Pro gradu

2019

Johanna Väisänen

LUT Yliopisto
School of Business and Management
Laskentatoimi

Kokonaisvaltainen riskienhallinta - riskienhallinnan prosessin toteuttaminen yrityksissä ISO 31000:2018 standardin mukaisesti

Ohjaaja: Satu Pätäri
Ohjaaja: Timo Leivo

TIIVISTELMÄ

Tekijän nimi:	Johanna Väisänen
Tutkielman nimi:	Kokonaisvaltainen riskienhallinta – riskienhallinnan prosessin toteuttaminen yrityksissä ISO 31000:2018 standardin mukaisesti
Tiedekunta:	LUT School of Business and Management
Koulutusohjelma:	Laskentatoimi
Vuosi:	2019
Pro gradu –tutkielma:	LUT-yliopisto 80 sivua, 8 kuviota, 5 taulukkoa, 1 liite
Tarkastajat:	Professori Satu Pätäri & Yliopisto-opettaja Timo Leivo
Hakusanat:	riski, kokonaisvaltainen riskienhallinta, ERM, ISO 31000:2018 standardi

---

Tämän tutkimuksen tarkoituksena oli selvittää, miten yrityksissä järjestetään riskienhallinnan prosessi ja miten ISO 31000:2018 riskienhallinnan standardin mukaiset suositukset prosessin järjestämisestä toteutuvat näissä yrityksissä. Lisäksi tutkimuksessa perehdyttiin kokonaisvaltaisen riskienhallinnan (Enterprise Risk Management) sisältöön ja kehitykseen, ja miten se vastaa nykyisen globaalin liiketoimintaympäristön haasteisiin ja yritysten jatkuvasti muuttuvaan riskikenttään, jota yrityksen tulisi kyetä hallitsemaan saavuttaakseen sen liiketoiminnalliset tavoitteet. Tutkimusmenetelmänä käytettiin laadullista tutkimusta ja aineisto kerättiin teemahaastatteluilla, haastattelemalla kolmen eri yrityksen riskienhallinnasta vastaavaa henkilöä.

ISO 31000:2018 standardi antaa suosituksia siitä, kuinka riskienhallintaa kannattaa yrityksissä järjestää. Riskienhallinnan prosessi sisältää päävaiheina riskien tunnistamisen, analysoimisen ja niiden käsittelyn, joiden lisäksi siihen sisältyy viestintää ja raportointia. Empiirisen tutkimuksen perusteella kaikissa kohdeyrityksissä riskienhallinta seurasi säännönmukaisia käytäntöjä ja pääasiassa muutamia poikkeuksia lukuun ottamatta jokaisen yrityksen toimintatavat vastasivat standardin esittämiä päävaiheita. Suurimmat eroavaisuudet esiintyivät siinä, mihin prosessin vaiheisiin kukin yritys eniten panosti.

ABSTRACT

Author:	Johanna Väisänen
Title:	Enterprise Risk Management – Conducting risk management process in companies according to ISO 31000:2018 standard
Faculty:	LUT School of Business and Management
Master's programme:	Accounting
Year:	2019
Master's thesis:	LUT University 80 pages, 8 figures, 5 tables, 1 appendix
Examiners:	Professor Satu Pätäri & University lecturer Timo Leivo
Keywords:	risk, enterprise risk management, ERM ISO 31000:2018 standard

---

The aim of this study is to describe how companies are organizing their risk management process and how the process is in line with the new ISO 31000:2018 Risk management standard and its guidelines and recommendations. In addition, the study focuses on the content of Enterprise Risk management, its development and how it responds the challenges of the global business environment and the constantly changing risk field, of which the company should be able to manage to achieve its business goals. The research method was qualitative research and the research material was collected by theme interviews by interviewing people responsible of risk management in three different companies.

The ISO 31000:2018 gives recommendations on how to organize risk management. The risk management process includes risk identification, risk analysis and risk mitigation as well as communication and reporting. Based on empirical research, in all interviewed companies, the risk management process was followed by regular practices, and with a few exceptions, the practices were corresponding with the main phased of the ISO 31000:2018 standard. The biggest differences were in what process phases each company put the most effort.

Sisällysluettelo

LIITTEET

LYHENTEET

COSO = Committee of Sponsoring Organization of the Treadway Commission
ERM = Enterprise Risk Management
ISO = International Organization for Standardization
SFS = Suomen Standardisoimisliitto SFS ry

KUVIOT

TAULUKOT

1 JOHDANTO

Volkswagenin päästöhuijaus vuonna 2015, Toshiban kirjanpitopetos vuonna 2015, Chipotlen ruokamyrkytyskriisi vuonna 2015 ja Wells Fargon valetiliskandaali vuonna 2016 (Ferdman & Bhattarai 2015; Talouselämä 2015; Vehviläinen 2016). Kaikkia näitä maailmalle levinneitä skandaaleja yhdistää ainakin yksi tekijä: riittämätön riskienhallinta. Talouselämän (2015) mukaan Volkswagenin autoihin asentama päästötesteissä huijaava laite sulatti paljastuessaan noin 20 miljardia euroa yrityksen markkina-arvosta. Elektroniikkayritys Toshiba sen sijaan myönsi liioitelleen tulojaan seitsemän vuoden aikana lähes kahdella miljardilla dollarilla, minkä paljastuessa yhtiö on joutunut maksamaan vahingonkorvauksia jo lähes miljardin dollarin edestä. Vielä kaksi vuotta skandaalin jälkeenkin, uudet vahingonkorvausvaateet pyörivät miljoonissa dollareissa (Connolly 2017; Talouselämä 2015).

Dynaaminen globaali liiketoimintaympäristö yhdistettynä nopeasti kehittyvään tekniikkaan, geopoliittisiin muutoksiin, talous- ja rahoitusmarkkinoiden epävakaisuuteen sekä muuhun kehitykseen luovat yrityksille valtavia kasvumahdollisuuksia. Samalla kun yritysjohtajat hallitsevat jatkuvasti muuttuvaa taloudellista, poliittista ja teknologista ympäristöä, he kohtaavat eksponentiaalisesti kasvavaa epävarmuutta, joka luo heille erittäin monimutkaisen riskiportfolion hallittavaksi. Nämä riskit voivat hallitsemattomana rampauttaa, jos ei jopa tuhota, koko liiketoiminnan ja yrityksen brändin. (Beasley, Branson & Hancock 2018, 1)

Riskienhallinnan tarkoituksena on sekä luoda että säilyttää yrityksen arvoa parantamalla suorituskykyä, tukemalla tavoitteiden saavuttamista sekä edistämällä innovointia (SFS-ISO 31000 2018, 7). Riskien hallitseminen on keskeinen huolenaihe nykyisessä dynaamisessa globaalissa ympäristössä (Gordon, Loeb & Tseng 2009, 301). Koska riskit muuttuvat ja kehittyvät jatkuvasti, niiden kautta esiin nousevat uhat ja mahdollisuudet voivat vaikuttaa joko negatiivisesti tai positiivisesti yrityksen liiketoimintaan ja strategiaan. (Viscelli, Hermanson, Beasley 2017, 70)

2000-luvulla yritysten käsitys riskienhallinnasta on kuitenkin muuttunut kapeasta perspektiivistä kohti koko organisaation käsittävää kokonaisvaltaisempaa riskienhallintaa, jota kutsutaan yleisemmin termillä Enterprise Risk Management (ERM) (Gordon, Loeb & Tseng 2009, 301) Beasley et al. (2018, 1) toteavat, että lukemattomat organisaatiot ovat omaksuneet ERM-mallin, joka on kehitetty tarjoamaan yrityksen johdolle ylhäältä alaspäin tapahtuvaa strategista näkökulmaa, jonka avulla riskejä voidaan hallita ennakoivasti, jotta todennäköisyys organisaation tavoitteiden saavuttamiseksi kasvaa.

1.1 Tutkimuksen tausta

Yrityksen riskienhallinnan järjestämiseen on olemassa useita erilaisia viitekehyksiä, suosituksia, näkökulmia ja standardeja. Näitä ovat muun muassa International Organization for Standardizationin (ISO) vuonna 2018 julkaisema *”ISO 31000 Risk management - Guidelines”*-standardi, joka korvasi alun perin vuonna 2009 julkaistun ensimmäisen version *”ISO 31000 Risk management – Guidelines and Principles”.* Eräs tunnettu viitekehys on The Committee of Sponsoring Organizations of the Treadway Commissionin (COSO) vuonna 2004 julkaisema ”*Enterprise Risk Management – Integrated Framework*” viitekehys, jonka päivitetty versio ”*Enterprise Risk Management – Integrating with Strategy and Performance”* julkaistiin vuonna 2017. COSO:n viitekehys tunnetaan nimellä COSO-ERM. (IRM 2018a, 4; COSO 2018; ISO 2018a; ISO 2018b)

Standards Australia ja Standards New Zealand ovat yhdessä julkaisseet vuonna 2004 riskienhallintaa käsittelevän *”AS/NZS 4360:2004 – Risk Management”* standardin, jonka alkuperäinen versio julkaistiin jo vuonna 1999 (AS/NZS 4360:2004, 2004). Institute of Risk Management (IRM), The Association of Insurance and Risk Manager (AIRMIC) ja The Public Risk Management Association (Alarm) ovat yhdessä julkaisseet vuonna 2002 *”A Risk Management Standard”* riskienhallinnan standardin, jonka myös Federation of European Risk Management Association (FERMA) omaksui seuraavana vuonna itselleen kehittääkseen siitä yhdenmukaisen yleiseurooppalaisen lähestymistavan riskienhallinnan järjestämiseksi (IRM 2018b; FERMA 2018).

IRM:n mukaan erilaisia riskienhallinnan standardeja on kehitetty maailmanlaajuisesti auttamaan organisaatioita toteuttamaan niiden riskienhallintaa tehokkaasti sekä järjestelmällisesti. Standardeja julkaisee usein kansainväliset standardoimiselimet tai toimialaryhmät, ja standardien tarkoituksena on luoda yhteinen näkemys riskienhallinnan prosesseista, käytännöistä ja viitekehyksistä. Eri standardeilla on erilaiset painopisteet, jolloin ne myös sopivat eri organisaatioihin sekä tilanteisiin. Useimmiten standardien noudattaminen on vapaaehtoista vaikkakin yksittäisiä sopimuksiin perustuvia standardin noudattamisvelvollisuuksia voikin esiintyä. (IRM 2018c).

1.2 Tutkimuksen tavoitteet ja tutkimuskysymykset

Tämän tutkimuksen tarkoituksena on perehtyä syvemmin kokonaisvaltaisen riskienhallinnan ilmiöön, ottamalla tutkimuksen pohjaksi sekä ERM (Enterprise Risk Management) ajattelumallin, että SFS-FI ISO 31000:2018 riskienhallinnan standardin mukaiset suositukset (jäljempänä ISO 31000:2018). Tavoitteena on löytää teoriasta tietoa riskienhallinnan järjestämisestä, kokonaisvaltaisesta riskienhallinnasta, riskienhallinnan prosessista sekä verrata havaintoja siihen, miten reaalimaailman yrityksissä riskienhallinnan prosessi järjestetään. Seuraavassa kappaleessa on esitetty tarkemmin tutkimuksen teoreettista viitekehystä ja aikaisempaa tutkimusta.

Tutkimuksen tavoitteet ovat muotoiltu kahteen tutkimuskysymykseen, jotka ovat esitetty seuraavaksi:

Tutkimuksen päätutkimuskysymys on:

”Miten ISO 31000:2018-standardin mukaiset suositukset riskienhallinnan prosessin järjestämisestä toteutuvat yrityksissä?”

Tutkimuksen alakysymys on:

”Millaisilla säännönmukaisilla toimenpiteillä riskienhallintaa yrityksissä järjestetään?”

Päätutkimuskysymyksellä pyritään saamaan vastaus siihen, miten yrityksissä noudatetaan ISO 31000:2018 standardin mukaisia suosituksia yritysten riskienhallinnan prosessin järjestämisestä. Päätutkimuskysymykseen pyritään saamaan vastaus haastatteluiden ja tarvittaessa sekundääriaineiston pohjalta, mikä käsittää yritysten julkaisemat vuosikertomukset, taloudelliset katsaukset tai muut viralliset julkaisut, joista riskienhallintaa koskevaa tietoa on saatavilla. Sekundääriaineistoa käytetään pääasiassa täydentämään saatua haastattelumateriaalia. Tutkimuksen tavoitteena on verrata, millä tavalla yrityksen riskienhallinnan prosessia toteutetaan verrattuna ISO 31000:2018 standardin mukaisiin suosituksiin, eli onko yrityksen riskienhallinnan prosessin ja standardin väliltä löydettävissä selkeitä yhteneväisyyksiä tai eroavaisuuksia. Alatutkimuskysymys pyrkii tukemaan päätutkimuskysymystä ja saamaan vastauksia siihen, millaisia elementtejä ja tietoisesti järjestettyjä toimintatapoja yritysten riskienhallinnan prosessiin sisältyy.

1.3 Teoreettinen viitekehys ja rajaukset

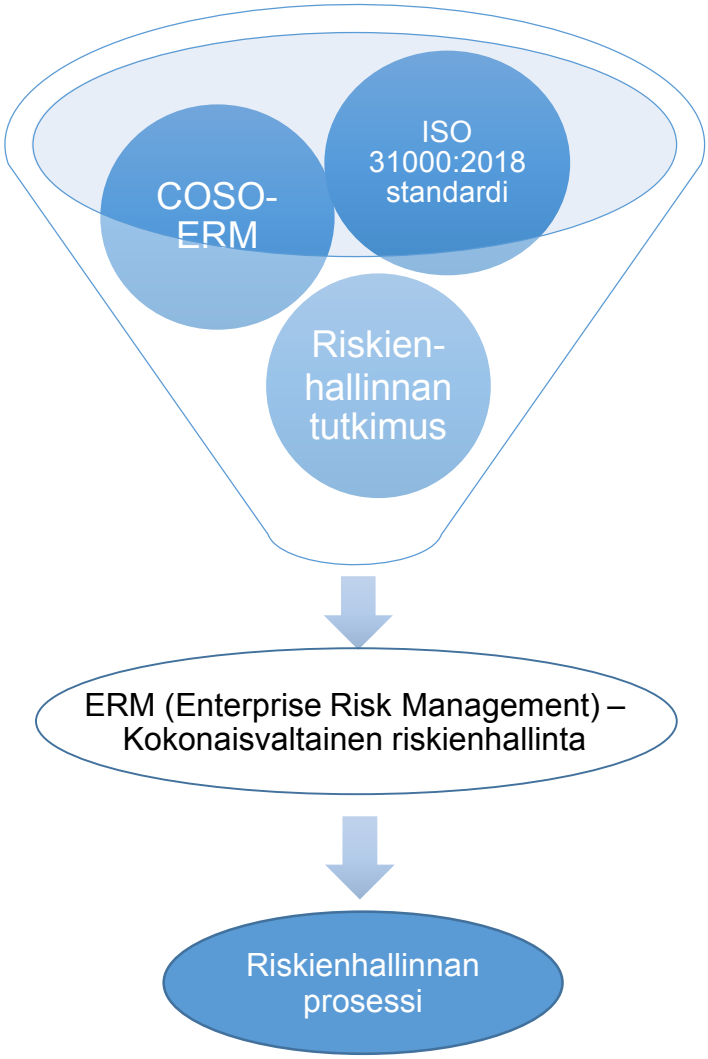
Teoreettinen viitekehys kuvastaa sitä näkökulmaa, josta tutkimuksen havaintoja tarkastellaan (Alasuutari 1999, 79). Riskienhallinnan ja tarkemmin kokonaisvaltaisen riskienhallinnan teoreettinen pohja on melko laaja. Kokonaisvaltaista riskienhallintaa voidaan tutkia monesta eri näkökulmasta, kuten strategisesta tai taloudellisesta näkökulmasta. Tässä tutkimuksessa on tarkoitus tutkia sitä, kuinka riskienhallinnan prosessi järjestetään yrityksessä sisäisesti eli millaisia vaiheita riskienhallinnan prosessin järjestämiseen sisältyy, millaisia asioita on otettava huomioon ja kuinka järjestelmällistä riskienhallinta on.

Uudistettu ISO 31000-standardi on julkaistu vuonna 2018 ja siten hyvin uusi. Siitä syystä tieteellisiä julkaisuja ei uudistetusta standardista ole vielä läheskään yhtä

laajasti, kun taas standardin aiemmasta vuonna 2009 julkaistusta versiosta. Pääosin tästä syystä tutkielmassa käsitellään myös julkaisuja, joissa viitataan vuoden 2009 standardiin. Tutkielman kappaleessa 4.2. kuitenkin huomioidaan ja käsitellään eri vuosina julkaistujen standardien keskeisimmät erot ja uudistukset. Aikaisemmat kokonaisvaltaista riskienhallintaa koskevat tutkimukset keskittyvät pääosin ERM:in käyttöönottoon tai hyötyihin ja haasteisiin. ISO 31000 standardia koskevat tutkimukset sen sijaan käsittelevät hyvin paljon standardin soveltamista ja käyttöönottoa. Tämän tutkimuksen näkökulmana on se, millaisia standardin suosittelemia riskienhallinnan prosessin vaiheita ja elementtejä yritykset toteuttavat omassa riskienhallinnassaan.

Keskeisiä kokonaisvaltaista riskienhallintaa koskevia tutkimuksia ovat Louisotin ja Ketchamin (2014) julkaisema ”ERM – Enterprise Risk management” sekä Beasleyn, Bransonin ja Hancockin (2018) artikkeli ”The State of Risk Oversight: an Overview of Enterprise Risk Management Practices”. ISO 31000 standardia koskevia keskeisiä julkaisuja ovat sen sijaan Purdyn (2010) ”ISO 31000:2009 – Setting a new Standard for Risk Management”, joka keskittyy kuitenkin lähinnä standardin aiempaan versioon. Lisäksi globaaleja riskienhallinnan tutkimuksia tuottaa eri konsulttiyritykset, kuten Aon ja Deloitte, jotka ovat kummatkin julkaisseet vuonna 2019 ”Global Risk Management Survey” tutkimukset toimialakohtaisista riskeistä ja niiden tulevaisuudennäkymistä.

Tutkimuksen viitekehys on havainnollistettu alla olevassa kuviossa. Kuviossa esitetään, kuinka riskienhallinnan tutkimus ja erilaiset standardit, kuten COSO-ERM ja AS/NZS 4360:2004 ovat vaikuttaneet kokonaisvaltaisen riskienhallinnan muotoutumiseen. Kokonaisvaltaisesta riskienhallinnasta on erotettavissa riskienhallinnan prosessi, johon tässä tutkimuksessa on tarkoitus perehtyä. ISO 31000:2018 Riskienhallinnan standardi antaa suosituksia riskienhallinnan prosessin järjestämiseksi yrityksissä, ja kyseisen standardin antamat suositukset ovat lähtökohtana tälle tutkimukselle, kun yritysten riskienhallinnan prosessia tutkitaan ja tulkitaan.



Kuvio 1. Tutkimuksen teoreettinen viitekehys

Tutkimus on rajattu koskemaan riskienhallinnan prosessin järjestämistä, pääosin ottamatta kantaa kuitenkaan siihen, kuinka prosessi todellisuudessa yrityksissä toteutuu tai tehoaa.

1.4 Tutkimusmenetelmä ja –aineisto

Tämän Pro gradu-tutkimuksen tutkimusmetodologia on kvalitatiivinen eli laadullinen tutkimus, jossa ensin kirjallisuuden, kansainvälisten artikkeleiden sekä erilaisten riskienhallintaa koskevien julkaisuiden kuten standardien ja suositusten avulla on tarkoitus perehtyä kokonaisvaltaisen riskienhallinnan prosessiin ja teemahaastatteluiden avulla tutkitaan, kuinka riskienhallinnan prosessi yrityksissä järjestetään.

Laadullista tutkimusta voidaan kuvailla kokonaisvaltaisen tiedon hankkimiseksi, jossa aineisto kootaan todellisista tilanteista suosien ihmistä tiedonkeruun lähteenä. Laadullinen tutkimus suosii tiedonhankintametodina haastatteluja, sillä silloin tutkittavien henkilöiden omat näkökulmat tulevat esille. Laadullisessa tutkimuksessa käytettäviä tutkimusmetodeja ovat esimerkiksi teemahaastattelu, ryhmähaastattelu, osallistuva havainnointi sekä erilaisten dokumenttien analysointi. (Hirsjärvi, Remes & Sajavaara 1997,164)

Tutkimusmetodiksi on valittu teemahaastattelu, joka suoritetaan kahden kesken haastattelijan ja haastateltavan välillä. Hirsjärven ja Hurmeen (2008, 14, 34) mukaan haastattelu on tiedonkeruumenetelmänä joustava, sopii moneen tarkoitukseen ja sen avulla voidaan tuoda esille myös vastauksen takana olevia motiiveja. He jatkavat (2009, 35-36), että haastattelun etuina on, että haastateltavalta saatavia tietoja voidaan täsmentää ja syventää, pyytää perusteluja, esittää lisäkysymyksiä sekä saada kuvailevampia vastauksia.

Puolistrukturoitu haastattelu, josta käytetään myös nimeä teemahaastattelu, kohdennetaan tiettyihin teemoihin, joiden mukaan haastattelu etenee, eikä se siten ole sidottu yksityiskohtaisiin ja tarkkoihin kysymyksiin. Tämä jättää tilaa tutkittavien omalle äänelle ja tulkinnoille. Teemahaastattelussa kysymysrunko joustaa ja aiheita voidaan käsitellä eri järjestyksessä. Kaikki teemat ovat kuitenkin tärkeä käsitellä haastateltavan kanssa, vaikka vastausten laajuus voi vaihdella riippuen haastateltavasta (Hirsjärvi & Hurme 2008, 47; Näpärä 2017)

Tässä tutkimuksessa käytetään haastattelurunkoa, jonka kysymykset ovat muotoiltu tarkoituksella melko laajoiksi, ne liittyvät riskienhallinnan prosessin vaiheisiin ja haastattelun yhteydessä voidaan haastateltavan vastausten perusteella esittää tarkentavia lisäkysymyksiä kyseiseen teemaan liittyen. Laajoilla avoimilla haastattelukysymyksillä on tavoiteltu sitä, että haastateltava kertoo mahdollisimman kattavasti kyseisen organisaation riskienhallinnan prosessista ilman, että haastattelija liikaa johdattelee tiettyihin asioihin. Haastattelurunko on esitetty tämän tutkimuksen liitteenä 1.

Laadullisen tutkimusaineiston ominaisuuksia ovat monitasoisuus, monimutkaisuus sekä ilmaisullinen rikkaus. Tavanomaista on, että pyritään keräämään sellaista aineistoa, joka mahdollistaa mahdollisimman monenlaisen tarkastelun, jolloin näkökulmaa voidaan tarpeen mukaan melko vapaastikin muuttaa. (Alasuutari 1999, 84) Tutkimuksen kohderyhmä pyritään valitsemaan tarkoituksenmukaisesti tutkimusta parhaiten palvelevalla tavalla. Laadullisen tutkimuksen tyypillisenä piirteenä pidetään myös sitä, että tutkimussuunnitelma kehittyy tutkimuksen edetessä ja suunnitelmat mukautuvat olosuhteiden muuttuessa. Tutkimuksen lähtökohtana ei myöskään ole sinänsä hypoteesien osoittaminen oikeaksi tai vääräksi, vaan aineiston monitahoinen tarkastelu ja analysointi. (Hirsjärvi, Remes & Sajavaara 1997,164)

Tässä tutkimuksessa käytetään sekä primääri- että sekundääriaineistoa, joista yksilöhaastattelut ovat tutkijan itse luomaa primääriaineistoa, kun taas kohdeyritysten erilaiset viralliset julkaisut toimivat sekundäärisenä tutkimusaineistona. Tutkimusaineisto kerätään kolmesta yksilöhaastattelusta, joiden avulla pyritään saamaan tietoa siitä, miten näissä tutkittavissa yrityksissä riskienhallinnan prosessi järjestetään, jotta näitä havaintoja voidaan verrata suurempaan ilmiöön. Sekundääriaineisto sen sijaan hankitaan yritysten internetsivuilta. Kuten Alasuutari (1999, 87) on todennut, laadullinen aineisto koostuu näytteistä ja nämä näytteet ovat *”pala tutkittavaa maailmaa”.*

1.5 Tutkimuksen rakenne

Tämä tutkimus jakautuu viiteen päälukuun. Johdannossa on esitelty aluksi tutkimuksen tausta ja tavoitteet, jotka ovat muodostettu tutkimuskysymyksiksi. Sen lisäksi johdannossa kuvaillaan tutkimusaineistoa ja –menetelmää sekä keskeisimpiä aikaisempia tutkimuksia aiheesta. Tutkimuksen toinen luku koostuu teemoista riski ja kokonaisvaltainen riskienhallinta. Tässä luvussa on tarkoitus yleisemmin käsitellä riskiin liittyviä määritelmiä ja luokittelutapoja sekä mitä riskienhallinnalla tarkoitetaan, mitä se sisältää ja mitä sillä tavoitellaan. Lisäksi perehdytään tarkemmin kokonaisvaltaiseen riskienhallintaan, missä kuvataan

kehitystä perinteisestä riskienhallinnasta kohti kokonaisvaltaista riskienhallintaa, kokonaisvaltaisen riskienhallinnan ilmiötä, erilaisia näkökulmia sen järjestämiseen sekä kokonaisvaltaisen riskienhallinnan hyötyjä ja haasteita. Toisessa luvussa luodaan siis taustateoriaa varsinaiselle tutkimukselle.

