johtamisen ja toiminnan prosesseja, jolloin riskienhallinnan kontekstissa johdolta edellytetään sitoutumista, osallistumista sekä hyväksymistä. Toisin sanoen riskienhallinta on osa johdon vastuualuetta, mutta organisaatioiden sisällä on kuitenkin kyettävä huomioimaan, että riskienhallinta on samalla myös tärkeä osa kaikkia organisaation prosesseja.

Tämä voikin tarkoittaa sitä, että riskienhallinta tulisi hajauttaa organisaation yksiköiden sisällä suoritettaviin pienempiin kokonaisuuksiin, jolloin erilaisista riskeistä olisivat vastuussa aihealuetta parhaiten hallitsevat henkilöt. Riskienhallinnan hajauttaminen organisaation eri yksiköihin voi kuitenkin koitua ongelmalliseksi, sillä riskienhallinnalle voidaan asettaa yksiköiden sisällä liian alhainen panostus, jolloin riskienhallinnan taso on organisaation kannalta heikkoa (Bruce, ym. 2022).

Vaikka riskienhallinta tulisikin jakaa pienempiin osa-alueisiin, viime kädessä riskienhallinnan riittävyydestä ja asianmukaisuudesta vastaa organisaation johto. Tästä syystä riskienhallinta tulisikin sisällyttää osaksi organisaatioiden yleistä hallintotapaa, strategiaa, suunnittelua, arvoja ja organisaation kulttuuria. Toimittaessa edellä mainitun mukaisesti riskienhallinta tukee organisaation tavoitteiden saavuttamista samalla suojaten sen henkilöstöä ja toimintoja.

2.6 Yhteenveto

Tässä luvussa on käyty läpi mitä riskit ovat, mitä riskienhallinta on sekä minkälaisia työkaluja ICT-organisaatiot voivat hyödyntää pyrkiessään hallitsemaan organisaatioihin kohdistuvia riskejä. Luvun alussa riskille esitettiin olevan useita erilaisia määritelmiä, mutta määritelmiä kuitenkin yhdisti se, että riskit nähdään negatiivisessa valossa niiden aiheuttaessa epävarmuutta tai poikkeamia oletetusta. Riskiä tarkasteltaessa huomattiin, että edullisessa tapauksessa riskit voivat avata uhkien lisäksi myös uusia mahdollisuuksia.

Luvussa riskienhallinta esitettiin järjestelmällisenä ja jatkuvana toimintana, jonka avulla organisaatiota tulee ohjata erilaisten riskien ja uhkien osalta. Riskienhallinnan esitettiin muodostuvan toimenpiteistä, joiden avulla pyritään lisäämään oman toiminnan onnistumisen todennäköisyyttä esimerkiksi tekemällä päätöksiä riskin ottamisesta tai sen ottamatta jättämisestä.

Riskienhallinnan selkeyttämiseksi luvussa myös avattiin riskienhallinnalle oleellisia ohjeita ja standardeja, joiden tarkoituksena on helpottaa riskienhallinnan toteuttamista. Tutkielmassa käsiteltävät standardit ja ohjeet ovat sekä kansallisia että kansainvälisiä. Standardien käyttöjen eduksi esitettiin yhdenmukaiset toimintatavat sekä organisaation kannalta mahdollisuus osoittaa, että he toimivat yhteisesti sovittujen periaatteiden mukaisesti. Akateemisen kirjallisuuden havaittiin myös kritisoivan standardeja, sillä standardien olemassaolo

vaikuttaa tärkeämmältä kuin niiden soveltamiselle käytössä olevien työkalujen käyttö ja saatavuus.

Luvun viimeiset kolme kappaletta käsittelivät riskienhallintaa ICT-organisaatiossa, riskienhallintapolitiikkaa, riskienhallinnan vastuuta sekä samalla vastaavat tutkielman ensimmäiseen tutkimuskysymykseen *"Miten riskienhallinta tulisi toteuttaa ICT-alan organisaatiossa?"*. ICT-organisaatioissa suoritettavan riskienhallinnan esitettiin olevan täynnä haasteita ja onnistunut riskienhallinta vaatiikin paljon enemmän kuin sokeaa standardien ja ohjeiden seuraamista.

Onnistuneesta riskienhallinnasta ovat vastuussa organisaation johtajat, joiden tehtävänä on jalkauttaa riskienhallinta osaksi organisaation yleistä hallintotapaa ja kulttuuria. Onnistumisen tueksi organisaatioissa tulisi hyödyntää myös erilaisia sisäisiä ohjeita ja politiikkoja. Politiikkojen avulla organisaation ylin johto ja hallitus pystyvät osoittamaan sitoutuneisuutensa riskienhallintaan, ja sisäiset ohjeet tuovat edellytykset organisaation sisäiseen tehokkaaseen toimintaan ja riskiperusteiseen käyttäytymiseen, jossa riskejä osataan käsitellä ja tarvittaessa välttää.

3 RISKIENHALLINNAN MALLEJA

Kolmannessa luvussa tarkastellaan ISO 31000:2018 Risk management – Guidelines -standardia, eli riskienhallinnan ohjeita. Ohjeiden kannalta erityisen tarkastelun alla on mallissa esitetty riskienhallintaprosessi. ISO 31000:2018-ohjeiden lisäksi luvussa käsitellään NIST SP 800-37r2 riskienhallinnan viitekehystä, jonka tarkoitukseksi esitetään riskienhallintaprosessin parantaminen sekä organisaation tietoturvallisuuden ja organisaatioiden välisen vuorovaikutuksen edistäminen.

3.1 Riskienhallinta ISO 31000:2018-standardin mukaisesti

SFS-ISO 31000:2018 (2018) mukainen riskienhallintaprosessi perustuu kolmen osatekijän muodostamaan kokonaisuuteen: standardissa määriteltyihin periaatteisiin, puitteisiin ja prosessiin. Barafortin, Mesquidan ja Masin (2018) sekä Wilbanksin ja Byrdin (2020) mukaan ISO 31000:2018 riskienhallintastandardi tuo mukanaan systemaattisen perspektiivin ja prosessimaisen lähestymistavan organisaation riskienhallintaan. Standardin osatekijöitä on mahdollista muokata tai kehittää, jotta organisaation riskienhallinta on tehokasta, vaikuttavaa sekä johdonmukaista. Osatekijät voivat olla organisaation käytössä joko kokonaisuudessaan tai osittain. (SFS-ISO 31000:2018, 2018.)

Riskienhallinnan ohjeet on tarkoitettu henkilöille, jotka luovat ja suojaavat arvoa organisaatioissa hallitsemalla riskejä, tekemällä päätöksiä, asettamalla ja saavuttamalla tavoitteita sekä parantamalla organisaation suorituskykyä. Ohjeiden tarkoituksena ei kuitenkaan ole toimia yksityiskohtaisena ohjeena riskienhallinnan suorittamisessa. Ohjeet tarjoavat riskienhallinnasta vastaaville henkilöille periaatteet, puitteet sekä prosessimallin, joita tulee soveltaa organisaation tarpeiden ja vaatimusten mukaisesti. (SFS-ISO 31000:2018, 2018.)

Nykyinen helmikuussa 2018 julkaistu ISO 31000:2018 versio esitetään aiempaa vuonna 2009 julkaistua versiota kattavammaksi, sillä se tuottaa käyttäjilleen strategisen vision riskienhallinnan menetelmistä (Rampini, ym., 2019).

ISO 31000:2009 oli kritiikin kohteena erityisesti siksi, että riskin määritelmä nähtiin heikoksi, sillä osa standardia hyödyntävistä tahoista tulkitsi riskin mahdollisuuksia avaavaksi tekijäksi, toisten nähdessä riskin liittyvän vaaroihin ja ennaltaehkäisyyn (Barafort, Mesquida & Mas, 2016). Dalin ja Lajthan (2012) mukaan ISO 31000:2009 ohjeiden rajoitteet tulisi tunnistaa myös siksi, että niissä kuvataan vapaaehtoisia riskienhallintaohjeita, jolloin todelliset noudattamisvaatimukset eivät sisälly ohjeeseen. Myös nykyiset ISO 31000:2018 ohjeet sisältävät vastaavan rajoitteen.

SFS-ISO 31000:2018 (2018) mukaan suurimmat muutokset aiempaan versioon nähden tapahtuivat sisällön yksinkertaistamisessa luomalla riskienhallinnan puitteet, riskienhallinnan kannalta keskeisimpien kriteereiden päivittämisessä sekä ylimmän johdon johtajuuden ja riskienhallinnan sisällyttämisen korostamisessa organisaation johtamisjärjestelmään ja hallintatapaan. Standardissa annetaan myös aiempaa suurempi painoarvo riskienhallinnan iteratiivisuudelle, jolla tarkoitetaan uusien kokemusten, tietämyksen ja analyysin mahdollisuutta johtaa prosessin osien, toimintojen ja hallintakeinojen uudistamiseen prosessin jokaisessa vaiheessa (SFS-ISO 31000:2018, 2018).

3.2 ISO 31000:2018 riskienhallinnan periaatteet

ISO 31000:2018 riskienhallintamallin mukaiset periaatteet kuvaavat vaikuttavan ja tehokkaan riskienhallinnan ominaisuuksia. Samalla periaatteet myös esittävät riskienhallinnan tavoitteet ja tarkoituksen sekä viestivät sen arvosta. (SFS-ISO 31000:2018, 2018.)

Periaatteet toimivat riskienhallinnan perustana ja ne tuleekin ottaa huomioon määriteltäessä organisaation riskienhallinnan puitteita ja prosesseja. Organisaation kannalta periaatteiden tarkoitus on auttaa sitä hallitsemaan epävarmuudesta aiheutuvaa vaikutusta organisaation tavoitteille. (SFS-ISO 31000:2018, 2018.) Riskienhallinnan periaatteet ovat usean osatekijän muodostama kokonaisuus, joiden avulla voidaan toteuttaa vaikuttavaa riskienhallintaa (SFS-ISO 31000:2018). Seuraavassa kuviossa (kuvio 1) esitetään SFS-ISO 31000:2018 mukaiset riskienhallinnan periaatteet.

KUVIO 1 Periaatteet SFS-ISO 31000:2018 (2018) riskienhallintamallin mukaisesti

ISO 31000:2018 riskienhallintamallin puitteiden mukaisesti organisaation johtamisjärjestelmän tulee olla olennainen osa kaikkia organisaation toimintoja (SFS-ISO 31000:2018, 2018). Valtionvarainministeriön (2017) mukaan johto onkin riskienhallinnan edistämisessä keskeisessä asemassa, sillä johdolla on selkeä merkitys organisaation tavoitteiden saavuttamisessa ja toiminnan onnistumisen edellytysten luomisessa. Periaatteiden tulee olla myös jäsennellyt sekä kattavat, sillä niiden avulla riskienhallinnan toimintamalli tekee tuloksista yhdenmukaisempia ja vertailukelpoisempia (SFS-ISO 31000:2018, 2018). Riskienhallinnan periaatteiden ydinajatuksena on siis luoda ja suojata arvoa sekä tarjota perusteet, joiden avulla riskejä voidaan tehokkaasti kuvata (Hardjomidjojo, ym., 2022).

Räätälöinnillä tarkoitetaan sitä, että puitteet ja prosessi sovitetaan osaksi organisaation tavoitteita ja niihin liittyvään ulkoiseen ja sisäiseen toimintaympäristöön sopiviksi (SFS-ISO 31000:2018, 2018). Jotta ulkoisia näkemyksiä, tietämystä ja havaintoja voidaan huomioida, myös organisaation sidosryhmät on otettava sopivalla tavalla ja oikeaan aikaan mukaan osaksi riskienhallintaa. Tämä lisää tietoisuutta riskienhallinnasta ja sillä myös varmistetaan parhaimpaan saatavilla olevaan tietoon perustuva riskienhallinta. (SFS-ISO 31000:2018, 2018.) SFS-EN IEC 31010:2019 (2019) tarjoaa sidosryhmien osallistamisesta myös toisenlaisen näkökulman, jossa sidosryhmien tiedot ja taidot voidaan valjastaa kohdeorganisaation riskienhallinnan tueksi. Tällöin sidosryhmien tietämys- ja

asiantuntemusalueet voivat auttaa organisaatiota tunnistamaan ja ymmärtämään riskejä tehokkaammin (SFS-EN IEC 31010:2019, 2019).

Dynaamisuus tarkoittaa sekä toimintaympäristössä mahdollisesti tapahtuvia muutoksia että riskienhallinnan valmiutta mukautua ympäristönsä vaatimuksiin. Toimintaympäristön muutoksista johtuen voi ilmentyä uusia riskejä, riskit voivat myös muuttua tai kokonaan hävitä. Riskienhallinnan avulla on siis tarkoitus ennakoida, havaita ja varmistaa muutokset ja tapahtumat sekä reagoida niihin sopivalla tavalla. (SFS-ISO 31000:2018, 2018.)

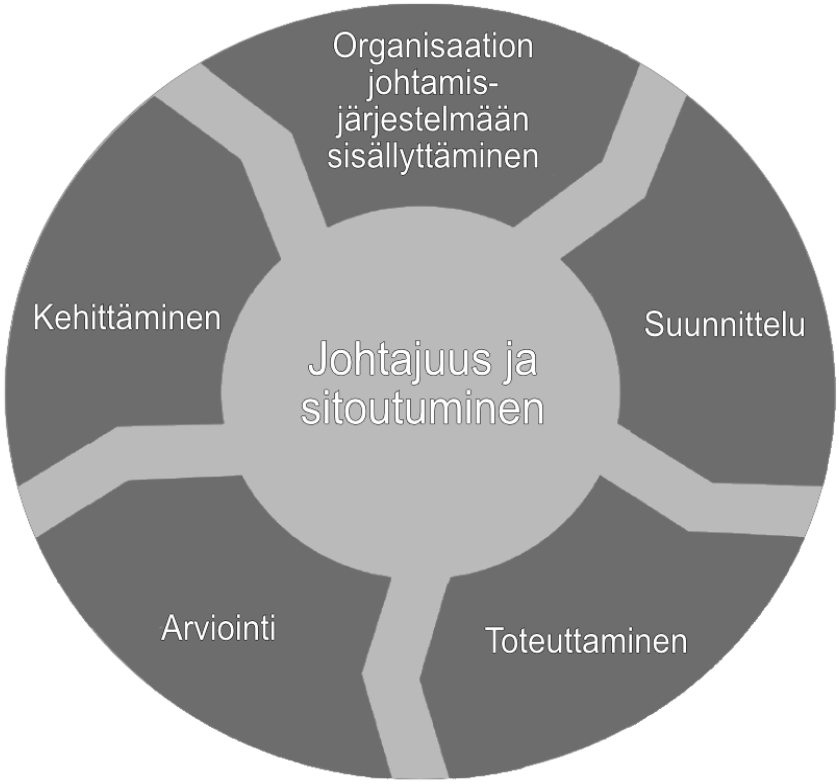
Periaatteiden mukaisesti riskienhallinnassa tulee käyttää parasta mahdollista saatavilla olevaa tietoa. Useimmiten riskienhallinnan lähtötiedot perustuvat historiatietoihin, nykyisiin tietoihin sekä tulevaisuutta koskeviin odotuksiin. Ihanteellisessa tilanteessa tieto on myös oikea-aikaista, selkeää ja oleellisten sidosryhmien saatavilla. Tietojen kannalta on myös tärkeä huomioida niiden perusteella tehtyihin odotuksiin liittyvät rajoitukset ja epävarmuudet. (SFS-ISO 31000:2018, 2018.)

Riskienhallinnassa tulee myös pystyä huomioimaan inhimilliset ja kulttuuriset tekijät, sillä ne vaikuttavat riskienhallintaan kaikilla sen tasoilla (SFS-ISO 31000:2018, 2018). Inhimilliset ja kulttuuriset tekijät voivat suoraan vaikuttaa esimerkiksi siihen, miten hyvin organisaatiossa työskentelevä henkilöstö noudattaa sisäisiä ohjeitaan. Da Veigan (2016) mukaan organisaatioiden on mahdollista kehittää organisaatiokulttuuriansa turvallisemmaksi kouluttamalla henkilöstöään. Jatkuva kehittäminen on myös osa ISO 31000:2018 riskienhallintamallin periaatteita ja sen mukaan riskienhallintaa kehitetään jatkuvasti oppimisten ja kokemusten myötä (SFS-ISO 31000:2018, 2018).

3.3 ISO 31000:2018 riskienhallinnan puitteet

ISO 31000:2018 mallin mukaisten puitteiden tarkoituksena on auttaa organisaatiota yhdistämään riskienhallinta osaksi organisaation keskeisiä tehtäviä ja toimintoja. Riskienhallinnan vaikuttavuus onkin suoraan riippuvainen siitä, kuinka hyvin organisaatio on onnistunut sisällyttämään sen hallintotapaansa ja päätöksentekoonsa. On myös huomioitava, että vaikuttavuuden onnistuminen vaatii myös sidosryhmien sekä etenkin ylimmän johdon tuen. (SFS-ISO 31000:2018, 2018.)

Puitteille on oleellista, että organisaation ylin johto ja hallitus varmistavat riskienhallinnan kehittämisen sisällyttämisen osaksi organisaation johtamisjärjestelmää. Puitteiden mukaisesti myös riskienhallinnan suunnittelu, toteuttaminen, arviointi ja kehittäminen muodostavat iteratiivisen kokonaisuuden, jotka sisältyvät osaksi organisaation johtamisjärjestelmää. (SFS-ISO 31000:2018, 2018.) Johtajuus ja sitoutuminen kuvataan tärkeiksi, sillä niiden avulla riskienhallintaa kehitetään samansuuntaiseksi organisaation tavoitteiden, strategian ja kulttuurin osalta. Alla olevassa kuviossa (Kuvio 2) on esitetty ISO 31000:2018 mukaiset riskienhallinnan puitteet.



KUVIO 2 Puitteet SFS-ISO 31000:2018 (2018) riskienhallintamallin mukaisesti

SFS-ISO 31000:2018 (2018) mallin mukaisissa puitteissa riskienhallinnan sisällyttäminen osaksi organisaation johtamisjärjestelmää perustuu ymmärrykseen organisaatiorakenteista ja sen toimintaympäristöstä. Björnsdóttir ym. (2022b) esittävät riskienhallinnan sisällyttämisen osaksi organisaation johtamisjärjestelmää erittäin tärkeäksi, sillä riskienhallinnan integroiminen ja päätöksenteon kyvykkyydet lopulta määrittelevät riskienhallinnan tehokkuuden.

Riskienhallinnan sisällyttäminen osaksi organisaation johtamisjärjestelmää on sekä dynaaminen että iteratiivinen prosessi, joka tulee mukauttaa vastaamaan organisaation tarpeita ja kulttuuria. Tällöin riskienhallinta on osa organisaation tarkoitusta, hallintotapaa, johtajuutta ja sitoutumista, strategiaa, tavoitteita ja toimintoja. (SFS-ISO 31000:2018, 2018.) Organisaation kannalta on tärkeää, että riskienhallinta on osana sen hallintotapaa, sillä hallintotapa ohjaa organisaation toimintaa, suhteita, prosesseja ja käytäntöjä, jotka ovat kriittisiä tavoitteiden saavuttamiseksi (SFS-ISO 31000:2018, 2018).

SFS-ISO 31000:2018 (2018) mukaan riskienhallintaan liittyvien vastuiden ja valvontaroolien määrittäminen on tärkeä osa organisaation hallintapaa. Organisaation johtamisrakenteet muuntavat hallintotavat strategiaksi sekä siihen liittyviksi tavoitteiksi, joiden avulla organisaatiossa on mahdollista ylläpitää pysyvää suoritustasoa ja toimintaa (SFS-ISO 31000:2018, 2018).

SFS-ISO 31000:2018 (2018) puitteiden mukainen suunnittelu koostuu viidestä vaiheesta: (1) organisaation ja sen toimintaympäristön ymmärtämisestä, (2) riskienhallinnan sitoutumisen ilmaisemisesta, (3) organisaation roolien, vas-

tuiden ja valtuuksien määrittelemisestä, (4) resurssien kohdentamisesta sekä (5) viestintä- ja tiedonvaihtomallien luomisesta. Suunnittelu voi alkuun vaikuttaa erittäin laajalta ja vaativalta tehtävältä. On kuitenkin huomioitava, että sen alkuvaiheessa tehtävä sisäisten ja ulkoisten toimintaympäristöjen tarkastelu ja niistä käsityksen muodostaminen helpottavat ja rajaavat suunnittelun muita vaiheita.

SFS-ISO 31000:2018 (2018) mukaan organisaation sisäisen toimintaympäristön tarkasteluun voivat kuulua esimerkiksi vision, mission, arvojen ja kulttuurin tarkastelu, mutta myös organisaation sisäisten kyvykkyyksien sekä keskinäisten riippuvuuksien ja yhteyksien tarkastelu. Ulkoista toimintaympäristöä tarkasteltaessa tulisi huomioida esimerkiksi sopimus- ja sidosryhmäsuhteet sekä kansainväliseen, kansalliseen että alueelliseen tai paikalliseen yhteiskuntaan liittyvät erilaiset riskitekijät (SFS-ISO 31000:2018, 2018).

Suunnittelun toinen vaihe käsittelee riskienhallintaan sitoutumisen ilmaisua organisaation sisäisesti ja sidosryhmien keskuudessa. Tämä voidaan tehdä laatimalla toimintaperiaatteet, politiikka tai vastaava tiedonanto, josta käy selkeästi ilmi organisaation tavoitteet ja sitoutuminen riskienhallintaan (SFS-ISO 31000:2018, 2018). Paanasen, Lapken ja Siposen (2019) mukaan esimerkiksi tietoturvapolitiikka (engl. Information security policy, ISP) viittaa dokumentteihin, joiden avulla säännellään ihmisten tietoturvallisuutta koskevia toimia tai ilmaistaan organisaation tietoturvatavoitteita. Heidän mukaansa tietoturvapolitiikalla voidaan organisaation kannalta myös kuvata sen haluttua turvallisuustilaa, aikomuksia, tavoitteita ja saavutuksia (Paananen, ym., 2019).

Vaikka useat eri turvallisuuden politiikat osoittaisivat organisaation sitoutumisen riskienhallintaan, on huomattava, että riskienhallintapolitiikka on osa riskienhallinnan periaatteita. (Valtionvarainministeriö, 2021). SFS-ISO 31000:2018 (2018) mukaan sitoumuksessa tulisi käydä ilmi seuraavat asiat:

- Organisaation riskienhallinnan tarkoitus sekä yhteydet asetettuihin tavoitteisiin ja toimintaperiaatteisiin
- Korostaminen riskienhallinnan sisällyttämisestä organisaation kulttuuriin
- Johtavan roolin ottaminen riskienhallinnan sisällyttämisessä keskeisiin toimintoihin ja päätöksentekoon
- Vastuut ja valtuudet
- Riittävien resurssien asettaminen saataville
- Toimintatavat, joiden avulla ristiriitaiset tavoitteet voidaan käsitellä
- Organisaation suorituskykymittareihin liittyvät riskienhallinnan mittarit ja niiden raportointi
- Katselmointi ja kehittäminen

Organisaation roolien, vastuiden ja valtuuksien määritteleminen on suunnittelun kolmas vaihe. Vaiheen tarkoituksena on varmistua siitä, että riskienhallinnan kannalta olennaiset roolit, vastuut ja valtuudet ovat määritelty ja niistä kyetään tarvittaessa viestimään organisaation kaikilla tasoilla (SFS-ISO

31000:2018, 2018). Edellä mainitun lisäksi vaiheessa tulisi korostaa riskienhallintaa keskeisenä vastuualueena sekä samalla yksilöidä sellaiset henkilöt, joilla on valtuudet ja vastuu riskienhallinnasta. Tällaisia henkilöitä voidaan kutsua myös riskin omistajiksi. (SFS-ISO 31000:2018, 2018.)

Suunnittelun neljäs vaihe käsittelee resurssien kohdentamista. Tämä tarkoittaa nimensä mukaisesti sitä, että ylin johto ja hallitus varmistavat tarvittavien resurssien kohdentamisen riskienhallintaa varten. Jotta tarvittavia resursseja olisi mahdollista arvioida, organisaatioiden tulisi arvioida sen nykyisiä kyvykkyyksiä ja mahdollisia rajoituksia. Riskienhallinnalle oleellisia resursseja ovat esimerkiksi ihmiset, heidän taitonsa, kokemuksensa ja osaamisensa, organisaation riskienhallintaan käytettävät menetelmät, työkalut ja prosessit sekä tarvittava ammatillinen kehitys ja koulutus. (SFS-ISO 31000:2018, 2018.)

Viestintä- ja tiedonvaihtomallien luominen on suunnittelun viimeinen vaihe, jonka ideana on luoda riskienhallinnan puitteita ja vaikuttavaa soveltamista tukeva viestinnän ja tiedonvaihdon toimintamalli. Oikea-aikaisuuden lisäksi viestinnän ja tiedonvaihdon tarkoituksena on varmistua olennaisen tiedon keräämisestä ja kokoamisesta. Koottu tieto on mahdollista jakaa eteenpäin ja siitä saatavaa palautetta tulisi hyödyntää parannuksien tekemisessä. (SFS-ISO 31000:2018, 2018).

SFS-ISO 31000:2018 (2018) mukaisten riskienhallinnan puitteiden seuraava vaihe on toteuttaminen, jonka aikana laaditaan asianmukainen toteutussuunnitelma, joka määrittelee käytettävät resurssit ja aikataulun. Toteuttamisessa organisaation tulee varmistua siitä, että riskienhallintajärjestelyt ovat selvästi ymmärretty ja viety käytäntöön. Oikein suunnitellut ja toteutetut riskienhallinnan puitteet varmistavat riskienhallintaprosessin toimivan osana kaikkia organisaation toimintoja, organisaation koko toimintaympäristössä ja päätöksenteossa. SFS-ISO 31000:2018 (2018.) Riskienhallinnan puitteiden ansiosta organisaatiot pystyvät käsittelemään epävarmuutta suoraan päätöksenteossa sekä samalla huomioimaan uudet tai tulevat epävarmuutta aiheuttavat tekijät niiden ilmetessä (SFS-ISO 31000:2018, 2018).

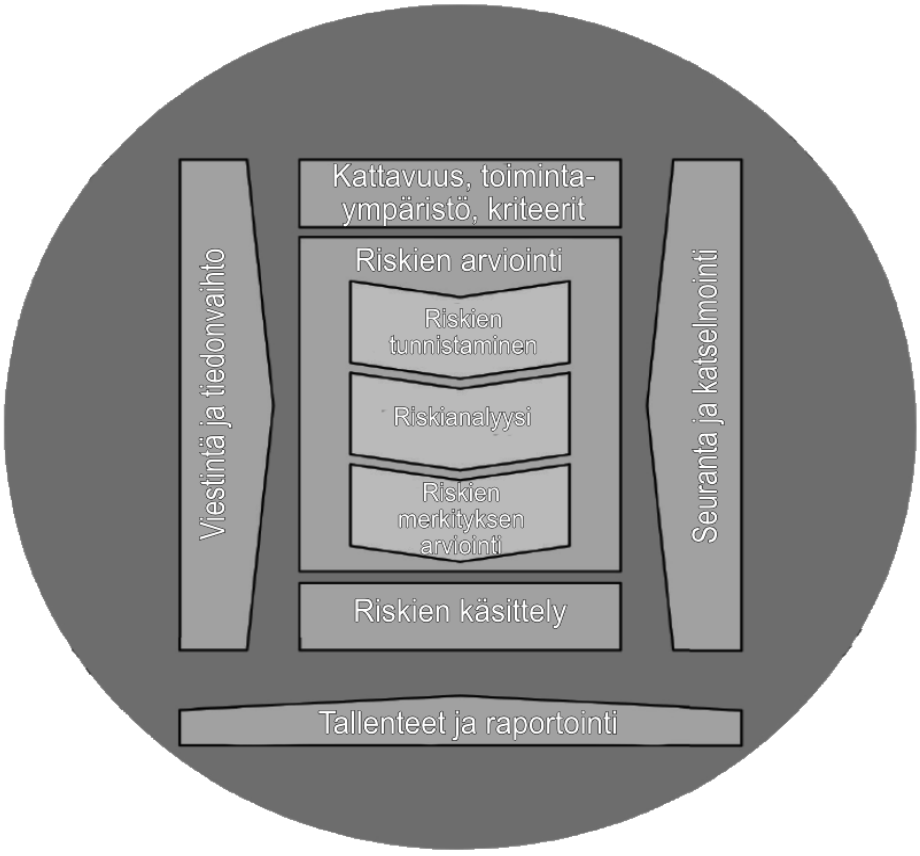
Toteuttamisen jälkeiset vaiheet ovat sen arviointi ja kehittäminen. SFS-ISO 31000:2018 (2018) mukaan riskienhallinnan puitteiden vaikuttavuutta arvioitaessa organisaation olisi kyettävä säännöllisin väliajoin mittaamaan riskienhallinnan puitteiden toimivuutta suhteessa niiden tarkoitukseen, toteuttamissuunnitelmaan, indikaattoreihin ja odotettuun käyttäytymiseen. Tämän lisäksi organisaation tulisi määritellä soveltuvatko riskienhallinnan puitteet organisaation nykyisten tavoitteiden tukemiseen (SFS-ISO 31000:2018, 2018).

Vaikka riskienhallinnan puitteet vastaisivatkin tarkasteluhetkellä haluttua tilaa, puitteiden mahdolliset kehittämis- ja muokkaustarpeet tulee silti huomioida. Tunnistettuja puutteita tai kehittämistarpeita varten organisaation tuleekin laatia suunnitelmat ja tehtävät, jossa määritellään parannuksista vastaavat tahot (SFS-ISO 31000:2018 2018). Toisin sanoen organisaation tulee seurata ja mahdollisesti muokata riskienhallinnan puitteita, jotta mahdollisiin toimintaympäristössä tapahtuviin muutoksiin voidaan reagoida. Puitteiden kehittämisen tulisi perustua kohdeorganisaation toimintatapoja ja tarpeita vastaaviksi,

jolloin ne myös kehittävät organisaation riskienhallintaa SFS-ISO 31000:2018 (2018).

3.4 ISO 31000:2018 riskienhallinnan prosessi

ISO 31000:2018 mukainen riskienhallintaprosessi sisältää toimintaperiaatteet, menettelytavat sekä käytäntöjen järjestelmällisen soveltamisen viestinnässä ja tiedonvaihdossa sidosryhmien kanssa. Prosessiin kuuluu myös toimintaympäristön määritteleminen, riskien arviointi, käsittely, seuranta, katselmoinnit, kirjaaminen ja raportointi. (SFS-ISO 31000:2018, 2018.) SFS-ISO 31000:2018 mukainen riskienhallintaprosessi esitetään usein järjestyksessä eteneväksi, mutta todellisuudessa prosessi on iteratiivinen, jolloin sen yksittäisiä osia on mahdollista myös toistaa (SFS-ISO 31000:2018, 2018). Toistettavuuden lisäksi Shameli-Sendi, Aghababaei-Barzegar ja Cheriet (2016) esittävät, että riskienhallintaprosessin tulisi olla myös mitattavissa, auditoitavissa ja mallinnettavissa. Seuraava kuvio (Kuvio 3) esittää ISO 31000:2018 mukaista riskienhallintaprosessia.



KUVIO 3 Prosessi SFS-ISO 31000:2018 (2018) riskienhallintamallin mukaisesti

SFS-ISO 31000:2018 (2018) mukaan riskienhallintaprosessin tulisi sisällyttää osaksi organisaation rakennetta, toimintoja ja prosesseja sekä organisaation johtamista ja päätöksentekoa. Riskienhallintaprosessi on monikäyttöinen ja laajasti sovellettavissa, esimerkiksi organisaation strategisella tai operatiivisella tasolla, mutta myös yksittäisen projektin tai ohjelman tasolla, jossa se on mahdollista räätälöidä tavoitteiden saavuttamista varten. Vaikka prosessi onkin mahdollista räätälöidä tarpeita vastaaviksi, riskienhallintaprosessille on oleellista huomioida ihmisten käyttäytymisen ja kulttuurin muuttuva luonne sen kaikissa vaiheissa.

3.4.1 Viestintä ja tiedonvaihto

Organisaation viestinnän ja tiedonvaihdon tarkoituksena on auttaa tärkeitä sidosryhmiä ymmärtämään riskejä, tehtyjä päätöksiä ja erilaisten toimenpiteiden tarvetta. Viestinnän ja tiedonvaihdon erottavat toisistaan se, että viestinnällä organisaatio pyrkii lisäämään tietoisuutta riskeistä, kun taas tiedonvaihto nimensä mukaisesti hankkii uutta tietoa ja palautetta päätöksenteon tueksi. (SFS-ISO 31000:2018, 2018.) Kellyn (2022) mukaan tietoisuus tehdyistä päätöksistä, kyky ratkaista ongelmia, harkintakyky, johtajuus, ryhmätyöskentely ja viestintä edistävät johdon kompetenssia riskienhallinnan osalta.

Jotta viestinnästä ja tiedonvaihdosta olisi mahdollista saada hyötyä, niiden olisi edistettävä tosiasioihin perustuvan, oikea-aikaisen, olennaisen, tarkan ja ymmärrettävän tiedon jakamista (SFS-ISO 31000:2018, 2018). Avenin ja Zion (2014) mukaan riskienhallinnassa käytettävä terminologia voi monesti koitua haasteelliseksi viestinnän ja kommunikoinnin kannalta, sillä terminologian kannalta oleelliset määrittelyt ja periaatteet ovat puutteellisia tai vaikeaselkoisia. Tästä huolimatta asiaankuuluvien sisäisten ja ulkoisten sidosryhmien kanssa olisi pystyttävä viestimään ja vaihtamaan tietoa kaikkien riskienhallintaprosessin vaiheiden aikana. Viestinnän ja tiedonvaihdon olisi myös kyettävä huomioimaan tiedon luottamuksellisuus, oikeellisuus sekä henkilöiden yksityisyydensuoja. (SFS-ISO 31000:2018, 2018.)

SFS-ISO 31000:2018 (2018) esittää viestinnän ja tiedonvaihdon keskeisten tavoitteiden tiivistyvän neljään osaan:

- Eri aihealueiden asiantuntemuksen yhdistäminen riskienhallintaprosessin jokaisessa vaiheessa
- Jokaisen näkökohdan asianmukainen huomioiminen riskikriteerien määrittelyssä ja riskien merkityksen arvioinnissa
- Riittävän tiedon tuottaminen riskien valvonnan ja päätöksenteon helpottamiseksi
- Riskeihin vaikuttavien sidosryhmien osallistaminen mukaan kuuluvuuden ja omistajuuden tunteen luomiseksi

3.4.2 Toimintaympäristön määrittäminen, kattavuus ja riskikriteerit

Toimintaympäristön, sen kattavuuden ja kriteereiden määrittäminen on varsin laaja prosessin osa, sillä sen tarkoituksena on määritellä riskienhallintatoimintojen laajuus ja kattavuus. Koska riskienhallintaprosessi on sovellettavissa organisaation strategisella tasolla aina yksittäisen projektin tasolle asti, on erittäin tärkeää määritellä riskienhallintaprosessin laajuus. Tämän aikana tulisi siis huomioida riskienhallinnan olennaiset tavoitteet ja niiden yhdenmukaistaminen organisaation tavoitteiden kanssa. (SFS-ISO 31000:2018, 2018.)

Toisin sanoen toimintaympäristön, sen kattavuuden ja kriteereiden määrittelyn tarkoituksena on räätälöidä riskienhallintaprosessi organisaatiolle sopivaksi, jolloin se pystyy vaikuttavasti arvioimaan ja käsittelemään riskejä (SFS-ISO 31000:2018, 2018). SFS-ISO 31000:2018 (2018) mukaisesti toimintamallin suunnittelun aikana tulisi huomioida:

- Tehtävät päätökset ja tavoitteet
- Vaiheet ja odotettavat tulokset prosessin aikana
- Paikka, ajankohta sekä sisällytettävät ja poissuljettavat asiat
- Soveltuvat riskien arvioinnin työkalut ja tekniikat
- Tarvittavat resurssit, vastuut ja tallenteet
- Muihin projekteihin, prosesseihin tai toimintoihin liittyvät suhteet

SFS-ISO 31000:2018 (2018) -standardin mukaisesti ulkoinen ja sisäinen toimintaympäristö muodostavat sen ympäristön, jonka puitteissa organisaatio määrittelee ja saavuttaa tavoitteensa. Toimintaympäristön ymmärrystä voidaan pitää tärkeänä, sillä organisatoriset tekijät voivat olla yksi riskien lähteistä. Tämän lisäksi riskienhallinnan kannalta toimintaympäristö määräytyy organisaation tavoitteiden ja toimintojen mukaan, jolloin riskienhallintaprosessin laajuus ja tarkoitus voivat olla yhteydessä koko organisaation tavoitteisiin. (SFS-ISO 31000:2018, 2018.)

Toimintaympäristön määrittelyn aikana organisaatiot voivat myös hyödyntää ISO 31000:2018 ohjeissa esitettyjä puitteita, jossa organisaation toimintaympäristö on ollut jo kertaalleen tarkastelun kohteena. SFS-EN IEC 31010:2019 (2019) esittää toimintaympäristön laajemman kuvan ymmärtämisen tärkeäksi erityisesti niillä alueilla, jossa on huomattavaa monimutkaisuutta. Tällä voidaan viitata esimerkiksi organisaation keskinäisiin riippuvuussuhteisiin tai erilaisiin sitoumuksiin ja sopimussuhteisiin.

Riskikriteereiden määrittely toteutetaan riskienarviointiprosessin alussa suhteessa organisaation tavoitteisiin. Sen tarkoituksena on selvittää, kuinka paljon ja millaisia riskejä organisaatio voi tai ei voi ottaa. (SFS-ISO 31000:2018, 2018.) Riskikriteereitä määriteltäessä voidaan myös spesifioida rajat, jonka ylimenevää riskiä ei voida hyväksyä tai riskiä ei haluta ottaa (SFS-EN IEC 31010:2019, 2019).

Kriteereiden määrittelyssä tulisi myös huomioida organisaatiota koskevat velvoitteet ja sidosryhmien näkemykset (SFS-ISO 31000:2018, 2018). Sidosryh-

mien tavoitteiden ja näkemysten huomioiminen on tärkeää, jotta heidän osallistumisensa ja näkemyksensä voidaan huomioida riskikriteerien asettamisessa (McShane, 2018). Riskikriteereiden tulisi myös heijastaa organisaation arvoja, tavoitteita ja resursseja sekä samanaikaisesti olla johdonmukainen riskienhallintaa koskevien käytänteiden ja asetettujen vaatimusten kanssa (SFS-ISO 31000:2018, 2018; Björnsdóttir, ym., 2022b).

SFS-ISO 31000:2018 (2018) esittää riskien olevan muuttuvia ja näin ollen niihin tulisi kohdistaa jatkuvaa arviointia, jonka perusteella kriteereitä voidaan tarvittaessa muuttaa. SFS-ISO 31000:2018 (2018) mukaan riskikriteereitä asetettaessa tulee huomioida seuraavat asiat:

- Sellaiset epävarmuuden ominaisuudet, jotka voivat vaikuttaa sekä aineellisiin että aineettomiin tuloksiin ja tavoitteisiin
- Miten sekä positiiviset että negatiiviset seuraukset ja todennäköisyys määritellään ja mitataan
- Aikaan liittyvät tekijät
- Johdonmukaisuus mittausten käytössä
- Miten riskitasot määritellään
- Miten useiden erilaisten riskien yhdistelmät ja järjestys huomioidaan
- Organisaation valmiudet

SFS-EN IEC 31010:2019 (2019) mukaan riskikriteerit voivat olla laadullisia, puolimäärällisiä tai määrällisiä. Täsmällisten kriteereiden määrittelyn puuttuessa on myös mahdollista, että sidosryhmät käyttävät harkintaansa reagoidessaan analyysistä saatuihin tuloksiin (SFS-EN IEC 31010:2019, 2019).