Kolmannessa luvussa keskitytään kokonaisvaltaisen riskienhallinnan järjestämistä ohjeistavaan SFS-FI ISO 31000:2018 riskienhallinnan standardiin. Luvussa tutkitaan standardin sisältöä ja suosituksia, keskittyen eritoten standardin suosituksiin riskienhallinnan prosessin järjestämisestä. Neljännessä luvussa siirrytään empiiriseen havainnointiin riskienhallinnan prosessin järjestämisessä tämän tutkimuksen kohteena olevissa yrityksissä. Luvussa kuvaillaan ensin tässä tutkimuksessa käytetty tutkimusmetodologia ja –aineisto, ja sen jälkeen teemahaastatteluina toteutettujen yksilöhaastatteluiden havainnot ja tulokset. Viidennessä eli viimeisessä luvussa kuvataan tämän tutkimuksen perusteella tehdyt johtopäätökset, otetaan kantaa tutkielman luotettavuuteen ja esitetään mahdolliset jatkotutkimusideat.

2 RISKIN MÄÄRITTÄMINEN JA KOKONAISVALTAISEN RISKIENHALLINNAN MERKITYS

Luku 2 käsittelee teemoja riski ja riskienhallinta, mistä muodostuu tälle tutkimukselle taustateoriaa. Ensin käsitellään riskin käsitettä, luonnetta ja siihen tiiviisti liittyviä elementtejä, kuten yrityksen riskinottohalua ja –kykyä. Sen jälkeen siirrytään riskienhallintaan ja pureudutaan erilaisiin riskienhallinnan keinoihin ja riskienhallinnan tavoitteisiin ja lopuksi kokonaisvaltaisen riskienhallintaan, sen tavoitteisiin, hyötyihin ja haasteisiin.

2.1 Mikä on riski?

Usein riskillä tarkoitetaan tapahtumaa tai tapahtumatta jäämistä, joka on henkilön vaikutusvallan ulkopuolella sekä aiheuttaa vahinkoa tai menetyksiä. Joskus riskillä voidaan myös tarkoittaa ainoastaan riskitapahtumaa, tunnistamatta riskin aiheuttajaa tai sen seurauksia. (Kurkela, 2014, 3). COSO:n (2004, 1) mukaan negatiivisen vaikutuksen riski voi estää arvonnousun, kun taas positiivisen vaikutuksen riski voi joko kompensoida negatiivisia vaikutuksia tai luoda täysin uusia mahdollisuuksia.

SFS-FI ISO 31000:2018 (2018, 5) standardin mukaan riski voi kuitenkin olla myönteinen, kielteinen tai yhdistelmä kumpaakin, sekä luoda joko mahdollisuuksia tai uhkia. Riski usein ilmaistaan yhdistelmänä riskin lähteitä, riskitapahtumaa, riskien seurauksia sekä riskin todennäköisyyttä. Standardin mukaan riskienhallinta on koordinoitua toimintaa, joka on osa organisaation kaikkia toimintoja, jossa otetaan huomioon sekä organisaation sisäinen, että ulkoinen toimintaympäristö, mukaan lukien ihmisen käyttäytyminen sekä sidosryhmät (SFS-FI ISO 31000 2018, 5-7).

Purdyn (2010, 882) mukaan riski on epävarmuutta, joka johtuu joko sisäisistä tai ulkoisista tekijöistä, joita organisaatio ei hallitse. Hän jatkaa, että nämä epävarmuudet voivat johtaa siihen, että organisaatio ei saavuta tavoitteitaan tai

toisaalta ne voidaan myös jopa ylittää. Riski on siis epävarmuuden vaikutusta tavoitteisiin (SFS-FI ISO 31000 2018, 6) Purdy (2010, 882) siten toteaakin, ettei riski ole juuri positiivinen kuten ei myöskään negatiivinenkaan, vaan siitä aiheutuvat seuraukset voivat vaihdella voittojen ja menetysten välillä. Louisotin ja Ketchamin (2012, 33) mukaan ilman riskiä ei ole myöskään palkintoa ja riskit ovat lopulta niitä, jotka synnyttävät innovaatioita. Heidän mukaansa riski on siten tekijä, joka rohkaisee organisaatiota toimimaan niin kauan, kun riski on hyvin hallittu.

Kaplan, Garrick & Apostolakis (1981, 944) kuitenkin huomauttavat, että riski on subjektiivinen käsite, suhteellista sen havainnoitsijaan nähden ja riippuu siten havainnoitsijan tietämyksen tasosta. Toisaalta riski on objektiivinen siltä kannalta, että kaksi rationaalista havainnoitsijaa täysin samoilla taustatiedoilla ja todisteilla todennäköisesti arvioivat riskin samalla tavalla. (Kaplan et al.1981, 944)

2.1.1 Riskin määrittäminen

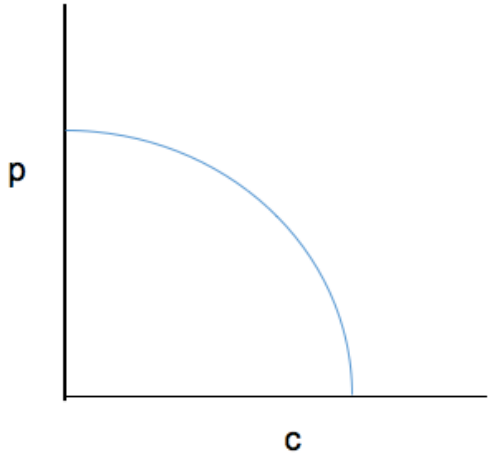
Kaplan et al. (1981, 944) ovat antaneet riskille kvantitatiivisen määritelmän. Kun mietitään hypoteettista toimenpidettä X, voidaan kyseiselle toimenpiteelle suorittaa riskiarviointi etsimällä vastaus kolmeen kysymykseen:

1) Mitä voi tapahtua, eli mikä voi mennä pieleen? (s = scenario)
2) Mikä on tapahtuman todennäköisyys? (p= probability)
3) Jos 1. kysymyksen tapahtuma toteutuu, mikä on sen seuraus? (c = consequence)

Voimme todeta, että riski (r = risk) on yhdistelmä yllä saatuja vastauksia ja se voidaan kirjoittaa seuraavaan muotoon:

$$R = \{s_i, p_i, c_i\}$$

Toteutuva riski voi siten olla mikä tahansa yhdistelmä yllä olevia arvoja, joista saadaan muodostettua riskikäyrä x-y-asteikolle:



Kuvio 2. Riskikäyrä (mukaillen Kaplan et al. 1981, 944)

Yllä oleva riskikäyrä on riskin ensimmäisen tason määritelmä, jossa toteutunut riski voi olla mitä tahansa käyrällä tai sen sisäpuolella. (Kaplan et al. 1981, 944) Toteutunut riski on ISO 31000:2018 (2018, 7) standardin mukaan nimitykseltään riskitapahtuma, joka voi olla joko yksittäinen tapahtuma tai usean eri tapahtuman yhdistelmä, mihin voi olla monia syitä eli riskin lähteitä ja monia seurauksia.

Riski on seurausta riskin lähteistä, joilla tarkoitetaan tekijää tai tekijöiden yhdistelmää, joilla on kyky aiheuttaa riski. Kyseiset lähteet voivat olla sekä aineettomia että aineellisia tekijöitä. (SFS-FI ISO 31000 2018, 6; SFS-Opas 73 2011, 11). Kun riski realisoituu, voi riskin seurauksilla ISO 31000:2018 (2018, 7) standardin mukaan olla sekä haitallisia että myönteisiä seurauksia, jotka voivat vaikuttaa joko suoraan tai epäsuoraan yrityksen tavoitteisiin. Standardin mukaan riskin seuraukset saattavat myös laajentua vaikutusten kumuloitumisen sekä muiden seurannaisvaikutusten johdosta. Alla olevassa kuviossa 3. on esitetty, mallinnuksena, miten ensin riskin lähteet muodostavat riskin, joka realisoituessaan aiheuttaa riskitapahtuman ja sitä seuraavat vaikutukset.

Kuvio 3. Riskin mallinnus (mukaillen SFS ISO 31000 2018, 6; SFS-Opas 73 2011, 11)

2.1.2 Riskilajit

Riskejä voidaan luokitella eri riskilajeihin sen mukaan, minkä tyyppisiä ne ovat ja mihin organisaation toimintoon ne vaikuttavat. Erilaisia riskilajeja voi esimerkiksi olla omaisuusriskit, keskeytysriskit, liikeriskit, henkilöriskit ja ympäristöriskit. (Malmén & Wessberg 2004) Louisot & Ketcham (2014, 105) määrittelevät riskit myös laajempiin kokonaisuuksiin, kuten strategisiin riskeihin, taloudellisiin riskeihin sekä vahinkoriskeihin. He jatkavat, että strategisiksi riskeiksi voidaan määritellä sellaiset riskit, joilla voi olla vaikutusta organisaation kykyyn saavuttaa sen tavoitteet ja päämäärät. Tällaisia voivat olla esimerkiksi maineriski tai riski markkina-aseman menettämisestä.

Taloudelliset riskit voidaan yleisesti määritellä riskeiksi, jotka vaikuttavat yrityksen kannattavuuteen sekä taloudelliseen tehokkuuteen. Vahinkoriskit ovat riskejä, jotka realisoituessaan aiheuttavat menetyksiä tai vahinkoja organisaation fyysisille omaisuuserille tai vahinkoja toisen osapuolen omaisuudelle, kuten toimittajan, asiakkaan, muun yhteistyökumppanin tai kolmannen osapuolen. (Louisot & Ketcham 2014, 104)

2.2 Mitä on riskienhallinta?

Riskienhallinta saatetaan kuvitella joko toimenpiteiksi jo tapahtuneiden virheiden korjaamiseksi tai toisena ääripäänä täysin riskivapaan toimintaympäristön luomisena (Louisot & Ketcham 2014, 15). Malménin ja Wessbergin (2004) mukaan

riskienhallinta on organisaation toimintaa, jolla varmistetaan toiminnan jatkuvuus, henkilöstön hyvinvointi sekä ympäristön kestävä käyttö. He jatkavat, että hyvän riskienhallinnan tunnusmerkkejä ovat toiminnan suunnitelmallisuus, järjestelmällisyys sekä tietoisuus. Myös ISO 31000:2018 (2018, 6) kuvaa riskienhallintaa koordinoiduksi toiminnaksi, jonka avulla organisaatiota johdetaan ja ohjataan riskien osalta ja SFS-Opas 72 (2011, 8-9) tarkentaa riskienhallinnan käsitteen sisältävän myös riskienhallintapolitiikan ja –suunnitelman.

Yleisesti ilmaistuna riskienhallinta on riskien tunnistamista, analysoimista sekä kontrollointia (Thun & Hoenig 2011, 243). Tosiasiassa riskienhallinta on riskin hallitsemista vakaan riskienhallintaprosessin avulla. Se kuitenkin vaatii sitä, että riskienhallinta on sulautettu osaksi organisaation johtamisprosessia kaikilla tasoilla: strategisella, operatiivisella ja taktisella tasolla. Jotta tämä toteutuisi, on tärkeää, että riskienhallinta on mukana sekä tavoitteiden asettamisprosessissa, että strategian implementointiprosessissa. (Louisot & Ketcham 2014, 15) Riskienhallinta ei myöskään saisi olla staattinen prosessi, sillä riskit muuttuvat ja kehittyvät jatkuvasti (Viscelli et al. 2017, 70).

Riskienhallintaan kuuluu riskien ymmärtäminen, analysoiminen ja käsittely, jotta organisaatio voi saavuttaa sen tavoitteensa. Sen vuoksi riskienhallinta onkin sopeutettava kyseisen organisaation tyyppiin sopivaksi. Riskienhallinnalla voidaan minimoida uhat ja maksimoida potentiaali. (IRM 2018c) Yhtä enenevissä määrin riskienhallinnan on katsottu koskevan sekä riskin negatiivista, että positiivista aspektia ja olevan keskeinen osa yrityksen strategista johtamista (IRM 2002, 2).

Riskienhallinnan tulisi myös olla jatkuvasti käynnissä oleva kehittyvä prosessi, joka kulkee organisaation strategian implementoinnin mukana ja jota seurataan ja tarpeen mukaan myös muutetaan (IRM 2002, 2; COSO 2004, 3). Riskienhallinnassa tulisi järjestelmällisesti käsitellä kaikkia riskejä, jotka ovat osa organisaation toimintaa ensinnäkin tulevaisuudessa mutta myös nykyhetkessä ja menneisyydessä. Ylimmän johdon tehtävänä on sisällyttää riskienhallinta organisaation kulttuuriin tehokkaan riskienhallintapolitiikan avulla. Johdon tulisi

muuntaa riskienhallinnan strategia operatiiviselle tasolle ja osoittaa riskienhallinnan vastuut organisaation jäsenille heidän työnkuvansa mukaisesti. (IRM 2002, 2)

Jokaisella riskillä on oltava riskin omistaja, toisin sanoen *”orvot riskit eivät ole hyväksyttäviä*”. Organisaation riskienhallinnasta vastaavien tahojen on kyettävä avustamaan ja kouluttamaan riskin omistajia, joilla tulee olla tarpeeksi kykyä ja resursseja riskin hallitsemiseksi, valtuudet tehdä riskiä koskevia päätöksiä toimivaltansa puitteissa sekä osoittaa toimenpiteet myös omien alaistensa suoritettavaksi. (Louisot & Ketcham 2014, 16)

Riskienhallinnassa tavoitteiden asettaminen on tehtävä ennen kuin organisaatiossa voidaan tunnistaa potentiaalisia tapahtumia, jotka voivat vaikuttaa tavoitteiden saavuttamiseen. Tämän jälkeen voidaan määritellä sekä sisäiset että ulkoiset tekijät, jotka vaikuttavat asetettuihin tavoitteisiin ja jakaa ne riskeihin ja mahdollisuuksiin. (COSO 2004, 3) Koska riski on luontainen osa kaikkea yrityksen tekemistä, riskienhallinnan ammattilaisten tehtävät ovat erittäin moninaisia. Ne voivat sisältää muun muassa työturvallisuuden, liiketoiminnan jatkuvuuden, hyvän hallinnointitavan, teknisen puolen, taloudellisen ulottuvuuden sekä vakuutusten järjestämisen. (IRM 2018c)

2.2.1 Riskinottohalu, riskinsietokyky ja riskikriteerien määrittäminen

Riskinottohalua on alettu viime aikoina yhä enemmän käyttämään kokonaisvaltaisen riskienhallinnan kontekstin yhteydessä. Vaikka riskinottohalulle on useita erilaisia määritelmiä, se liittyy lähes aina riskin hyväksyttävyyteen sekä yrityksen arvoihin ja tavoitteisiin. (Aven 2013, 462) Riskienhallinnan sanastoa määrittelevän ja ISO 31000 standardien ISO-OPAS 73:n (2011, 14) mukaan riskinottohalu tarkoittaa sitä *”missä määrin ja minkä tyyppisiä riskejä organisaatio on halukas tavoittelemaan tai säilyttämään”.*

Yrityksen tulee ymmärtää, kuinka paljon riskiä he haluavat ottaa ja riskinottohalulla kuvataan sitä, kuinka paljon riskiä voidaan hyväksyä (Viscelli et al. 2017, 79) Riskinottohalun määrittäminen on avainasemassa yrityksen strategisten

tavoitteiden asettamisella (Deloitte 2019, 5). Lisäksi riskinottohalua määritettäessä tulee Berlingerin & Váradin (2015, 55-56) mukaan pohtia, millaista kompensaatiota otettavalta riskiltä odotetaan ja siten riskinottohalukkuudella onkin selkeä yhteys yrityksen tuotto-odotukseen.

Louisotin & Ketchamin (2014, 11) mukaan riskinottohalun tulee olla yrityksessä määritetty ja ymmärretty, ja yrityksen tulee kyetä tasapainottamaan hyväksyttävän riskinottotason kustannusten ja hyötyjen välillä, jotta se voi saavuttaa strategiset tavoitteet ja päämäärät. He jatkavat (2014, 11), että on hallituksen vastuulla määrittää riskinottohalu sekä riskinottokyky, joiden puitteissa organisaatio voi turvallisesti operoida, sekä lisäksi hallituksen tulee määrittää riskimittarit johdolle, jotta johto voi valvoa, että toiminta pysyy asetettujen raja-arvojen sisällä ja tulokset ovat luotettavia.

Riskinsietokyvyllä sen sijaan tarkoitetaan sitä, mikä on organisaation tai sen sidosryhmien valmius ottaa vastuu riskistä sen käsittelyn jälkeen. (SFS Ohje 73 2011, 14) Frijns, Gilbert, Lehnert & Tourani-Rad (2013, 2458) ovat jakaneet riskinsietokyvyn kahteen eri osaan: riskin välttämiseen ja riskin havaitsemiseen. Heidän mukaansa (2013, 2458) riskin välttämisellä mitataan henkilön riskin välttämisen astetta, kun taas riskin havaitseminen osoittaa sen, että vaikka kahdella henkilöillä olisi sama riskin välttämisen aste, he saattavat tulkita riskin ja sen mahdolliset menetykset eri tavalla.

Jotta organisaatio voi tunnistaa, analysoida ja priorisoida riskit, sen tulee ensin määrittää riskikriteerit. Usein riskikriteerit sisältävät asteikon, jolla mitataan riskin todennäköisyyttä, vaikutusta, kontrolleja sekä muita mitattavia parametreja. Tällaisten riskikriteerien asteikkojen etuna nähdään keskustelu ja yhteisymmärrys asianmukaisista skaaloista. Riskikriteerit myös edesauttavat riskien ja riskienhallintatoimenpiteiden priorisoinnin sekä ohjaavat ERM prosessia. (Fraser & Simkins 2016, 693, 696)

Riskikriteereinä käytetään usein numeerisia vaikutusasteikkoja esimerkiksi arvoja välillä 1-5, joilla voidaan kuvata riskin todennäköisyyttä ja vakavuutta, esimerkiksi

aiheuttaako riskin toteutuminen mahdollisesti myöhästymisiä, loukkaantumisia tai kuolemantapauksia ja mikä on niiden ilmentymistiheys. Riskikriteerit tyypillisesti sisältävät määritelmiä eri tyyppisistä vaikutuksista sekä todennäköisyyksistä ja lisäksi ne voivat myös sisältää informaatiota siitä, millaisia toimenpiteitä kukin riskilukema vaatii. (University of Cambridge 2018)

2.2.2 Riskienhallintakeinot

Aiemmin riskiä oli tapana pitää vain negatiivisena asiana, joka tulisi mahdollisuuksien mukaan välttää tai siirtää. Nykyään on kuitenkin ymmärretty, että riski ei ole luonnostaan negatiivinen eikä positiivinen, jolloin riskistä luopuminen kokonaan on osittain organisaation tavoitteiden saavuttamisesta luopumista. (Purdy 2010, 882) COSO:n (2004, 3) mukaisia riskienhallintakeinoja onkin riskin välttämisen, vähentämisen ja siirtämisen lisäksi myös riskin hyväksyminen.

Jos riski voidaan havaita ja ymmärtää ajoissa sekä ymmärtää mikä aiheuttaa riskin ja mihin se voi johtaa, organisaatio voi parhaimmillaan muuttaa riskiä siten, että se auttaa organisaatiota saavuttamaan sen tavoitteet nopeammin ja tehokkaammin. (Purdy 2010, 882) Organisaation ei kannata pyrkiä hallitsemaan joka ikistä riskiä, vaan ensin tulisi suojautua sellaisia riskejä vastaan, joilla on suurin merkitys organisaation strategisten tavoitteiden toteutumisen kannalta. Tunnistamalla ja pyrkimällä vaikuttamaan ensin sellaisiin riskiin, joilla on olennaisin merkitys strategian toteuttamiseen, organisaation on mahdollista saavuttaa myös niin sanottuja pikavoittoja. Riskikriteerien määrittämisen avulla voidaan priorisoida riskit ja toteuttaa toimenpiteet välittömästi. (Fox 2012, 36)

Jotta riskienhallinnan toimenpiteet voidaan toteuttaa, toimenpide pitää delegoida riskin omistajalle. Luonnollinen riskin omistaja on henkilö, joka on vastuussa siitä toiminnosta, jota lähimpänä riski koskettaa. Esimerkiksi tietovuotoriskin luonnollinen omistaja on täten IT-päällikkö. Vaikka kaikkia riskejä ei voida osoittaa henkilöille suoraan toiminnoittain, yksilöity riskin omistaja tulisi kuitenkin aina olla, eli kuka on vastuussa kyseisen riskin hallitsemisesta ja toimenpiteiden toteuttamisesta. (Fox 2012, 36)

Riskienhallinnan kannalta välttämättömänä pidetään yleensä riskirekisterin ylläpitämistä. Riskirekisterissä ylläpidetään tunnistettuja riskejä sekä niihin liittyvää informaatiota. Tällaisen rekisterin ylläpitämisessä on kuitenkin haasteensa, jotta riskien määrä ei kohoa liialliseksi, jolloin rekisterin ylläpitäminen muodostuu hallinnolliseksi taakaksi ja turhauttaa johtoa. Koska riskienhallinta on reaaliaikainen ja muuttuva prosessi, ei riskirekisterikään saa jäädä päivittämättömäksi dokumentiksi. (Fraser & Simkins 2016, 691, 694)

2.3 Perinteisen ja kokonaisvaltaisen riskienhallinnan eroavaisuudet

Riskienhallinta on kehittynyt kapeasta lähinnä riskin arvioimiseen keskittyvästä näkökulmasta kokonaisvaltaiseen koko riskin kattavaan näkemykseen, jota kutsutaan yleisemmin termillä ERM (Enterprise Risk Management) (Pagach & Warr 2011, 187). Perinteinen riskienhallinta lähestyy riskejä siilotekniikalla, jossa jokainen riski käsitellään yksinään, ottamatta huomioon eri riskien keskinäisiä suhteita. Sen sijaan kokonaisvaltainen riskienhallinta (ERM) on koko yrityksen käsittävää riskien arviointia, määrittämistä, rahoittamista sekä hallintaa, jossa ERM mahdollistaa yritysten riskien hallitsemisen integroidulla ja kokonaisvaltaisella tavalla. (Grace, Leverty, Phillips & Shimpi, 2015, 289-290; Hoyt & Liebenberg, 2011, 795)

Pääomamarkkinoiden kasvu, terrorismi, luonnonkatastrofit, kyberuhat, nopeat innovaatiot ja verouudistukset ovat haasteita, joiden parissa johto ja hallitus nykypäivänä painivat, kun he yrittävät hallita yrityksen riskikenttää. Tällaiset kehityssuunnat lisäävät riskien suuruutta sekä monimutkaisuutta, samalla kun johto ja hallitus yrittävät pitää silmällä merkittävimpiä riskejä. (Beasley et al. 2018, 3) Fraserin & Simkinsin (2016, 689) mukaan yrityksen tulisikin muodostaa koko yrityksen käsittävä riskiportfolio, jota hallitaan kokonaisuutena. Tähän kokonaisvaltainen riskienhallinta tuo helpotusta.