3.4.3 Riskien arviointi

Riskien arviointi kuvataan SFS-ISO 31000:2018 (2018) -ohjeissa kokonaisvaltaiseksi prosessiksi, joka kattaa riskien tunnistamisen, riskianalyysin ja riskien merkityksen arvioinnin. Tehokas riskienarviointi on iteratiivista, se edellyttää järjestelmällisyyttä ja yhteistyötä sidosryhmien kanssa sekä parhaan saatavilla olevan tiedon hyödyntämistä (SFS-ISO 31000:2018, 2018). Kitsiosis, Chatzidimitriou ja Kamariotou (2022) esittävät riskien arvioinnin olevan organisaation riskienhallinnan kannalta tärkeimpiä ja aikaa vievimpiä prosesseja.

Jotta riskejä olisi mahdollista arvioida, ne on ensin tunnistettava, jolloin myös tiedon asianmukaisuus ja ajantasaisuus korostuvat. Riskin tunnistamisen tarkoituksena on löytää, havaita ja kuvata riskit, jotka voivat vaikuttaa organisaation toimintaan tai tavoitteiden saavuttamiseen joko negatiivisesti tai positiivisesti. Tämä tarkoittaa sitä, että organisaation tulisi huomioida myös sellaiset riskit, joiden lähteet eivät ole suoraan sen hallinnassa. (SFS-ISO 31000:2018, 2018; Kitsiosis, ym., 2022.)

Riskien tunnistamisen aikana organisaation on mahdollista hyödyntää useita menetelmiä, joiden avulla se tunnistaa tavoitteisiinsa vaikuttavia epä-

varmuuksia. SFS-EN IEC 31010:2019 (2019) esittää toimivien menetelmien koostuvan esimerkiksi historiatietojen analyyseistä, tarkistusluetteloista tai taksonomioista, kyselytutkimuksia, tai menetelmiä, jotka synnyttävät ”mitä jos” -kysymyksiä, kuten HAZOP tai FMEA. SFS-ISO 31000:2018 (2018) mukaan riskien tunnistamisen aikana ainakin seuraavat tekijät ja niiden väliset suhteet olisi otettava huomioon:

- Aineellisten ja aineettomien riskien lähteet
- Riskien syyt ja tapahtumat
- Uhkat ja mahdollisuudet sekä haavoittuvuudet ja voimavarat
- Toimintaympäristössä tapahtuvat muutokset
- Indikaattorit uusista riskeistä
- Omaisuuden ja resurssien ominaisuudet ja arvo
- Mahdolliset seuraukset ja niiden vaikutukset tavoitteisiin
- Tietämyksen määrä ja rajoitukset tiedon luotettavuudessa
- Aikaan liittyvät tekijät
- Ennakkoluulot, oletukset ja uskomukset niillä henkilöillä, jotka osallistuvat riskien tunnistamiseen

Riskien tunnistamisen jälkeen riskit olisi analysoitava, jotta riskin luonnetta, ominaisuuksia ja mahdollisesti tasoa voitaisiin ymmärtää (SFS-ISO 31000:2018, 2018). Riskin luonteen ja ominaisuuksien lisäksi riskianalyysin avulla pyritään myös löytämään selityksiä vaarojen ja haittojen syille (Aven & Zio, 2014). SFS-EN IEC 31010:2019 (2019) mukaan riskianalyysillä tarkoitetaankin kirjaimellisesti vaaran tiedettä ja se tarjoaa panokset tehtäville päätöksille ja suoritettaville toimenpiteille.

SFS-ISO 31000:2018 (2018) mukaan riskianalyysimenetelmät voivat olla laadullisia tai määrällisiä sekä niiden yhdistelmiä, mutta menetelmän yksityiskohtaisuus ja monimutkaisuus ovat riippuvaisia analyysin tarkoituksesta ja siihen käytetyn tiedon saatavuudesta, laadusta ja resursseista. Riskianalyysiin voivat vaikuttaa useat tekijät, kuten eriävät mielipiteet ja oletukset, mutta se voi olla myös alttiina sosiaaliselle väärinkäytölle. Tämän takia riskianalyysissä tehdyt havainnot ja niihin vaikuttaneet tekijät tuleekin dokumentoida ja viestiä päätöksentekijöille. (SFS-ISO 31000:2018, 2018; Baskerville, 1991)

Koska riskianalyysi toimii lähtökohtana riskien merkitysten arvioinneille ja päätöksille riskien käsittelystä, analyysin tulisi kyetä huomioimaan ainakin tapahtumien seurausten todennäköisyyttä, luonnetta ja suuruutta. Tämän lisäksi nykyisten hallintakeinojen vaikuttavuus, erilaiset herkkyys- ja luottamustasot sekä aikaan liittyvät tekijät ovat tärkeä osa riskianalyysiä. (SFS-ISO 31000:2018, 2018.) Kuzminykh, Ghita, Sokolov ja Bakhshi (2021) esittävät, että riskianalyysin avulla organisaatiot pystyvät myös priorisoimaan riskejä, jotka ovat merkityksellisiä tavoitteiden saavuttamisen kannalta.

Päätöksentekoa tukevaan riskien merkityksen arviointiin kuuluu riskianalyysin tulosten vertaaminen organisaation määrittämiin riskikriteereihin. Vaihe on tärkeä, sillä sen avulla tiedetään, tulisiko organisaation suorittaa mahdollisia

lisätoimenpiteitä, tarkastella erilaisia vaihtoehtoja riskin käsittelylle tai pyrkiä ymmärtämään riskiä paremmin. Päätöksissä tulisi huomioida toimintaympäristö mahdollisimman laajasti, ja miettiä tulisiko organisaation ylläpitää sen nykyisiä hallintakeinoja tai esimerkiksi harkita sen tavoitteita uudelleen. Riskien merkityksen arvioinnin perusteella saadut tulokset olisi dokumentoitava ja tiedotettava sekä hyväksytettävä organisaation edellyttämillä päätöksenteontasoilla. (SFS-ISO 31000:2018, 2018.)

3.4.4 Riskien käsittely

Riskien käsittely on toistuva prosessi, jonka tarkoituksena on valita ja toteuttaa erilaiset vaihtoedot riskien käsittelyä varten. Riskien käsittely koostuu viidestä vaiheesta, johon kuuluu riskien käsittelyn vaihtoehtojen kehittäminen ja valinta, riskien käsittelyn suunnittelu ja toteuttaminen, käsittelyn vaikuttavuuden arviointi ja päätös jäännösriskin hyväksymisestä tai sen käsittelyn jatkamisesta, jos riskiä ei voida hyväksyä. (SFS-ISO 31000:2018, 2018.)

SFS-ISO 31000:2018 (2018) mukaan riskien käsittelyn vaihtoehdot eivät välttämättä ole toisiaan poissulkevia, mutta sopivaa menetelmää valittaessa tulee huomioida vaaditut kustannukset, työmäärä sekä toteutuksen mahdolliset heikkoudet verrattuna saataviin hyötyihin tavoitteiden saavuttamisessa. Riskienhallinnan ohjeissa kuitenkin todetaan myös se, että käsittelytavat tulisi valita huomioiden organisaation tavoitteet, riskikriteerit sekä saatavilla olevat resurssit (SFS-ISO 31000:2018, 2018).

Riskinkäsittelytavoiksi nimetään riskin torjuminen tai riskin lähteen poistaminen, riskin ottaminen ja lisääminen, todennäköisyyden tai riskin seurausten muuttaminen sekä riskin jakaminen tai säilyttäminen. Vaikka valittu menetelmä toteutettaisiinkin huolellisesti, se ei välttämättä tuota haluttuja tuloksia, vaan vaihtoehtoisesti ei-toivottuja seurauksia, kuten uusia riskejä. (SFS-ISO 31000:2018, 2018.) Toisin sanoen riskien käsittelyn tulokset voivat olla ennalta luonteeltaan ja laajuudeltaan arvaamattomia ja niistä tulisikin raportoida päätöksentekijöille ja sidosryhmille, etenkin jäännösriskien osalta (SFS-ISO 31000:2018, 2018).

SFS-ISO 31000:2018 (2018) esittää riskinkäsittelysuunnitelman tarkoitukseksi määritellä valittujen käsittelyvaihtoehtojen toteuttaminen ja järjestys. Käsittelysuunnitelman tulisi sisältää riskinkäsittelytapojen valintaperusteet, suunnitelman hyväksymisestä ja toteuttamisesta vastaavat tahot, muut ehdotetut toimenpiteet, resurssivaatimukset, rajoitukset ja suorituskyvyn mittarit sekä vaatimus raportoinnista, seurannasta ja ajankohdasta, jolloin toiminnot oletetaan suoritetuiksi. Käsittelysuunnitelmat tulisi myös integroida osaksi organisaation johtamissuunnitelmia ja -prosesseja asiaan kuuluvien sidosryhmien kanssa. (SFS-ISO 31000:2018, 2018.)

3.4.5 Seuranta ja katselmointi

Seurannan ja katselmoinnin tarkoitukseksi SFS-ISO 31000:2018 (2018) esittää prosessin suunnittelun, toteutuksen ja tulosten laadun varmistamisen sekä nii-

den parantamisen. Barafortin ym. (2018) mukaan sekä seuranta että katselmointi määritellään ISO riskienhallinnan sanastossa. Seuranta määritellään jatkuvaksi kriittiseksi tarkkailuksi, jonka avulla tunnistetaan muutos vaaditussa tai odotetussa suoritustasossa. Katselmoinnilla tarkoitetaan toimintaa, jonka tarkoituksena on tarkastella toiminnan tehokkuutta, riittävyyttä ja soveltuvuutta. (Barafort, ym., 2018.)

SFS-ISO 31000:2018 (2018) mukaan säännöllisen seurannan ja katselmoinnin tulee olla suunniteltu ja vastuiden osalta selkeästi määritelty osa riskienhallintaprosessin kaikkia kuutta vaihetta. Vaiheen tarkoituksena on suunnittelu, tiedon kerääminen ja analysoiminen, tulosten kirjaaminen sekä palautteen antaminen ja niistä saatuja tuloksia olisi hyödynnettävä organisaation suorituskyvyn hallinnassa, mittauksessa ja raportoinnissa (SFS-ISO 31000:2018, 2018).

3.4.6 Tallenteet ja raportointi

Tallenteet ja raportointi ovat viimeinen osa ISO 31000:2018 (2018) mukaista riskienhallinnan prosessia, ja sen tarkoituksena on varmistaa riskienhallintaprosessin tarkoituksenmukainen raportointi ja dokumentointi. Tallenteiden ja raportoinnin tavoitteena esitetään olevan organisaation tukeminen viestiessä riskienhallinnan toiminnoista ja tuloksista, vuorovaikutuksen kehittäminen, päätöksenteon tukeminen ja riskienhallintatoimien kehittäminen (SFS-ISO 31000:2018, 2018).

SFS-ISO 31000:2018 (2018) myös muistuttaa dokumentoitavan tiedon arkaluonteisuudesta, joka tulisikin huomioida tietoa luodessa, sen käsittelyssä ja säilyttämisessä. Raportoinnin tulisi myös huomioida eri sidosryhmien toisistaan poikkeavat vaatimukset, raportointimenetelmä ja sen oikea-aikaisuus, raportoinnista aiheutuvat kustannukset ja tiedon merkitys organisaation tavoitteiden ja päätöksenteon kannalta (SFS-ISO 31000:2018, 2018).

3.5 NIST SP 800-37r2

National Institute of Standards and Technology (NIST) kehittämä NIST SP 800-37r2 riskienhallinnan viitekehys tarjoaa ohjeita riskienhallinnan viitekehyksen soveltamiseen erityisesti tietojärjestelmien ja organisaatioiden osalta. NIST SP 800-37r2 julkaisu on kehitetty yhteistyönä Joint Task Force Interagency Working Groupissa ja siinä toimineeseen työryhmään kuului siviili-, puolustus- ja tiedusteluyhteisöjen edustajia (Ross ym., 2018).

Viitekehyksen numerotunnisteen lopussa oleva r2 eli tarkistettu painos (engl. Revision) viittaa tällä hetkellä uusimpaan versioon, joka julkaistiin joulukuussa 2018. Viitekehys sisältää myös toimenpiteitä, jotka valmistavat organisaatiota toteuttamaan riskienhallintaa viitekehyksen mukaisesti. (Ross, ym., 2018.) Rossin ym. (2018) mukaan NIST SP 800-37r2 mukainen viitekehys edistää lähes reaaliaikaista riskienhallintaa, se toteuttaa jatkuvia seurantaprosesseja ja

auttaa organisaatioita hallitsemaan turvallisuuteen ja tietosuojaan kohdistuvia riskejä.

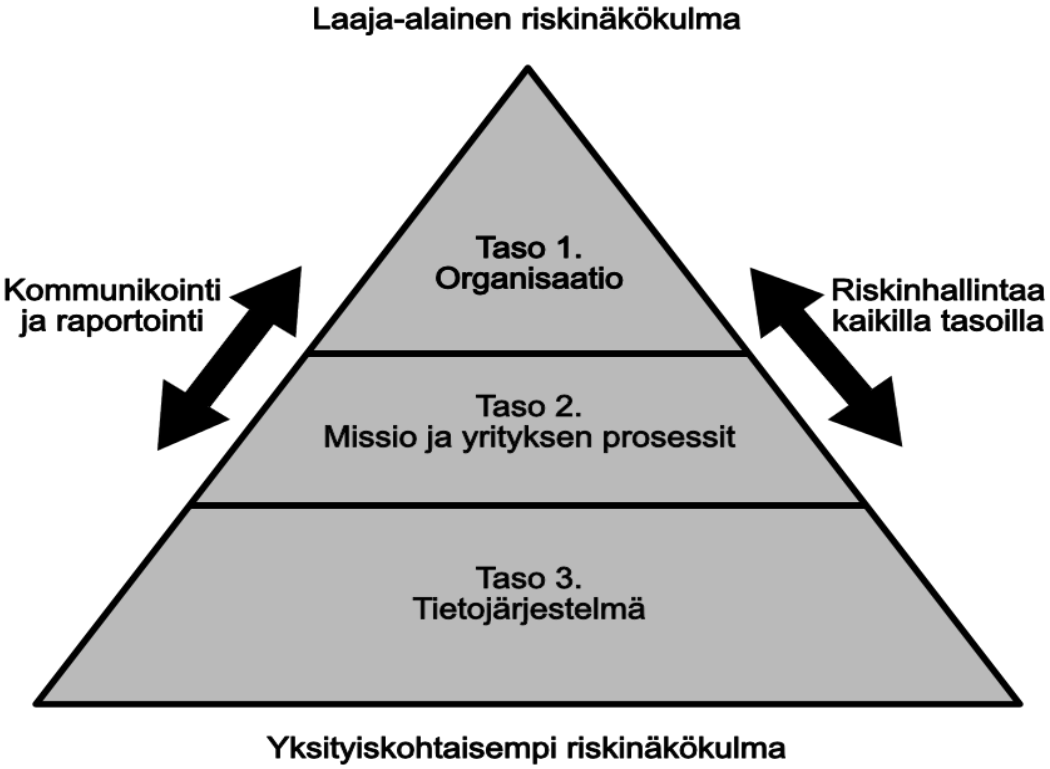
NIST SP 800-37r2 esittämän riskienhallinnan viitekehyksen tehtävien suorittaminen yhdistää olennaiset järjestelmätason riskienhallintaprosessit organisaation riskienhallintaprosesseihin. Viitekehys antaa myös johdolle tarvittavat tiedot parempaa ja kustannustehokkaampaa riskienhallinnan päätöksentekoa varten, erityisesti liiketoimintaa ja turvallisuuden elinkaarta koskevissa asioissa. (Ross, ym., 2018.) Schmidtin (2023) mukaan NIST SP 800-37r2 on osa laajempaa NIST SP 800 -sarjaa, joka yhdistää loogisesti muita siihen kuuluvia julkaisuja, kuten turvallisuuden kontrolleja käsittelevän NIST SP 800-53 julkaisun.

3.6 NIST SP 800-37r2 mukainen riskienhallinnan viitekehys ja prosessi

NIST SP 800-37r2 riskienhallinnan viitekehys kuvataan teknologianeutraaliksi, sillä se on suunniteltu mihin tahansa tietojärjestelmään sovellettavaksi ilman vaatimuksia erillisten muutosten tekemisestä. Viitekehyksessä kuitenkin määritellään soveltuva tietojärjestelmä sellaiseksi erilliseksi tietoresurssiksi, joka on järjestetty tiedon keräämiseen, käsittelyyn, ylläpitoon, käyttöön, jakamiseen, levittämiseen tai luovuttamiseen. Tieto voi olla digitaalisessa tai ei-digitaalisessa muodossa ja itse tietoresurssiin kuuluvat myös siihen liittyvät resurssit, kuten henkilöstö, laitteet, varat ja tietotekniset laitteet. (Ross, ym., 2018.)

NIST SP 800-37r2 mukainen malli esittää tietojärjestelmien turvallisuuteen ja tietosuojaan vaikuttavien riskien olevan monimutkainen kokonaisuus, joka edellyttää koko organisaation osallistumista, kaksisuuntaista viestintää ja raportointia. (Ross, ym., 2018). Riskienhallinta kuvataankin kokonaisvaltaiseksi toiminnaksi, joka vaikuttaa organisaation kaikkiin osa-alueisiin. NIST SP 800-37r2 mukaista riskienhallinnan viitekehystä voisi luonnehtia uhkalähtöiseksi, sillä Ross, ym. (2018) esittää sen painottavan laajaa riskien tunnistamista, kuvaamista ja niistä tiedottamista.

Riskienhallinnan päävastuu on kuitenkin organisaation ylimmällä johdolla (Taherdoost, 2022). Strategiasta vastaa ylin johto, keskijohdon suunnitellessa ja hallitessa organisaation projekteja, jolloin yksittäiset henkilöt organisaatiossa vastaavat kehityksestä ja implementoinnista sekä tukevat organisaation missiota ja liiketoimintoja. (Ross, ym., 2018.) Seuraava kuvio (Kuvio 4) esittää NIST SP 800-39 mukaisen, kolmitasoisen lähestymistavan organisaation riskienhallintaan, jota sovelletaan myös NIST SP 800-37r2 riskienhallinnan viitekehyksessä.



KUVIO 4 NIST SP 800-39 esittämä lähestymistapa organisaationlaajuiseen riskienhallintaan mukaisesti (Ross, ym., 2018).

Ross ym. (2018) esittävät kahden ensimmäisen tason olevan kriittisiä organisaation valmistautuessa toteuttamaan viitekehyksen mukaista riskienhallintaa. Valmistelun esitetään sisältävän useita välttämättömiä toimintoja turvallisuus- ja tietosuojariskien asianmukaisen hallinnan kannalta koko organisaatiossa, eikä tällaisia päätöksiä tule tehdä eristäytyneenä muista tasoista. (Ross, ym., 2018).

Kahden ensimmäisen tason päätöksistä vastaa organisaation ylin johto yhdessä keskijohdon kanssa. Ross ym. (2018) esittävät heidän tekemiensä päätösten vaikuttavan pääsääntöisesti organisaation kehitykseen ja riskienhallinnan viitekehyksen käyttöönottoon valmistautumiseen, esimerkiksi seuraavien toiminteiden kautta:

- Organisaation tehtävät ja tavoitteet liiketoiminnalle
- Järjestelmien ja palveluiden mahdolliset modernisointialoitteet
- Yritysarkkitehtuurin tarve hallita ja vähentää kompleksisuutta esimerkiksi optimoinnin, konsolidoinnin ja standardoinnin avulla
- Resurssien kohdentaminen organisaation tehokkuuden varmistamiseksi
- Roolien ja vastuiden jakaminen organisaation riskienhallintaprosessille
- Riskienhallintastrategian ja organisaation riskinsietokyvyn laatiminen

- Tietojärjestelmän tukemat liiketoiminnot, tehtävät ja prosessit
- Tietojärjestelmiin ja organisaatioon kohdistuvien uhkien ymmärtäminen
- Organisaation- ja järjestelmätason riskiarviointien tekeminen
- Tietoturva- ja tietosuojavaatimusten tunnistaminen, priorisointi yhdenmukaistaminen ja ristiriitojen purkaminen
- Turvallisuus- ja tietosuojavaatimusten kohdentaminen
- Yksilöihin kohdistuvien mahdollisten haitallisten vaikutusten ymmärtäminen

Kolmannella tasolla riskejä käsitellään tietojärjestelmien näkökulmista ja toteutus perustuukin kahdella ensimmäisellä tasolla tehtyihin päätöksiin, sillä ne voivat vaikuttaa esimerkiksi erilaisten kontrollien valintaan ja toteutukseen. Jos organisaatio ei kykene valmistautumaan riskienhallinnan viitekehyksen käyttöönottoon, lopputulos voi koitua kalliiksi, mutta myös tehottomiin ratkaisuihin ja haavoittuvaisiin järjestelmiin, palveluihin ja sovelluksiin (Ross, ym., 2018.)

3.6.1 Viitekehyksen käyttöönoton valmistelu

Viitekehyksen käyttöönoton valmistelu on ensimmäinen prosessin seitsemästä vaiheesta. Käyttöönottovaihe jakautuu yhteensä 18 tehtävään, joista seitsemän ensimmäistä keskittyvät valmistelemaan tehtäviä ja tuloksia organisaation ylimmällä tasolla. Loput tehtävät keskittyvät tietojärjestelmätason valmisteluun, mutta tehtävät vaikuttavat myös missioon ja yrityksen prosesseihin tasolla kaksi, esimerkiksi tunnistamalla tehtävien vastuualueiden roolit ja liiketoiminnan päätavoitteet. (Ross, ym., 2018.) Tehtävien vaiheet ja niistä odotetut tulokset ovat havainnollistettu seuraavaan taulukkoon (Taulukko 1).

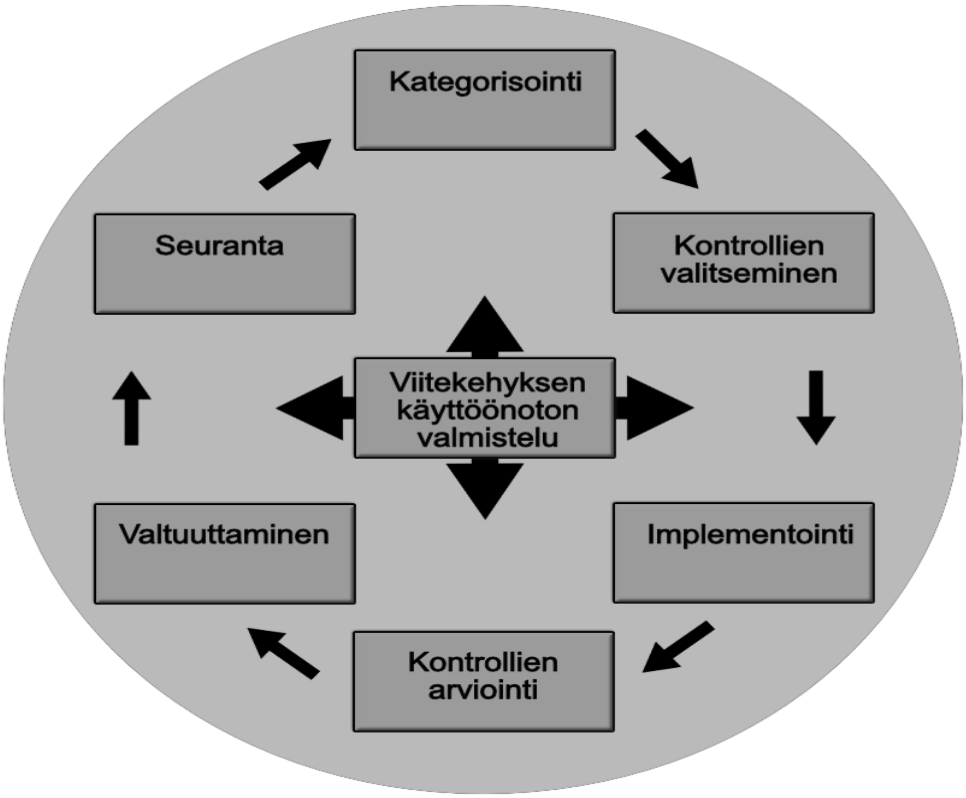
TAULUKKO 1 Valmisteluvaiheen tehtävät ja niiltä odotetut tulokset (Ross, ym., 2018).

Tehtävä-numero.	**Tehtäväkuvaus**	**Tehtävältä odotetut tulokset**	**Tehtävien suorittaminen tasolla**
1	Tunnista ja määritä henkilöt riskienhallinnan rooleihin.	Dokumentti roolimäärityksistä, esimerkiksi organisaatiokaavio.	Taso 1
2	Organisaation riskienhallintastrategian laatiminen ja riskinsietokyvyn määrittäminen	Riskienhallintastrategia ja -lausunto riskinsietokyvystä, voidaan toteuttaa esimerkiksi politiikan muodossa.	Taso 1
3	Organisaation turvallisuus- ja tietosuojariskien arviointi ja riskiarvioinnin päivittäminen.	Riskiarvion tulokset. Esitettäviä asioita voivat olla esimerkiksi uhkatiedot ja tiedonvaihtosopimukset.	Taso 1
4	Organisaation mukaisten hallintakeinojen perusteiden luominen, dokumentointi ja julkaisu.	Luettelo organisaatiolle räätälöidyistä ja hyväksytyistä valvonnan lähtökohdista, esimerkiksi dokumentoidut turvallisuus ja tietosuojavaatimukset.	Taso 1

5	Tunnista, dokumentoi ja julkaise organisaation yleiset saatavilla olevat kontrollit organisaation järjestelmille.	Tietoturvaan ja -suojaan liittyvät suunnitelmat sekä organisaatio ja järjestelmätason turvallisuus- ja tietosuojariskien arvioinnin tulokset.	Taso 1
6	Organisaation saman vaikutustason järjestelmien priorisointi.	Organisaation järjestelmien priorisointi kategorioittain vähäisistä vaikutuksista suurimpiin, esimerkiksi turvallisuusluokitustietoja ja järjestelmäkuvauksia hyödyntämällä.	Taso 1
7	Strategian kehittäminen ja toteuttaminen organisaationvalvonnan ja tehokkuuden jatkuvaa seuraamista varten.	Toteutettu jatkuvan seurannan strategia, esimerkiksi riskienhallintastrategian sekä organisaation turvallisuus ja tietosuojakäytäntöjen avulla.	Taso 1
8	Tehtävien, liiketoimintojen ja prosessien tukeminen, joita tietojärjestelmien on tarkoitus tukea.	Listaus järjestelmän tukemista tehtävistä, liiketoiminnoista ja prosesseista, esimerkiksi organisaation politiikkoja hyödyntämällä.	Tasot 2 ja 3
9	Tietojärjestelmille olennaisten sidosryhmien tunnistaminen.	Listaus tietojärjestelmille oleellisista sidosryhmistä.	Tasot 2 ja 3
10	Suojattavan omaisuuden tunnistaminen.	Suojattavan omaisuuden tunnistamisessa voidaan hyödyntää esimerkiksi liiketoiminnanvaikutusanalyysejä ja sisäisiä sidosryhmiä.	Taso 3
11	Järjestelmän valtuuttamisrajojen määrittäminen.	Dokumentti valtuuttamisrajoista, jossa voidaan hyödyntää esimerkiksi järjestelmän dokumentaatiota.	Taso 3
12	Järjestelmän käsittelemien, tallentamien ja lähettämien tietotyyppien tunnistaminen.	Lista tietotyypeistä, tunnistamisen apuna voidaan hyödyntää järjestelmän suunnitteludokumentaatiota.	Taso 3
13	Tiedon elinkaaren tunnistaminen ja ymmärtäminen järjestelmän käsittelemien, tallentamien ja lähettämien tietotyyppien osalta.	Dokumentti vaiheista, joiden kautta tieto kulkee järjestelmässä, esimerkiksi malli, joka havainnollistaa järjestelmän käsittelemän datan koko sen elinkaaren ajan.	Taso 3
14	Tietojärjestelmätason riskiarvioinnin suorittaminen ja sen jatkuva päivittäminen.	Turvallisuus- ja tietosuojariskien arviointiraportit.	Taso 3
15	Tietojärjestelmän ja toimintaympäristön turvallisuus- ja tietosuojavaatimusten määrittäminen.	Dokumentti turvallisuus- ja tietosuojavaatimuksista, jonka tukena voidaan hyödyntää esimerkiksi organisaation- ja tietojärjestelmätason riskiarviointien tuloksia.	Taso 3
16	Järjestelmän sijainnin määrittäminen yritysarkkitehtuurissa.	Päivitetty yritysarkkitehtuuri ja suojausarkkitehtuuri, sekä mahdolliset suunnitelmat pilvipohjaisten järjestelmien tai jaettujen järjestelmien	Taso 3

		käytöstä.	
17	Tietoturva ja tietosuojavaatimusten kohdistaminen tietojärjestelmälle ja sen toimintaympäristölle.	Luettelo järjestelmälle tai siihen kohdistuville elementeille kohdistetuista tietoturva ja tietosuojavaatimuksista.	Taso 3
18	Tietojärjestelmän rekisteröinti organisaation tehtävää tai hallintoa varten.	Organisaation politiikkojen mukaisesti rekisteröity järjestelmä ja osoitus sen olemassaolosta.	Taso 3

Valmisteluvaiheen tarkoituksena on varmistua siitä, että organisaatio on valmis ja kykenevä toteuttamaan prosessin kuusi päävaihetta (Ross, ym., 2018). Kokonaisuudessaan riskienhallinnan viitekehys on havainnollistettu seuraavassa kuviossa (Kuvio 5).



KUVIO 5 Mukaillen esitetty NIST SP 800-37r2 riskienhallinnan viitekehys (Ross, ym., 2018).

Riskienhallinnan viitekehyksessä esitetyt vaiheet aloitetaan valmisteluvaiheen jälkeen kategorisointi -vaiheesta, jonka jälkeen muut vaiheet seuraavat kuvion 5 mukaisesti peräkkäisessä järjestyksessä. On kuitenkin mahdollista, että riskienhallintaprosessia seuratessa organisaatiolle voi tulla tarve poiketa mallin mukaisesta järjestyksestä esimerkiksi riskin tai järjestelmän toiminnallisuudessa kohdatun poikkeaman takia. (Ross, ym., 2018.)

3.6.2 Kategorisointi

Kategorisointivaiheen ydinajatuksena on tiedottaa organisaation riskienhallinnan prosesseista ja tehtävistä määrittämällä haitalliset vaikutukset organisaation toimintoihin ja omaisuuteen sekä yksilöihin ja muihin organisaatioihin. Kategorisointivaihe koostuu kolmesta tehtävästä: (1) tietojärjestelmän ominaisuuksien dokumentoinnista; (2) tietojärjestelmien kategorisoinnista ja dokumentoinnista; (3) Kategorisoinnin tulosten ja päätösten tarkistamisesta ja hyväksymisestä. (Ross, ym., 2018.)

Jotta vaiheen ensimmäisen tehtävän suorittamista voitaisiin pitää onnistuneena, organisaation tulisi dokumentoida ja kuvata tietojärjestelmänsä esimerkiksi hyödyntämällä järjestelmän suunnittelussa ja vaatimuksissa käytettyjä tietoja. Tämän lisäksi kahden jälkimmäisen tehtävän tuloksina, organisaation tulisi muodostaa vaikutustasot tietotyypeille ja turvallisuustavoitteille sekä hyväksyttää tietojärjestelmänsä kategorisointi. (Ross, ym., 2018.) Rose (2022) tiivistääkin vaiheen dokumentoivan tietojärjestelmän ominaisuudet, vaaditut resurssit ja niihin liittyvät työnkulut.

3.6.3 Kontrollien valitseminen

Kolmannen vaiheen tarkoituksena on kontrollien valitseminen ja se koostuu kuudesta tehtävästä. Vaiheen aikana valitaan, räätälöidään ja dokumentoidaan tietojärjestelmän ja organisaation suojaamiseen tarvittavat hallintakeinot, joiden on oltava oikeassa suhteessa organisaation toimintoihin, omaisuuteen, henkilöihin sekä muihin organisaatioihin kohdistuviin riskeihin nähden. (Ross, ym., 2018.)

Ensimmäisen tehtävän aikana organisaation tulee valita kontrollit tietojärjestelmää ja toimintaympäristöä varten. Toisen tehtävän aikana valitut kontrollit räätälöidään organisaatiolle sopiviksi ja niiden lähtötasot dokumentoidaan. Kun kontrollit ovat räätälöity, ne tulee kohdistaa organisaation tietojärjestelmälle ja toimintaympäristölle. (Ross, ym., 2018). Tarpeen vaatiessa kontrolleja on myös mahdollista lisätä tai kokonaan poistaa (Rose, 2022).

Neljäntenä tehtävänä on tietojärjestelmän ja toimintaympäristön kontrollien dokumentointi osaksi turvallisuuden ja tietosuojan suunnitelmia. Tämän jälkeen organisaation tulisi kehittää ja toteuttaa tietojärjestelmätason strategia kontrollien tehokkuuden seuraamista varten. Vaiheen viimeisenä tehtävänä on tarkistaa ja hyväksyä tietojärjestelmää varten laaditut suunnitelmat. (Ross, ym., 2018.)

3.6.4 Implementointi

Implementointivaiheen tarkoituksena on toteuttaa tietojärjestelmän sekä organisaation tietoturva- ja tietosuojasuunnitelmissa olevat suunnitelmat. Toteuttamisen lisäksi vaiheen aikana tulee tarkasti dokumentoida konfiguraation valvonnan toteutuksen yksityiskohdat. (Ross, ym., 2018.) Rosen ym. (2022) mu-

kaan vaiheen molemmat tehtävät edellyttävät resursseja myös tietojärjestelmän ylläpitäjiltä ja sen käyttäjiltä.

Kontrolleja implementoitaessa tulee huomioida, että tietojärjestelmän tietoturva- ja tietosuojasuunnittelumenetelmiä käytetään järjestelmän tietoturva- ja tietosuojasuunnitelmien hallintaan. Kun kontrollit ovat implementoitu, organisaation tulisi dokumentoida kontrollien implementointiin kohdistuvat mahdolliset muutokset. (Ross, ym., 2018.)

3.6.5 Kontrollien arviointi

NIST SP 800-37r2 mukaisen riskienhallinnan viitekehyksen viidentenä vaiheena on valittujen ja implementoitujen kontrollien arviointi. Vaiheen tarkoituksena on selvittää, onko valitut kontrollit implementoitu suunnitelmien mukaisesti ja tuottavatko ne halutun tuloksen samalla noudattaen tietojärjestelmän ja organisaation asettamia tietoturva- ja tietosuojavaatimuksia (Ross, ym., 2018).

Vaihe sisältää kuusi tehtävää, joista ensimmäisenä on arvioijan tai tiimin valitseminen. Arviointi voidaan suorittaa organisaation omaa henkilöstöä hyödyntämällä, mutta vaihtoehtoisesti organisaatio voi hankkia käyttöönsä riippumattomia kontrollien arvioijia tehtävää varten. Toisena vaiheena on arviointisuunnitelma, jonka aikana arviointien suorittamiseen tarvittavat asiakirjat toimitetaan arvioijalle, turvallisuuden ja tietosuojan arviointisuunnitelmia kehitetään ja dokumentoidaan sekä tarkistetaan ja hyväksytään, jolloin valvonta-arvioinneille asetettava työmäärä ja odotukset on mahdollista selvittää. (Ross, ym., 2018.)

Kolmantena tehtävänä hallintakeinoja arvioitaessa organisaation tulisi varmistua arvioinnin vastaavan turvallisuuden- ja tietosuojan arviointisuunnitelmia. Tehtävän aikana tulisi myös hyödyntää aiempia arviointeja ja automatisointia, jonka avulla prosessin kustannustehokkuutta ja nopeutta voidaan parantaa. Neljäntenä tehtävänä ovat arviointiraportit, joihin kerätään keskeiset turvallisuutta ja tietosuojaa koskevat havainnot ja suositukset. (Ross, ym., 2018.)

Viidentenä tehtävänä ovat korjaustoimet, jonka aikana tietojärjestelmälle ja toimintaympäristölle toteutettujen kontrollien puutteet korjataan. Tämän lisäksi myös tietoturva- ja tietosuojasuunnitelmat päivitetään vastaamaan arviointien ja myöhempien korjaustoimenpiteiden perusteella tehtyjä valvonnan toteutusmuutoksia. Viimeisenä tehtävänä on toimintasuunnitelman ja virstanpylväiden kehittäminen, jotka sisältävät yksityiskohtaiset korjaussuunnitelmat turvallisuuden ja tietosuojan arviointiraporteissa tunnistetuille ei-hyväksyttäville riskeille. (Ross, ym., 2018.)

3.6.6 Valtuuttaminen

Valtuuttamisvaiheen tarkoituksena on osoittaa organisaation vastuuvelvollisuus vaatimalla ylimmän johdon määrittävän turvallisuuden ja tietosuojan riskitaso hyväksyttäväksi verrattuna organisaation toimintoihin, varoihin, henkilöstöön sekä muihin organisaatioihin. Vaihe koostuu viidestä tehtävästä, joista ensimmäisenä on valtuutuspaketin toimittaminen valtuutetulle virkamiehelle.

Valtuutetulla virkamiehellä tarkoitetaan henkilöä, jolla on valtuudet ja vastuu tietojärjestelmän käytöstä. Paketti koostuu turvallisuus- ja tietosuojasuunnitelmista, tietoturva- ja tietosuoja-arviointiraporteista sekä toimintasuunnitelmista, virstanylväistä ja niiden yhteenvedosta. (Ross, ym., 2018.)

Toisena tehtävänä on riskianalyysi, jonka aikana valtuutettu suorittaa riskienhallintastrategiaa heijastavan riskienmäärityksen ja riskinsietokyvyn. Kolmantena tehtävänä on tunnistettuihin riskeihin vastaaminen. Tehtävät neljä ja viisi ovat valtuuttamisen päätöksen tekeminen ja siitä raportointi. Päätös koskee tietojärjestelmän tai yleisten kontrollien hyväksymistä tai hyväksyttämättä jättämistä, jonka jälkeen organisaation toimihenkilölle tulisi raportoida tehty päätös, merkittävät haavoittuvuudet ja riskit. (Ross, ym., 2018.)

3.6.7 Seuranta

Riskienhallinnan viitekehyksen viimeisenä vaiheena on seuranta, joka koostuu seitsemästä tehtävästä. Vaiheen tarkoituksena on ylläpitää jatkuvaa tilannetietoisuutta tietojärjestelmän ja organisaation turvallisuutta ja tietosuojaa koskevista asioista, jotka tuottavat tietoa organisaation riskienhallintapäätösten tueksi. (Ross, ym., 2018.)

Vaiheen ensimmäinen tehtävä käsittelee tietojärjestelmän ja toimintaympäristön muutoksia, joita tulee seurata jatkuvan seurantastrategian mukaisesti. Toisena tehtävänä ovat jatkuvat arvioinnit, joiden avulla pyritään varmistumaan siitä, että kontrollit toimivat tehokkaasti ja noudattavat myöskin jatkuvaa seurantastrategiaa. Jatkuvan seurannan tulokset analysoidaan ja niihin vastataan tehtävässä kolme. (Ross, ym., 2018.)

Tehtävän neljä aikana valtuutuspakettia päivitetään, jotta riskienhallinnan dokumentit vastaavat jatkuvan seurannan aktiviteetteja. Viides tehtävä sisältää turvallisuuden ja tietosuojan raportoinnin, joka tulee toimittaa valtuutetulle virkamiehelle, sekä muille johdon henkilöille. Valtuutetut hyödyntävät tehtävän kuusi aikana jatkuvan seurannan aktiviteetteja ja kommunikoivat mahdollisista muutoksista, jotka kohdistuvat riskinmääritys- ja hyväksymispäätöksiin. Viimeisenä tehtävänä on suorittaa toimenpiteet järjestelmän mahdollista hävittämistä varten. (Ross, ym., 2018.)