Alla olevassa taulukossa on Butterfieldin (2017) mukaan merkittävimmät erot perinteisen ja kokonaisvaltaisen riskienhallinnan välillä:

Taulukko 1. Perinteisen ja kokonaisvaltaisen riskienhallinnan keskeiset erot (mukaillen: Butterfield 2017)

	Perinteinen riskienhallinta	**Kokonaisvaltainen riskienhallinta**
Lähestymistapa	Segmenttikohtainen, jossa liiketoimintayksiköt/-segmentit käsittelevät omat riskinsä	Kokonaisvaltainen (holistinen), jossa toiminta lähtee johdosta alaspäin
Käsitys riskeistä	Vähän tai ei lainkaan tietoa organisatoristen riskien kokonaiskuvasta	Laaja kokonaisnäkemys organisatorisista riskeistä
Painopiste	Liiketoimintayksikön tappioiden ehkäisemisessä (taktinen taso)	Riskin vähentämisessä, pitkäjänteisyydessä sekä arvon tuottamisessa läpi organisaation (strateginen taso)
Omaisuuserät	Keskittyy fyysisiin ja taloudellisiin omaisuuseriin	Arvioi koko omaisuusportfolion ja aineettomat omaisuuserät kuten asiakkaat, työntekijät, toimittajat, innovaatioprosessit ja immateriaalioikeudet
Tavoite	Etsii ratkaisuja riskin pienentämiseen kunkin siilon oman osaamisen ja päätöksentekokyvyn puitteissa	Etsii ratkaisuja riskin pienentämiseen koko organisaatiossa asetetun strategian puitteissa

Vaikka kokonaisvaltainen riskienhallinta painottaa laajaa kokonaiskäsitystä organisatorisista riskeistä, ei Butterfieldin (2017) mukaan tosiasiassa yksikään organisaation jäsen kykene tiedostamaan jokaista riskialttiutta, jota yritys kohtaa, vaan paras tieto ja osaaminen löytyvät siitä liiketoimintayksiköstä, jota riski koskettaa. Hänen mukaan perinteinen riskienhallinta kuitenkin keskittyy liikaa vertikaaliseen viestintään organisaatiossa alhaalta ylöspäin luoden suorituspaineita alatasoille, ja ERM:in tehtävänä onkin nostaa riskienhallinta strategiselle tasolle.

Yritykset harjoittavat liiketoimintaa asiakkaiden, toimittajien, hallinnollisten toimielinten sekä muiden sidosryhmien kanssa. Yritysten toimintaan vaikuttaa useat organisatoriset rajat ylittävät tekijät, joihin yritys ei välttämättä voi itse juurikaan vaikuttaa. Tällaisia ovat esimerkiksi muutokset lainsäädännössä, sosiaalisessa käyttäytymisessä sekä yleisessä taloudellisessa tilanteessa. Organisaation arvoketjuun vaikuttavat muun muassa verotus ja valuuttakurssit. Toimintaympäristö ja siihen liittyvät elementit vaikuttavat organisaation tavoitteiden saavuttamiseen sille ne ovat liiketoimintariskien lähteitä. (Oliva 2016, 67-68)

Aonin vuonna 2019 julkaistun ”Global Risk Management Survey”[1] tutkimuksen mukaan tänä päivänä yritykset jokaisella toimialalla kohtaavat enemmän riskejä kuin koskaan ennen. Tutkimuksen mukaan yritysten suurimpia huolenaiheita ovat talouskasvun hidastuminen, vahingot maineelle ja brändille sekä nopeat muutokset markkinaolosuhteissa. Yritykset ovat myös yhä haavoittuneempia uusille riskeille, kuten kyberhyökkäyksille, aineettomista tekijöistä johtuvalle liiketoiminnan keskeytymiselle sekä työvoimapulalle. (Aon 2019, 1)

Perinteisen ajattelutavan mukaan yritykset aiemmin keskittyivät lähinnä vain sellaisiin riskeihin ja tapahtumiin, jotka olivat vakuutettavissa, kuten esimerkiksi omaisuusriskeihin. Taloudellisella puolella sen sijaan keskityttiin lähinnä korko-, valuutta- ja hyödykeriskeihin. Pääasiassa keskityttiin siis riskeihin, jotka pystyttiin arvioimaan määrällisesti. 1990-luvun puolivälissä riskienhallintaa koskevat julkaisut alkoivat painottaa sitä, että riskienhallintaan tulisi sisällyttää kaikki riskit, eikä vain

[1] Aon Global Risk Management Survey 2019 tutkimuksessa vastaajia oli globaalisti 2672 kpl ja 33 eri toimialalta (Aon 2019, 2).

helposti numeerisesti määritettävissä olevat. (Fraser & Simkins 2016, 689) Myös Deloitten (2019, 2, 6) mukaan tulisi keskittyä yhä enemmän ei-taloudellisiin riskeihin, kuten kyberriskeihin ja yritysten tulisikin siksi arvioida uudelleen perinteisemmät lähestymistavat riskienhallintaa kohtaan.

Aonin julkaisemassa tutkimuksessa 10 tärkeimmän riskin joukkoon mahtui useita ei-vakuutettavissa olevia riskejä, mikä osoittaa, ettei perinteinen riskienhallinta kykene enää vastaamaan nykyhetken liiketoimintaympäristöön ja uudenlaisiin riskeihin. Alla olevassa taulukossa 2. on esitetty tutkimuksen tuloksena saadut top 10 riskit:

Taulukko 2. Top 10 riskit Aonin "Global Risk Management Survey" tutkimuksen mukaan (Aon 2019, 3)

Nro.	Riski
1	Talouden hidastuminen / hidas elpyminen
2	Vahinko maineelle / brändille
3	Nopea muutokset markkinatekijöissä
4	Liiketoiminnan keskeytyminen
5	Lisääntyvä kilpailu
6	Kyberhyökkäykset / tietoturvaloukkaukset
7	Hyödykkeiden hintariski
8	Kassavirta- / likviditeettiriski
9	Epäonnistuminen innovoinnissa / asiakkaiden tarpeisiin vastaamisessa
10	Muutokset lainsäädännössä / sääntelyssä

Kuten Aonin tutkimuksessa (2019, 10) on todettu, nykyään riskejä pystyään yhä vähemmän vakuuttamaan, jolloin muuttuvan riskiprofiilin ja uusien riskien hallitseminen on haastavaa yrityksille, joilla ei ole asianmukaista riskienhallintaprosessia. Sen vuoksi kokonaisvaltaisella riskienhallinnalla ja asianmukaisella riskienhallintaprosessilla on yhä suurempi merkitys organisaatioille kaikilla toimialoilla ympäri maailman.

2.4 Kokonaisvaltaisen riskienhallinnan kehittyminen ja tausta

Vuosien 2008 ja 2009 aikana vallinnut pankkikriisi osoitti, että riskienhallinta on monissa yrityksissä riittämätöntä. (Fraser & Simkins 2016, 690) Vaikka rahoitus- ja vakuutusalalla toimivat yritykset ovat perinteisesti investoineet prosesseihin ja teknologiaan riskialttiuden tunnistamiseksi ja arvioimiseksi, siitä huolimatta useat alan yritykset ovat kokeneet suuria epäonnistumisia organisatoristen riskien hallinnassa, esimerkiksi sallimalla yksittäisten henkilöiden tehdä liiallisilla valtuuksilla erittäin riskialttiita osakekauppoja. (Callahan & Soileau 2017, 122)

1990-luvun puolivälin jälkeen, kun riskienhallintaa alettiin painottaa koko yritystoiminnan käsittävänä toimintana, useita riskienhallintaa koskevia julkaisuja ja standardeja alkoi ilmestyä. Kokonaisvaltaista riskienhallintaa koskevia tutkimuksia julkaisivat jo aiemminkin mainittu Purdy (2010) ja Louisot & Ketcham (2014) sekä tuoreimpina aiheen tutkijoina Fraser & Simkins (2016) sekä Butterfield (2017). ISO 31000 riskienhallinnan standardia ja sen uudistumisen myötä tulleita muutoksia ovat tutkineet Fox (2018) ja IRM (2018a). Fox on keskittynyt pääasiassa siihen, kuinka standardia tulisi tulkita ja kuinka yritykset pystyisivät implementoimaan ERM:n. Myös IRM on julkaissut oman riskienhallinnan standardin sekä julkaissut useampia ohjeita ISO 31000 standardin käyttöönottoon.

Standardeista ja viitekehyksistä kehityksen kärjessä olivat muun muassa Australian ja Uuden-Seelannin riskienhallinnan standardi (AS/NZS 4360:1995), Kanadan riskienhallinnan standardi (CAN/CSA-Q850-97), Tillinghast-Towers Perr (nykyinen Willis Towers Watson) sekä Conference Board of Canada. (Fraser & Simkins 2016, 689) Myös COSO-ERM viitekehyksen tarkoituksena on toimia yrityksen kokonaisvaltaisena riskienarviointi- ja hallintaprosessina tavoitteenaan korjata puutteet koko yritystoiminnan kattavassa systemaattisessa riskienhallinnassa. (Callahan & Soileau 2017, 122-123). Kokonaisvaltaisen riskienhallinnan (ERM) konteksti on siten kehittynyt useiden eri standardien, julkaisujen ja tutkimusten yhdistelmänä.

2.5 Kokonaisvaltaisen riskienhallinnan tavoitteet ja hyödyt

ERM on integroitu lähestymistapa hallita riskejä läpi organisaation ja sekä sen sidosryhmäverkostossa (IRM 2018c). Pagachin & Warrin (2011, 187) mukaan ERM:llä tarkoitetaan johtamisprosessia, joka edellyttää yrityksen johtoa tunnistamaan ja arvioimaan riskit, jotka vaikuttavat yrityksen arvoon sekä soveltaa koko yrityksen kattavaa strategiaa riskien hallitsemiseksi, jotta voidaan luoda tehokas riskienhallintastrategia. Tehokkaan ERM-prosessin perimmäinen tavoite on auttaa johtoa hallitsemaan riskejä strategian yhteydessä, jotta organisaatio pystyy todennäköisimmin saavuttamaan sen keskeiset tavoitteet (Viscelli et al. 2017, 69). Fox:n (2012, 34) mukaan ERM on pohjimmiltaan keino luoda riskienhallinnan kyvykkyyttä koko organisaatioon.

Viscelli et al. (2017, 70) jatkavat, että ERM-prosessin tavoitteena on tunnistaa, hallita ja seurata riskejä, jotka voivat vaikuttaa organisaation kykyyn saavuttaa tavoitteensa, jolloin ERM:iä pidetäänkin yrityksen strategisena työkaluna. Myös Grace et al. (2015, 290) toteavat, että ERM voi lisätä yrityksen riskitietoisuutta, joka edistää sekä operatiivista että strategista päätöksentekoa. COSO:n (2004, 2) mukaan yrityksen riskienhallinta on prosessi, jota yrityksen hallitus, johto ja muu henkilöstö toteuttavat ja jota sovelletaan sekä strategiassa että koko yrityksessä. COSO:n (2004, 2) mukaan riskienhallinnan tarkoituksena on tunnistaa sellaiset mahdolliset tapahtumat, jotka voivat vaikuttaa koko yritykseen ja hallita riskejä riskinottohalun puitteissa sekä tarjota riittävä varmuus tavoitteiden saavuttamisesta.

ERM auttaa varmistamaan, että organisaation kaikki tärkeimmät riskit on tunnistettu, eri riskien väliset riippuvuudet havaittu sekä riskit ovat tasapainossa yrityksen riskinottohalun kanssa (Deloitte 2019, 25) Meidellin & Kaarboen (2017, 39) mukaan ERM parantaa päätöksentekoprosesseja ja sitä kautta organisaation suorituskykyä. Eräänä ERM:in hyötynä nähdään se, että sen käyttöönotto voi täyttää myös organisaation sidosryhmien vaatimukset. ERM huomioi organisaation toiminnan kaikki ulottuvuudet ja riskienhallintaprosessin riskin arvioinnista sen mittaamiseen ja pienentämiseen. (Daukant & Hirst 2009, 64) Fox:n (2012, 35) mukaan erityisesti ERM:in implementointiin tulisi hakea apua ja tukea niiltä, jotka

eniten ymmärtävät riskejä, joita organisaatio kohtaa. Hän jatkaa (2012, 25), että implementointiin tulisi osallistua henkilöitä eri toiminnoista ja sen lisäksi tulisi harkita myös ulkopuolista tukea, kuten konsultteja ja vakuutusmeklareita.

Omaksumalla systemaattisen ja johdonmukaisen prosessin kaikkia organisaatioon kohtaamia riskejä kohtaan, ERM:in odotetaan alentavan yrityksen yleistä epäonnistumisen riskiä ja siten parantamaa sen suorituskykyä sekä sitä kautta yrityksen arvoa (Gordon et al. 2009, 302) Viscelli et al. (2017, 70) toteavat, että ERM on suunniteltu kehittyväksi prosessiksi, joka tuottaa johdolle tietoa riskeistä, jotka voivat olla näköpiirissa ja vaikuttaa yrityksen ydinliiketoimintamalliin sekä tuleviin strategisiin avauksiin ja siksi ERM prosessi tulisikin nähdä panostuksena strategiseen suunnitteluun ja toteutukseen.

Viscelli et al. (2017, 76) mukaan ERM auttaa tunnistamaan yrityksen nykyiseen strategiaan kohdistuvia riskejä, se johtaa parempaan riskitietoisuuteen yli siilojen, edistää riskien läpinäkyvyyttä sekä lisää riskitiedon jakamisen oikea-aikaisuutta organisaatiossa. He jatkavat (2017, 76), että nämä tekijät auttavat yrityksen johtoa ymmärtämään riskien vaikutuksia läpi organisaation ja mahdollistaa riskien hallitsemisen proaktiivisesti reaktiivisen sijasta.

2.6 Haasteet kokonaisvaltaisen riskienhallinnan implementoinnissa

Tutkimusten mukaan useat yritykset ovat kokeneet haasteita integroida riskienhallintaa osaksi strategiaa, eikä riskienhallinnan hyötyjen ole välttämättä uskottu ylittävän sen aiheuttamia kustannuksia (Beasley et al. 2018, 2) Fraser & Simkins (2016, 690) ovat tunnistaneet useampia haasteita, joita on todettu esiintyvän organisaatioiden yrittäessä implementoida ERM:iä. Ensimmäisenä on ERM:in sisällöstä esiintyvät väärinkäsitykset, sillä eri tahot ovat luoneet ERM:stä omia versioitaan, kuten jo aiemmin mainitun COSO:n luoma COSO-ERM viitekehys sekä eri luottoluokituslaitosten, kuten Standard & Poorin käyttämät ERM arvioinnit. Toisena Fraser & Simkins ovat maininneet organisaation sisäiset haasteet, jotka liittyvät muun muassa yrityskulttuuriin, johdon ja hallituksen tietämykseen,

kouluttamiseen, ajankäyttöön sekä ERM prosessin mielekkyyteen. (Fraser & Simkins, 2016, 690)

Sisäisiä haasteita ovat esimerkiksi soveltumaton yrityskulttuuri, sillä onnistunut implementointi edellyttää, että organisaatio on avoin ja sillä on halu kehittää yhteistyötä kaikkien organisaation jäsenten kesken. Toisena mainitaan hallituksen ja johdon riittämätön tietämys riskeistä ja ERM:stä, joka voi johtua osaksi siitä, etteivät he koe olevansa lisäkoulutuksen tarpeessa. (Fraser & Simkins, 2016, 690-691) Lisäksi organisaatioiden nykyiset riskienhallinnan käytännöt voivat olla epäkypsiä eikä ihmisiä ole siten kyetty esimerkiksi kannustimilla sitouttamaan riskienhallinnan toteuttamiseen (Beasley et al. 2018 2). Sen sijaan, kun organisaation muita jäseniä koulutetaan, haasteena on myös se, ettei koulutuksen lisäksi järjestetä esimerkiksi käytännön riskityöpajoja, jossa oppi yhdistettäisiin todellisen liiketoiminnan tilanteisiin. Lisäksi kun ERM:iä implementoidaan, voi johdolla olla kiusaus implementoida koko prosessi kaikkine ominaisuuksineen kerralla, mikä voi johtaa prosessin monimutkaisuuteen ja liialliseen hallinnolliseen taakkaan. Sen sijaan prosessi tulisi implementoida vaiheittain, pilotoimalla ensin yksinkertaisen version ja lisäämällä haluttuja ominaisuuksia mukaan myöhemmin. (Fraser & Simkins, 2016, 690-691)

Sisäisenä haasteena nähdään myös se, että organisaatio tunnistaa riskejä jopa liian paljon. Kun esimerkiksi yli 700 riskiä tunnistetaan, listataan riskirekisteriin ja päivitetään säännöllisesti, hallinnollinen taakka kasvaa eikä sitä enää nähdä merkityksellisenä tai hyödyllisenä. (Fraser & Simkins, 2016, 691) Syynä tähän voi olla se, että Beasley et al. (2018, 3) mukaan yrityksissä on todettu, että riskien määrä ja monimutkaisuus on kasvanut merkittävästi viimeisen viiden vuoden aikana. Fraserin ja Simkinsin (2016, 691) mukaan esimerkiksi lyhyemmän top 10-20 riskilistan monitorointi nähdään usein parempana vaihtoehtona. Lisäksi heidän mukaan riskien tunnistamisessa ja niiden todennäköisyyksien määrittämisessä haasteena voi esiintyä aikarajojen puuttuminen, sillä todennäköisyyksistä ei voi keskustella luotettavasti, mikäli ajanjaksoa ei ole määritetty. Apuna toimii todennäköisyysprosentin määrittäminen seuraavan viiden vuoden sisällä tai

vaihtoehtoisesti määrittelemättömän ajanjakson kuluessa antaa vastaajalta täysin eri arvon.

Sisäisiä haasteita ovat myös se, että ERM:iä ei koeta organisaatiossa mielekkääksi vaan lähinnä hallinnolliseksi taakaksi, mikä lisää paperityötä. Fraser & Simkins ovat nähneet tähän erääksi ratkaisuksi sen, että prosessiin valitaan tietotaidoltaan oikeat ihmiset. Heidän mukaan mielekkyyttä lisäävät esimerkiksi riskityöpajat ja äänestysmenetelmät joiden kautta osallistujat kokevat oppivansa, lisäävän tietoisuuttaan riskeistä, ratkovansa oikeita liiketoiminnallisia ongelmia, kokevan jopa jännitystä sekä tuntevansa ajankäytön tehokkaaksi. Koska ERM on myös eräs muutoksenhallinnan työkalu, se vaatii tiedon jakamista, ja haasteena voikin olla se, että vain johto osallistuu riskienhallintaan muiden organisaatioiden jäsenten jatkaessaan toimintaansa kuten ennen ERM:in implementointia. (Fraser & Simkins, 2016, 691-692)

3 ISO 31000-STANDARDI KOKONAISVALTAISEN RISKIENHALLINNAN VIITEKEHYKSENÄ

3.1 Standardin tausta

Kaikenlaisten organisaatioiden, yksityisten tai julkisten, voittoa tavoittelevien tai tavoittelemattomien, on tehtävä luotettavia sekä tasapainoisia päätöksiä kaikkien niiden riskien osalta, joita he kohtaavat. Päätöksentekijöille voi olla haasteellista yhdistellä tietoja näennäisesti samanlaisista riskienhallinnan prosesseista ja toimintatavoista, joilla on kuitenkin erilaiset tarkoitukset. Tästä syystä kansainvälinen standardoimisjärjestö ISO on kehittänyt riskienhallinnan standardin, joka pyrkii luomaan johdonmukaisuutta ja luotettavuutta riskienhallinnassa ja joka sopisi kaikkiin riskimuotoihin. Tällainen standardi sisältää sekä yhdenmukaisen riskienhallinnan sanaston, suorituskykyvaatimukset, yhteisen kattavan prosessin riskien tunnistamiseksi, analysoimiseksi, arvioimiseksi ja käsittelemiseksi sekä ohjeet kuinka prosessi tulisi implementoida ja integroida organisaation päätöksentekoprosessiin. (Purdy 2010, 881)

Standardi on usein joukko periaatteita, ohjeita, suuntaviivoja ja vaatimuksia, mitkä tarjoavat organisaatioille yhtenäisen ja systemaattisen lähestymistavan toimia (Preda 2012, 112). Standardista on kuitenkin huomattava se, että se on SFS ry:n (2018) mukaan tarkoitettu nimenomaisesti oppaaksi eikä vaatimukseksi, jolloin sitä ei ole tarkoitettu esimerkiksi organisaation sertifiointiin. Vaikka standardien noudattaminen Predan (2013, 112) mukaan ei useinkaan ole pakollista, monet organisaatiot noudattavat niitä osoittaakseen sitoutumisensa toimialan parhaiden käytäntöjen noudattamiseen.

SFS ry:n (2018) mukaan ISO 31000 standardi perustuu hyvän riskienhallinnan periaatteisiin ja organisaatiot voivat omaksua standardista juuri omaan toiminnanohjaukseensa parhaiten soveltuvat ohjeet ja periaatteet. Standardi sopii kaikkiin organisaatioihin riippumatta niiden koosta tai toimialasta ja se soveltuu myös monenlaisten riskien käsittelyyn. Standardista on huomioitava myös se, että

sitä ei ole pääsääntöisesti luotu vain riskienhallinnan ammattilaisten käyttöön, vaan se on tarkoitettu avuksi kaikille niille, jotka ovat jollain tapaa tekemisissä riskien ja päätöksentekoprosessien kanssa. (SFS, 2018) Osbichin (2018) mukaan standardi on tarkoitettu kaikille niille organisaation jäsenille, jotka hallitsevat riskejä, tekevät päätöksiä, asettavat tavoitteita, pyrkivät edistämään suorituskykyä tai muulla tapaa osallistuvat arvon luomiseen.

IRM:n (2018a, 4) mukaan yritysten tulisi omaksua niiden toimintaan sopivimmat ISO 31000:n periaatteet ja komponentit ja muokata tarpeen mukaan muita osioita omaan toimintaan sopivimmaksi. Standardi toimiikin siten suosituksena ja lähtökohtana, jota yritys voi hyödyntää oman riskienhallinnan suunnittelussa. IRM:n (2018a, 4) mukaan ISO 31000-standardi sisältää korkean tason suuntaviivat riskien hallitsemiseksi, mutta se ei kuitenkaan sisällä minkäänlaisia vaiheittaisia ohjeita, kuinka riskienhallinnan järjestäminen tulisi aloittaa. IRM:n (2018a, 4) mukaan joidenkin riskienhallinnan ammattilaisten voi olla vaikea mukauttaa uuden ISO 31000:2018 standardin mukaisia suosituksia sopivaksi heidän nykyisten riskienhallinnan käytäntöjen kanssa.

3.2 Keskeisimmät muutokset uudistetussa standardissa

Standardoimisliittojen periaatteisiin kuuluu, että kaikkien ISO standardien sisältö tarkastetaan uudistamistarkoituksessa viiden vuoden välein, mikä takaa sen, että standardeissa esitetty tieto pysyy ajantasaisena ja käyttökelpoisena. Myös tästä syystä alun perin vuonna 2009 julkaistu ISO 31000 standardin ensimmäinen versio uusittiin vuonna 2018. Uudessa standardissa huomioitiin tapahtunut markkinakehitys ja uudet haasteet, joita organisaatiot kohtaavat. Eräitä uudistamiseen johtaneita syitä olivat muun muassa digivaluutat ja talousjärjestelmien lisääntynyt monimutkaisuus. (SFS ry, 2018)

Keskeisimpiä muutoksia vuosien 2009 ja 2018 versioiden välillä ovat olleet strategiset ohjauksen lisääntyminen, ylimmän johdon osallistaminen sekä riskienhallinnan sisällyttäminen eri toimintoihin (SFS ry, 2018). Foxin (2018, 6) mukaan uuden standardin tarkoituksena on helpottaa riskienhallinnan integroimista

toimintaan ja päätöksentekoon. Standardin uudempi versio painottaa SFS ry:n (2018) mukaan sitä, että riskienhallinta tulisi olla kiinteä osa organisaatiota, jolloin se tulisi sisällyttää muun muassa strategiaan, tavoitteisiin ja prosesseihin sekä ottamalla mukaan myös sidosryhmät ja huomioimalla organisaation inhimillisten ja kulttuuristen tekijöiden vaikutuksen. Vuoden 2018 standardi myös painottaa organisaation eri toimijoiden sitouttamista riskienhallintaan määrittämällä vastuualueita ja varaamalla resursseja läpi organisaation (SFS ry, 2018).

Uudistettua standardia on yksinkertaistettu vuoden 2009 versioon nähden muun muassa termistön osalta, pyrkien tekemään riskienhallinnan sanastosta selvempää ja helpommin ymmärrettävää sekä vähentämällä riskienhallinnan jargonia. (Fox 2018, 6; SFS ry, 2018)

3.3 Standardin sisältö ja tavoitteet

Riskienhallinta koostuu standardin mukaisista periaatteista, puitteista ja prosesseista, jotka voivat olla käytössä organisaatiossa joko täysimääräisesti tai osittain ja niitä on voitu muokata organisaatioon sopivaksi. (SFS-ISO 31000 2018, 5) SFS ry:n (2018) mukaan standardin tavoitteena on auttaa organisaatioita luomaan sellaiset riskienhallinnan puitteet, joiden avulla ne pystyvät tunnistamaan, arvioimaan sekä käsittelemään riskit tehokkaasti sekä arvioimaan niiden vaikutuksen tavoitteiden saavuttamiseen.