3.7 Yhteenveto

Tässä luvussa käsiteltiin ISO 31000:2018 riskienhallinnan ohjeita ja siihen sisältyviä riskienhallinnan periaatteita, puitteita ja prosessia. Tämän lisäksi luvussa käsiteltiin NIST SP 800-37r2 mukaista seitsemänvaiheista riskienhallinnan viitekehystä ja NIST SP 800-39 mukailtua, kolmitasoista lähestymistapaa organisaation riskienhallintaan, jota sovelletaan myös NIST SP 800-37r2 riskienhallinnan viitekehyksessä.

ISO 31000:2018 riskienhallinnan ohjeiden käsittely aloitettiin periaatteista, joiden ydinajatuksen esitettiin olevan arvon luominen ja suojaaminen sekä pe-

rusteiden tarjoaminen, jotta riskejä on mahdollista tehokkaasti kuvata. Tämän jälkeen tutustuttiin ISO 31000:2018 mukaisiin riskienhallinnan puitteisiin. Puitteiden vaikuttavuuden esitettiin korostuvan erityisesti sen sitoessa riskienhallinnan osaksi organisaation hallintotapaa, johtamisjärjestelmää ja päätöksentekoa. ISO 31000:2018 riskienhallintaprosessi käsiteltiin muita osia kattavammin. Prosessi sisältää kuusi riskienhallinnalle oleellista vaihetta ja se esitettiin räätälöitäväksi kokonaisuudeksi, jonka on mahdollista toimia kaikilla organisaation tasoilla.

Luvun jälkipuoliskolla käsiteltiin NIST SP 800-37r2 riskienhallinnan viitekehystä, jonka esitettiin olevan osa laajempaa NIST SP 800 -sarjaa. Viitekehys rakentuu seitsemästä vaiheesta, jotka sisältävät useita tehtäviä ja ohjeita näiden toteuttamiseksi. Viitekehyksen tarkoituksena on edistää lähes reaaliaikaista riskienhallintaa toteuttamalla jatkuvia seurantaprosesseja ja siten auttamalla organisaatiota hallitsemaan turvallisuuteen ja tietosuojaan kohdistuvia riskejä.

Kokonaisuutena luvun tarkoituksena oli kerätä tietoa esitetyistä riskienhallintamalleista, jotta tutkielman luvussa neljä olisi mahdollista suorittaa riskienhallintamallien välinen vertailu. Vertailun lisäksi kolmannen luvun aikana kerätty aineisto ja ymmärrys yhdessä haastattelujen kanssa tukevat pohdintaa esitettyjen riskienhallintamallien samanaikaisen käytön tarjoamista hyödyistä ja mahdollisista muista vaikutuksista.

4 RISKIENHALLINTAPROSESSIN JA RISKIENHALLINNAN VIITEKEHYKSEN VERTAILUA

Tutkielman neljännessä luvussa vertaillaan luvussa kolme käsiteltyä ISO 31000:2018 riskienhallintaprosessia ja NIST SP 800-37r2 mukaista riskienhallinnan viitekehystä. Vertailun lisäksi luvussa esitetään pohdintaa mallien samanaikaisen käytön mahdollisuuksista ja hyödyistä. Luvun tarkoituksena on teorian pohjalta vastata tutkielman toiseen tutkimuskysymykseen: *"Miten ISO 31000:2018 riskienhallintamallin ohjeet ja NIST SP 800-37r2 riskienhallinnan viitekehys vertautuvat toisiinsa?"*.

4.1 Riskienhallintamallien vertailu

Kuten luvun kolme aikana huomattiin, SFS-ISO 31000:2018 (2018) mukainen riskienhallintaprosessi perustuu kolmen osatekijän muodostamaan kokonaisuuteen, eli standardissa määriteltyihin periaatteisiin, puitteisiin ja prosessiin. SFS-ISO 31000:2018 (2018) esittää osatekijöiden voivan olla käytössä joko kokonaisuutena tai erikseen. Teknologianeutraaliksi kuvattu NIST SP 800-37r2 riskienhallinnan viitekehys tarjoaa myöskin ohjeita riskienhallinnan viitekehyksen soveltamiseen erityisesti tietojärjestelmien ja organisaatioiden osalta (Ross, ym., 2018). Sekä ISO 31000:2018 että NIST SP 800-37r2 tarjoavat lukijalleen keskeiset käsitteet, jotta riskienhallinnan terminologiaa voidaan sujuvasti hyödyntää.

Käsitellyt mallit eroavat toisistaan jo aivan alussa. ISO 31000:2018 tarjoamaa prosessia voidaan kuvailla laveaksi ja se on mahdollista räätälöidä organisaation tarpeita vastaaviksi. Malli ei sisällä toiminnallisia pakotteita, vaan se pyrkii ohjaamaan riskienhallintaprosessin toteuttamista asettamalla erilaisia huomioitavia asioita, jonka avulla riskienhallintaprosessin toteuttamisessa on mahdollista onnistua. Toisin sanoen ISO 31000:2018 mukainen malli osoittaa kuljettavan suunnan, mutta se ei pidä kulkijan kädestä niin tiukasti kiinni, etteikö mallia olisi mahdollista soveltaa.

NIST SP 800-37r2 mukainen malli sen sijaan pyrkii tiukasti ohjaamaan riskienhallinnan toteutusta. Mallin ensimmäisenä vaiheena on käyttöönoton valmistelu. Vaihe jakautuu 18 tehtävään, joiden suorittaminen on pääasiassa välttämätöntä, jotta NIST SP 800-37r2 mallin mukaisia riskienhallintaprosessin muita vaiheita on mahdollista toteuttaa (Ross, ym., 2018.) ISO 31000:2018 (2018) mukainen riskienhallintaprosessi ja NIST SP 800-37r2 riskienhallinnan viitekehys painottavat molemmat ylimmänjohdon sitoutumisen ja vastuun tärkeyttä riskienhallinnan onnistumiselle (Ross, ym., 2018).

SFS-ISO 31000:2018 (2018) mukainen riskienhallinnan prosessi aloitetaan käsittelemällä viestintää ja tiedonvaihtoa, jonka ydinajatuksena on tiedon ja ymmärryksen lisääminen riskeistä sekä päätöksentekoa tukevan palautteen ja tiedon antaminen. NIST SP 800-37r2 mukainen kategorisointivaihe ei itsessään avaa organisaation sisäisen tai ulkoisen viestinnän tärkeyttä. Vaiheen tehtävänä on kuitenkin tiedottaa organisaation riskienhallinnan prosesseista ja tehtävistä määrittämällä haitalliset vaikutukset organisaation toimintoihin, omaisuuteen, yksilöihin ja muihin organisaatioihin. Rossin, ym. (2018) mukaan NIST SP 800-37r2 kuitenkin korostaa sidosryhmien välisen viestinnän tärkeyttä viitekehyksen jokaisessa vaiheessa.

Sekä ISO 31000:2018 että NIST SP 800-37r2 käsittelevät kattavuutta, toimintaympäristöä ja kriteereitä, sillä ne vaikuttavat organisaation suojaamiseen tarvittavien hallintakeinojen määrittelyyn. Molemmat mallit painottavat myös jatkuvaa arviointia mahdollisten muutosten tekemistä esimerkiksi riskikriteereitä määriteltäessä (ISO 31000:2018, 2018; Ross, ym., 2018). NIST SP 800-37r2 viitekehyksessä organisaation tulisi kehittää ja toteuttaa strategia, jonka avulla asetettujen hallintakeinojen tehokkuutta voidaan mitata, tästä syystä hallintakeinojen konfiguroinnin dokumentoinnin tärkeyttä on myös painotettu. Hallintakeinojen arviointi on tärkeää myös siksi, että sen avulla selvitetään tuottavatko ne halutun tuloksen samalla noudattaen tietojärjestelmän ja organisaation asettamia tietoturva- ja tietosuojavaatimuksia. (Ross, ym., 2018.) SFS-ISO 31000:2018 (2018) mittaamisen painotus kohdistuu vastaavasti riskikriteereihin, jolloin organisaation velvoitteet ja sidosryhmien näkemykset korostuvat.

Riskien käsittelyn ja riskianalyysin osalta molemmat mallit ovat hyvin samankaltaisia. Mallit ohjaavat organisaatiota määrittämään toimintatavat havaittujen riskien kanssa toimimiseen ja niiden mahdolliseen hyväksymiseen. Molemmissa malleissa käsitellään myös tehtyjen päätösten raportoinnin ja dokumentoinnin tärkeyttä. NIST SP 800-37r2 ei kuitenkaan sisällä erillisiä riskinarviointimenetelmiä, vaan viittaa menetelmien osalta NIST SP 800-30 -ohjeeseen (Lambrinoudakis, ym., 2022).

Seuranta on olennainen vaihe ISO 31000:2018 riskienhallintaprosessia ja NIST SP 800-37r2 riskienhallinnan viitekehystä. Molemmat mallit ovat yhtä mieltä toimintaympäristöä ja riskienhallintaa koskevan tiedon seurannan tärkeydestä. Seurannan painotus NIST SP 800-37r2 riskienhallinnan viitekehyksessä korostuu asetettujen kontrollien seurantaan ja niiden tehokkuuden ylläpitämiseen. Seurannan ja katselmointien tulisi olla osa kaikkia riskienhallintaprosessin vaiheita, jolloin tiedon keruu ja analysoiminen korostuvat. Muodostetut

tallenteet ja raportit tarjoavat tukea päätöksentekoa varten ja edistävät vuorovaikutusta sidosryhmien kanssa. (SFS-ISO 31000:2018 2018.) NIST SP 800-37r2 viitekehyksessä tallenteiden ja raporttien roolia ei ole yhtä kattavasti esitetty, vaikka ne ovatkin osoitettu johdon hyödynnettäviksi.

Vertailun loppuun on kerätty mallien eroavaisuuksista ja samankaltaisuuksista taulukko (Taulukko 2). Taulukon pyrkimyksenä on esittää havainnot selkeässä muodossa.

TAULUKKO 2 Käsiteltyjen riskienhallintamallien vertailu.

Havainto	**ISO 31000:2018**	**NIST SP 800-37r2**
Mallin keskeiset käsitteet tai sanasto on löydettävissä.	Keskeiset käsitteet ovat osana mallia.	Keskeiset käsitteet ovat osana mallia.
Malli sisältää toimintamenetelmiä riskienhallintaprosessin tai viitekehyksen käyttöönottamisesta.	Suorat esimerkit toimintamenetelmien soveltamisesta eivät ole sisällytettyinä.	Viitekehyksen käyttöönottoa edeltävät tehtävät sisältyvät osana viitekehystä.
Malli on organisaation sovellettavissa.	ISO 31000:2018 mukainen riskienhallintaprosessi on periaatteeltaan lavea ja sovellettavissa.	NIST SP 800-37r2 mukainen viitekehys sisältää tehtäviä, jotka ohjaavat viitekehyksen käyttöä. Osittainen räätälöinti on mahdollista.
Riskienhallintaprosessin -tai viitekehyksen fokus.	ISO 31000:2018 mukaista riskienhallintaprosessia voidaan soveltaa organisaatiosta riippumatta myös yksittäisen prosessin tasolla.	NIST SP 800-37r2 riskienhallinnan viitekehyksen esitetään soveltuvan valtion organisaatioihin ja tietojärjestelmiin (Ross, ym., 2018) sekä yksityisen sektorin organisaatioihin (Lambrinoudakis, ym., 2022).
Viestintä ja tiedonvaihto.	Viestintä ja tiedonvaihto toimivat päätöksenteon tukena ja luomat mukaan kuulumisen ja omistajuuden tunteen niille, joihin riskit vaikuttavat (SFS-ISO 31000:2018, 2018).	Viestinnän ja tiedonvaihdon tärkeys tuodaan esille, mutta tietojärjestelmien välinen kommunikointi on korostettuna (Ross, ym., 2018).
Hallintakeinot.	Painotus kohdistuu kattavuuden, organisaation tavoitteiden ja toimintaympäristön määrittelyyn, jonka perusteella hallintakeinot ja riskikriteerit määritellään.	Hallintakeinoissa panostetaan konfiguroinnin ja dokumentoinnin tärkeyttä.
Seuranta.	Seuranta ja katselmoinnit tarjoavat tietoa riskienhallinnan toteutusten, tulosten ja vaikuttavuuden laadusta.	Seurannassa painottuu asetettujen kontrollien tehokkuuden ylläpitäminen.
Tallenteet ja raportointi.	ISO 31000:2018 painottaa tallenteiden ja raportoinnin tuomia hyötyjä, jotka näkyvät erityisesti riskienhallintatoimien ja vuorovaikutuksen kehittämisessä.	Tallenteiden ja raportoinnin hyödyt tarjoavat johdolle työkaluja, joista kommunikoidaan havaittaessa mahdollisia muutostarpeita.

Vaikka käsitellyt riskienhallintamallit sisältävätkin selkeitä eroavaisuuksia, myös samankaltaisuuksia on havaittavissa. Pohjimmiltaan eroavaisuudet liittyvät ISO 31000:2018 riskienhallintaprosessin ja NIST SP 800-37r2 riskienhallinnan viitekehyksen painotukseen. ISO 31000:2018 tarjoaa laajemmat mahdollisuudet soveltaa riskienhallintaprosessia erilaisiin tarpeisiin ja NIST SP 800-37r2 osoittaa suoraan välttämättömät tehtävät riskienhallinnan suorittamiselle.

Malliltaan lavea riskienhallintaprosessi voi tarjota käyttäjälleen riittävän määrän työkaluja riskienhallintaa varten. Vastaavasti se myös pakottaa ohjeiden käyttäjän aidosti ymmärtämään organisaation toimintakentän asettamat vaatimukset, joka onkin tarpeellista riskienhallintaprosessia räätälöidessä.

Tarkkaan laaditut riskienhallinnan ohjeet voivat tarjota organisaatiolle hyvät lähtöasetelmat riskienhallinnan toteuttamista varten, mutta tarkkojen ohjeiden varjopuolena voivat olla jatkokehitykseen liittyvät haasteet. Jatkokehitys voi olla haasteellista esimerkiksi siksi, että organisaatiossa on totuttu seuraamaan valmista ajatustyötä, eikä ohjeen ulkopuolisille toimenpiteille haluta myöntää resursseja. Liian tarkat ohjeet voivat olla haitallisia myös siksi, että riskienhallinnasta voi muodostua suorituskeskeistä. Tällöin valmiiden ohjeiden seuraaminen voidaan kokea riittäväksi, eikä ohjeiden ulkopuolista työtä haluta tehdä.

4.2 Riskienhallintamallien samanaikainen käyttö

Esitettyjen riskienhallintamallien samanaikaisen käytön voidaan ajatella olevan teoriasta kerätyn tiedon pohjalta mahdollista. Täysin vastaavista riskienhallintamalleista ei ole tehty tutkimusta, mutta Al-Fikri, ym. (2019) esittivät tietoturvariskien hallinnan standardin ISO 27005 ja NIST SP 800-30r1 riskiarvioinnin ohjeiden yhdistämisen mahdolliseksi. Mallien tekniikoita oli mahdollista yhdistää, sillä NIST SP 800-30r1 ei sisältänyt ohjeita riskien kuvaamiseen, jolloin ISO 27005 -standardin ohjeita oli mahdollista hyödyntää (Putra, Pradana & Setiawan, 2017). Toisin sanoen ohjeista löytyviä puutteita oli mahdollista täydentää hyödyntämällä toista standardia.

SFS-ISO 31000:2018 (2018) esittääkin riskienhallintaprosessille olevan useita käyttökohteita organisaation sisällä, jolloin prosessia tulisi räätälöidä tavoitteiden saavuttamista varten, sekä ulkoisessa että sisäisessä toimintaympäristössä. Tämän voisikin ajatella olevan eräänlainen kannustin muiden viitekehysten ja mallien hyödyntämiseen. ISO 31000:2018 (2018) ei myöskään sisällä velvoitteita tai pakotettuja toimenpiteitä, vaan pyrkii lavealla ohjeistuksellaan tarjoamaan systemaattista ohjausta riskienhallinnasta vastaaville, jolloin myös soveltamiselle jää tilaa.

Riskienhallintamallien mahdollisesta samanaikaisesta käytöstä kiinnostuneiden tulisi kuitenkin ymmärtää, että malleja ei ole tarpeellista noudattaa orjallisesti. Tällä tarkoitetaan sitä, että ISO 31000:2018 sisältämiä ohjeita voitaisiin tarpeen vaatiessa täydentää hyödyntämällä NIST SP 800-37r2 yksittäisiä vaiheita tai tehtäviä. Lambrinoudakis, ym. (2022) esittävätkin riskienhallinnan viite-

kehysten tarjoavan erilaisia vaihtoehtoja riskienhallintaa varten. Mallien käyttöä ei voida kuitenkaan pitää täysin ongelmattomana, sillä yksittäisenkin ohjeen käyttäminen vaatii laajaa ymmärrystä riskienhallinnasta ja organisaation toimintaympäristöstä.

Yksittäiset vaiheet tai tehtävät voisivat kuitenkin tuoda organisaatiolle valmiuksia sekä uusia ajatuksia riskienhallinnan toimenpiteiden suorittamiseksi. Tästä hyvänä esimerkkinä toimii NIST SP 800-37r2 riskienhallinnan viitekehyksen ensimmäinen vaihe, käyttöönoton valmistelu, jota ei ole sisällytetty ISO 31000:2018 riskienhallinnan ohjeisiin.

5 TUTKIMUKSEN TOTEUTUS

Luvussa viisi esitetään tutkimuksen tavoitteet, käytetty tutkimusmenetelmä, sekä tutkimuskysymykset. Luvun aikana käsitellään myös tutkimusprosessi ja tutkimuksen rajaukset. Luvun tarkoituksena on esittää, miten tutkimusongelmaan pyrittiin vastaamaan.

5.1 Tutkimuksen tavoitteet ja tutkimusmenetelmä

Tutkielman tavoitteena oli kerätä tietoa ja selvittää, miten ICT-organisaatioiden tulisi toteuttaa riskienhallintaa ja kannattaisiko yleisesti sovellettujen ISO 31000:2018 riskienhallinnan ohjeiden lisäksi hyödyntää NIST SP 800-37r2 riskienhallinnan viitekehystä. Tutkimusote oli laadullinen. Kirjallisuuden lisäksi tietoa kerättiin haastattelemalla erään suomalaisen ICT-organisaation turvallisuusjohtajia. Turvallisuusjohtajien valitseminen haastateltaviksi oli tarkoituksenmukainen valinta, sillä kattavan tietopääoman lisäksi he omaavat laajan kokemuksen riskienhallinnasta ICT-alalta. Juutin ja Puusan (2020) mukaan laadullisessa tutkimuksessa valitaan harkinnanvaraisesti pieni määrä tapauksia, jotka tietävät tutkittavasta ilmiöstä mahdollisimman paljon, ja joilla on tutkittavasta asiasta kokemusta.

Laadullisessa tutkimuksessa pyritään tyypillisesti ymmärtämään tutkimuksessa tarkasteltavaa ilmiötä tutkimuksen kohteena olevien henkilöiden asemasta. Tällöin kohteena olevien henkilöiden kokemukset, tunteet sekä ajatukset käsiteltävistä asioista ovatkin tarkastelun erityisenä kohteena. (Juuti & Puusa, 2020.) Hirsjärven, Remeksen ja Sajavaaran (2010) mukaan laadulliselle tutkimukselle on myös tyypillistä, että kohdejoukko valitaan tarkoituksenmukaisesti. Vaikka laadullisessa tutkimuksessa painotetaankin kohteena olevien henkilöiden tärkeyttä, Juuti ja Puusa (2020) muistuttavat teorian ja aineistojen välisen vuoropuhelun olevan tärkeässä asemassa esimerkiksi aineistojen hankinnan suunnittelussa, analysoinnissa ja tulkinnassa.

Juuti ja Puusa (2020) esittävät laadullisen tutkimuksen koostuvan seuraavista vaiheista: (1) aiheen valinnasta; (2) tutkimuksen tavoitteiden asettamisesta; (3) tutkimuskysymysten muotoilemisesta; (4) tutkimuksen rajauksien esittelystä; (5) teoreettisen viitekehyksen laatimisesta kirjallisuuden avulla; (6) lähestymistavan valinnasta ja perustelusta; (7) tutkimusmenetelmien, näytteen tai aineiston valinnasta, kuvailusta ja perustelusta; (8) aineiston hankinnasta; (9) aineiston analysoinnista ja tulkinnasta; (10) tulosten kirjoittamisesta, raportoinnista sekä tutkimuksen luotettavuuden arvioinnista.

Laadullinen tutkimus sisältää vaikutteita useista ajattelusuunnista ja tutkimustraditioista. Laadullisen tutkimuksen kenttä ei myöskään muodosta yhtenäistä kokonaisuutta, jota voidaankin pitää yhtenä laadullisen tutkimuksen vahvuuksista. Tämän lisäksi laadullisen tutkimuksen muina vahvuuksina ovat sen joustavuus sekä mahdollisuus tarkentaa tutkimuskysymyksiä aineistonkeruun jälkeen. (Juuti & Puusa, 2020.)

Juutin ja Puusan (2020) mukaan laadullinen tutkimus keskittyy tutkimaan yksittäisiä tapauksia, jolloin laadullista tutkimusmenetelmää voidaan pitää tämän tutkielman kannalta sopivana menetelmänä. Myers (2015) esittääkin, että tietojärjestelmien sekä johtamis- ja organisaatiotutkimuksen aloilla laadullinen tutkimus on aiemmin ollut huomattavasti harvinaisempaa kuin määrällinen tutkimus. Nykyisin alan laadullisia julkaisuja pidetään kuitenkin parhaina (Myers, 2015).

Vaikka laadullinen tutkimus ei olekaan täysin aineistolähtöistä, menetelmä mahdollistaa sekä kirjallisuuden että haastattelujen samanaikaisen hyödyntämisen tutkimuskysymyksiin vastattaessa. On siis mahdollista, että teoriatiedon pohjalta nousevat havainnot voisivat osoittaa myönteisiä vaikutuksia yhdistettäessä useita riskienhallinnan standardeja ja ohjeita, mutta tutkimukseen osallistuneiden subjektiiviset kokemukset eivät tukisi tällaista toimintatapaa.

Tutkimus rajattiin käsittelemään ICT-organisaatioita ja niissä suunniteltavaa ja toteutettavaa riskienhallintaa. Tutkimuskysymykset olivat:

- *Miten riskienhallinta tulisi toteuttaa ICT-alan organisaatiossa?*
- *Miten ISO 31000:2018 riskienhallintamallin ohjeet ja NIST SP 800-37r2 riskienhallinnan viitekehys vertautuvat toisiinsa?*
- *Voiko ISO 31000:2018 riskienhallintamallin ohjeiden ja NIST SP 800-37r2 riskienhallinnan viitekehyksen yhdistäminen tehostaa riskienhallinnan suunnittelua ja toteutusta ICT-organisaatiossa?*

Teoreettista viitekehystä varten kirjallisuutta kerättiin hyödyntämällä seuraavia tietokantoja: Google Scholar, Elsevier, IEEE Xplore, ProQuest, Science Direct sekä Springer. Tiedonhaku suoritettiin pääosin englanninkielisiä hakutermejä hyödyntämällä, kuten ”Risk management”, ”Information security frameworks” ”ISO 31000:2018”, ”NIST SP 800-37” ja ”Risk management Guidelines”. Kirjallisuutta pyrittiin arvioimaan hyödyntämällä Julkaisufoorumin kolmiportaista luokitteluasteikkoa.

5.2 Aineiston keruu

Juutin ja Puusan (2020) mukaan laadullisen tutkimuksen keskittyessä tutkimaan yksittäisiä tapauksia, on tyypillistä suosia ihmistä tiedon keruun instrumenttina näille luonnollisissa tilanteissa. Laadulliselle tutkimukselle ominaista on siis tuoda esiin siihen osallistuvien ihmisten näkökulma ja ajatukset, jolloin tiedonkeruumenetelminä toimivat erilaiset haastattelu- ja havainnointimenetelmät. Tämän lisäksi laadulliselle tutkimukselle on tavallista hyödyntää myös valmiita, tutkijasta riippumattomia aineistoja, kuten lehtiartikkeleita tai erilaisista dokumenteista koottua tietoa. (Tuomi & Sarajärvi, 2018; Juuti & Puusa, 2020.)

Juutin ja Puusan (2020) mukaan laadullisessa tutkimuksessa aineiston riittävä määrä on tutkimuskohtaista, jolloin esimerkiksi haastateltavien määrä on aina riippuvainen tutkimuksen tarkoituksesta ja tavoitteista. Tuomen ja Sarajärven (2018) mukaan laadullinen tutkimus ei pyri tilastollisiin yleistyksiin, vaan ilmiöiden ja tapahtumien kuvaamiseen, toiminnan ymmärtämiseen tai teoreettisesti mielekkään tulkinnan antamiseen jollekin ilmiölle.

Hirsjärvi ja Hurme (2022) kuvaavat haastattelua joustavaksi menetelmäksi, joka sopii moniin erilaisiin tutkimustarkoituksiin. Tämä johtuu siitä, että haastattelutilanteessa ollaan suorassa vuorovaikutuksessa tutkittavan kanssa, jolloin tilanne luo mahdollisuuden suunnata tiedonhankintaa itse tilanteessa (Hirsjärvi & Hurme, 2022). Hirsjärven ja Hurmen (2022) mukaan haastattelu voidaan valita useasta syystä. Heidän mukaansa haastattelu sopii esimerkiksi sellaisiin tilanteisiin, joissa tutkittava aihe on vähän kartoitettu, tutkijan on vaikea tietää etukäteen vastausten suuntia tai vaihtoehtoisesti tiedetään ennalta, että tutkimuksen aihe tuottaa monitahoisesti ja moniin suuntiin viittaavia vastauksia (Hirsjärvi & Hurme, 2022).

Tutkielman aineistonkeruu suoritettiin hyödyntämällä puolistrukturoituja yksilöhaastatteluja, jonka kysymykset näkyvät ensimmäisessä liitteessä (Liite 1). Tutkimushaastattelujen erot syntyvät lähinnä strukturointiasteen perusteella, eli miten kiinteästi kysymykset on muotoiltu ja missä määrin haastattelija jäsentää tilannetta. Puolistrukturoituihin haastatteluihin päädyttiin, sillä ne pysyvät johdonmukaisina, mutta samalla mahdollistavat kysymysten järjestyksen muuttamisen. (Hirsjärvi & Hurme, 2022.) Myersin (2020) mukaan puolistrukturoidut haastattelut myös mahdollistavat sen, että haastateltavat voivat tarkentaa vastauksiaan esitettyihin kysymyksiin yksittäisen vastausvaihtoehdon valitsemisen sijasta. Tuomi ja Sarajärvi (2018) lisäävät puolistrukturoidun haastattelun etuihin myös sen, että haastattelija voi tarkentaa ja syventää kysymyksiä haastateltavien vastauksiin perustuen. Kysymysten tarkentaminen mahdollistaa myös sen, että haastattelujen aikana tehdään havaintoja asioista, joista ei ollut ennalta määriteltyjä kysymyksiä.

Hirsjärvi ja Hurme (2020) esittävät puolistrukturoitujen haastatteluiden haittapuoleksi sen, että haastatteluista voi kertyä paljon tutkimusaiheen kannalta epärelevanttia materiaalia. Epärelevantin materiaalin lisäksi heidän mukaan-

sa haastatteluissa ei voida taata samaa anonyymiutta kuin kyselylomakkeilla (Hirsjärvi & Hurme, 2020). Qun ja Dumayn (2011) mukaan myös haastattelijan tulee kattavasti ymmärtää käsittelemänsä aihekokonaisuus, jotta perusteltuja kysymyksiä on mahdollista esittää.

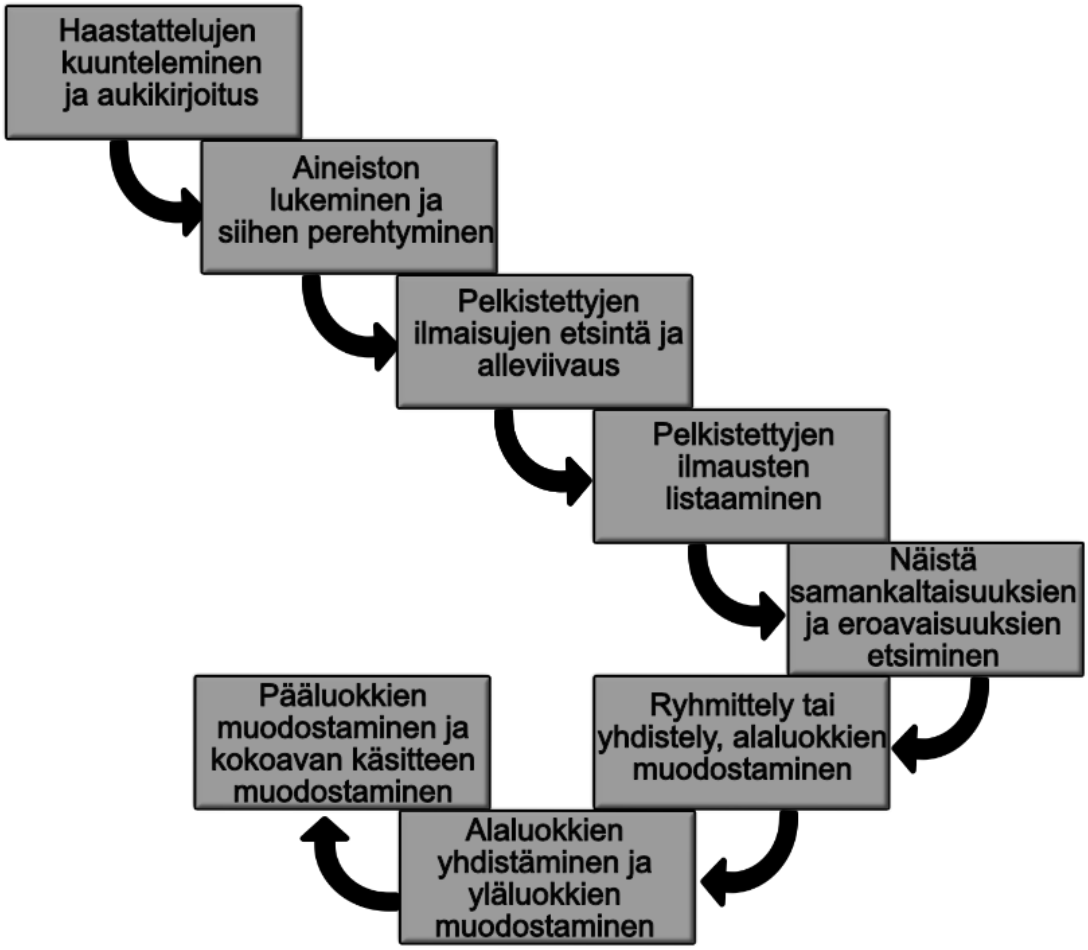
Tutkielman aikana siihen osallistuville haastateltaville esitettiin haastattelun käyttötarkoitus ja haastattelujen nauhoittamiseen pyydettiin erikseen lupa jokaiselta haastateltavalta. Haastateltavia myös informoitiin haastattelun anonymisoinnista, eli sellaisesta henkilötietojen käsittelystä, josta henkilöä ei voida enää tunnistaa ja nauhoitteiden poistamisesta työn valmistuttua.

5.3 Sisällön analyysi

Juutin ja Puusan (2020) mukaan laadullisessa tutkimuksessa aineiston analyysi kytkeytyy kiinteästi aineiston hankintaan, sillä tutkijan esiymmärrys vaikuttaa aineiston hankintaan ja tällöin myös sen analyysiin. Hyvärinen (2010) esittää laadulliselle analyysille olevan tyypillistä aineiston ja tutkimusongelman tiivis vuoropuhelu. Analyysin tavoitteena on luoda kerätystä aineistosta mielekäs kokonaisuus, jonka avulla on mahdollista tuottaa sekä perusteltu tulkinta että johtopäätöksiä tutkittavasta aiheesta (Juuti ja Puusa, 2020).

Tuomi ja Sarajärvi (2018) esittävät sisällönanalyysin olevan perusanalyysimenetelmä, jota voidaan käyttää kaikissa laadullisen tutkimuksen perinteissä. Heidän mukaansa useimmat eri nimillä kulkevat laadullisen tutkimuksen analyysimenetelmät perustuvat sisällönanalyysiin, jos sillä tarkoitetaan kirjoitettujen, kuultujen tai nähtyjen sisältöjen analyysia laveana teoreettisena kehyksenä (Tuomi & Sarajärvi, 2018).

Hirsjärven ja Hurmen (2022) mukaan analyysi on monivaiheinen prosessi, jonka aikana eritellään ja luokitellaan aineistoa. Tämän jälkeen synteesissä pyritään luomaan ja esittämään kokonaiskuva tutkittavasta ilmiöstä. Juutin ja Puusan (2020) mukaan sisällönanalyysi voidaan ymmärtää väljänä metodisena viitekehyksenä, joka mahdollistaa aineiston monipuolisen tarkastelun. Tutkielmassa toteutettu aineistolähtöinen sisällön analyysi voidaan esittää seuraavan kuvion (Kuvio 6) mukaisesti.



KUVIO 6 Aineistolähtöisen sisällönanalyysin eteneminen (Tuomi & Sarajärvi, 2018).

Aineiston litterointi aloitettiin yllä olevan kuvion (Kuvio 6) mukaisesti kuuntelemalla nauhoitetut haastattelut läpi, jonka aikana haastatteluista saatu aines myös kirjoitettiin auki. Aukikirjoitettuun aineistoon perehdyttiin ja siitä pyrittiin löytämään keskeisiä pelkistettyjä ilmauksia. Tällaista prosessia kutsutaan redusoinniksi, eli alkuperäisdatan pelkistämiseksi, jossa aineistosta karsitaan tutkimukselle epäolennainen pois (Tuomi & Sarajärvi, 2018). Juuti ja Puusa (2020) esittävät aineiston pelkistämisen ja tiivistämisen välttämättömäksi, sillä rikas aineisto on sellaisenaan hajanaista. Pelkistetyt ilmaukset kerättiin omalle dokumentilleen listattuun muotoon, jotta niistä pystyttiin etsimään mahdollisia samankaltaisuuksia ja eroavaisuuksia. Vaiheen jälkeen aloitettiin aineiston luokittelu.

Hirsjärven ja Hurmen (2022) mukaan aineiston luokittelu on olennainen osa analyysiä, sillä se luo pohjan tai kehyksen, jonka varassa haastatteluaineistoa voidaan myöhemmin tulkita, yksinkertaistaa ja tiivistää. Vaiheen tarkoituksena on käydä läpi aineistosta koodatut alkuperäisilmaukset ja etsiä niistä sa-

mankaltaisuuksia ja mahdollisia eroavaisuuksia kuvaavia käsitteitä. Tällöin alkuperäisdatasta muodostetut pelkistetyt ilmaukset myös ryhmitellään omiin alaluokkiinsa. (Tuomi & Sarajärvi, 2018.)

Kun datasta oli muodostettu omat alaluokat, niitä yhdisteltiin yläluokiksi, jotka vastaavasti muodostivat omat pääluokkansa. Seuraava taulukko (Taulukko 3) toimii esimerkkinä aineistosta kerätyistä pelkistetyistä ilmauksista, joiden pohjalta luokat muodostettiin.

TAULUKKO 3 Käsitteellistetty aineisto.

Pelkistetyt ilmaukset	Alaluokat	Yläluokat	Pääluokka
Ohjeet riittävät. Ohjeita voisi täsmentää. Yleisellä tasolla riittävät. Terminologian haasteellisuus. Vaatii sisäistämistä. Määritelmien tärkeys. Tulkinnanvaraisuus.	Ohjeen täsmentäminen. Soveltamisen mahdollisuudet. Asian sisäistäminen. Sisällön riittävyys.	Tulkinnalliset erot. Kokemus käytöstä.	Ymmärrys ja kokemus.

Tuomen ja Sarajärven (2018) mukaan abstrahointia tulee jatkaa yhdistelemällä luokituksia, niin kauan kuin se on aineiston sisällön kannalta mahdollista. Heidän mukaansa abstrahoinnissa empiirinen aineisto liitetään teoreettisiin käsitteisiin ja tuloksissa esitetään empiirisestä aineistosta muodostettu malli, käsitteet tai mahdollisesti aineistoa kuvaavat teemat. Tuloksissa tulisi myös kuvata luokittelujen pohjalta muodostetut käsitteet tai kategoriat ja niiden sisällöt. (Tuomi & Sarajärvi, 2018.)

Hirsjärven ja Hurmen (2022) mukaan haastatteluaineistoihin perustuvissa tutkimuksissa ja erityisesti laadullisesti suuntautuneissa analyyseissä tutkijan tarkoituksena on pyrkiä onnistuneisiin tulkintoihin. Tulkinnan esitetään olevan onnistunutta, kun lukija omaksuu tutkijan kanssa saman näkökulman ja pystyy löytämään tekstistä ne asiat, jotka tutkijakin löysi, vaikka tutkija ja lukija olisivatkin näkökulmasta eri mieltä. Samaa haastattelutekstiä on kuitenkin mahdollista tulkita monin tavoin useasta näkökulmasta. (Hirsjärvi & Hurme, 2022.) Juuti ja Puusa (2020) pitävät kuitenkin keskeisenä sitä, että tutkija pystyy aineistonsa esiteltyään esittämään perustellun idean siitä, mitä asiasta voitaisiin tutkimuksen perusteella väittää.

Tutkielman aikana aineistolähtöisen sisällönanalyysin avulla haastatteluista kerätystä aineistosta muodostettiin sitä kuvaavat teemakokonaisuudet. Kokonaisuuksien sisältö käsitteli organisaation valmiuksia, mahdollisia tarpeita ja kyvykkyyksiä riskienhallinnan tehostamisessa. Teemakokonaisuuksia hyödynnettiin yhdessä kirjallisuudesta kerätyn teoriatiedon kanssa erityisesti tutkielman viimeiseen tutkimuskysymykseen vastaamisessa.

5.4 Tutkimuksen luotettavuuden ja eettisyyden arviointi

Juutin ja Puusan (2020) mukaan laadullisen tutkimuksen luotettavuutta pohditaan useimmiten kolmen käsitteen avulla. Käsitteet nimetään uskottavuudeksi, luotettavuudeksi ja eettisyydeksi. Käsitteet esitetään abstrakteiksi ja vaikeaselkoisia kokonaisuuksiksi, jotka ovat toisiinsa kytkeytyneitä. Vaikka käsitteitä ei olekaan yksiselitteisesti helppoa määritellä, yhdenkin kokonaisuuden ollessa heikko, voi koko tutkimukselta kadota pohja. (Juuti & Puusa, 2020.)

Tuomi ja Sarajärvi (2018) esittävät tutkimuksen luotettavuutta kuvaavien käsitteiden saaneen laadullisen tutkimuksen piireissä monenlaisia tulkintoja. Tulkinnallisten erojen lisäksi suomalaisessa kirjallisuudessa esiintyy myös erilaisia käännöksiä (Tuomi & Sarajärvi, 2018). Tulkinnasta ja käännöksistä johtuvat erot voivatkin vaikuttaa millaisia asioita tutkimuksessa oikein huomioidaan ja arvioidaan.

Tässä on myös hyvä huomioida, että laadullisen tutkimuksen luotettavuuden arvioinnista ei ole olemassa mitään yksiselitteistä ohjetta. Tutkimusta arvioitaessa, arvioinnin kriteereinä voitaisiin hyödyntää esimerkiksi seuraavia käsitteitä: uskottavuus, vastaavuus, siirrettävyys, luotettavuus, tutkimustilanteen arviointi, varmuus, riippuvuus ja vakiintuneisuus. Toisin sanoen käsitteet toimivat apuna luotettavuuden arvioinnissa, mutta itse tutkimusta arvioidaan kokonaisuutena, jolloin sen sisäinen johdonmukaisuus painottuu. (Tuomi & Sarajärvi, 2018.)