ISO 31000:2018 standardissa määritelty riskin määritelmä *”epävarmuuden vaikutus tavoitteisiin*” siirtää painopisteen pelkästä huolenaiheesta positiivisen tapahtuman mahdollisuuteen, jolloin riskienhallinta onkin yksinkertaisesti optimointiprosessi, joka tekee tavoitteiden saavuttamisesta todennäköisempää. Riskit ovat oikeastaan kuvauksia siitä, mitä voisi tapahtua, kun taas riskikontrollit ovat työkaluja, joiden tarkoituksena on muokata näitä riskiä. (Purdy 2010, 882) Myös SFS ry:n (2018) mukaan ISO 31000:2018 standardi auttaa organisaatioita tunnistamaan ja ymmärtämään riskien pelkkien negatiivisten seurausten lisäksi myös positiiviset seuraukset ja standardia voi hyödyntää tehokkaamman suorituskyvyn kehittämisessä sekä hyvän hallintotavan luomisessa.

ISO 31000:2018 standardin mukaan on olemassa tiettyjä selkeitä suorituskykyvaatimuksia, jotka varmistavat sen, että riskit hallitaan sekä tehokkaasti että vaikuttavasti (Purdy 2010, 882). Nämä ovat standardin (2018, 7-8) mukaan seuraavat kahdeksan periaatetta eli elementtiä, jotka yhdessä luovat riskienhallinnan tarkoituksen, eli arvon luomisen ja säilyttämisen:

1) *”Organisaation johtamisjärjestelmään sisällytetty*
2) *Jäsennelty ja kattava*
3) *Räätälöity*
4) *Sidosryhmät mukaan ottava*
5) *Dynaaminen*
6) *Paras saatavilla oleva tieto*
7) *Inhimilliset ja kulttuuriset tekijät*
8) *Jatkuva kehittäminen”*

Yllä oleva lista kuvaa standardin (2018, 8) mukaan sitä, että riskienhallinta sisältyy organisaation jokaiseen toimintoon, ja myös Foxin (2018) mukaan riskienhallinta ei olekaan enää yksittäinen organisaation toiminto, vaan kiinteä ja olennainen osa sekä organisaation että yksilön päätöksentekoa. Standardin mukaan (2018, 8-9) riskienhallinta tulee räätälöidä sopivaksi organisaation sisäiseen ja ulkoiseen toimintaympäristöön ja sen avulla havaitaan muutokset riskeissä. Riskienhallinnan ollessa jäsennelty myös tulokset ovat yhdenmukaisia.

Lisäksi standardin mukaan (2018, 8-9) riskienhallinnassa tulisi ottaa organisaation sidosryhmät sopivissa määrin mukaan heidän oman tietotaitonsa ja havaintojen puitteissa sekä varmistaa riskienhallinnassa tarvittavien tietojen oikea-aikaisuus ja olennaisuus. Sidosryhmien mukaanotto on tärkeää, sillä Olivan (2016, 67) mukaan yritykset harjoittavat liiketoimintaa useiden eri sidosryhmien kanssa. Myös ihmisten käyttäytyminen ja organisaatiokulttuuri vaikuttavat riskienhallintaan ja riskienhallintaa tulee myös kehittää jatkuvasti havaittujen kokemusten ja oppimisen myötä (SFS-FI ISO 31000 2018, 8-9).

Tranchardin (2018) mukaan riskienhallinta tulisi sisällyttää organisaation kaikkiin toimintoihin sisältäen muun muassa tietohallinnon, henkilöstöhallinnon, työturvallisuuden, laadun, liiketoiminnan jatkuvuuden sekä hyvän hallinnointitavan. Myös Fox (2018, 4) toteaa, että sen sijaan että riskienhallinta olisi jaksoittain tapahtuvaa riskien arviointia, sen tulisi olla kiinteä osa organisaation päätöksentekoa.

Riskienhallinta ei saisi olla vain teknisten toimenpiteiden toteuttamista, vaan myös riskienhallinnan kulttuurin luomista. Organisaatiossa tulisi kiinnittää huomiota niin sanotun turvallisuuskulttuurin luomiseen ja siihen, että riskienhallinta ulottuu organisaation jokaiselle tasolle. Konkreettisia riskienhallintatoimia ovat käytännön toimenpiteet kuten henkilöstön koulutus sekä tiedonvaihto. (Malmén & Wessberg 2005a)

ISO 31000:2018 standardin mukaan (2018, 9) riskienhallinnan puitteiden tarkoitus on toimia apuna siinä, miten organisaatio pystyy sisällyttämään riskienhallinnan sen keskeisiin toimintoihin. Standardin mukaan (2018, 9) riskienhallinnan vaikuttavuus on seurausta pääasiassa siitä, kuinka hyvin se saadaan osaksi päätöksentekoa ja hallintotapaa ja onnistuminen vaatii ylimmän johdon tuen. Standardin mukaan (2018, 10) ylimmän johdon tulee osoittaa sitoutumista riskienhallintaa kohtaan laatimalla riskienhallinnan politiikan tai toimintasuunnitelman, varmistamalla tarvittavat resurssit sekä nimeämällä riskienhallinnan vastuuhenkilöt jokaiselle organisaatiotasolle. Lisäksi johdon tulee määrittää riskikriteerit, riskinottohalukkuus sekä kehittää ja seurata riskienhallintaa sekä viestiä riskienhallinnan hallinnan arvosta ja hyödyistä asianmukaisesti sekä organisaation sisällä, että sen sidosryhmille (SFS-ISO 31000:2018, 9).

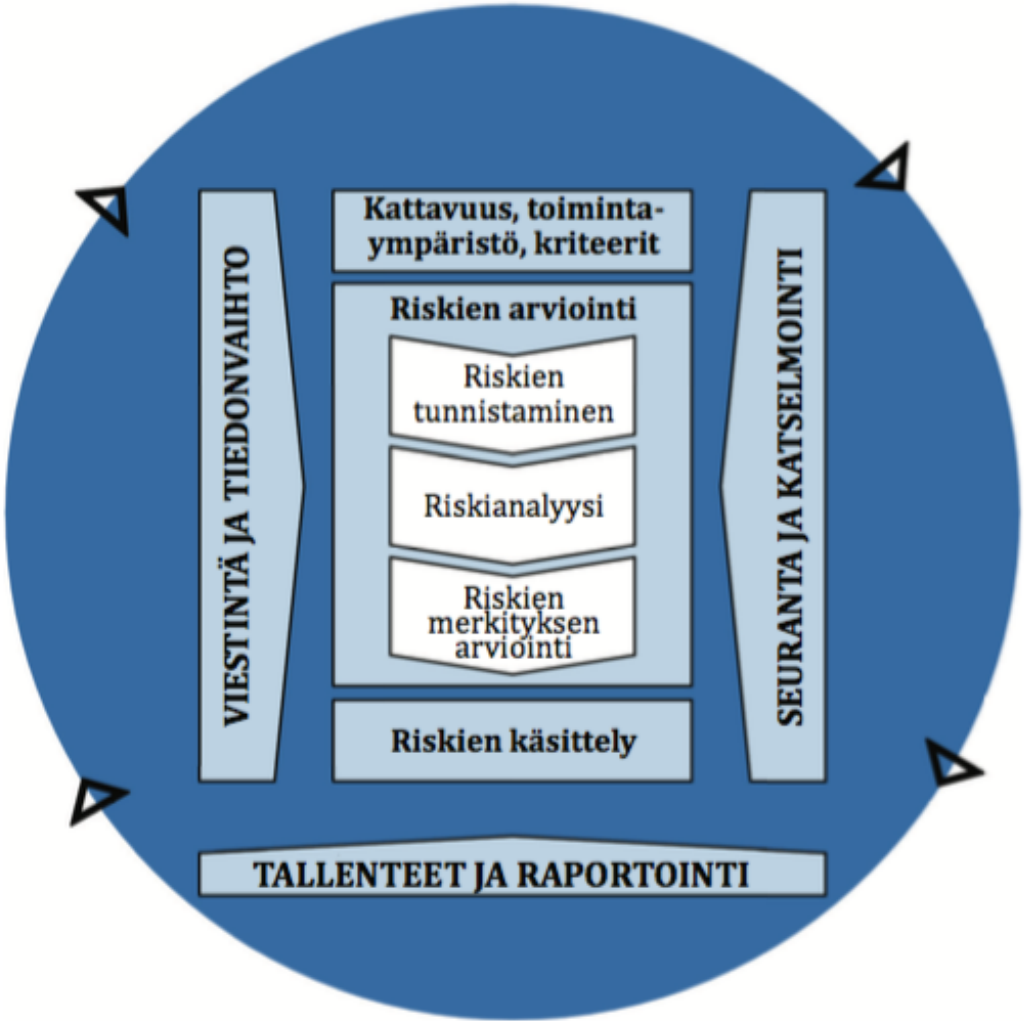
3.4 ISO 31000 mukainen riskienhallinnan prosessi

ISO 31000:2018 standardi sisältää riskienhallinnan periaatteiden ja puitteiden lisäksi myös riskienhallinnan prosessin. ISO 31000:2018 standardin mukainen riskienhallinnan prosessi jäljittelee suurelta osin myös aiemmin mainitun AS/NZS 4360:2004 standardin mukaista riskienhallinnan prosessia. Vaikka ISO 31000:2018

standardin mukainen prosessi on esitetty askelmaisena kuviona, on huomioitava, että prosessissa on kaksi elementtiä, joita pidetään jatkuvina läpi muun prosessin. Nämä ovat viestintä ja tiedonvaihto sekä seuranta ja katselmointi. (Purdy 2010, 883)

Viestinnällä ja tiedonvaihdolla viitataan sekä sisäisten että ulkoisten sidosryhmien antamaan panokseen prosessin hyväksi, jolloin on myös tärkeää ymmärtää sidosryhmien omat tavoitteet. Jatkuvalla seurannalla ja katselmoinnilla pyritään siihen, että voidaan ryhtyä heti toimenpiteisiin, kun uusia riskejä syntyy tai olemassa olevat riskit muuttuvat toimintaympäristön muuttuessa. Seuranta ja katselmointi edellyttävät riskin omistajilta toimintaympäristön jatkuvaa havainnointia, valvontaa, uuden tiedon hankintaa sekä oppimista aiempien kokemusten kautta. (Purdy 2010, 883)

Alla olevassa kuviossa on esitetty ISO 31000:2018 mukainen riskienhallinnan prosessi vaiheineen.



Kuvio 4. Riskienhallinnan prosessi ISO 31000:2018 standardin mukaan (SFS-FI ISO 31000 2018, 14)

ISO standardin mukainen riskienhallinnan prosessi soveltuu sekä strategiselle ja operatiiviselle tasolle mutta myös projekteihin ja ohjelmiin. Lisäksi se voidaan aina räätälöidä sisäiseen tai ulkoiseen toimintaympäristöön sopivaksi. Vaikka prosessi on esitetty peräkkäisenä, mutta se on tarkoitus olla iteratiivinen jatkuva prosessi. (Fox 2018, 6; SFS-FI ISO 31000 2018, 14)

Seuraavaksi on esitetty jokainen ISO 31000:2018 standardin riskienhallintaprosessin vaihe erikseen ja kuhunkin vaiheeseen liittyvät erityispiirteet.

3.4.1 Kattavuus, toimintaympäristö ja kriteerit

Riskienhallinnan kattavuuden, toimintaympäristön sekä riskikriteereiden määrittämisen tarkoituksena on sovittaa riskienhallinnan laajuus organisaatioon sopivaksi sekä ymmärtää organisaation sisäinen ja ulkoinen toimintaympäristö. Riskienhallinnan kattavuus kuvastaa sitä, millä laajuudella ja millä tasoilla riskienhallintaa harjoitetaan. Riskienhallintaa voidaan harjoittaa esimerkiksi strategisella, operatiivisella, projektin tai jonkin tietyn muun toiminnon tasolla. Kattavuutta määritettäessä onkin huomioitava ainakin suoritettavat päätökset ja odotetut tulokset, ajankohta ja paikka, riskienhallinnan työkalut ja tekniikka, tarvittavat resurssit ja vastuut sekä riskienhallinnan suhde muihin toimintoihin ja projekteihin. (SFS-FI ISO 31000 2018, 15).

Yritysten liiketoimintaympäristön vaihtelevuus ja muutosten ennustamattomuus ovat yhä lisääntyvään päin, jolloin myös riskienhallintaa tulee muuttaa (Deloitte 2019, 2). Organisaation ulkoiseen toimintaympäristöön kuuluvat muun muassa kulttuuri, politikka, lainsäädäntö, teknologia, talous, ulkoiset sidosryhmät sekä sopimussuhteet. Sisäiseen toimintaympäristöön kuuluvat muun muassa organisaatiorakenne, hallintotapa, missio, organisaatiokulttuuri, henkilöstön kyvykkyydet ja tietojärjestelmät. Myös riskienhallinnan toimintaympäristö on määritettävä tätä sisäistä ja ulkoista toimintaympäristöä koskevan ymmärryksen avulla. (SFS-FI ISO 31000 2018, 11, 15).

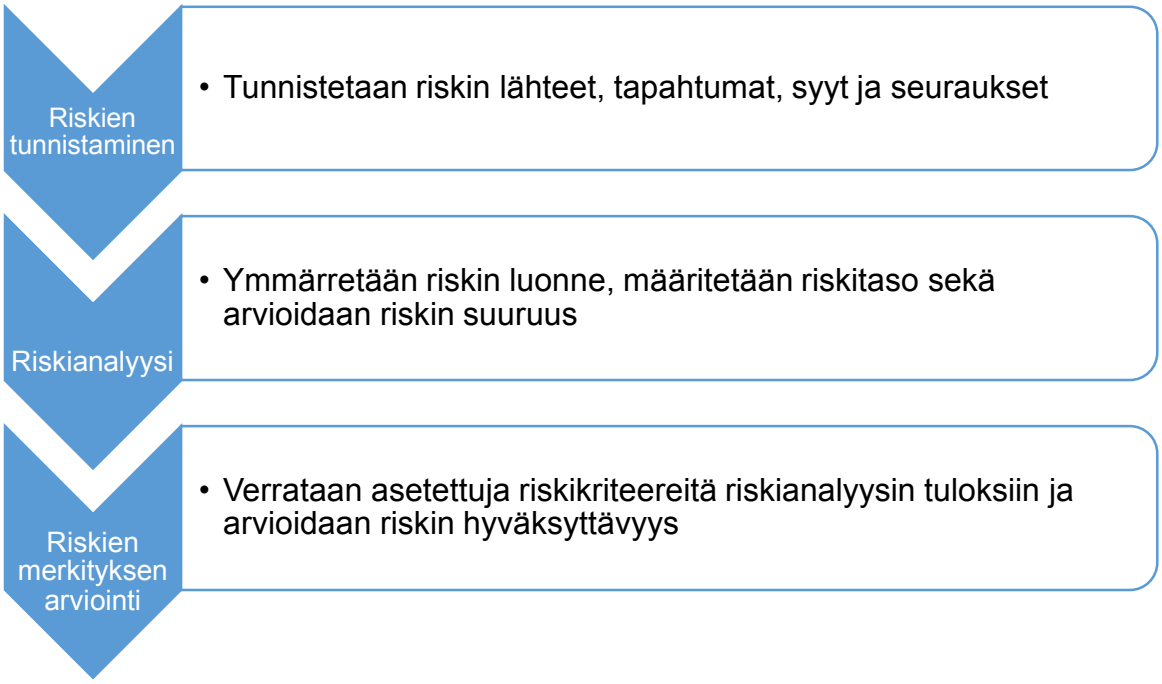
Riskikriteereiden tulisi olla oikeassa suhteessa organisaation tavoitteisiin, ja organisaation tuleekin määrittää minkälaisia riskejä ja kuinka paljon, se pystyy ottamaan. Riskikriteereiden tulisi lisäksi heijastaa organisaation arvoja sekä resursseja ja niitä määritettäessä tulisi huomioida myös sidosryhmien näkemykset sekä organisaatiota kohtaavat velvoitteet. (SFS-FI ISO 31000 2018, 16) Shahn ja Moosemillerin (2012, 369-370) mukaan riskikriteerit voivat vaihdella puhtaasti määrällisten, esimerkiksi onnettomuuksien määrä vuodessa, tai laadullisten kriteerien välillä, tai olla yhdistelmä niitä. He jatkavat (2012, 269-370), että yhdistelmä määrällisiä ja laadullisia kriteereitä voidaan luoda esimerkiksi

riskimatriisin avulla, jossa voidaan arvioida eri todennäköisyys ja vaikutus lukemien perusteella erilaisia riskiskenaarioita ja niiden hyväksyttävyyttä.

Riskikriteerien määrittämisessä haasteina voi olla liian vaativien tai liian löyhien kriteerien asettaminen. Organisaatio saattaa esimerkiksi asettaa riskikriteeriksi ”parhaan käytännön” mukaisen kriteerin, joka kuitenkin osoittautuu organisaatiolle saavuttamattomaksi. Liian löyhillä kriteereillä ei sen sijaan ole riittävää vaikutusta riskin vähentämistoimiin. Asianmukaisesti määritetyt määrälliset riskikriteerit tarjoavat johdolle keinon käsitellä monimutkaisiakin riskejä johdonmukaisesti eri prosesseissa. (Shah & Moosemiller 2012, 370-371) ISO 31000:2018 (2018, 16) standardin mukaan riskikriteerit ovat kuitenkin luonteeltaan dynaamisia, joten niitä on arvioitava jatkuvasti sekä tarpeen mukaan muutettava.

3.4.2 Riskien arviointi

Kuten aiemmin esitetyssä kuviossa 4. on esitetty, standardin mukaan riskien arviointi sisältää riskien tunnistamisen, riskianalyysin sekä riskien merkityksen arvioinnin. Alla olevassa kuviossa 5. on esitetty tarkemmin eri vaiheiden sisältämät toimenpiteet.



Kuvio 5. Riskien arviointiprosessin vaiheet (mukaillen SFS Ohje 73 2011, 21-14)

Riskien arvioimisella tarkoitetaan kokonaisprosessia, johon kuuluu sekä riskien tunnistaminen, riskianalyysi sekä riskin merkityksen arviointi. Ensin tapahtuva riskien tunnistaminen tarkoittaa yksinkertaisesti riskien havaitsemista ja kuvaamista, missä tunnistetaan riskin lähteet, riskitapahtuma sekä mahdolliset syyt ja seuraukset. Riskianalyysilla sen sijaan halutaan selvittää riskin luonne ja asettaa riskitaso. Jotta riskin merkityksen arviointia pystytään suorittamaan, tulee aina ensin suorittaa riskianalyysi, jonka avulla myös arvioidaan riskin suuruusluokka. Kun riskianalyysi on suoritettu, riskin merkityksen arviointi tapahtuu vertaamalla riskianalyysin perusteella saatuja tuloksia ennalta määritettyihin riskikriteereihin. Tämän perusteella arvioidaan, onko riski hyväksyttävä vai ei. (SFS-Opas 71 2011, 11-13)

COSO:n (2004, 3) mukaan riskien arvioinnissa riskit tulisi myös määrittää niiden todennäköisyyden ja vaikutuksen mukaan, jotta voidaan määritellä tavat, miten niitä tulisi käsitellä. Toimenpiteiden kehittämisellä pyritään linjaamaan riski oikeaan suhteeseen yrityksen riskitoleranssin ja riskinottohalun kanssa (COSO 2004, 3). Myös riskien tunnistamistekniikoita on runsaasti erilaisia. IRM:n (2002, 12) mukaan keinoina voidaan käyttää muun muassa kyselylomakkeita, eri skenaarioiden

analysointia, riskien arviointityöpajoja, tilintarkastusta, jo toteutuneiden vahinkojen tutkimista, yritystutkimuksia sekä toimialakohtaista benchmarkingia.

Riskien tunnistaminen tulisi toteuttaa suunnitelmallisesti, jotta saadaan varmuus siitä, että kaikki organisaation keskeiset toiminnot ovat tunnistettu ja näistä toiminnoista aiheutuvat riskit tunnistettu. Näihin toimintoihin liittyvät epävarmuudet on myös tunnistettava ja luokiteltava. Liiketoiminta voidaan jakaa usealla eri tavalla riskien tunnistamiseksi. Yksi IRM:n mukainen luokittelu on jakaa liiketoiminta strategisiin, operatiivisiin, taloudellisiin, tiedollisiin sekä määräyksenmukaisiin toimintoihin, joista riskejä tunnistetaan. (IRM 2002, 5)

Riskien tunnistamisvaihe on riskien havaitsemis- ja kuvaamisprosessi, jossa tunnistetaan riskin lähteet, tapahtuma, syyt ja seuraukset. Tähän tunnistamisprosessiin voi liittyä muun muassa tietoa ja mielipiteitä, asiantuntemusta, historiatietoa, teoreettista analyysiä sekä sidosryhmiltä lähtöisin olevia tarpeita (SFS Opas 73 2011, 11). Riskien tunnistamista voidaan tehdä sekä organisaatiossa sisäisesti, että ulkoisen konsultin avulla (IRM 2002, 5).

Organisaatio voi hyödyntää monenlaisia keinoja epävarmuuksien tunnistamiseen ja tärkeintä on, että organisaatiolla on käytössään ajantasaista, asianmukaista ja olennaista tietoa. Riskien arvioinnin ensimmäisen vaiheen eli riskien tunnistamisen tarkoituksena on riskien havaitseminen ja kuvaaminen. Tämän vaiheen avulla organisaatio voi tunnistaa ne tekijät, joiden avulla se joko voi päästä tavoitteisiinsa tai jotka toisaalta estävät tavoitteiden saavuttamisen. (SFS-FI ISO 31000 2018, 16)

Kun organisaatio tunnistaa riskejä, sen olisi ISO 31000:2018 standardin (SFS-FI ISO 31000 2018, 16-17) mukaan otettava huomioon seuraavat tekijät sekä niiden keskinäiset suhteet:

- *”aineettomat ja aineelliset riskin lähteet*
- *syyt ja tapahtumat*
- *uhkat ja mahdollisuudet*
- *haavoittuvuudet ja voimavarat*

- *muutokset ulkoisessa ja sisäisessä toimintaympäristössä*
- *uusien riskien indikaattorit*
- *omaisuuden ja resurssien ominaisuudet ja arvo*
- *seuraukset ja niiden vaikutus tavoitteisiin*
- *tietämyksen määrän ja tiedon luotettavuuden rajoitukset*
- *aikaan liittyvät tekijät*
- *riskien tunnistamiseen osallistuvien tahojen ennakkoluulot, oletukset ja uskomukset"*

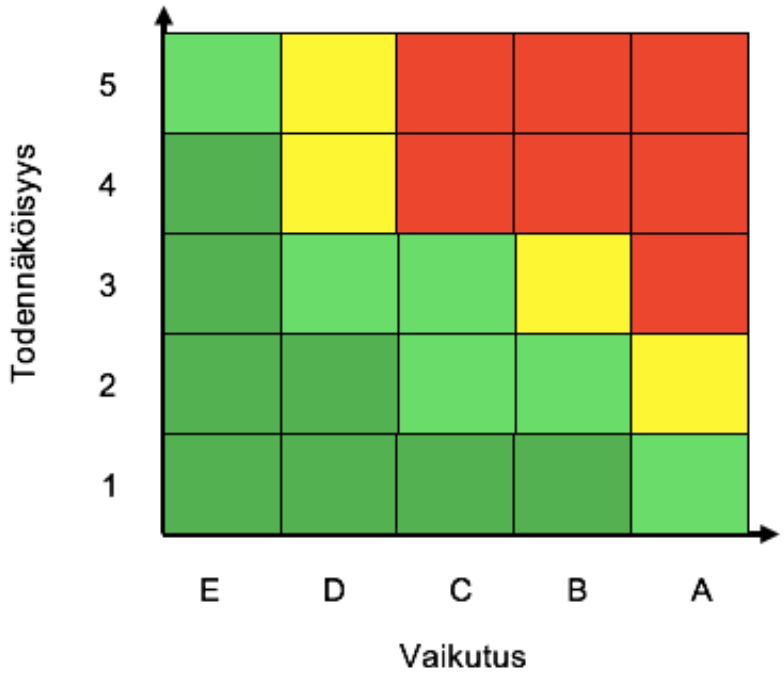
Osbichin (2018) mukaan merkittävä ero standardin aiemman version sekä uudistetun vuoden 2018 välillä on nimenomaan riskien tunnistamisessa, sillä uudessa versiossa on lueteltu runsaasti tekijöitä, joita tulisi ottaa huomioon organisaation tunnistaessa riskejä.