Juutin ja Puusan (2020) mukaan luotettavuudella tarkoitetaan tutkijan vakuuttavia ja uskottavia perusteluja ammattitaidostaan lukijalle. Ammattitaitoisuutta voidaan esittää valitsemalla ja käyttämällä perusteltuja ja oikeanlaisia lähestymistapoja sekä menetelmiä tutkimusongelmaa ratkaistaessa. Vaatimuksen esitetään kohdistuvan tutkimuksen jokaiseen vaiheeseen, jotta lukija pystyy vakuuttumaan tutkimuksen etenemisestä ja sen havainnoista. (Juuti & Puusa, 2020.)

Luotettavuuden ja uskottavuuden käsitteet vaikuttavat olevan hyvin lähellä toisiaan. Uskottavuudella viitataan Juutin ja Puusan (2020) mukaan siihen, missä määrin tutkimusta lukevat kollegat, tutkimuksen kohteena olevat henkilöt, sekä suuri yleisö hyväksyvät tutkimuksen tulokset tosiksi ja luottavat tutkimusaineiston asianmukaiseen keräämiseen ja huolelliseen analysointiin. Myös Tuomi ja Sarajärvi (2018) esittävät tutkijan olevan lukijoilleen velkaa uskottavan selityksen aineiston kokoamisesta ja sen analysoimisesta, koska myös tutkimustulokset tulevat selkeämmin ja ymmärrettävämmin esille, kun tehdyistä asioista kerrotaan yksityiskohtaisesti. Tutkimuksen uskottavuuteen liittyvät vahvasti myös se, että tutkija noudattaa hyvää tieteellistä käytäntöä, johon kuuluvat esimerkiksi rehellisyys, yleinen huolellisuus ja tutkimustyön tarkkuus (Tuomi & Sarajärvi, 2018).

Tuomen ja Sarajärven (2018) mukaan eettinen kestävyys on tutkimuksen luotettavuuden toinen puoli, vaikka eettisyys koskeekin myös tutkimuksen laatua. Heidän mukaansa tutkimuksen eettisyys mahdollisesti kiertyy tutkimuk-

sen luotettavuus- ja arviointikriteereihin, jolloin tutkimussuunnitelman ja valitun tutkimusasetelman laadukkuus, sopivuus ja raportointi korostuvat. Juutin ja Puusan (2020) mukaan eettisyydellä tarkoitetaan sitä, että tutkija on noudattanut eettisiä periaatteita koko tutkimuksen ajan, jolloin tutkimuksessa käytetyt menetelmät ja analyysitavat täyttävät kriteerin, jonka perusteella ne voisivat toimia minkä tahansa tehdyn tutkimuksen ohjenuorina. Heidän mukaansa tutkimuksen eettisyydessä korostuu myös se, että tutkimuksen kohteena oleville tai muille tutkimukseen liittyville tahoille ei saa koitua tutkimuksesta haittaa (Juuti & Puusa, 2020).

Tämän tutkielman aikana luotettavuus ja eettisyys on pyritty huomiomaan koko tutkimusprosessin ajan. Eettisyyden vuoksi tutkielman haastatteluihin osallistuneille henkilöille esitettiin haastattelun käyttötarkoitus ja haastattelun nauhoittamiseen pyydettiin lupa jokaiselta haastateltavalta. Tämän lisäksi haastattelut anonymisoitiin ja nauhoitteet hävitettiin tutkielman teon päätyttyä.

Tutkielman luotettavuutta ja uskottavuutta edistettiin osoittamalla tutkimuksen toteutuksessa käytetyt metodit sekä aineiston keruun että analyysin osalta. Tutkimuksen luotettavuutta pyrittiin myös parantamaan huolellisella perehtymisellä teoriaan sekä osoittamalla teoreettisen viitekehyksen rakentamiseksi käytetyt tietokannat ja kirjallisuuden arvioinnissa hyödynnetty Julkaisufoorumin luokitteluasteikko. Tutkimuksen aikana on noudatettu hyviä tieteellisiä käytänteitä, kuten esimerkiksi huolellisuutta ja hyviä viittauskäytänteitä. Tutkielman kirjoittamisen aikana tehdyt asiat ovat raportoitu yksityiskohtaisesti ja läpinäkyvästi, jotta tutkimustulokset ovat selkeästi ja ymmärrettävästi tulkittavissa.

6 TULOKSET JA POHDINTA

Tutkielman kuudennessa luvussa esitetään tutkielman tulokset. Luvussa esitetään pohdintaa käsiteltyjen riskienhallintamallien yhdistämisestä, samalla vastaten tutkielman viimeiseen tutkimuskysymykseen: *"Voiko ISO 31000:2018 riskienhallintamallin ohjeiden ja NIST SP 800-37r2 riskienhallinnan viitekehyksen yhdistäminen tehostaa riskienhallinnan suunnittelua ja toteutusta ICT-organisaatiossa*?". Viimeiseen tutkimuskysymykseen vastataan aiemmissa luvuissa kerätyn teoriatiedon sekä haastattelujen pohjalta kerätyn aineiston avulla.

6.1 Tulokset

Tämän tutkielman tavoitteena oli kerätä tietoa ja selvittää, miten ICT-organisaatioiden tulisi toteuttaa riskienhallintaa ja kannattaisiko yleisesti sovellettujen ISO 31000:2018 riskienhallinnan ohjeiden lisäksi hyödyntää NIST SP 800-37r2 riskienhallinnan viitekehystä. Tutkimustulosten avulla vastattiin seuraaviin tutkimuskysymyksiin:

- *Miten riskienhallinta tulisi toteuttaa ICT-alan organisaatiossa?*
- *Miten ISO 31000:2018 riskienhallintamallin ohjeet ja NIST SP 800-37r2 riskienhallinnan viitekehys vertautuvat toisiinsa?*
- *Voiko ISO 31000:2018 riskienhallintamallin ohjeiden ja NIST SP 800-37r2 riskienhallinnan viitekehyksen yhdistäminen tehostaa riskienhallinnan suunnittelua ja toteutusta ICT-organisaatiossa?*

Tutkielman aikana tehtiin päätelmä, että ISO 31000:2018 riskienhallinnan ohjeet ja NIST SP 800-37r2 riskienhallinnan viitekehyksen yhdistäminen voi tehostaa riskienhallinnan suunnittelua ja toteutusta ICT-organisaatiossa. Ohjeiden on mahdollista täydentää sekä toisiaan että niitä hyödyntävien ihmisten tietoisuutta riskienhallinnasta. Erilaiset ohjeet tarjoavat monipuolisia näkökulmia ja uusia menetelmiä riskienhallinnan suorittamista varten. Jotta viitekehysten samanai-

kaisesta käytöstä on mahdollista saada hyötyä, ohjeiden kattava ymmärrys sekä kyky niiden soveltamiseen korostuu.

Riskienhallinnan ohjeiden tai viitekehysten suora käyttäminen ilman kattavaa organisaation ja oman toiminnan ymmärtämistä leikkaa ja liimaa -periaatteella on täysin turhaa, eikä se palvele ketään organisaatiossa. Toisin sanoen riskienhallinnan ohjeet tai mikään viitekehys yksin tai yhdistettynä ei takaa onnistunutta riskienhallintaa, vaan riskienhallinnan tulee olla räätälöity organisaation tarpeita ja tavoitteita vastaaviksi. Tällöin riskienhallinta tuottaa arvoa myös organisaation muille toiminnoille, eikä sitä tehdä vain muodollisuuksien vuoksi.

6.1.1 Riskienhallinnan toteuttaminen ICT-organisaatiossa

Tutkielman alussa pyrittiin luomaan pohja riskienhallinnan käsittelyä varten tutustumalla riskin käsitteeseen, riskienhallinnan standardeihin sekä riskienhallintaan ICT-organisaatiossa. Riskienhallinta on järjestelmällistä ja jatkuvaa toimintaa, jonka avulla organisaatiota tulee ohjata erilaisten riskien ja uhkien osalta. Se koostuu toimenpiteistä, joiden avulla organisaatio pyrkii lisäämään oman toiminnan onnistumisen todennäköisyyttä.

ICT-organisaatioiden, kuten myös muiden organisaatioiden, tulisi hyödyntää riskienhallinnalle oleellisia standardeja ja muita ohjeita, sillä ne helpottavat riskienhallinnan toteuttamista. Standardien avulla organisaatiot voivat yhdenmukaistaa toimintaansa sekä samalla osoittaa muille organisaatioille toimivansa yhteisesti hyväksyttyjen periaatteiden ja parhaiden käytänteiden mukaisesti.

Vaikka akateemisen kirjallisuuden esitettiinkin kritisoivan standardeja ja niiden hankalasti ymmärrettävää termistöä, tutkielman aineiston perusteella termistön kritiikki on osittain aiheetonta. Aineiston perusteella termistöä pidettiin riittävänä, mutta termistöön perehtymistä painotettiin vahvasti. Terminologian aiheuttamat haasteet voivatkin liittyä riskienhallintaa tekevien henkilöiden vähäiseen riskienhallinnan kokemuspohjaan. On myös huomioitava, että riskienhallintaa varten organisaation tulee osallistaa myös sellaisia henkilöitä, joiden pääsubstanssi on jotakin muuta kuin riskienhallinta. Tällöin termien ja määritelmien tärkeys korostuu, sillä eri taustoilla olevat ihmiset voivat tulkita termejä oman aihealueensa kautta.

Onnistuneesta riskienhallinnasta päävastuussa ovat organisaation johtajat. Heidän tehtävänään on riskienhallinnan jalkauttaminen osaksi organisaation yleistä hallintotapaa ja kulttuuria. Organisaatioon turvallisen kulttuurin tärkeys osoittautui myös seuraavien aineistosta poimittujen katkelmien kautta.

> *Jos riskienhallinnan tekijät kokevat, ettei siitä ole mitään hyötyä, riskienhallinnasta tulee suorittamista, jonka arvo on nolla.*

Palautteen antaminen on tärkeää, sillä sen avulla voidaan osoittaa tehtyjen toimintojen tärkeys, jonka seurauksena riski ei realisoitunut.

Johdon sitoutumisen osoittaminen riskienhallinnalle on erittäin tärkeää. Vastaavasti myös turvallisuuteen ohjaava kulttuuri ja ympäristö voivat ohjata yksilöitä toimimaan turvallisella tavalla. Tällöin riskienhallinnasta ei muodostu ahdistavaa ja epämukavan oloista, vain vuosikellon mukaisesti etenevää prosessia, jota käsitellään vain silloin kun on pakko.

6.1.2 ISO 31000:2018 riskienhallintamallin ohjeiden ja NIST SP 800-37r2 riskienhallinnan viitekehysten toisiinsa vertautuminen

Tutkielman toinen sisältöluku käsitteli ISO 31000:2018 mukaisia riskienhallinnan ohjeita erityisesti riskienhallinnan prosessin osalta. Luvun aikana tarkasteltiin myös NIST SP 800-37r2 riskienhallinnan viitekehystä. Kolmannessa sisältöluvussa malleja vertailtiin toisiinsa.

Mallien vertailun aikana riskienhallinnan lähestymistapojen erot olivat heti havaittavissa. ISO 31000:2018 ohjeen ollessa lavea ja suuntaa antava, NIST SP 800-37r2 viitekehyksessä riskienhallintaa lähestytään pakotettujen tehtävien kautta. Tehtävien toteuttaminen toimii viitekehyksessä edellytyksenä seuraavaan vaiheeseen siirtymisessä. Pakotetut tehtävät voivat ohjata riskienhallintaa tehokkaasti varsinkin aluksi, mutta pidemmällä tähtäimellä riskienhallinnan räätälöinti voi olla organisaatiolle tehokkaampaa.

Toinen selkeä ero riskienhallinnan ohjeiden ja viitekehyksen välillä oli niiden painotus. ISO 31000:2018 toimii erityisesti johdon työkaluna riskienhallinnan jalkauttamiseksi, kun taas NIST SP 800-37r2 käsittelee riskienhallintaa painottuen organisaation tietojärjestelmiin ja tietosuojaan. Vastaava painotus näkyi riskienhallintaprosessin ja -viitekehyksen useassa vaiheessa. Esimerkiksi viestinnän ja tiedonvaihdon osalta ISO 31000:2018 korostaa niiden toimivan päätöksenteon tukena ja NIST SP 800-37r2 painottaa tietojärjestelmien välistä kommunikointia. Sama teema näkyi myös hallintakeinojen ja seurannan osalta, sillä ISO 31000:2018 painotus kohdistui yleisesti toimintaympäristöön sekä laatuun, kun taas NIST SP 800-37r2 keskittyi hallintakeinojen konfigurointiin, dokumentointiin ja tehokkuuden ylläpitämiseen.

Sisällöllisesti ISO 31000:2018 riskienhallinnan ohjeet ja NIST SP 800-37r2 viitekehys erosivat toisistaan myös viitteiden puolesta. ISO 31000:2018 sisältää lyhyitä suosituksia erilaisten prosessin vaiheiden suorittamisesta, ilman tarkempia viitteitä ja esimerkkejä. NIST SP 800-37r2 sen sijaan sisältää selkeät viitteet ja esimerkit erilaisten menetelmien suorittamiseksi. Samalla NIST SP 800-37r2 viitekehys osoittaa tehtävältä odotetut tulokset.

Aineiston perusteella mahdollisten viitteiden ja esimerkkien ajateltiin olevan hyödyllisiä. Viitteiden kuitenkin tunnistettiin samalla vievän lisää resursseja, sillä kattava tutustuminen muihin mahdollisiin toimintatapoihin voi vaikeuttaa riskienhallintatyön kanssa tasapainoilua. Erilaisten lähestymistapojen lisäksi viitteiden ajateltiin helpottavan riskienhallintaprosessin jatkuvaa käyttöä ja ymmärrystä. Tämän lisäksi niiden ajateltiin olevan erityisen hyvänä apuna ris-

kienhallinnan käyttöönotossa. Esimerkkien positiivisten vaikutusten lisäksi, niitä osattiin tarkastella myös mahdollisten negatiivisten vaikutusten kautta, sillä, esimerkkien todettiin voivan olla vaarallisia, jos niitä aletaan pitämään faktoina. Tällöin totuus löytyy ohjeesta ja muille toteutustavoille ei jää tilaa, tai niitä ei haluta huomioida.

6.1.3 ISO 31000:2018 riskienhallintamallin ohjeiden ja NIST SP 800-37r2 riskienhallinnan viitekehyksen yhdistämisen vaikutukset

Teorian perusteella ISO 31000:2018 riskienhallinnan ohjeet ja NIST SP 800-37r2 riskienhallinnan viitekehys olisi mahdollista yhdistää riskienhallinnan suunnittelun ja toteutuksen tehostamiseksi. Mallien yhdistäminen ja siitä koituvat vaikutukset ovat kuitenkin täysin käyttäjän vastuulla, sillä riskienhallinnan tehokkuutta ei voida kasvattaa vain lisäämällä erilaisia standardeja, ohjeita tai viitekehyksiä organisaation käyttöön.

> *Riskienhallinnan teho perustuu siihen, miten organisaatiossa osataan kokonaisuudessaan ottaa riskienhallinta osaksi organisaation arkea.*

Aineisto antoi ymmärtää, että ISO 31000:2018 mukaista riskienhallinnan ohjeita ja prosessia pidettiin sekä riittävänä että tehokkaana ICT-organisaation riskienhallinnalle. Tämä johtui siitä, että ISO 31000:2018 mukaiset riskienhallinnan ohjeet koettiin laveiksi, jolloin riskienhallintaprosessi tulee itse kyetä kohdistamaan organisaation tarpeita ja tavoitteita vastaaviksi. Laveat ohjeet kannustavat myös niiden soveltamiseen. Vastaavasti liian tiukasti laaditut ohjeet koettiin kahlitseviksi, eivätkä ne tällöin palvele organisaatiota.

Toisaalta aineistoa tarkasteltaessa havaittiin myös se, että ISO 31000:2018 mukaisia riskienhallinnan ohjeita olisi mahdollista täydentää, tai niiden rinnalla voitaisiin käyttää esimerkiksi NIST SP 800-37r2 riskienhallinnan viitekehystä. Ohjeiden mahdolliseen yhdistämiseen viittaavia tarpeita tuli aineistossa ilmi esimerkiksi seuraavasti:

> *Siitähän tavallaan puuttuu riskienkäsittelyyn valmistautuminen, eli minkä tyyppisiä ihmisiä kutsutaan ja mikä on se tieto-osa-alue.*
>
> *Prosessi tuntuu menevän heti asiaan, eikä erilaisia näkökulmia käsitellä niin paljon, vaan käsitellään suurempia kokonaisuuksia.*
>
> *Pelkän vanhan materiaalin tai prosessien ei pidä suunnata ajattelua, myös laatikon ulkopuolelta voi tulla hyviä ajatuksia.*
>
> *Laaja-alainen perehtyminen eri metodeihin on tarpeen, eikä niitä kuitenkaan tarvitse käyttää ja noudattaa "By the book" -tyylillä.*

Vaikka riskienhallinnan ohjeiden yhdistämistä pidettiin mahdollisena sekä teorian että aineiston perusteella, myös eriäviä näkemyksiä oli havaittavissa. Eriävät näkemykset liittyivät siihen, millä tavalla ohjeiden yhdistämisen ajateltiin toteutettavan. Tämä tarkoittaa sitä, että osa koki mallien yhdistämisen tarkoittavan tilannetta, jossa ISO 31000:2018 riskienhallinnan ohjetta ja NIST SP 800-

37r2 riskienhallinnan viitekehystä sovellettaisiin täsmällisesti juuri ohjeiden mukaisesti.

> *Riskienhallintaprosessin fokus tulisi itse löytää, en haluaisi sotkea ISO 31000 mukaan muita viitekehyksiä, koska silloin riskiprosessit voivat ruveta pyörittämään toimintaa.*
>
> *Ihmisillä pitää olla enemmän päätäntävaltaa.*

ISO 31000:2018 riskienhallinnan ohjeiden ja NIST SP 800-37r2 viitekehyksen yhdistämisen ongelmallisuus on hyvä huomio, sillä yksittäisenkin ohjeen noudattaminen ja sen omaan toimintaan suhteuttaminen vaatii organisaatiolta korkeaa kypsyystasoa. Korkeaa kypsyystasoa ei saavuteta hetkessä, sillä riskienhallinta kilpailee resursseista myös muiden organisaation toimintojen kanssa.

ISO 31000:2018 riskienhallinnan ohjeiden ja NIST SP 800-37r2 riskienhallinnan viitekehyksen yhdistäminen voi tehostaa organisaation riskienhallintaa. On kuitenkin todettava, että työvälineiden määrällä ei voida korvata laatua. Riskienhallinnan tulee muodostua luontevaksi osaksi organisaation toimintaa, jolloin se on jatkuvasti käsiteltävänä.

7 YHTEENVETO JA JATKOTUTKIMUSAIHEET

Tämän tutkielman aiheena oli riskienhallinnan suunnittelu ja toteutus ICT-alan organisaatiossa. Tutkielman tavoitteena oli kerätä tietoa ja selvittää, miten ICT-organisaatioiden tulisi toteuttaa riskienhallintaa. Tämän lisäksi pyrittiin selvittämään, kannattaisiko ICT-organisaatioiden hyödyntää yleisesti sovellettujen ISO 31000:2018 riskienhallinnan ohjeiden lisäksi NIST SP 800-37r2 riskienhallinnan viitekehystä.

Tutkielman teoreettinen viitekehys muodostui kahden ensimmäisen sisältöluvun aikana, jossa käsiteltiin riskejä ja riskienhallintaa varsin yleisellä tasolla. Riskienhallinnan käsittely kuitenkin rajattiin tarkemmin käsittelemään ICT-organisaatioiden riskienhallintaa. Käsittelyn rajausta voitiin pitää onnistuneena, sillä riskienhallinta itsessään on erittäin laaja kokonaisuus. Toisin sanoen riskienhallintaa toteutetaan useissa erilaisissa ympäristöissä, jolloin riskienhallinnan työkalut ja metodit voivat erota sekä soveltuvuudeltaan että käyttäjiltään erittäin paljon.

ICT-organisaatioissa riskienhallinnan onnistumisen tueksi organisaatioiden tulisi hyödyntää erilaisia ohjeita ja politiikoita, jotka ohjaavat organisaation toimintaa. Tämän lisäksi organisaation tulisi tuntua turvalliselta ympäristöltä myös sen työntekijöille, sillä ympäristön positiiviset vaikutukset voivat ohjata myös yksilöitä toimimaan turvallisesti.