Seuraava riskien arvioinnin vaihe on ISO 31000:2018 (2018, 17) standardin mukaan riskianalyysi, joka on riskin luonteen sekä ominaisuuksien analyysiä, jossa määritetään myös mahdollinen riskitaso. Riskianalyysissa tavoitteena on tarkastella riskin lähteitä, todennäköisyyttä, eri skenaarioita, mahdollisia seurauksia, tapahtumia ja yleisesti epävarmuuksia. Lisäksi siinä analysoidaan riskienhallintakeinoja sekä niiden vaikuttavuutta. (SFS-FI ISO 31000 2018, 17)

Riskianalyysin tarkkuus ja monimutkaisuus riippuvat siitä, mihin tarkoitukseen analyysiä tehdään ja millaiset tietovarannot ja resurssit ovat saatavilla. Analyysi menetelmiä on sekä laadullisia että määrällisiä, joita voidaan yhdistellä tarpeen mukaisesti ja lisäksi analyysin tulos voidaan ilmaista kuvailevana tai numeerisena. (Malmén & Wessberg 2005b; SFS-FI ISO 31000 2018, 17) Malménin & Wessbergin (2005b) mukaan tunnistetut epävarmuudet voidaan määrittää riskilukuna, jonka ensisijaisena tarkoituksena on kertoa riskin suuruudesta sekä siedettävyydestä. He jatkavat (2005b), että riskiluku muodostuu riskin esiintymistaajuudesta sekä aiheutuvasta vahingosta, ja näiden kahden tekijän avulla voidaan arvioida riskin suuruus käyttämällä erilaisia luokituksia.

Malmén & Wessberg (2005b) kuitenkin kritisoivat yleistä tapaa siitä, että riskiluku muodostetaan kertomalla numeerisesti riskin todennäköisyys sen vaikutuksella. Heidän mukaansa syy tähän on se, että täysin sama riskiluku voi muodostua kahden eri todennäköisyyden ja vaikutuksen yhdistelmästä, vaikka riskin siedettävyys on kummassakin tapauksessa täysin erilainen.

Yksi tunnetuimmista sekä yleisimmin käytetty riskienhallinnan työkalu on riskimatriisi (Shah & Moosemiller 2012, 370) Myös Malmén & Wessberg (2005b) käyttävät apunaan riskimatriisia, jonka avulla riskit voidaan jakaa luokkiin riskin todennäköisyyden ja vaikutuksen yhteisvaikutuksen mukaan. Esimerkki riskimatriisisista on havainnollistettu alla olevassa kuviossa:



Kuvio 6. Riskimatriisi (mukaillen Malmén & Wessberg 2005b)

Ennen riskimatriisin muodostamista, on ensin määritettävä arvot todennäköisyyksille ja vaikutuksille siten, että analyysin tarkoitus tulee mahdollisimman hyvin katetuksi. Vaikutusta voidaan arvioida esimerkiksi termein ”pysyvä haitta”, ”kohtalainen haitta” tai ”vähäinen haitta”. Esimerkkejä todennäköisyysarvoista ovat esimerkiksi ”useammin kuin kerran vuodessa” tai ”kerran 10.vuodessa”. (Malmén & Wessberg 2005b)

ISO 31000:2018 standardin mukaan riskianalyysissa on huomioitava todennäköisyyden ja suuruuden lisäksi myös aikaan liittyvät tekijät sekä nykyisten riskienhallintakeinojen vaikuttavuus. Lisäksi analyysin suorittavien henkilöiden omat mielipiteet, ennakkoluulot, oletukset ja havainnot on otettava huomioon sekä käytetyn tiedon laatu. Kaikki nämä on huomioitava, dokumentoitava ja annettava tiedoksi päätöksentekijöille. (SFS-FI ISO 31000 2018, 17)

Riskianalyysi on perusta riskin merkityksen arvioinnille sekä sille, miten riskejä tulisi käsitellä. Riskin merkityksen arviointi on prosessi, jossa riskin hyväksyttävyys arvioidaan ja minkä on tarkoitus toimia päätöksenteon tukena. (SFS-FI ISO 31000 2018, 17-18; Malmén & Wessberg 2004)

Riskien merkityksen arvioinnin perusteella voidaan SFS-FI ISO 31000:n (2018, 18) mukaan päättää seuraavista askeleista:

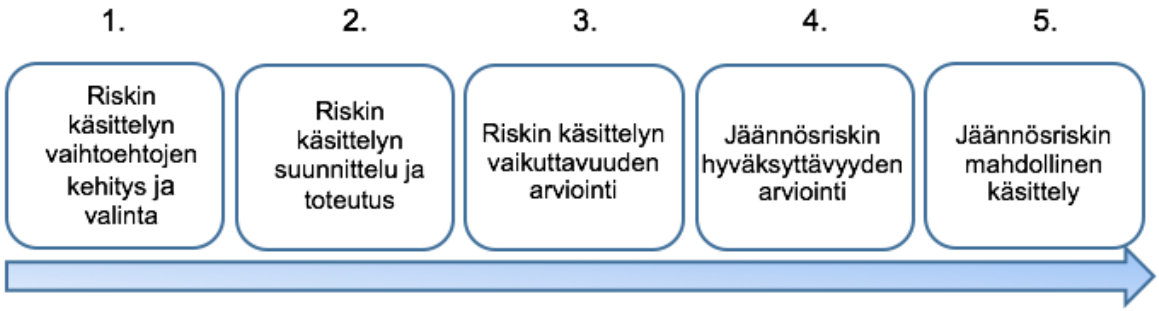
1) Tehdäänkö riskille muita toimenpiteitä?
2) Mitkä ovat vaihtoehdot riskin käsittelylle?
3) Tarvitaanko riskistä parempaa ymmärrystä tekemällä lisäanalyysejä?
4) Jatketaanko nykyisten riskienhallintakeinojen ylläpitämistä?
5) Tulisiko tavoitteita harkita uudelleen?

3.4.3 Riskien käsittely

Kun riskin suuruus on selvillä, tulee tehdä päätökset jatkotoimenpiteistä. Riskinkäsittelytapoina voivat olla pääasiassa riskin poistaminen, pienentäminen tai siirtäminen. Joskus kuitenkaan mikään näistä vaihtoehtoista ei sovellu, jolloin harkittavaksi voi tulla tilanne, jossa riski tulee vain hyväksyä. (Malmén & Wessberg 2004)

ISO 31000:2018 standardin mukaan riskin käsittelyyn kuuluu sekä riskinkäsittelytavan valinta, että riskienkäsittelysuunnitelmien laadinta ja toteutus.

Riskin käsittely on prosessi, joka standardin mukaan tulisi edetä alla olevassa kuviossa esitettyjen askeleiden mukaan (SFS-FI ISO 31000 2018, 18-19):



Kuvio 7. Riskin käsittelyn vaiheet (mukaillen SFS-FI ISO 31000 2018, 18)

Riskinkäsittelytapoja on useita erilaisia, eivätkä ne ole toisiaan poissulkevia. ISO 31000:2018 standardi (SFS-FI ISO 31000 2018, 18) esittää vaihtoehtoisia riskinkäsittelytapoja, joita ovat esimerkiksi, riskin lähteiden poistaminen, riskin todennäköisyyden tai seurausten muuttaminen, riskin jakaminen vakuutuksin tai sopimuksin, riskin aiheuttaman toiminnan lopettaminen tai riskin hyväksyminen tietoisella päätöksellä.

Standardissa myös todetaan, että kun riskinkäsittelytapaa valitaan, on huomioita myös muut kuin puhtaasti taloudelliset seikat, kuten esimerkiksi sidosryhmien näkemykset ja arvot, muut velvoitteet sekä sitoumukset. (SFS-FI ISO 31000 2018, 18-19)

3.4.4 Viestintä, tiedonvaihto ja seuranta

ISO 31000:2018 standardin mukaan organisaatioon olisi luotava viestinnän ja tiedonvaihdon toimintamalli, joka sisältää tiedonjaon sidosryhmien kanssa sekä palautteen vastaanottamisen. Viestinnän ja tiedonvaihdon tulisi olla oikea-aikaista, jolloin voidaan varmistaa se, että olennaista tietoa saadaan kerättyä ja yhdistettyä se kokonaisuudeksi. Tiedon jakamisessa on tärkeää ottaa huomioon tiedon arkaluontoisuus, luottamuksellisuus sekä yksityisyydensuoja. (SFS-FI ISO 31000 2018, 13-14) Deloitten (2019, 51) mukaan oikeanlainen tiedonjako mahdollistaa

paremman päätöksenteon, mutta lisäksi tuo lisäarvoa johtajille siitä, mitä heidän kannattaisi seuraavaksi tehdä sen sijaan, että todetaan mitä on jo tapahtunut.

Viestinnän ja tiedonvaihdon tarkoitus riskienhallinnan prosessissa on auttaa sidosryhmiä ymmärtämään riskejä sekä perusteita päätöksenteolle ja tarvittaville toimenpiteille. Viestinnän rooli on enemmänkin lisätä tietoa ja ymmärrystä riskeistä, kun taas tiedonvaihdolla pyritään hankkimaan tarvittavaa tietoa ja palautetta päätöksenteon tueksi. (SFS-FI ISO 31000 2018, 14) Kuten ISO 31000:2018 standardin (2018, 15) riskienhallinnan prosessin kuviossa 4. on esitetty, viestinnän ja tiedonvaihdon tulisi sisältyä kaikkiin riskienhallinnan prosessin vaiheisiin, ja tietoa tulisi vaihtaa kaikkien asianmukaisten sekä sisäisten että ulkoisten sidosryhmien kanssa.

Läpi riskienhallinnan prosessin tapahtuvalla viestinnällä ja tiedonvaihdolla tavoitellaan ISO 31000:2018 standardin (2018, 15) mukaan myös sitä, että sen avulla voidaan yhdistää eri alueiden asiantuntemusta riskienhallinnan prosessin eri vaiheissa. Lisäksi tavoitteena on varmistaa eri näkökulmien kantojen huomioonotto, tuottaa tarpeeksi tietoa riskien valvontaan sekä luoda omistajuuden tunnetta niille tahoille, joihin riskit vaikuttavat (SFS-FI ISO 31000 2018, 15).

ISO 31000:2018 standardin mukaan seurantaa ja katselmointia tulisi toteuttaa läpi riskienhallintaprosessin. Siihen sisältyy suunnittelun lisäksi tiedon keruu ja analysointi sekä tulosten dokumentointi ja palaute. Seurannan ja katselmoinnin tarkoituksena on sekä varmistaa että parantaa prosessin toteutusta sekä tulosten laatua ja vaikuttavuutta. (SFS-FI ISO 31000 2018, 19)

3.4.5 Tallenteet ja raportointi

Sekä riskienhallintaprosessi kokonaisuudessaan, että sen tulokset tulisi dokumentoida asianmukaisella tavalla. Dokumentaation ja raportoinnin tavoitteina on auttaa riskienhallinnan tulosten sekä toimintojen viestimisestä läpi organisaation, tuottaa tietoa päätöksentekoa varten, edistää sidosryhmävuorovaikutusta sekä yleisesti kehittää riskienhallinnan toimia. (SFS-FI ISO 31000 2018, 20) Deloitten

(2019, 6) mukaan riskienhallinnan tuottaman tiedon sekä sitä tukevien järjestelmien olemassaolo tulisi olla yritysten tärkeä tavoite ja yritysten tulisi pyrkiä tehostamaan tiedon laatua, oikea-aikaisuutta ja saatavuutta.

Kun riskienhallinnan tuottamaa tietoa dokumentoidaan, säilytetään sekä käsitellään, on kuitenkin huomioitava tiedon arkaluonteisuus. Lisäksi raportoinnissa tulisi huomioida sidosryhmien vaatimukset ja tarpeet, raportointimenetelmä sekä raportoinnin oikea-aikaisuus ja sen kustannukset, sekä lisäksi millainen merkitys raportoitavalla tiedolla on organisaation päätöksenteon sekä tavoitteiden näkökannalta. (SFS-FI ISO 31000 2018, 20)

3.4.6 Haasteet standardin sovellettavuudessa

IRM:n (2018a, 7) mukaan eräs vaara ISO 31000:2018 standardin käyttöönotossa on se, että sen tuottama informaatio on irrallista verrattuna yrityksen muuhun informaatiovirtaan eikä se siten tue yrityksen onnistunutta johtamista. IRM:n (2018a, 7) mukaan siksi onkin tärkeää, että riskimanagerit toteuttavat toimintaa siten, että se on linjassa yrityksen liiketoimintamallin ja strategian kanssa.

IRM:n (2018a, 7) mukaan tähän haasteeseen voidaan vastata siten, että riskien huomioonotto tulisi sisällyttää osaksi johtamisjärjestelmää ja päivittäistä toimintaa, millä varmistetaan nimenomaisesti se, että riski-informaatio on osa myös muuta yrityksen hyödyntämää informaatiota, eikä riskienhallinta jää vain riskilistan kokoamiseksi ja sen irralliseksi hallinnoimiseksi.

4 RISKIENHALLINNAN PROSESSIN JÄRJESTÄMINEN YRITYKSISSÄ

Tässä luvussa kuvaillaan ensin työssä käytettyä tutkimusmenetelmää, tutkimusaineistoa sekä aineistonkeruutapaa, jonka jälkeen jälkeen analysoidaan kerättyä tutkimusaineistoa.

4.1 Tutkimusmetodologia

Tutkimus on tehty käyttäen laadullista tutkimusmenetelmää ja laadulliselle tutkimukselle on Vilkkaan (2015) mukaan ominaista se, että tarkoituksena ei ole löytää juuri oikeaa totuutta, vaan näyttää esimerkkejä ihmisten toiminnasta. Anttilan (2014) mukaan laadullisen tutkimuksen avulla pyritään luomaan selitysmallia tietylle ilmiölle, ja tätä varten tulee olla käsitteellinen kehikko, jonka avulla ilmiötä tutkitaan. Laadullinen tutkimusmenetelmä sopii tämän tutkielman tutkimusmetodologiaksi siitä syystä, että tutkimuksen kohteena oleva SFS ISO 31000:2018 riskienhallinnan standardi on suosituksen omainen ohje, jota yritykset voivat halutessaan noudattaa, eikä niinkään kuvaa objektiivista totuutta.

Teemahaastattelussa teemojen käsittelyjärjestyksellä ei ole olennaista merkitystä ja tavoitteena on, että haastateltava henkilö antaa valituista teemoista oman näkemyksensä hänen kannaltaan luontevassa esitysjärjestyksessä (Vilkka 2015). Teemahaastattelun hyödyntäminen tukee hyvin tutkimuksen aihetta, jossa pyritään saamaan mahdollisimman kattava käsitys yrityksen riskienhallinnan prosessin järjestämisestä, johon ei kuitenkaan ole vain yhtä ja oikeaa tapaa.

Vilkkaan (2015) mukaan laadulliselle aineistolle on tärkeämpää sen sisällöllinen laajuus kuin aineiston määrä kappaleina. Tällä perusteella tutkimukseen on valittu kolme haastateltavaa henkilöä, keitä on pyritty haastattelemaan aiheen sisällöstä mahdollisimman kattavasti ja syvällisesti. Vilkka (2015) myös jatkaa, että haastateltavat henkilöt tulisi valita sen perusteella, mikä on heidän asiantuntemuksensa tai kokemuksensa aihetta kohtaan. Tähän tutkimukseen on

valittu henkilöt sen perusteella, että he työskentelevät joko pääsääntöisesti riskienhallinnan tehtävissä tai ovat vastuussa riskienhallinnan järjestämisestä muun toimenkuvansa ohessa. Haastateltavat henkilöt ovat esitetty seuraavan kappaleen taulukossa 3.

4.2 Tutkimusaineiston keruu ja kuvaaminen

Tutkimusaineisto kerättiin haastattelumenetelmällä, jossa kolmen eri yrityksen toimihenkilöä haastateltiin riskienhallintaan liittyvistä teemoista. Kaikille haastateltaville oli yhteistä se, että kukin toimii pääasiallisesti riskienhallinnan tehtävissä tai työtehtäviin sisältyi yrityksen riskienhallinnasta vastaaminen muiden tehtävien ohessa. Alun perin neljään potentiaaliseen haastateltavaan otettiin yhteyttä sähköpostitse, joista kolmen kanssa saatiin järjestettyä haastatteluaika joulukuun 2018 ja tammikuun 2019 väliselle ajalle. Perusteina tutkimuksen kohteeksi valittaviin yrityksiin olivat se, että ne olisivat eri kokoluokasta ja eri toimialoilta, vaikka tutkimuksen tavoite ei ollut verrata toimialoja. Yrityksen riskienhallinta voi kuitenkin poiketa riippuen yrityksen koosta ja saatavilla olevista resursseista.

Haastattelumenetelmänä käytettiin teemahaastattelua, jossa kysymysrunko muodostui laajemmista teemoista, ja haastattelun edetessä esitettiin tarkennettavia kysymyksiä sen mukaan, kuinka tarkasti kukin haastateltava vastasi kysymykseen. Jokaiselle haastateltavalle lähetettiin haastattelurunko noin viikkoa aikaisemmin etukäteen tutustuttavaksi, jotta haastattelun ajankäyttö olisi tehokasta ja siitä saataisiin mahdollisimman suuri hyöty. Jokaisen haastateltavan kanssa myös sovittiin kirjallisesti, että haastattelumateriaalia tullaan käyttämään anonyymisti ja ainoastaan tätä pro gradua varten.

Kullekin haastattelulle oli varattu aikaa noin tunnin verran ja kaikki haastattelut suoritettiin luottamuksellisesti kahden kesken haastattelijan sekä haastateltavan välillä. Kaksi haastatteluista suoritettiin kasvotusten ja yksi Webex onlinepuhelun välityksellä. Kaikki haastattelut nauhoitettiin sekä litteroitiin jälkikäteen aineiston käsittelyn helpottamiseksi. Vilkkaan (2015) mukaan litteroinnilla tarkoitetaan

haastattelun muuttamista kirjalliseen muotoon ja sen tarkkuus riippuu siitä, mitä tutkimuksella tavoitellaan. Koska tässä tutkimuksessa on tarkoitus keskittyä asiasisältöön eikä sen vuoksi ole tarvetta antaa painoarvoa kielelliselle rakenteelle, ei litteroinnissa ole huomioitu jokaista äännähdystä taikka mietintätaukoa.

Tutkimuksen aiheen luottamuksellisuuden ja arkaluontoisuuden vuoksi kaikkea haastattelumateriaalia käsitellään tutkimuksessa anonyymisti, jotta yrityksen olemassa olevia riskienhallinnan prosesseja ei voida yhdistää haastateltuun yritykseen. Riskienhallinta on yrityksen osa-alue, joka sisältää yrityksen kilpailuetuun ja strategiaan liittyvää kriittistä tietoa, joten myös tutkimuksen luotettavuuden kannalta tutkimusaineiston käsittely anonyymisti on perusteltua.

Haastattelu suoritettiin teemahaastatteluna ja alla olevassa taulukossa on esitetty haastattelun teemat, jotka mukailevat SFS ISO 31000:2018 standardin riskienhallinnan prosessin eri vaiheita. Tarkempi haastattelurunko on nähtävillä liitteessä 1.

Taulukko 3. Haastattelun teemat

Nro.	Teema
1	Riskienhallinnan toimintasuunnitelma/politiikka
2	Riskienhallinnan roolit, vastuut ja valtuudet
3	Riskienhallinnan resurssit
4	Riskien tunnistaminen
5	Riskien analysoiminen
6	Riskien merkityksen arviointi
7	Riskien käsittely
8	Riskienhallinnan seuranta ja arviointi
9	Riskienhallinnan raportointi
10	Riskienhallinnan viestintä

Haastateltavat henkilöt toimivat kaikki eri yrityksissä ja yritykset eri toimialoilla. Yritysten kokoluokat myös vaihtelevat, mutta tutkimuksen kannalta ja yritysten anonymiteetin säilyttämiseksi kokoluokkia ei ole tarpeen esittää. Alla olevassa taulukossa on esitetty haastateltavien henkilöiden ja yritysten tunnistetiedot, joita tässä tutkielmassa käytetään.

Taulukko 4. Haastateltavat henkilöt, tittelit ja toimialat

Yritys	Henkilö	Titteli	Toimiala
Yritys 1	Haastateltava 1	Head of Risk Management and Insurance	Pakkausteollisuus
Yritys 2	Haastateltava 2	Riskienhallintajohtaja	Metalliteollisuus
Yritys 3	Haastateltava 3	Talousjohtaja	Elintarviketeollisuus

Tutkielmassa käytetään teemahaastatteluin kerätyn aineiston lisäksi myös sekundääriaineistoa, joita ovat kohdeyritysten viralliset julkisesti saatavilla olevat julkaisut, joista riskienhallintaa koskevaa tietoa on saatavilla. Tätä aineistoa on tarkoitus käyttää täydentämään haastatteluista saatavaa materiaalia ja koska yritysten kokoluokat vaihtelevat melko runsaasti, ovat saatavilla olevat julkaisut myös erilaisia. Anonymiteetin säilyttämiseksi näitä julkaisuja tullaan käsittelemään yllä olevan mukaisesti. Esimerkiksi vuosikertomukseen voidaan viitata mainitsemalla ”*yrityksen 1 vuosikertomus”*. Täydentävänä aineistona käytetään yrityksen 1 osalta vuoden 2019 ”Selvitys hallinto- ja ohjausjärjestelmästä” julkaisua, yrityksen 2 osalta vuoden 2017 taloudellista katsausta sekä yrityksen 3 osalta ”Corporate Social Responsibility Report” julkaisua. Kyseisiin yritysten virallisiin julkaisuihin tutustutaan haastattelumateriaalin käsittelyn jälkeen ja niistä on pyritty löytämään sellaista lisäarvoa tuottavaa tietoa, jota haastateltava ei mahdollisesti itse tuonut haastattelun aikana esille.

4.3 Tutkimustulokset

Tutkimusaineistoa käsitellään ja tutkimustuloksia analysoidaan teemoittain ja teemat ovat SFS ISO 31000:2018 standardin riskienhallinnan prosessin sekä sen mukaan luodun haastattelurungon mukaiset. Koska teemat eivät kuitenkaan ole toisistaan irrallisia, niitä tullaan käsittelemään myös limittäin.

4.3.1 Riskienhallinnan toimintasuunnitelma/politiikka

Haastateltava 1 kertoo, että heillä on olemassa riskienhallinnan politiikka, johon liittyy myös tarkempia ohjeistuksia. Yrityksen 1 julkaisema dokumentti ”Selvitys hallinto- ja ohjausjärjestelmästä” (2019, 14) kertoo, että riskienhallinta on tiivis osa organisaation johtamis- ja valvontajärjestelmää ja yrityksen riskienhallintaprosessi perustuu jo aiemmin mainittuun COSO-ERM viitekehykseen. Dokumentissa (2019, 14) myös tarkennetaan, että yrityksen riskienhallintapolitiikka sisältää sekä riskienhallinnan tavoitteet, laajuuden ja vastuut sekä politiikalla varmistetaan, että riskit tunnistetaan ajoissa ja niitä hallitaan tarvittavin toimenpitein. Lisäksi dokumentissa mainitaan (2019, 14), että yrityksellä on erillinen ERM prosessiohjeistus, johon riskienhallinnan prosessi menettelytapoineen on dokumentoitu.

Haastateltava 2 kuvailee heidän riskienhallinnan politiikan olevan *”inspired by ISO 31000”,* eli riskienhallinnan prosessit eivät heillä suoraan ole standardin mukaisia, mutta sisältää elementtejä siitä. Hän jatkaa, että yritys otti ISO standardin mukaan riskienhallinnan politiikkaan siis lähinnä inspiroimaan työtä. Politiikan luomisesta ja hyväksyttävyydestä haastateltava 2 mainitsee, että:

”Kaiken takana on politiikka, eli meillä riskienhallintapolitiikka on hyväksytty ihan tuolla hallituksen tasolla. Käytännössä koko hallitus on sen hyväksynyt mutta nyt meidän tarkastusvaliokunta voi sitten siihen hyväksyä muutoksia tänä vuonna”
(Haastateltava 2)

Yrityksen 2 vuoden 2017 taloudellisessa katsauksessa yritys kertoo noudattavansa hallituksen hyväksymää riskienhallintapolitiikkaa, jossa riskienhallinnan tavoitteet, vastuut sekä lähestymistapa on määritetty. Lisäksi dokumentissa kerrotaan riskienhallintaprosessin olevan osa johtamisjärjestelmää, joka sisältää neljä vaihetta: riskien tunnistaminen, arviointi ja priorisointi, pienentäminen ja raportointi. (Yritys 2, 2017, 9) Nämä vaiheet mukailevat myös ISO 31000 standardin sisältämiä vaiheita, jotka ovat kuten kuviossa 4. on esitetty, riskien tunnistaminen, riskianalyysi, riskien käsittely ja raportointi (SFS-FI ISO 31000 2018, 14).

Vaikka yrityksessä 3 haastateltavan 3 mukaan riskienhallinnan toimintaperiaatteet tulevat hallitukselta ja hallituksessa käsitellään riskienhallinnan politiikkaa, ei yhtenäistä riskienhallinnan politiikkaa taikka toimintasuunnitelmaa ole. Haastateltavan 3 mukaan:

”*No varsinaisesti ei oo niinku erotettu riskienhallinnan politiikkaa, meillä on riskienhallinnan politiikka kyllä joka käy hallituksessa, mutta tämmöiset yleiset toimintaperiaatteet on osa tota meijän strategiaa ja strategista suunnittelua”*
(Haastateltava 3)

Haastateltava 3 kuvailee, että heillä voisi sanoa olevan osittainen riskienhallintapolitiikka, jossa hallitus tarkastelee asioita konsernitasolla, mutta virallisen riskienhallintapolitiikan sijasta kyseessä on enemmänkin operatiivinen ohjeisto, jossa käsitellään raaka-aineriskiä sekä taloudellisia riskejä.

4.3.2 Riskienhallinnan roolit, vastuut ja valtuudet

Jokaisessa yrityksessä riskienhallinnan vastuut on jaettu kahdelle eri henkilölle. Haastateltava 1 kertoi vastuiden jakamisesta seuraavaa:

”*...tietenkin tässä prosessissa on tietyt vastuuhenkilöt, jotka hoitaa sen informaation keräämisen, prosessoinnin ja konsolidoinnin, eli tällaiset tehtävät…riskienhallintahan on joka tapauksessa osa meidän jatkuvaa liiketoiminnan johtamista et tietysti niinkun liiketoimintayksikkötasolla päävastuu on*

aina sen yksikön toimitusjohtajalla…ja toki niinkun konsernitasolla johtoryhmä vastaa." (Haastateltava 1)

Yrityksessä 1 on siten määritetty erikseen riskienhallinnan prosessista vastaavat tahot sen lisäksi, että yksikkötasolla vastuut on jaettu vielä erikseen. Haastateltava 1 jatkaa, että:

"Ja kyl se niinkun on selkeetä ja aina aihepiiristä riippuen on tietty vastuuhenkilö ja niinkun hänen omalla vastuualueellaan ja osaamisalueellaan…sanotaanko vaikka että tunnistetaan joku riski, niin kyllähän se sit riskienhallintaan sitten osotetaan tietysti jos se on joku vähän spesifimpi asia niinkun vaikka valuuttariski, jollon on tietyt vastuuhenkilöt" (Haastateltava 1)

Kuten SFS-ISO 31000 (2018, 10) standardi suosittelee, riskejä tulisi hallita jokaisessa organisaation osassa. Tällä tavoin riskienhallintaa yrityksessä 1 myös järjestetään, sillä haastateltava 1 jatkaa, että *"…vastuu alkaa aina sieltä niinkun matalimmalta organisaatiotasolta, joka nyt jollain tapaa kykenee hallitsemaan sitä riskiä ja sit se siirtyy tietysti aina siitä eteenpäin…niinkun alemman organisaatiotason riskienhallintatoimenpiteet pitää niinkun aina olla sen ylemmän tason hyväksymiä ja valvomia"*

Yrityksen 2 haastateltava 2 kertoo heillä olevan jokaiselle riskille kaksi vastuuhenkilöä: *"meidän konsernin avainriskeille tuli niinkun johtoryhmätasolta riskin omistava johtoryhmän edustaja eli jokaisella riskillä on sen lisäks sit vielä tavallaan riskin vastuullinen".* Lisäksi haastateltava 2 kertoo, että konsernin jokainen tytäryhtiö on vastuussa sekä siitä, että he pystyvät tuottamaan riittävää riskitietoa pääjohtajalle ja johtoryhmälle mutta myös siitä, että he pystyvät itse rakentamaan sellaisen riskienhallintajärjestelmän, jolla he pystyvät tuottamaan kyseistä riskitietoa.

Yrityksessä 3 kerrotaan riskienhallinnan roolien ja vastuiden olevan kirjattu erilliselle dokumentille ja vastuuhenkilöitä on määritetty useammalla eri organisaatiotasolla

lähtien toimitusjohtajasta, johtoryhmästä ja alenevan yhtiökohtaisiin johtoryhmiin ja yksikkötasolle.

4.3.3 Riskienhallinnan resurssit

Haastattelun kolmannessa teemassa keskityttiin riskienhallinnan resursseihin, joiden haastattelussa tarkennettiin käsittävän ihmisten osaamisen, kouluttamisen, tarvittavat työkalut sekä ajan.

Haastateltava 1 kuvaili heidän riskienhallintaorganisaation olevan hyvin ”Lean” ja perusteli sen siten, että riskienhallinnan ei tulisikaan olla erillinen yksikkö vaan sisällä organisaation toiminnassa. Henkilöresursseista Haastateltava 1 jatkaa, että: *”henkilöstön puolesta ja kyllä tietenkin täytyy huolehtia, että vastuuhenkilöillä on riittävä ymmärrys ja saavat tarvittaessa koulutusta sitten niistä asioista mitä heidän vastuualueisiin kuuluu mukaan lukien riskienhallinta”.* Työkaluresurssien osalta haastateltava 1 toteaa, että vaikka heidän käytössään olevat työkalut eivät ole markkinoiden parhaimpia, niin ne täyttävät tehtävänsä erittäin kustannustehokkaasti.

Haastateltava 1 mainitsi hänen riskienhallintafunktionsa sisältävän riskienhallinnan kokonaisuuden hahmottamista, monitorointia, kommunikointia ja riskitiedon keräämistä, jotta voidaan havaita myös mahdolliset puutteet resursseissa. Lisäksi hän tarkentaa, että hänen tehtävänään riskienhallintajohtajana on nostaa esiin havaitut resurssipuutteet, oli ne sitten henkilöresursseja tai työkaluja, jonka jälkeen vastuu resurssien järjestämisestä siirtyy kyseisen vastuuorganisaation vastuulle. Lisäksi Haastateltava 1 nosti resursoinnissa ERM:in roolin esille, sillä hänen näkökulmastaan ERM:in tehtävänä on nimenomaisesti tuoda esille riskienhallinnan resurssien puutteisiin liittyviä tekijöitä. Haastateltavan 1 mukaan:

”…jos alkaa näyttää siltä, että hei meillä on täällä tällainen riski ja meillä ei itseasiassa ole siihen tarpeeksi resursseja et sitten tietenkin pitää tehdä päätöksiä ja valintoja, että siihen niinkun kohdennetaan riittävästi resursseja et se on

tietenkin yks aika tärkee tän ERM funktion tehtävä tuoda esille tällasii asioita jos siltä näyttää” (Haastateltava 1)

Haastateltava 3 koki, ettei resurssien kohdentamisessa ole heidän kohdallaan ongelmaa. Henkilöresurssit olivat järjestetty siten, että henkilöiden toimenkuviin on kirjattu riskienhallinnan osa-alueet ja työkaluresurssien osalta riskienhallinnan seurantavälineenä käytetään koko konsernin laajuista dokumenttienhallintajärjestelmää, jossa eri riskejä ja niiden toimenpiteitä voidaan seurata sekä ylläpitää ohjeistoa ja jatkuvuussuunnitelmia. Haastateltava 3 myös kertoi, että he hyödyntävät myös yrityksen sidosryhmiä tiiviisti riskienhallinnassa, eli sidosryhmät toimivat heille niin sanotusti riskienhallinnan työkaluina. Haastateltava 3 kertoo, että esimerkiksi vakuutusmeklari on heille kiinteä osa riskienhallintaa ja jonka työkaluja myös haastateltavan oma yritys voi hyödyntää.

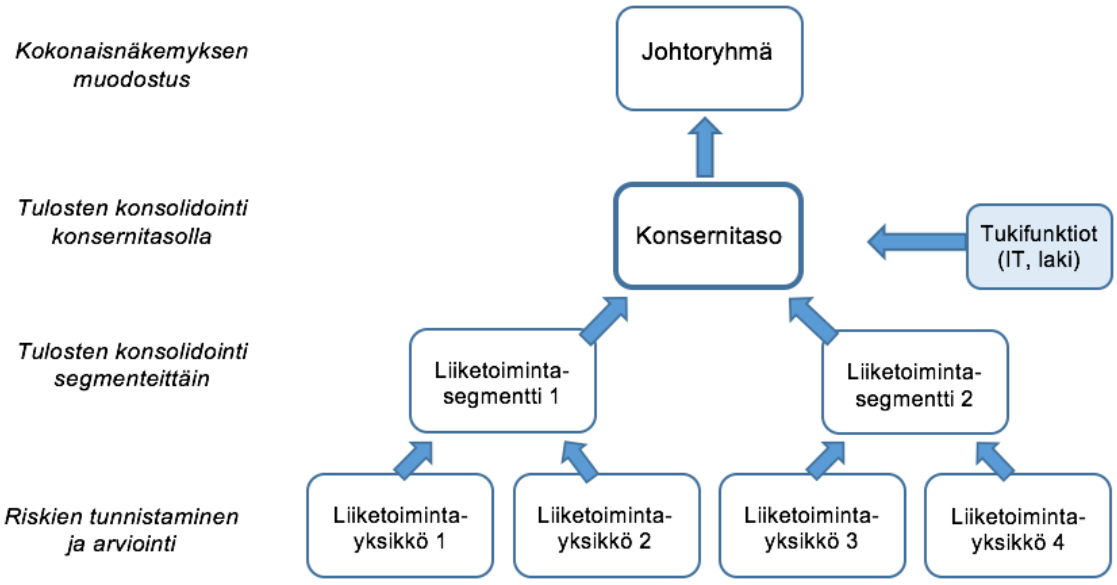
Haastateltava 2 ei haastattelussa erikseen ottanut kantaa riskienhallinnan resursseihin, niiden riittävyyteen tai puutteisiin. Haastateltava 2 kuitenkin kertoi yrityksen käyttävän muun muassa Exceleitä, riskilistoja ja riskirekistereitä, riskienhallinnan työkaluina.

4.3.4 Riskien tunnistaminen

Yrityksen 1 riskien tunnistamisprosessi osoittaa riskienhallinnan prosessin jatkuvuutta ja säännönmukaisuutta, sillä haastateltava 1 kertoo, että yrityksessä tehdään vuosittain koko konsernin käsittävä laajempi ERM riskikartoitus, minkä lisäksi kolme kertaa vuodessa käydään liiketoimintasegmenttitasolla läpi merkittävimmät riskit, tehdyt toimenpiteet sekä mahdolliset muutokset riskeissä sekä niiden prioriteettijärjestyksessä. Näiden lisäksi haastateltava 1 mainitsee, että myös ihan kuukausitasolla käydään ylimmän johdon ja segmentin johtoryhmän kanssa läpi liiketoimintaan vaikuttavia riskejä ”monthly review” kokouksissa.

Yrityksen 1 ERM riskikartoituksen eteneminen on havainnollistettu kuviossa 5. Prosessi etenee siten, että ensin konsernin eri liiketoimintayksiköt tekevät toimipaikkakohtaisen riskien tunnistamisen ja arvioinnin, jonka tulokset

konsolidoidaan ensin liiketoimintasegmenteittäin, johon kunkin liiketoimintasegmentin johto lisää oman riskinäkemyksensä. Tämän jälkeen liiketoimintasegmenttikohtaisesti tunnistetut ja arvioidut riskit konsolidoidaan konsernitasolla ja niihin yhdistetään konsernin globaalien tukifunktioiden kuten talouden ja lakiosaston riskiarvioinnit. Prosessin lopuksi johtoryhmä muodostaa lopullisen kokonaisnäkemyksen riskeistä, mikä esitetään tarkastusvaliokunnalle ja hallitukselle.



Kuvio 8. Yrityksen 1 ERM riskikartoitusta havainnollistava prosessikuvio (mukaillen Haastattelu 1)

Haastateltava 1 kertoi yrityksessä olevan myös käytössä Excel-pohjainen riskirekisteri, johon on kerätty riskejä ja jaoteltu ne pää- ja alakategorioihin. Pääkategorioiksi on valittu strategiset, operatiiviset, taloudelliset ja informaatioriskit. Haastateltava 1 tarkentaa, että jokaisen riskin kohdalla on sekä yleisempi riskin määritelmä, että kyseisen riskin arviointia tekevän henkilön oma kuvaus riskistä. Haastateltava 1 myös näkee riskirekisterin etuna sen, että sinne voidaan koota myös sellaisia riskejä ja mahdollisuuksia, jotka eivät ole läsnä jokapäiväisessä toiminnassa, mutta saattavat silti olla merkityksellisiä. Hän myös toteaa, ettei riskirekisteriin ole mahdollista sisällyttää kaikkea, mutta heillä on myös kategoria

”muut”, sellaisille asioille, jotka eivät suoranaisesti kuulu mihinkään muuhun riskikategoriaan.

Haastateltava 1 kertoo, että heidän riskienhallinnan prosessiin kuuluvien vuosittaisten riskikartoitusten ja riskirekisterin ylläpitämisen lisäksi he toteuttavat riskityöpajoja, joissa lähestymistapa riskien tunnistamiseen on erilainen. Työpajoissa riskien tunnistaminen on tarkoitus aloittaa niin sanotusti ”puhtaalta pöydältä”, jossa osallistujilta lähdetään hakemaan tietoa siitä, millaisia riskejä ja mahdollisuuksia he näkevät mihinkin aiheeseen liittyvän. Haastateltava 1 kertoo, että hän pyrkii pelkästään valmiin riskilistan tutkimisen sijaan painottamaan osallistujille sitä, että he pohtisivat myös täysin uusia liiketoiminnassa tapahtuneita muutoksia.

Riskirekisteristä haastateltava 1 kertoo, että se toimii tehokkaammin liiketoimintayksiköissä, kun taas riskityöpajat nähdään hyödyllisempänä konsernin tukifunktioille, kuten IT:lle ja talousosastolle, joilla on liittymäkohtia organisaation moneen eri toimintoon. Haastateltava 1 myös tarkentaa, että merkittävimpiin päätöksentekoprosesseihin, kuten investointeihin tai yrityskauppoihin heillä on käytössä oma riskien tunnistamisprosessi, jossa käytetään samanlaisia työkaluja ja lähestymistapaa, mutta joka kuitenkin on ERM prosessista irrallinen tapahtuma.

Yrityksessä 2 riskien tunnistaminen etenee myös ennalta määritetyn prosessin mukaisesti. Haastateltava 2 kertoo riskien tunnistamisen mukailevan sekä ISO 31000 standardia että Demingin laatuympyrää. Haastateltavan 2 mukaan:

”Täs prosessis ei sinällään oo mitään ihmeellistä, tää on hyvinkin tyypillinen just hyvinki samallainen ku toi ISO 31000, Demingin laatuympyrä joka on ollu plan, do, check, niin ihan sama tässä eli identify, evaluate, prioritize and mitigate ja jatkuvan parantamisen periaate tulee sitten raportoinnin ja kontrollien päivittämisen myötä.”

(Haastateltava 2)

Yrityksen 2 riskienhallinnan prosessi mukailee siis hyvin paljon ISO 31000 standardin mukaista prosessia, kuten aiemmin kuviossa 4. on esitetty. Lisäksi

haastateltava 2 mainitsee operatiivisen riskienhallinnan erikseen, mikä on ”lattiatason” toimintaa, eli tapahtuu siellä missä itse valmistustoimintakin. Tällaisina riskeinä haastateltava 2 mainitsee esimerkiksi tulipalot ja laiterikot. Haastateltava 2 mainitsee, että heillä on erikseen operatiivisten riskien hallintajärjestelmä, joka on jalkautettu konsernin tytäryhtiöihin.

Haastateltava 2 kuvailee heidän organisaation rakennetta siten, että ensin on ylin taso eli johtoryhmä, keskitasolla liiketoiminta-alue ja alimpana tuotantotoiminnot. Haastateltava 2 kuvailee riskienhallintaa termein ”top down” ja ”bottom up”, jossa ensimmäistä toteuttaa ylhäältäpäin johto ja jälkimmäistä toteutetaan alemmista tuotantotoiminnoista ylöspäin. Haastateltava 2 mainitsee, että myös keskitason liiketoiminta-alueisiin on joskus tehty riskianalyysejä. Hän myös jatkaa, että he ovat implementoimassa juuri uutta GRC järjestelmää, jonka yhteydessä aletaan toteuttaa myös tukitoimintojen kuten lakiosaston, talouden ja rahoituksen riskianalyysejä. Hän kertoo, että tavoitteena on, että myös tukitoiminnot alkaisivat tuottaa riskitietoa nostamalla asioita alhaalta ylös johdon tietoon.

Tunnistettujen riskien määrästä haastateltava 2 kertoo, että heillä on operatiivisia riskejä eri tuotanto-osastoilla listattuna jopa 1200 kappaletta, joita käsitellään niin sanotusti pohjadatana ja josta kunkin yksikön riskienhallintapäällikkö raportoi konsernin operatiivisten riskien järjestelmään noin 30-40 merkittävämpää riskiä. Haastateltava 2 mainitsee, että yksikkökohtaisia pienempiä riskejä saattaa olla enemmän, mutta niiden vaatimia toimenpiteitä voi olla helppo toteuttaa myös yksikkökohtaisesti, eikä niiden realisoitumisen vaikutus välttämättä edes näkyisi konsernitasolla. Haastateltava 2 kertoo, että kokonaisuudessaan heidän operatiivisten riskien järjestelmästä löytyy noin 300-400 eri yksiköiden raportoimaa riskiä, joiden vahingon suuruuden alaraja on käytännössä miljoona euroa. Eli alle miljoonan euron arvioituja vahinkoja ei käytännössä kyseiseen järjestelmään raportoida.

Haastateltava 2 myös kertoo, että operatiivisten riskien osalta eri yksiköt raportoivat ja päivittävät riskit kahdesti vuodessa, eli vuoden alussa sekä noin syyskuussa. Hän jatkaa, että sama riskien päivityssykli toteutuu myös konsernin avainriskien osalta,

mitkä päivitetään kerran vuodessa kokonaan ja kerran vuodessa valittujen avainriskien osalta.

Yrityksen 3 vuonna 2017 julkaisemassa ”Corporate Social Responsibility” (CSR) raportissa yritys mainitsee, että se on tunnistanut useita toimintaan liittyviä riskejä, kuten ympäristöriskit, työterveyteen ja –turvallisuuteen liittyvät riskit sekä kemikaali- ja elintarviketurvallisuusriskit. Lisäksi yrityksellä on suunnitelmissa toteuttaa koko konsernin laajuinen riskianalyysi. Myös liiketoimintariskien vaikutus yrityksen liiketoimintaan on arvioitu ja yrityksen jokaiseen yksikköön on luotu myös jatkuvuussuunnitelmat. (Yritys 3 2017, 3)

Haastateltava 3 itse kertoo, että heillä toteutetaan kahden tai kolmen vuoden välein ERM analyysi, jota hän myös nimittää ”risk mapping” nimityksellä, eli sen avulla käydään läpi yrityksen strategisia tavoitteita uhkaavat riskit ja luodaan niille toimenpidesuunnitelmat. Tällaisessa riskien tunnistamisharjoituksessa he käyttävät apunaan ulkopuolista kumppania, kuten vakuutusmeklaria. Sen sijaan yrityksen eri yksikköjen turvallisuuden ja omaisuuseriä uhkaavien riskien riskien osalta yrityksen 3 vakuutusyhtiö tekee säännöllisiä käyntejä eri yksiköissä, käy läpi turvallisuustilanteen ja antaa suosituksia ja toimenpiteitä toteutettavaksi. Haastateltava 3 toteaa, että tällainen perusteellinen ”lattiatason” analyysi on todettu työkaluna heille todella hyväksi. Haastateltava 3 kertoo, että he pystyvät käytössä olevan dokumenttienhallintajärjestelmän avulla seuraamaan, miten annettuja toimenpiteitä toteutetaan eri yksiköissä ja miten riskienhallinta niissä kehittyy. Sen lisäksi hän jatkaa, että samaan järjestelmään raportoidaan muun muassa laatuun liittyvät sertifikaatin sekä mahdolliset uudistukset.

Haastateltava 3 kertoo, että heillä riskien tunnistamista toteutetaan sekä ylhäältä alaspäin, että alhaalta ylöspäin. Riskien tunnistamista yritys toteuttaa strategiavalmistelun yhteydessä ja strategian päivityksen yhteydessä toteutetaan ulkopuolisen kumppanin kanssa jo edellä mainittu ”risk mapping”. Haastateltava 3 kuvaa heidän riskien tunnistamista seuraavasti:

”…meillä on yleensä siinä aika monen kuukauden tai muutaman kuukauden projekti jossa haastatellaan keskeiset tuota henkilöt tai avainhenkilöt, pääasiassa siinä on johtoryhmä ja avainhenkilöitä yksiköistä mukana ja sitte tuota pidetään tämmösiä yhteisiä workshoppeja jossa analysoidaan tärkeysjärjestystä ja tietysti todennäkösyyksiä ja priorisoidaan meijän niinku strategiaa uhkaavat riskit”
(Haastateltava 3)

Alhaalta ylöspäin tapahtuvaa riskien tunnistamista haastateltava 3 kuvailee siten, että yksikkötasolla jokaisen yksikön johtoryhmän tehtävänä on ylläpitää ja huolehtia paikallisista jatkuvuussuunnitelmista ja huolehtia, että toimenpiteet viedään käytännön tasolle. Lisäksi paikallisten johtoryhmien on tuotava tarvittaessa keskeisimpi asioita organisaatiossa ylöspäin käsittelyyn. Yrityksessä 3 on haastateltavan mukaan myös käytössä ”safety notice”- ilmoitukset, joiden avulla voidaan tuoda alimman tason havaintoja esimiehen tietoon ja jotka tarvittaessa nostetaan organisaatiossa vielä ylemmäs. Haastateltava 3 painottaa sitä, että erilaisten havaintojen osalta tulee toimia nopeasti, jotta toimenpiteet saadaan heti käytäntöön ja siksi päätöksentekoa pyritään hajauttamaan, jotta havainnoista voidaan hyötyä välittömästi. Haastateltava 3 tiivistää, että heillä riskien tunnistamista tehdään siis strategisella tasolla muutaman vuoden välein ja operatiivisella tasolla päiväkohtaisesti.

4.3.5 Riskien analysoiminen ja merkityksen arviointi

Haastateltava 1 kertoo, että heillä on käytössä valmis riskiluokittelu, jonka alle tunnistettuja riskejä jaotellaan. Haastateltavan mukaan riski tulisi aina kirjoittaa auki, eli mistä riski on lähtöisin, miten sen näkyy liiketoiminnassa ja mihin se voi johtaa, mutta haastateltava myöntää, ettei tällainen riskin kuvaaminen ole heillä täysin systemaattista. Hän jatkaa, että tämän jälkeen yrityksessä arvioidaan sen hetkiset riskienhallinnan toimenpiteet kyseistä riskiä kohtaan ja arvioidaan, mikä riskin vaikutus olisi yrityksen liikevoittoon (EBIT[2]).

[2] EBIT = Earnings Before Interest and Taxes

Haastateltava 1 kertoo, että heillä on riskien arvioimisessa käytössä numeerinen asteikko yhdestä yhdeksään, jossa jokainen arvo vastaa vaikutuksen osalta tiettyä menetystä suhteessa liikevoittoon, sekä todennäköisyyden osalta tiettyä toteutumistodennäköisyyttä. Hän jatkaa, että he arvioivat riskin todennäköisyyden ensin ilman nykyisiä riskienhallinnan toimenpiteitä ja sen jälkeen arvioidaan riskienhallintatoimet ja kuinka kykenevä yritys on hallitsemaan riskiä. Haastateltava 1 myös mainitsee, että heillä arvioidaan myös sitä, mikä olisi mahdollinen saavutettavissa oleva riskienhallinnan taso, sillä kaikkia mahdollisia riskejä, kuten poliittisia riskejä, ei ole mahdollista kontrolloida täysimääräisesti. Haastateltava 1 kertoo, että numeerisen arvioinnin lisäksi he tekevät myös laadullista arviointia kuvaamalla käytettävissä olevia riskienhallinnan keinoja ja mahdollisia lisäkeinoja.