Tutkielman toisessa sisältöluvussa tarkasteltiin yleisesti käytössä olevia ISO 31000:2018 riskienhallinnan ohjeita sekä NIST SP 800-37r2 riskienhallinnan viitekehystä. Käsittelyn tarkoituksena oli tutustua erilaisiin riskienhallinnan malleihin, jotta niitä oli mahdollista vertailla. Vaikka riskienhallinta onkin laajalti tutkittu aihealue, aiempaa tutkimusta vastaavien viitekehysten yhdistämisestä ei löytynyt. Vertailun lisäksi riskienhallintamallien samanaikaista käyttöä ja yhdistämistä pohdittiin. Vertailu osoitti riskienhallintamallien osittaisen yhdistämisen mahdolliseksi. Tämä johtui siitä, että ISO 31000:2018 riskienhallinnan ohjeet ja NIST SP 800-37r2 riskienhallinnan viitekehys lähestyvät riskienhallintaa eri näkökulmien kautta.

ISO 31000:2018 riskienhallinnan ohjeet painottuvat organisaation johtamisen ja sitoutumisen näkökulmiin, eivätkä ne sisällä selkeitä toimintamalleja tai

esimerkkejä riskienhallinnan toteuttamiseksi. Ohjeita voisi luonnehtia laveiksi ja sen takia jokaiselle organisaatiolle sopiviksi. Sen sijaan NIST SP 800-37r2 riskienhallinnan viitekehys lähestyy riskienhallintaa selkeästi erilaisen näkökulman kautta. Viitekehyksen vaiheet perustuvat pakotettuihin toimintoihin, jotka ovat edellytyksenä seuraavaan vaiheeseen siirtymiseksi.

Vaikka viitekehyksen keskiössä onkin sitä soveltava organisaatio, viitekehys itsessään on selkeästi teknologiapainotteisempi. Tämän pystyi huomaamaan tarkasteltaessa viitekehykseen sisältyviä vaiheita ja niiden erilaisia tehtäviä. Esimerkiksi ISO 31000:2018 riskienhallintaprosessissa viestinnän ja tiedonvaihdon korostetaan toimivan päätöksenteon tukena, jolloin viestiminen johtaa mukaan kuulumisen ja omistajuuden tunteeseen riskeihin vaikuttavien keskuudessa. NIST SP 800-37r2 viitekehyksessä sen sijaan keskitytään painottamaan viestinnän tärkeyttä erityisesti tietojärjestelmien välillä.

Tämä tutkielma toteutettiin laadullisella tutkimusotteella. Kirjallisuuden ja sen pohjalta tehdyn vertailun lisäksi tutkielmaa varten kerättiin empiirinen aineisto puolistrukturoitujen haastatteluiden avulla. Haastattelujen toteuttaminen vaatikin kattavaa aihepiiriin perehtymistä, sillä ilman sen ymmärtämistä kysymysten esittäminen ja vastausten tulkinta olisi voinut osoittautua ylivoimaisen vaikeaksi.

Puolistrukturoidut haastattelut osoittautuivat kuitenkin erinomaiseksi aineistonkeruumenetelmäksi, sillä ne mahdollistivat haastateltavien omien näkökulmien ja ajatusten esille tuomisen. Tähän toki vaikuttivat myös haastateltavat itse, sillä osaan kysymyksistä olisi hyvin voinut vastata vain ”Kyllä” tai ”Ei”. Aihepiiristä itsekin kiinnostuneet haastateltavat antoivat kuitenkin kattavat vastaukset jokaiseen kysymykseen. Vastaavien näkökulmien ja ajatusten saaminen muilla keinoilla olisi ollut haastavaa. Hirsjärven Ja Hurmen (2020) mukaan puolistrukturoiduista haastatteluista voi kertyä paljon tutkimukselle epärelevanttiakin materiaalia, mutta tämän tutkielman aikana laaja ja rikas, osittain epärelevantti aineisto tarjosi myös kiinnostavia ajatuksia mahdolliselle jatkotutkimukselle, joita käsitellään jäljempänä.

Tutkimuksen aikana kertynyt aineisto analysoitiin hyödyntämällä aineistolähtöistä sisällönanalyysiä. Analyysin aikana haastattelut kirjoitettiin auki ja niistä pyrittiin löytämään keskeisiä pelkistettyjä ilmauksia. Pelkistetyistä ilmauksista rakennettiin omia luokkiaan, joista myöhemmin muodostui pääluokkia, joiden avulla muodostettiin ainestoa kuvaavat teemakokonaisuudet. Tutkielman rajoitteena voidaan kuitenkin pitää sen pientä aineistoa ja sitä, että haastateltavat olivat samasta organisaatiosta.

Kirjallisuudesta kerätty teoria ja aineiston pohjalta muodostetuttujen teemakokonaisuuksien tieto yhdistettiin tutkielman viimeiseen kysymykseen vastaamiseksi. Sekä teoria että aineisto antoivat ymmärtää, että ISO 31000:2018 riskienhallinnan ohjeiden ja NIST SP 800-37r2 riskienhallinnan viitekehyksen yhdistäminen olisi mahdollista. Aineistossa korostui laveiden ISO 31000:2018 riskienhallinnan ohjeiden riittävyys, mutta samalla NIST SP 800-37r2 riskienhallinnan viitekehyksen tuomia näkemyksiä katsottiin myötämielisesti.

Tutkielmassa päädyttiin siihen, että ISO 31000:2018 riskienhallinnan ohjeiden ja NIST SP 800-37r2 viitekehyksen yhdistäminen voi tehostaa riskienhallintaa, mutta riskienhallinnan teho ei ole sidoksissa ohjeisiin, vaan ihmisiin. Yksittäisten ohjeiden hyödyntäminen vaatii organisaatiolta korkeaa kypsyystasoa, jolloin uusien ohjeiden lisääminen voi vaikeuttaa riskienhallinnan suorittamista, vaikka uutena tulleesta ohjeesta olisikin poimittu vain osa organisaation käyttöön. Aineiston perusteella erilaisten riskienhallintamallien tuntemus nähtiin kuitenkin positiivisessa valossa.

Tämän tutkielman perusteella jatkotutkimusta voitaisiin tehdä jatkamalla ISO 31000:2018 riskienhallinnan ohjeiden ja NIST SP 800-37r2 viitekehyksen yhdistämistä. Tutkimuksessa voitaisiin pyrkiä kehittämään uusi viitekehys, joka pyrkisi huomioimaan sellaisten organisaatioiden riskienhallinnan tarpeet, jotka kaipaavat erityisesti riskienhallinnan aloittamiseksi apua.

Aineiston perusteella toiseksi jatkotutkimusaiheeksi nousi kysymys, miten riskienhallinta olisi mahdollista tiiviimmin integroida osaksi organisaation muita toimintoja. Riskienhallinnan integroiminen organisaation muihin toimintoihin ylläpitäisi jatkuvaa keskustelua riskienhallinnasta, jolloin riskienhallintaa ei käsiteltäisi vain vuosikellon mukaisesti. Toisin sanoen riskienhallinta nähtäisiin tärkeänä osana organisaation onnistumista. Tämä myös lisäisi riskienhallinnan tehokkuutta.

LÄHTEET

Al-Fikri, M., Putra, F., Suryanto, Y. & Ramli, K. (2019). Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency. *Procedia Computer Science, 161*, 1206–1215.

Almeida, R., Teixeira, J., Mira da Silva, M. & Faroleiro, P. (2019). A conceptual model for enterprise risk management. *Journal of Enterprise Information Management, 32(5)*, 843–868.

Aven, T. (2011). On the new ISO guide on risk management terminology. *Reliability Engineering and System Safety, 96(7),* 719–726.

Aven, T. & Zion, E. (2014). Foundational Issues in Risk Assessment and Risk Management. *Risk Analysis, 34(7)*, 1164–1172.

Barafort, B., Mesquida, A. & Mas, A. (2016). Integrating risk mangement in IT settings from ISO standards and management systems perspectives. *Computer Standards & Interfaces, 54(3),* 176–185.

Barafort, B., Mesquida, A. & Mas, A. (2018). ISO 31000-based integrated risk management process assessment model for IT organizsations. *Wiley Evolution and Process.*

Baskerville, R. (1991). Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security. *European Journal of Information Systems 1(2):* 121–130.

Björnsdóttir, S., Jensson, P., Boer, R. & Thorsteinsson, S. (2022a). The Importance of Risk Management: What is Missing in ISO Standards? *Risk Analysis an International Journal.*

Björnsdóttir, S., Jensson, P., Thorsteinsson, S., Dokas, I. & Boer, R. (2022b). Benchmarking ISO Risk Management Systems to Assess Efficacy and Help Identify Hidden Organizational Risk. *Sustainability 14(9).*

Boholm, M., Möller, N. & Hansson, S. (2016). The Concepts of Risk, Safety, and Security: Applications in Everyday Language. *Risk Analysis, 36(2)*, 320–338.

Bruce, K., Lyon, N., Kadampi, P. & Popov, G. (2022). Costs & Benefits of Managing Risk. Taking a Risk-Informed, Performance-Based Approach. *Risk Management.*

Choo, B. & Goh, J. (2015). Pragmatic adaptation of the ISO 31000:2009 enterprise risk management framework in a high-tech organization using Six Sigma. *International Journal of Accounting & Information Management.*

Covert, E. & Nielsen, F. (2005). Measuring Risk Using Existing Frameworks. *Information Systems Security, 14(1),* 21–25.

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not. *Information Management & Computer Security, 24,(2),* 139–151.

Dali, A. & Lajtha, C. (2012). ISO 31000 Risk Management – ”The Gold Standard”. *The EDP Audit, Control, and Security Newsletter, 45(5),* 1–8.

Dionne, G. (2019). Corporate Risk Management. *Theories and Applications*. John Wiley & Sons, Incorporated.

Farrel, M. & Gallagher, R. (2014). The Valuation Implications of Enterprise Risk Management Maturity. *Journal of Risk and Insurance, 82,(3),* 625–657.

Gordon, L. & Loeb, M. (2002). The economics of information security investment. *ACM Transactions on Information & System Security (TISSEC), 5,(4),* 438–457.

Gorzen-Mitka, I. (2013). Risk management as challenge to today’s enterprises. *Problems of Management in the 21st Century, 22,(1),* 4–5.

Hallegatte, S. & Rentschler, J. (2015). Risk Management for Development – Assessing Obstacles and Prioritizing Action. *Risk Analysis, 35(2),* 193–210.

Hardjomidjojo, H., Pranata, C. & Baigorria, G. (2022). Rapid assessment model on risk management based on ISO 31000:2018. *IOP Conference Series: Earth and Environmental Science.*

Hirsjärvi, S. & Hurme, H. (2022). Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus.

Hirsjärvi, S., Remes, P., & Sajavaara, P. (2010). Tutki ja kirjoita. Helsinki: Tammi.

Hyungjin, L. & Han, J. (2019). Do employees in a ”good” company comply better with information security policy? A corporate social responsibility perspective. *Information Technology & People, 32(4),* 858–875.

Hyvärinen, M. (2010). Haastattelukertomuksen analyysi. Teoksessa J. Ruusuvuori, P. Nikander & M. Hyvärinen (toim.), Haastattelun analyysi. Tampere: Vastapaino.

ISO. (2019). International Organization for Standardization. Medical devices – Application of risk management to medical devices. Haettu 20.11.2022 osoitteesta https://www.iso.org/obp/ui/#iso:std:iso:14971:ed-3:v1:en

ISO. (2022). About us. Haettu 21.11.2022 osoitteesta https://www.iso.org/about-us.html

ISO. (2023). Home. Haettu 04.04.2023 osoitteesta https://www.iso.org/home.html

Jennex, M. & Durcikova, A. (2020). Creating Sustainable Knowledge Systems: Towards a Risk and Threat Assessment Framework. *Journal of Strateegic Innovation and Sustainability, 15(4),* 138–152.

Juuti, P. & Puusa, A. (2020). Laadullisen tutkimuksen näkökulmat ja menetelmät. Helsinki: Gaudeamus.

Kelly, P. (2022). Are you competent coping with uncertainty and risk? Implications for work-applied management. *Journal of Work-Applied Management.*

Kitsiosis, F., Chatzidimitriou, E. & Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. *Sustainability, 14(3),* 1–19.

Kuzminykh, I., Ghita, B., Sokolov, V. & Bakhshi, T. (2021). Information Security Risk Assessment. *Encylopedia, 1(3).*

Lalonde, C. & Boiral, O. (2012). Managing risks through ISO 31000: A critical analysis. *Risk Management, 14(4),* 272–300.

Lambrinoudakis, C., Gritzalis, S., Xenakis, C., KAtsikas, S., Karyda, M., Tsochou, A., Papadatos, K., Rantos, K., Pavlosoglou, Y., Gasparinatos, S., Pantazis, A. & Zacharis, A. (2022). Compendium of Risk Management Frameworks With Potential Interoperability: Supplement to the Interoperable EU Risk Mangement Framework Report. *Enisa.*

Menon, N. & Siponen, M. (2020). Executives' Commitment to Information Security: Interaction between the Preferred Subordinate Influence Approach (PSIA) and Proposal Characteristics. *Data Base for Advances in Information Systems, 51(2),* 36–53.

Myers, M. (2015). Ten years of Qualitative Research in Organizations and Management: some reflections. *Qualitative research in Organizations and Management, 10(4),* 337–339.

Myers, M. (2020). Qualitative research in business & management (kolmas versio). Lontoo: SAGE Publications.

Niemimaa, E. & Niemimaa, M. (2016). Information systems security policy implementationin practice: from best practices to situated practices. *European Journal of Information Systems, 26(1),* 1–20.

NIST. (2022). National Institute of Standards and Technology. Haettu (13.10) osoitteesta: https://www.nist.gov/about-nist

Okonofua, H. & Rahman, S. (2018). Evaluating the Risk Management Plan and Addressing Factors for Successes in Government Agencies. *IEEE International Conference On Trust, Security And Privacy In Computing And Communications.*

Ostrom, L. & Wilhelmsen, C. (2019). Enterprise Risk Management Overview. Risk Assessment: Tools, Techniques, and Their Applications, (Toinen painos.). John Wiley & Sons, Inc.

Paananen, H., Lapke, M. & Siponen, M. (2019). State of the art in information security policy development. *Computers & Security, 88(1),* 1–14.

Popov, B. & Popov, G. (2022). On the concept of RISK, UNCERTAINTY & BLACK SWANS. *Professional Safety, 67(3),* 18–23.

Putra, F., Pradana, A. & Setiawan, H. (2017). Design of Information Security Risk Management Using ISO/IEC 27005 and NIST SP 800-30 Revision 1: A case study at Communication Data Applications of XYZ Institute. *IEEE International Conference on Information Technology Systems and Innovation (ICITSI),* 251–256.

Pöyhönen, J. (2020). Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa. *Systeemiajattelu*. Jyväskylän yliopisto. Informaatioteknologian tiedekunta.

Qu, S. & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting and Management, 8(3),* 238–264.

Rampini, G., Takia, H. & Berssaneti, F. (2019). Critical Success Factors of Risk Management with the Advent of ISO 31000:2018 – Descriptive and Content Analyzes. *Procedia Manufacturing 39*, 894-903.

Rose, S. (2022). Planning for a Zero Trust Architecture: A Pallning Guide for Federal Administrators. *NIST Cybersecurity White Paper.*

Ross, R., Roberts, T., Burris, J., Marron, J., Pappas, D., Faigin, D., Dulany, K., Nadeau, E., Cutshall, C., Boeckl, K., Cussatt, D., Sames, C., Duspiva, P., Pillitteri, V., Herms, K., Moncada, K., Porter, E., Snyder, J., Dempsey, K., Lefkovitz, N., Bales, C., Boyens, J., Paulsen, C. & Stanley, M. (2018). NIST Special Publication 800-37 Revision 2. *Risk Management Framework for Information Systems and Organizations. A System Life Cycle Approach for Security and Privacy.*

Schiller, F. & Prpich, G. (2014). Learning to organise risk management in organisations: what future for enterprise risk management? *Journal of Risk Research, 17(8),* 999–1017.

Schmidt, M. (2023). Information security risk management terminology and key concepts. *Risk management, 25(2),* 1–23.

SFS-ISO 31000:2018. (2018). International Organization for Standardization. *Risk management – Guidelines.*

SFS-EN IEC 31010:2019. (2019). International Organization for Standardization. *Risk management – Risk assessment techniques.*

SFS. (2020). Standardien hyödyt. Haettu 23.10.2022 osoitteesta https://www.sfs.fi/ajankohtaista/standardien_hyodyt

SFS. (2022). Mitä standardi tarkoittaa? Haettu 20.11.2022 osoitteesta https://sfs.fi/standardeista/mika-on-standardi/

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers and Security, 57*, 14–30.

Siponen, M. (2006). Information Security Standards Focus on the Existence of Process, Not Its Content. *Communications of the ACM 49(8),* 97–100.

Siponen, M. & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46(5),* 267–270.

Stefanova-Stoyanova, V. & Danov, P. (2022). Comparative Analysis of Specialized Standards and Methods on Increasing the Effectiveness and Role of PDCA for Risk Control in Management Systems. *International Scientific Conference on Computer Science (COMSCI).*

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards–A Review and Comprehensive Overview. *Electronics, 11(14).*

TEPA-termipankki. (2022). Haettu 20.11.2022 osoitteesta https://termipankki.fi/tepa/fi/

Tsohou, A., Karyda, A., Kokolakis, S. & Kiontouzis, E. (2006) Formulating information systems risk management strategies through cultural theory. *Information Management & Computer Security, 14(3),* 198–217.

Tuomi, J. & Sarajärvi, A. (2018). Laadullinen tutkimus ja sisällön analyysi. Helsinki: Tammi.

Valtionvarainministeriö. (2017). Ohje riskienhallintaan. Valtiovarainministeriön julkaisuja 22/2017. Haettu 19.10.2022 osoitteesta http://urn.fi/URN:ISBN:978-952-251-862-0

Valtionvarainministeriö. (2019). Riskienhallinnan järjestämisen nykytila valtion virastoissa, rahastoissa ja liikelaitoksissa: *Yhteenveto riskienhallintakyselyn tuloksista.* Haettu 19.10.2022 osoitteesta http://urn.fi/URN:ISBN:978-952-367-046-4

Valtionvarainministeriö. (2021). Valtioneuvostotasoisen riskienhallinnan kehittäminen. *Työryhmän loppuraportti.* Haettu 19.10.2022 osoitteesta http://urn.fi/URN:ISBN:978-952-367-529-2

Von Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security, 7(1),* 50–58.

Walker, R. (2013). Winning With Risk Management. Singapore: World Scientific Publishing Co.

Wilbanks, D. & Byrd, T. (2020) The Relevance & Benefit of ISO 31000 to OSH Practice. *Professional Safety, 65(10)* 32–38.

LIITE 1 HAASTATTELUSSA KÄYTETYT KYSYMYKSET

Kysymykset haastattelua varten:

1. Ovatko ISO 31000:2018 riskienhallinnan ohjeet riittävät riskienhallinnan prosessin osalta?
2. Soveltuuko ISO 31000:2018 riskienhallintaprosessi ICT-alan riskienhallintaan?
3. Koetko ISO 31000:2018 riskienhallintaprosessin olevan tehokas?
4. Sisältääkö prosessi kaiken tarvitsemasi tiedon, vai onko prosessilla mahdollisia kehityskohteita, jos on niin millaisia?
5. Viestintä ja tiedonvaihto on olennainen osa riskienhallintaprosessia, aiheuttaako käytettävä terminologia haasteita?
6. ISO 31000:2018 riskienhallinnan prosessia voidaan pitää laajana, tulisiko prosessin sisältää viitteitä tai esimerkkejä prosessin toteuttamista varten?
7. Olisiko mielestäsi mahdollista, että ISO 31000:2018 riskienhallinnan prosessia tuettaisiin käyttämällä samanaikaisesti toista riskienhallinnan viitekehystä, prosessia tai yksittäisiä vaiheita?
8. Muuta?