Haastateltava 1 toteaa, että vaikka heillä tehdään vuosittain neljästi ERM:in mukaista arviointia, tulisi riskejä kuitenkin analysoida kaikessa yrityksen liiketoimintaan liittyvässä päätöksenteossa, kuten jokaisen projektin yhteydessä. Haastateltava 1 jatkaa että heillä riskianalyysiä ja toimenpiteiden riittävyyttä arvioidaan erikseen jokaisella organisaatiotasolla. Haastateltavan 1 mukaan:

”*Periaatteessa aina niinkun ylemmän organisaatiotason tulee tarkastaa sen alemman tason riskien määrän hyväksyttävyys ja niiden riskienhallintatoimenpiteiden riittävyys eli se kulkee aina sieltä business unit tasolta segmenttitasolle ja sieltä konsernitasolle ja viimeiseksi tietysti hallituksen tulee hyväksyä se riskitaso ja riskienhallinnan nykyiset käytössä olevat keinot ja suunnitelmat”*

(Haastateltava 1)

Haastateltava 2 kertoo, että heillä riskit analysoidaan todennäköisyyden ja vaikutuksen avulla. Hänen kertoo, että heidän riskimatriisissaan on asteikko sekä todennäköisyydelle ja vaikutukselle sekä niille asetetut arvot, joiden avulla voidaan laskea riskille odotusarvo. Haastateltava 2 kertoo, että arvioiduista riskeistä muodostetaan riskikartta, jossa riskikartan värit on määritetty riskin odotusarvon mukaan. Hän jatkaa, että mikäli esimerkiksi tiettyä riskiä ei enää koeta yrityksessä riskiksi, se muuttuu väriltään vihreäksi ja se tiputetaan pois riskikartalta.

Haastateltava 2 tarkentaa, että riskikartalla on siis heidän avainriskit sekä operatiiviset riskit.

Koska riskejä on hyvin paljon erilaisia, haastateltava 2 toteaa, että riskiarvioinnissa vaikutusasteikkoa saatetaan skaalata sellaisten riskien osalta, joiden pelkkiä rahallisia vaikutuksia ei pystytä arvioimaan, kuten esimerkiksi maineriskin toteutumisen osalta. Hän jatkaa, että riskiarvioinnissa tulisi aina olla mukana pelisilmää, sillä arvio on aina vain yhden ihmisen arvio ja matemaattisesti oikeaa riskilukua tärkeämpää on keskinäisten asioiden prioriteettijärjestys. Syyksi haastateltava 2 sanoo sen, että esimerkiksi markkinariskille voidaan laskea 10-20 % volatiliteetti, mutta maineriskin osalta samanlaista arvoa ei voida antaa, jolloin on vaikea arvioida, kumpi riskeistä on suurempi.

Haastateltava 2 kertoo, että heillä avainriskit päivitetään kahdesti vuodessa, joulukuussa kaikki avainriskit ja huhtikuussa valitut avainriskit. Hän kertoo, että jokaisesta riskistä on olemassa riskikuvaus, jossa on esitetty kyseinen riski, riskin kuvaus, riskin omistaja, todennäköisyys ja vaikutus sekä niistä muodostuva riskiluku sekä riskin vastuullinen henkilö. Haastateltava 2 tarkentaa, että riskin omistaja on aina johtoryhmän jäsen, kun taas vastuullinen henkilö voi olla esimerkiksi liiketoiminta-alueen vetäjä. Haastateltava 2 kertoo, riskikuvauksissa esitetään myös ”net damage” ja ”worst case scenario” arvot, joista ensimmäinen kuvaa menetystä, jossa on huomioitu riskiä pienentävät toimenpiteet, kun taas jälkimmäinen kuvaa riskistä realisoituvaa pahinta skenaariota. Lisäksi hänen mukaansa riskikuvauksessa on esitetty kyseisen riskin riskienhallinnan toimenpiteet.

Haastateltava 2 myös kertoo, että hän tekee avainriskien osalta riskipäivityksiä, jolloin hän haastattelee yksilöhaastatteluissa sekä riskin vastuullisia henkilöitä, että hallituksen jäseniä. Haastateltava 2 jatkaa, että riskianalyysiä toteutetaan työpajojen ja koulutuspakettien avulla, jolloin hän pyrkii opettamaan yrityksen henkilöitä kuvailemaan riskejä ja niiden syitä sekä seurauksia, jotta riskien arviointi olisi yhdenmukaista sekä haastateltavan 2 että muiden riskiä arvioivien henkilöiden kesken.

Haastateltava 3 kertoo että yrityksessä analysoidaan riskeissä tapahtuneita muutoksia aina uuden riskien tunnistus ja –arviointiprojektin jälkeen. Hän jatkaa, että analyysissa seurataan, mitkä riski ovat mahdollisesti nousseet top-listalla ja niille laaditaan toimenpidesuunnitelmat. Hän mainitsee, että esimerkiksi tällä hetkellä kymmenen suurinta strategiaa uhkaavaa riskiä on tunnistettu, joista viidelle on luotu useita toimenpiteitä riskin hallitsemiseksi.

Haastateltava 3 kertoo, että heillä on määritetty yrityksessä taloudellisten riskien kuten korko- ja valuuttariskien osalta selkeät toleranssit, joiden sisällä liikutaan ja mitkä vaativat ihan käytännön toimenpiteitä. Lisäksi hän tarkentaa, että vastuuhenkilöiden kohdalla on myös määritetty, että millaisiin määriin saakka heillä on valtuudet toimia, esimerkiksi avoimen valuuttaposition ylläpitämisen kohdalla. Myös raaka-aineriskin kohdalla heillä on käytössä positioseurantaa, eli määritetyt kriteerit ja raja-arvot, joita seurataan kuukausittain.

Haastateltava 1 kertoo, että riskin merkityksen arvioinnissa katsotaan, että mikä on riskin realisoituessa vaikutus yrityksen tulokseen. Hän jatkaa, että kun vaikutuksen lisäksi huomioidaan riskin todennäköisyys, saadaan selville alkuriski. Sen jälkeen todetaan miten hyvin riskiä pystyään hallitsemaan, ja mitä heikompaa riskienhallinta on, sitä korkeammaksi residuaalipisteytys nousee. Haastateltava 1 kertoo, että tällaisen perusarvioinnin lisäksi johtoryhmä lisää oman näkemyksensä arviointiin, sillä johtoryhmällä voi olla aiheesta sellaista tietoja, jota muualla organisaatiossa ei ole. Haastateltava 1 myös toteaa, että erot esimerkiksi merkittävimpien top 10 ja top 20 riskin välillä voivat olla melko pieniä, jolloin riskin nostamisella listan kärkeen on lähinnä viestinnällistä arvoa, millä yritys haluaa viestiä mitkä asiat ovat tällä hetkellä tärkeitä.

Myös yrityksessä 2 on käytössä riskitoleranssiasteikko, joka ei haastateltavan mukaan ole välttämättä kovinkaan tieteellinen, mutta missä määritetyistä tekijöistä johdetaan laskukaavan avulla riskitoleranssit, joita yritys käyttää riskien arvioinnissa. Yrityksen 2 riskitoleranssitekijät ja toleranssiarvot ovat esitetty alla olevassa taulukossa 5.

Taulukko 5. Yrityksen 2 riskitoleranssit (mukaillen Haastattelu 2)

Tekijä	Toleranssi
Pörssiarvo	Yli 10 % markkina-arvon muutos
Velkakapasiteetti	Velan ja EBITDA:n[3] suhde ylittää arvon 4
Likviditeettitilanne	Likviditeetti painuu miinukselle
Lainakovenantit	Lainasopimuksen kovenanttien rikkoutuminen

Yrityksessä on haastateltavan 2 mukaan käytössä jo aiemminkin mainittu riskimatriisi ja avainriskikartta, jossa asteikkona on vaikutus ja todennäköisyys. Vaikutuksen arvot tulevat yllä taulukossa 5. esitetyistä toleransseista ja todennäköisyys on määritetty asteikolla yhdestä neljään, esimerkiksi luku 1 vastaa riskin todennäköisyyttä kerran kolmessa vuodessa, josta asteikko harvenee ylöspäin mentäessä. Haastateltava 2 myös lisää, että riskitoleranssien lisäksi yrityksessä on vastikään määritetty kaikille riskeille myös riskinottohalukkuus.

Myös haastateltava 3 kertoo että heidän yrityksessään riskin merkittävyyttä arvioidaan todennäköisyyden ja vaikuttavuuden kautta, eli riskin taloudellista laajuutta arvioidaan vaikutuksena yrityksen EBIT lukuun. Haastateltava 3 tarkentaa, että kun merkittävimmät riskit ja niiden taloudellinen vaikutus on tunnistettu, erityisellä työkalulla arvioidaan riskien prioriteettijärjestys, jolloin pystytään pureutumaan liiketoiminnan jatkuvuuden kannalta merkittävimpiin riskeihin.

4.3.6 Riskien käsittely

Haastateltava 1 kertoo, että yrityksen ensimmäinen askel riskin käsittelyssä on se, että pyritään tekemään kaikki mahdolliset toimenpiteet, jotta negatiivisesti vaikuttava riski ei koskaan toteutuisi. Hän jatkaa, että he pyrkivät aina tunnistamaan riskeissä myös mahdollisuuksia ja ajamaan toimintaa siihen suuntaan, että tätä

[3] EBITDA = Earnings Before Interest, Taxes, Depreciation and Amortization

mahdollisuutta pystyttäisiin jollain tapaa hyödyntämään. Haastateltava 1 kertoo, että esimerkiksi tunnistettu riski jätteiden lisääntymisestä valtamerissä pyrittiin kääntämään mahdollisuudeksi, jonka seurauksena yrityksen tuotteista pyrittiin kehittämään entistä ympäristöystävällisempiä ja kierrätettäviä. Eli negatiivisten vaikutusten minimoimisen lisäksi yrityksessä 1 pyritään aina tunnistamaan myös riskin positiiviset puolet.

Mikäli riski kuitenkin realisoituu, haastateltava 1 kertoo, että heillä on olemassa toimenpiteitä, joilla negatiiviset vaikutukset pyritään minimoimaan. Tällaisia keinoja ovat haastateltavan 1 mukaan muun muassa liiketoiminnan jatkuvuussuunnitelmat esimerkiksi tulipalon sattuessa, kriisinhallinta- ja kommunikaatiosuunnitelma esimerkiksi maineriskin osalta sekä myös muita toimintasuunnitelmia. Haastateltavan 1 mukaan kaikki sellaiset riskit, jotka ovat vakuutettavissa pyritään vakuutuksen avulla siirtämään toiselle taholle. Lisäksi haastateltava 1 toteaa, että on kuitenkin olemassa myös sellaisia riskejä, joihin yritys ei kaikesta huolimatta pysty juurikaan vaikuttamaan.

Haastateltava 1 myös kertoo, että kaikkein tehokkaimpana keinona yrityksessä nähdään riskin taustatekijöihin vaikuttaminen. Hän jatkaa, että esimerkiksi tulipaloriskin juurisyihin pyritään vaikuttamaan käynnissä olevalla omaisuudenhallintaohjelmalla, joka pyrkii minimoimaan tulipalojen mahdollisuuden. Hän jatkaa, että joihinkin asioihin, kuten lainsäädännön muutoksiin saatetaan pystyä vaikuttamaan esimerkiksi informaation ja kommunikoinnin kautta, jolloin yritys pyrkii saamaan oman näkökantansa kuuluviin julkisessa keskustelussa ja päätöksenteossa.

Yrityksessä 2 taas todetaan riskien käsittelyn olevan heille selkeästi heikoin osa-alue. Haastateltava 2 kertoo, että koska yritystä johdetaan strategian johdolla, yrityksen strategiset riskit tulevat niin sanotusti annettuina strategiaprosessin mukana. Tällöin riskienhallinta koetaan heillä haastateltavan 2 mukaan lähinnä reaktiivisesti ja raportteja tuottavaksi toiminnaksi, jolla pyritään vain täyttämään ne velvoitteet, joita riskienhallinnalle on asetettu. Haastateltava 2 mukaan yrityksessä ei toteuteta riskianalyysiä ennen strategian asettamista, jolloin riskienhallinnan

lähtötilanne on se, minkä yrityksen strategia on asettanut. Hän toteaa, että suurimmat riskienhallinnan toimenpiteet sisältyvät jo siten yrityksen strategisiin toimenpiteisiin. Haastateltava 2 kertoo omasta tehtävästään, että käytännössä hän siis kerää tietoa siitä, millaisia toimenpiteitä yrityksessä jo strategian kautta tehdään.

Riskien käsittelystä haastateltava 3 toteaa, että yrityksessä ei ole nimenomaista riskinkäsittelysuunnitelmaa, mutta käsittely ja seuranta tapahtuvat johtoryhmissä. Hän tarkentaa, että riskianalyysin lopputulokset käsitellään johtoryhmissä, jossa arvioidaan vaativatko lopputulokset välittömiä toimenpiteitä vai ei. Hän jatkaa, että tässä vaiheessa johtoryhmissä keskitytään useimmiten suurimpiin riskeihin, kun taas pienemmät käydään läpi vuosikellon mukaisesti strategian päivityksen yhteydessä. Yrityksen riskin käsittelytavoista haastateltava 3 esittää esimerkin poissaoloon johtavasta työtapaturmasta. Hän kertoo, että mikäli yrityksessä sattuu työtapaturma, niin koko tapahtuma perataan auki prosesseiksi ja mietitään mikä tapaturmaan johti ja mitkä ovat korjaavia toimenpiteitä.

4.3.7 Riskienhallinnan seuranta ja arviointi

Yrityksessä 1 riskien tunnistamisen jälkeen riskeille määritetään vastuuhenkilöt ja mahdollisuuksien mukaan myös tavoitetasot sekä seurannan mittaristo. Hän jatkaa, että riskienhallinnan mittaristoja ei aina kuitenkaan löydy, eikä yrityksessä sellaisia aktiivisesti vaaditakaan. Haastateltava 1 painottaa, että riskienhallinnan tulisi riskien tunnistamisen jälkeen kuulua tiiviisti yrityksen päivittäiseen tekemiseen ja liiketoimintaan, jolloin vastuiden ja seurannan tulisi hoitua luontevasti.

Haastateltava 1 myös kertoo, että riskienhallinnan seuranta ja arviointi ovat osa yrityksen strategisten tavoitteiden saavuttamista, sillä riskien tunnistamisessakin lähdetään liikkeelle siitä, mikä on yrityksen strategia, millaisia tavoitteita se sisältää ja miten tavoitteiden saavuttaminen voisi vaarantua. Haastateltava 1 siksi toteaakin, että koska strategisten tavoitteiden seurannassa on jo valmiiksi olemassa mittareita, kuten taloudelliset mittarit, ei yrityksessä ole suoranaisesti enää ERM:in osalta omaa toimenpiteiden seurantaa, vaan seuranta tapahtuu tehokkaimmin muun liiketoiminnan yhteydessä.

Haasteltava 2 kertoo, että heillä on tavoitteena ottaa käyttöön riskienhallinnan KPI-mittaristo, jolloin jokaiselle riskille asetettaisiin tavoitteita strategian puitteissa, ja joiden toteutumista KPI-mittaristolla seurataan. Haastateltava 2 kokee, että viime aikoina on sattunut runsaasti pieniä vahinkoja, joita on operatiivisten riskienhallinnan toimenpiteiden ja vahingontorjunta auditointien kautta pyritty hallitsemaan. Hän myös kertoo, että heillä on tällä hetkellä meklarin vahingontorjuntasuositus raporteissa yli 200 toimenpidettä, joiden toteuttamista parhaillaan seurataan ja joista myös raportoidaan.

Haastateltava 2 myös kertoo, että vahingontorjunta auditointeja tehdään vuosittain noin muutama kymmenen. Hän jatkaa, että käyntien jälkeen yksikkö saa suosituksia, joiden toimeenpanoa seurataan ja mahdollisesti tehdään myös pistokokeita käymällä yksiköissä paikan päällä. Riskienhallinnan toimenpiteistä haastateltava 2 kuitenkin toteaa, että:

” tääl on myös vähän tällasii maailmaa syleilevii toimenpiteitä, jotka on taas sinällään muissa toimintasuunnitelmissa se ei niinku varsinaisesti oo riskienhallinnan tehtävä seurata... Et se niinkun strategia edellä meneminen ei oo välttämättä huono juttu ollenkaan, että me ollaan enemmän tällasessa tietoa koostavassa raportoivassa roolissa. Ei se tarkota et riskienhallintaa ei olis hoidettu vaan et se on vaa hoidettu niinku toista kautta.” (Haastateltava 2)

Haastateltava 3 kertoo, että heillä riskienhallinnan seurantaa hoidetaan paikallisesti operatiivisten riskien kuten työturvallisuuteen liittyvien riskien osalta, kun taas konsernitason riskejä ja taloudellisia riskejä seurataan johtoryhmässä. Haastateltava 3 mainitsee, että esimerkiksi asiakasreklamaatioiden määrää heillä seurataan omalla KPI eli suorituskykymittaristolla.

Yritys 3 mainitsee myös CSR raportissaan (2017, 7), että työturvallisuuden osalta yritys arvioi kehitystoimenpiteiden tarpeellisuutta riskianalyysin ja saatujen turvallisuushavaintojen perusteella sekä seuraa ja raportoi turvallisuuden KPI-

mittarin tuloksia. Haastateltava 3 kertoo, että varsinkin työturvallisuuden puolella he seuraavat säännöllisesti kuukausittaisia työtapaturmia jo aiemmin mainittujen ”safety notice” ilmoitusten kautta ja heillä on käytössä työturvallisuuspyramidi, jossa pyritään runsaisiin turvallisuushavaintoihin, ihmisten osallistumiseen sekä poissaoloihin johtavien työtapaturmien minimoimiseen.

4.3.8 Riskienhallinnan raportointi

Haastateltava 1 kertoo yrityksessä olevan käytössä erillinen tietokanta, johon riskitietoa siirretään erillisistä Excel-tiedostoista. Hän jatkaa, että tietokannassa voidaan yhdistää tietoja organisaatiotasolla, analysoida raportoitua tietoa ja tehdä erilaisia hakuja. Tietokanta toimii haastateltavan 1 mukaan raportointityökaluna, sillä sieltä voidaan ajaa ulos erilaisia riskienhallinnan raportteja ja riskigrafiikoita, joissa on kuvattu muun muassa alkuriski, kontrollin taso, kontrollin tehokkuus sekä vaikutus liiketoimintaan. Lisäksi suurimmista riskeistä tietokanta muodostaa haastateltavan 1 mukaan yhteenvetoja riskistä, sen hallintakeinosta, lisäkeinoista, vastuuhenkilöistä ja mittareista. Haastateltava 1 toteaa, että näitä yhteenvetoja heillä käytetään riskienhallinnan seurannassa.

Haastateltava 1 myös lisää, että kaikki riskityöpajat ja mahdolliset riskihaastattelut dokumentoidaan, mikä toimii sisäisenä raportointina, mutta esimerkiksi suurempien yritysjärjestelyiden osalta raportoidaan uhat ja mahdollisuudet sekä integraatiovaiheessa tehdään myös riskien listaamista ja seurantaa. Haastateltava 1 mainitsee sisäisen raportoinnin lisäksi erikseen yrityksen ulkoisen raportoinnin, joka sisältää muun muassa toimintakertomuksen, GMI-raportin sekä Corporate Governancen, minkä lisäksi yritys saattaa vastata sijoittajakyselyihin sekä raportoida suoraan asiakkaiden omiin raportointikanaviin.

Haastateltava 2 kertoo, että heillä toteutetaan riskiraportointia kvartaaleittain eli jokaisen kvartaalitilinpäätöksen jälkeen, jolloin koostetaan raportti johdolle, hallitukselle sekä tilintarkastajalle. Hän jatkaa, kyseisessä riskiraportissa käydään läpi kvartaalin aikaiset riskit sekä myös tulevaa. Haastateltavan 2 mukaan riskiraportti toimii kerronnallisena dokumenttina siitä, mitkä riskit ovat tällä hetkellä

tai aiemmalla kvartaalilla olleet pinnalla, miten riskejä on hallittu ja millaiset toimenpiteet on ollut käytössä. Haastateltava 2 kertoo, että operatiiviset riskit raportoidaan kahdesti vuodessa niiden päivityksen yhteydessä. Riskienhallinnan raportoinnista haastateltava 2 kuitenkin toteaa, että liikaa ei saisi vain kehua miten riskienhallinta onnistuu tietyllä alueella, vaan tulisi kertoa realistisesti, miten asiat todellisuudessa ovat.

Haastateltava 3 kertoo, että heillä riskienhallinnan raportointia tehdään sekä paikallisesti eri yksiköissä, että konsernitasolla. Hän kertoo, että esimerkiksi tuotteen laatuun liittyvissä asioissa raportoidaan koko konsernin johtoryhmälle, kun taas esimerkiksi paikalliseen työturvallisuuteen liittyvissä asioissa saatetaan raportoida kyseisen yksikön paikalliseen johtoryhmään. Lisäksi haastateltava 3 kertoo, että kaikki riskianalyysin lopputulokset dokumentoidaan.

4.3.9 Riskienhallinnan viestintä

Haastateltava 1 kertoo, että hän pitää henkilöstölle joko suullisesti tai kirjallisesti motivointipuheita riskienhallinnan tärkeydestä. Hän toteaa, että joillekin organisaation jäsenille riskienhallinnan merkitys saattaa olla itsestäänselvyys, mutta on tärkeää jakaa tietoa myös siksi, että riskejä saatetaan tunnistaa paremmin organisaation yhdessä osassa verrattuna toiseen. Haastateltava 1 myös kertoo, että merkityksellisimmistä riskienhallinnan teemoista kommunikoidaan ylhäältä alaspäin ja lisäksi koska riskit liittyvät strategisten tavoitteiden saavuttamiseen, on myös ylimmän johdon tehtävä kommunikoida riskienhallinnasta. Haastateltava 1 myös toteaa, että organisaation riskinottohalukkuus vaikuttaa siihen, millaisista riskeistä eniten kommunikoidaan.

Haastateltava 1 tiivistää, että riskienhallinnan kommunikaation ja viestinnän tulisi toimia läpi organisaation ja liittyä siihen, miten liiketoiminnasta ylipäätänsä viestitään. Hän jatkaa, että heillä on olemassa riskienhallinnanpolitiikka ja tietysti Code of Conduct ohjeistus, mikä sisältää yleisiä periaatteita eettisistä, laillisista ja arvojen mukaisista toimintatavoista.

Yrityksen 2 vuoden 2017 taloudellisessa katsauksessa (2017, 9-10) on esitetty yrityksen toimintaan vaikuttavia keskeisiä riskejä, kuten strategiset ja liiketoimintariskit, toiminnalliset riskit, rahoitusriskit, ympäristöriskit, maineriskit sekä henkilöstöön ja turvallisuuteen liittyvät riskit. Kaikille julkinen dokumentti toimii siten viestintäkeinona sidosryhmien suuntaan. Sisäisestä viestinnästä haastateltava 2 kertoo, että riskienhallinnan onnistumisista viestitään organisaation sisällä, vaikka virallista foorumia riskienhallinnan informaation välittämiseen ei ole. Haastateltava 2 myös tunnustaa, että riskienhallinnan hyödyistä ja tuloksista pitäisi viestiä vielä enemmän organisaation sisällä. Haastateltava 2 kuitenkin kertoo yrityksen järjestävän riskienhallinnan koulutuksia koko henkilöstölle, riskien päivityksen yhteydessä pidetään päivityskoulutuksia ja ensi vuonna lanseerataan myös verkkokoulutusta.

Yrityksessä 3 riskienhallinnan viestintää toteutetaan esimerkiksi kahden kuukauden välein pidettävissä henkilöstöinfoissa, joissa käydään läpi riskienhallintaan kuten työturvallisuuteen liittyviä asioita sekä kerrotaan käytännön esimerkkejä riskienhallinnan tuloksista ja hyödyistä. Haastateltava 3 kertoo riskienhallinnan viestinnän toimivan samalla myös henkilöstön kouluttamisena. Hän jatkaa, että heillä on yrityksen omilla sisäisillä internetsivuilla käytännön ohjeita, ajankohtaisia turvallisuustiedotteita sekä esimerkiksi ohjeistus kriisinhallintaviestintään. Lisäksi hän toteaa, että varsinkin tietoturvan osalta yrityksessä on paljon ohjeita ja koulutusta, kuten myös kilpailulainsäädännön kohdalla. Haastateltava 3 myös mainitsee, että varsinkin uuden rekrytoinnin jälkeen on pidettävä huolta siitä, että uusi työntekijä tietää yrityksen toimintatavat ja –ohjeet.

Lisäksi haastateltava 3 kertoo, että viestintää toteutetaan kaikissa päätöksentekoelimissä sekä paikallisesti yksikkötasolla, että konsernitasolla ja hallituksessa. Haastateltava 3 mainitsee erikseen, että yrityksen toimitusjohtaja kiertää vuosittain yrityksen jokaisessa yksikössä ja käsittelee riskienhallintaan liittyviä teemoja henkilöstön kanssa. Lisäksi haastateltava 3 kertoo, että he itse keräävät riskitietoa omilta toimittajiltaan esimerkiksi toimittaja-auditointien yhteydessä.

5 YHTEENVETO JA JOHTOPÄÄTÖKSET

Tämän tutkielman tavoitteena oli selvittää, miten uuden vuonna 2018 julkaistun ISO 31000 riskienhallinnan standardin mukainen riskienhallinnan prosessi etenee, mitä kokonaisvaltainen riskienhallinta on, miten yrityksissä riskienhallintaa järjestetään ja kuinka riskienhallinnan prosessi toteutuu ISO 31000:2018 standardin suositusten mukaisesti. Lisäksi tutkielman teoriaosuudessa taustoitettiin riskin määrittämistä ja erilaisia riskienhallinnan keinoja sekä kokonaisvaltaisen riskienhallinnan kehittymistä.

Tutkielman keskeisiä teemoja olivat riski, riskienhallinta, kokonaisvaltainen riskienhallinta (ERM, Enterprise Risk Management), riskienhallinnan prosessi, ISO 31000:2018 riskienhallinnan standardi, riskien tunnistaminen ja hallinta sekä reaalimaailman yritysten riskienhallintaan liittyvät toimenpiteet. Tutkielman tekemiseen motivoi standardin ajankohtaisuus, sillä se on julkaistu vuonna 2018.

Tutkielma on jaettu viiteen päälukuun, joista ensimmäinen on johdanto. Toinen pääluku käsittelee riskiä, kokonaisvaltaista riskienhallintaa ja sen kehittymistä, kolmas luku käsittelee ISO 31000:2018 riskienhallinnan standardin sisältöä sekä sekä neljäs luku empiiristä havainnointia kolmen eri kohdeyrityksen riskienhallinnan prosessin järjestämisestä edellä mainitun ISO standardin mukaisesti. Viimeisessä eli tässä luvussa käsitellään tutkimuksen johtopäätökset, luotettavuus ja jatkotutkimusehdotukset.

Alla on esitetty johtopäätökset tutkimustuloksista suhteessa asetettuihin tutkimuskysymyksiin. Sen jälkeen on otettu kantaa tutkielman luotettavuuteen ja ehdotettu mahdollisia aihioita jatkotutkimukselle.

5.1 Johtopäätökset

Tämän tutkielman tavoitteet on muodostettu kahden tutkimuskysymyksen muotoon, jotka ovat päätutkimuskysymys sekä sitä tukeva alatutkimuskysymys.

Tutkielman päätutkimuskysymyksenä oli:

Miten ISO 31000:2018-standardin mukaiset suositukset riskienhallinnan prosessin järjestämisestä toteutuvat yrityksissä?

Alakysymyksenä oli:

”Millaisilla säännönmukaisilla toimenpiteillä riskienhallintaa yrityksissä järjestetään?”

Vastauksia asetettuihin tutkimuskysymyksiin pyrittiin saamaan haastatteluista, riskienhallintaa koskevasta aiemmasta tutkimuksesta, tieteellisistä julkaisuista, asiantuntija-artikkeleista ja ISO 31000:2018 standardista. Tutkimusaineistoa kerättiin haastattelemalla riskienhallinnan tehtävissä toimivia henkilöitä sekä tutustumalla kyseisten yritysten virallisiin julkaisuihin. Tutkielmaa varten haastateltiin kolmea eri henkilöä heidän yrityksensä riskienhallinnan prosessista ja haastattelurunko oli rakennettu perustuen ISO 31000:2018 mukaisen riskienhallinnan prosessin eri vaiheisiin. Tämän tutkimuksen avulla saatiin melko kattavasti vastaus kumpaankin asetettuun tutkimuskysymykseen.

Tämän tutkielman perusteella voidaan todeta vastauksena päätutkimuskysymykseen, että jokaisen haastatellun yrityksen riskienhallinnan prosessi jäljittelee lähestulkoon kokonaan tai joitakin poikkeuksia lukuun ottamatta ISO 31000:2018 mukaista riskienhallinnan prosessia. Se, millaiset riskienhallinnan tavat ja keinot yrityksissä on, vaihtelee kuitenkin yrityksittäin, vaikka pääpiirteet riskienhallinnan prosessille on hyvin samankaltaiset. Muutamia poikkeuksia lukuun ottamatta, kuten yhden yrityksen puutteellisen riskien käsittelytapojen, jokaisessa yrityksessä on myös selkeät toimenpiteet, kuinka riskienhallintaa vuosittain

toteutetaan ja millaisia vaiheita siihen sisältyy. Haastateltavat henkilöt eivät myöskään juurikaan epäröineet vastauksissaan tai sanoneet etteivät tietäisi kuinka kulloinkin kyseessä olevaa asiaa heillä hoidetaan. Se osoittaa, että prosessi on pääpiirteissään selkeä. Haastattelut tuottivat hyödyllistä tietoa yritysten riskienhallinnan suunnitelmanmukaisista käytännöistä, mihin alakysymyksellä haluttiin perehtyä.

Kaksi kolmesta haastateltavasta kertoivat, että yrityksessä on olemassa kirjallinen riskienhallinnanpolitiikka ja yksi haastateltavista totesi, että vaikka virallista politiikkaa ei ole, tulee riskienhallinnan toimintaperiaatteet silti hallitukselta. Yritysten riskienhallintapolitiikka joko perustui tai pohjautui osittain ISO 31000:2018 standardiin tai aiemmin tässäkin tutkielmassa mainittuun COSO-ERM viitekehykseen, joka voidaan nähdä vaihtoehtoisena ohjeistuksena ISO standardille. Se, että yrityksen riskienhallintapolitiikka on saanut inspiraation standardista, jäljittelee standardin perimmäistä tarkoitusta, eli sitä, että yritys omaksuu standardista juuri ne omaan toimintaansa sopivat elementit ja muokkaa niitä omaan liiketoimintaympäristöön sopivaksi. Standardia ei ole tarkoitettu noudatettavan orjallisesti, vaan toimivan enemmänkin ohjeistavaksi suositukseksi.

ISO 31000:2018 standardi (2018, 9) myös ohjeistaa, että on johdon vastuulla varmistaa riskienhallinnan resurssit ja vastuuhenkilöt. Riskienhallinnan resurssit käsittävät muun muassa työkalut, ihmiset ja tarvittavan ajan. Standardin (2018, 10) suositusten mukaan riskiä tulisi hallita organisaation jokaisessa osassa. Kaikki yritykset noudattivat vastuiden osalta kahden vastuuhenkilön tapaa, jossa vastuu on jaettu kahdelle henkilölle, joista toinen toimii niin sanotusti riskin omistajana ja toinen riskin vastuullisena. Tällöin riskin hallinnollinen omistajuus on esimerkiksi johtoryhmän edustajalle, kun taas operatiivinen vastuu osoitetaan sinne, missä itse riskikin on. Riskienhallinnan vastuiden osoittaminen organisaatioissa oikeille tahoille ja nimenomaan eri organisaatiotasoilla on siten hyvin hoidossa kaikissa tutkimuksen kohdeyrityksissä.

Haastateltava 1 nosti kokonaisvaltaisen riskienhallinnan eli ERM:in roolin esille resursoinnissa, sillä hänen mukaansa juuri ERM:in tehtävä on tuoda esille

riskienhallinnan resurssipuutteita. Kuten tutkielmassa on aiemmin todettu, ERM:in tulisi olla koko organisaatioon jalkautettu johdon strateginen työkalu, jolloin sen tehtävänä onkin tuoda esille kokonaisvaltaisesti myös puutteita eri funktioissa, kuten riskienhallinnassa. Ymmärrys ERM:stä ja sen hyödyistä on siten sisällytetty hyvin yrityksen 1 toimintaan. Resurssien osalta kaikissa yrityksissä käytettiin jonkinlaista työkalua, oli se sitten dokumenttienhallintajärjestelmä, vakuutusmeklari tai Excel. Käytössä olevien työkalujen vaihtelevuus osoittaa, että riskienhallinnan prosessissa voidaan hyödyntää hyvin monenlaisia keinoja ja työkaluja, sellaisia mitkä kukin yritys kokee itselleen sopiviksi ja riittäviksi. Tärkeintä myös standardia tulkitessa on se, että yrityksellä on riittävät ja tavoitteet täyttävät työkaluresurssit.

Riskien tunnistamista tehtiin jokaisessa kohdeyrityksessä järjestelmällisesti ja erillisen prosessin mukaisesti, mikä vastaa tutkimuksen alakysymykseen säännönmukaisesta riskienhallinnan käytännöstä. Yrityksillä on ennalta määritetty riskien tunnistamisprosessi, jonka mukaan vuosittain tai muutaman vuoden välein toimitaan. Riskien tunnistamiseen oli myös erilaisia tekniikoita, joskin yhdessä yrityksessä jopa 1200 tunnistetun riskin rekisteri kuulostaa jo jokseenkin epätehokkaalta, sillä kuten teoriassakin on todettu, että liian raskaan riskirekisterin ylläpitäminen johtaa vain hallinnolliseen taakkaan, eikä se enää palvele tarkoitustaan. Tässä vaiheessa yrityksen kannattaisi keskittyä standardissakin esiintyvään riskin arviointivaiheeseen syvemmin, jotta se kykenisi priorisoimaan riskit tärkeysjärjestykseen ja mahdollisesti tiputtamaan merkityksettömämpiä riskiä pois listalta, ja keskittyä käsittelemään toiminnan kannalta tärkeimpiä riskejä. Sama yritys myös totesi riskin käsittelyn olevan heille heikoin osa-alue, mikä voi osittain myös johtua siitä, että riskejä tunnistetaan jopa hallitsemattoman paljon.

Kaikissa yrityksissä riskien tunnistamisen voidaan sanoa jäljittelevän vahvasti ISO 31000:2018 standardin riskien arviointia, jossa ensin tunnistetaan riski, analysoidaan se sekä arvioidaan sen merkittävyys. Järjestelmällistä ERM tason riskien tunnistamista tehtiin yrityksissä vuosittain tai muutaman vuoden välein, minkä lisäksi riskien päivitystä ja raportointia useamminkin. Standardin mukaan prosessin tulisi olla jatkuva ja säännönmukainen, jolloin kaikissa yrityksissä on onnistuttu luomaan jatkuva prosessi, jossa tunnistetaan riskin lähteet, uhat ja

mahdollisuudet sekä seuraukset ja vaikutukset tavoitteisiin. Lisäksi kun standardi painotti sidosryhmien huomiointia, on ainakin yhdessä yrityksessä hyödynnetty vakuutusmeklaria apuna. Sidosryhmät voivat tuottaa tärkeää riskitietoa yritykselle sekä tutkia epävarmuuksia hieman eri näkökulmasta.

Kaikissa kolmessa kohdeyrityksessä tehdään määrällistä riskianalyysiä numeerisen asteikon avulla sekä hyödynnetään jo aiemmin kuviossa 6. esitettyä riskimatriisia, jossa huomioidaan sekä vaikutus että todennäköisyys, mitkä saavat tietyt lukuarvot. Kuten ISO 31000:2018 standardi (2018, 17) suosittelee, riskianalyysissa tulisi huomioida riskitapahtuman todennäköisyys, seurausten suuruus eli riskin vaikutus, sekä lisäksi myös nykyisten hallintakeinojen riittävyys. Haastateltava 1 kertoo, että he arvioivat riskin todennäköisyyden ilman nykyisiä riskienhallinnan toimenpiteitä mutta nimenomaan arvioidaan myös nykyiset riskienhallintatoimen sekä niiden riittävyys, aivan kuten standardi ehdottaa. ISO 31000:2018 (2018, 18) mukaan riskin merkittävyyden arviointi on juurikin sitä, että arvioidaan ovatko riskienhallinnan toimenpiteet riittävät vai tulisiko harkita vielä lisätoimia. Riskienhallinnan toimenpiteiden riittävyyden arviointi on tärkeää, sillä sen avulla yritys voi määritellä onko jäljelle jäävä jäännösriski hyväksyttävä vai ei. Myös riskianalyysia toteutetaan kaikissa yrityksissä ennalta määritetyn tietoisen prosessin mukaan, mikä antaa jälleen vastausta tutkimuksen alakysymykseen. Kun yritykset käyttävät todennäköisyyden ja vaikutuksen osalta numeerista asteikkoa, heidän on tullut määritellä etukäteen jokaiselle asteikon luvulle sitä vastaava arvo, jotta riskianalyysin tuloksia voidaan hyödyntää ja suhteuttaa yrityksen toiminnan laajuuteen.

Kuten aiemmin on esitetty, ISO 31000:2018 (2018, 17) standardin mukaan riskianalyysissä tulisi tarkastella riskin lähteitä ja seurauksia, riskitapahtumia eli eri skenaarioita sekä ottaa huomioon aikaan liittyvät tekijät sekä myös eri riskien liittymäkohdat ja monimutkaisuus. Esimerkiksi haastateltavan 2 mukaan, heillä jokaisesta riskistä esitetään riskin kuvaus sekä analyysin perusteella saatu riskiluku mutta myös eri skenaarioita, kuten ”worst case scenario”, mikä ilmentää pahinta mahdollista riskitapahtumaa ja menetystä. Tällaisten eri skenaarioiden esittäminen hyvin havainnollistava tapa esittää erilaisia mahdollisuuksia, sillä kuten kuvion 2.

riskikäyrä osoittaa, riskin toteutumisen seuraus voi olla mitä tahansa tietyllä todennäkösyys- ja vaikutusasteikolla. Eri skenaarioiden käyttö on siten myös hyödyllistä, kun halutaan arvioida eri riskienhallintatoimenpiteiden tehokkuutta. Esimerkiksi miten toimenpide X riskin vaikutuksen pienentämiseksi voisi vaikuttaa arvioidun vahingon suuruuteen.

ISO 31000:2018 (2018, 18) standardin mukaan riskin käsittelyyn kuuluu riskinkäsittelysuunnitelman luominen ja toteuttaminen sekä riskinkäsittelytavan valinta. Erityistä huomiota voidaan antaa sille, että ainoastaan yhdessä näistä kolmesta yrityksestä voidaan todeta olevan selkeä prosessi riskien käsittelylle, kun taas yhdessä riskien käsittely todettiin suoraan olevan riskienhallinnan selkeästi heikoin kohta. Toteamus on siksi mielenkiintoinen, sillä riskin käsittely on hyvin merkittävä osa riskienhallintaprosessia ja riskin pienentämistä. Pelkän yrityksen strategian avulla voi olla haastavaa hallita laajaa riskiportfoliota, jossa jokainen riski vaatii omat toimenpiteensä. Riskin juurisyihin vaikuttaminen eli riskin lähteiden poistaminen on tehokas keino pienentää riskiä, ja riskin juurisyihin vaikuttaminen on ISO 31000:2018 (2018, 18) mukaan eräs riskinkäsittelytapa, jota tämänkin tutkimuksen yrityksistä osa harjoittaa.

ISO 31000:2018 (2018, 19) standardin prosessin mukaan seurannan ja katselmoinnin on oltava jatkuvaa ja sisältävän muun muassa tulosten dokumentoinnin ja palautteen, jotta prosessi toimii tarkoituksenmukaisesti. Sekä yrityksessä 1 että 3 on jo käytössä erilliset seurannan mittarit ja yrityksessä 2 on tarkoituksena ottaa sellaiset käyttöön. Seuranta on siten järjestelmällistä ja standardin suositusten mukaista. Kaksi haastateltavista myös mainitsee strategisten tavoitteiden saavuttamisen riskienhallinnan seurannan yhteydessä, mikä osoittaa, että riskienhallinta on tiivis osa yrityksen strategiaa ja riskienhallinnan tehokkuutta arvioidaan luonnollisella tapaa myös strategian toteutumisen yhteydessä.

Riskienhallinnan tuottama tieto on erittäin tärkeää organisaation johdolle päätöksentekoa varten ja kuten aiemmin tutkielmassa on jo mainittu ISO 31000:2018 (2018, 20) standardin mukaan riskienhallinnan raportoinnin ja

dokumentoinnin tehtävä on nimenomaan tuottaa kaikki tämä tarvittava tieto päätöksenteon tueksi. Jokainen haastateltava yritys kertoi dokumentoivansa riskienhallinnan prosessia sekä tuottavansa raportteja niin sisäiseen kuin ulkoiseenkin käyttöön, joko esimerkiksi tietyin väliajoin tai tarpeen tullessa. Lisäksi kaikissa haastatelluista yrityksissä toteutetaan sekä sisäistä henkilöstön suuntaa kohdistuvaa riskienhallinnan viestintää muun muassa henkilöstöinfojen muodossa, sekä lisäksi ulkoista riskienhallinnan viestintää esimerkiksi julkisten toimintakertomusten ja taloudellisten katsausten muodossa.

Tämän tutkielman johtopäätöksinä voidaan todeta, että kaikissa kolmessa haastatellussa yrityksessä riskienhallinnan prosessi on ensinäkin pääsääntöisesti ennalta määritetty ja säännönmukaisesti etenevä. ISO 31000:2018 standardi esittää riskienhallinnan prosessista kaksi päävaihetta, jotka ovat riskien arviointi ja niiden käsittely. Varsinkin riskien arviointia tehdään jokaisessa yrityksessä säännöllisesti ja hyödyntäen erilaisia työkaluja. Riskien käsittely oli ainoastaan yrityksessä 2 selkeämmin kahta muuta yritystä ennalta määrittelemättömämpää. Haastateltava 2 kuitenkin tunnisti riskien käsittelyn hoituvan strategian kautta, mikä toisaalta voidaan sisällyttää yhdeksi riskinkäsittelytavaksi.

Jokaisessa yrityksessä riskianalyysiä tehtiin samalla tavoin arvioimalla riskin todennäköisyyttä ja vaikutusta, mikä on selkeästi teorian ja empirian perusteella hyvin yleinen tapa arvioida riskejä sekä myös asettaa ne riskimatriisiin. Kaikissa yrityksissä riskeille luotiin myös jonkintasoisia toimenpiteitä ja niiden toteutumista ja tehokkuutta seurattiin prosessin mukaisesti. Yrityksissä voisi siten sanoa olevan järjestelmällinen seurantaprosessi riskienhallinnan vaikuttavuudelle. Myös kaikki ISO 31000:2018 standardin mukaiset prosessin jatkuvat elementit kuten viestintä, raportointi ja seuranta toteutuivat yrityksissä, ja viestintää toteutettiin sekä sisäisesti että ulkoisesti.

Tämän tutkimuksen päätutkimuskysymyksenä haluttiin selvittää, kuinka ISO 31000:2018 standardin mukaiset suositukset riskienhallinnan prosessin järjestämisestä yrityksessä toteutuvat, ja lopputulemana voidaan todeta, että vaikka standardi sisältää melko yksityiskohtaisiakin asioita, kaikki prosessikuvion mukaiset

teemat ovat jollain tapaa käytössä kaikissa haastatelluissa yrityksissä. Yksikään yritys ei siten suoranaisesti ohittanut vaiheita, mutta eri vaiheisiin kuten riskien tunnistamiseen tai riskien käsittelyyn yritykset panostivat vaihtelevasti. Yritykset siten jäljittelevät vaiheita, mutta yksikään yrityksistä ei toteuta riskienhallinnan prosessiaan ainoastaan seuraten täsmällisesti standardin vaiheita. Eroavaisuudet yritysten käytäntöjen ja standardin suositusten välillä painottuukin siten pääasiassa siihen, millaisia elementtejä kukin yritys on standardista omaksunut, joko tietoisesti tai tiedostamatta. Riskienhallinta kuitenkin pääasiassa etenee samoin vaihein, eli riskin tunnistamisesta siirrytään sen arviointiin, jonka jälkeen riski käsitellään ja toimenpiteitä seurataan. Koska kaikissa yrityksissä kuitenkin on riskienhallinnasta vastaava henkilö ja yrityksen riskienhallinta on asianmukaisesti järjestetty, suurempia eroavaisuuksia standardin ja yritysten käytäntöjen välillä olisi odotettu löydettävän siinä tapauksessa, että yrityksen riskienhallinnassa olisi ollut merkittäviä puutteita.

5.2 Tutkimuksen luotettavuus

Tutkimuksen luotettavuuden arvioinnissa tulee arvioida, onko tutkimuksen aineisto, tutkimustulokset sekä tutkimus kokonaisuudessaan luotettava, eli validi. Tutkimuksen validiteetilla tarkoitetaan sitä, onko tutkimusmenetelmä ollut riittävän pätevä mittaamaan sitä, mitä on haluttu tutkittavan ja onko tutkimuksen aineisto vastannut tutkittavaa ilmiötä. Tutkimuksen reliabiliteetilla sen sijaan tarkoitetaan sitä, onko aineiston käsittely ja analysoiminen ollut luotettavaa. (Anttila 2014)

Tutkimuksen empiirisen osion tiedonkeruu suoritettiin haastatteluina joko kasvotusten tai online videopuhelun välityksellä, mikä lisäsi tutkimuksen luotettavuutta. Vastaajat saivat kertoa riskienhallinnan prosessin eri teemoista vapaamuotoisesti, jolloin tutkimuksen tiedonkeruutapa ei rajoittanut vastaamista, vaan mahdollisti erilaiset ja monipuoliset vastaukset. Myös haastateltavien henkilöiden ja yritysten käsitteleminen anonyymisti edisti tutkimuksen luotettavuutta, sillä riskienhallinta sisältää usein kriittistä tietoa muun muassa strategiasta ja kilpailuedusta, minkä vuoksi tietoa ei ole juurikaan julkisesti saatavilla. Kaikki haastateltavat henkilöt olivat myös tutustuneet

haastattelukysymyksiin etukäteen, jolloin heillä on ollut aikaa miettiä teemoja etukäteen ja siten valmistautua haastatteluun. Haastattelut myös nauhoitettiin ja litteroitiin, jolloin aineiston käsittely oli huolellista ja aineistoa pystyi tulkita useaan otteeseen välttääkseen mahdolliset väärät tulkinnat.

Tutkimuksen luotettavuutta lisäsi se, että vastaajat tunsivat työtehtäviensä ja kokemuksensa kautta käytetyt riskienhallinnan termit, määritelmät sekä yrityksen riskienhallinnan sisältöä ja kokonaisvaltaisen riskienhallinnan (ERM) käsitteen. Tutkimukseen pyrittiin myös saamaan moniulotteisuutta haastattelemalla yrityksiä eri toimialoilta, vaikkakaan tutkimuksen pienen otannan perusteella ei voida ottaa kantaa toimialakohtaisiin käytäntöihin tai vertailla eri toimialoja. Pienen otannan vuoksi päätutkimuskysymykseen nähden tuloksilla ei myöskään voida tehdä kovinkaan kattavia yleistyksiä. Empiirisen havainnoinnin otanta oli siten melko pieni, joskin tavoitteena oli saada syvällistä ja laajaa tietoa yhden yrityksen käytännöistä.

5.3 Jatkotutkimusehdotukset

Koska riskienhallinta on aiheena melko laaja, voi siitä pilkkoa useita syvällisemmin tutkittavia aihioita. Tämän tutkimuksen perusteella jatkotutkimuksena voisi olla keskittyä syvemmin esimerkiksi yrityksen riskien tunnistamisprosesseihin ja siihen, kuinka kattavaa tietoa erilaiset riskien tunnistamismenetelmät tuottavat. Pidemmän aikavälin tutkimusehdotuksena voisi olla yrityksen vuosikellonmukaisen riskien tunnistamis- ja hallitsemisprosessin toteutuminen, eli kuinka yritykset ovat onnistuneet hallitsemaan ja erityisesti pienentämään tunnistettujen riskien vaikutusta ja todennäköisyyttä.

Tässä tutkimuksessa ei myöskään oteta kantaa ISO 31000:2018 standardin mukaisen riskienhallinnan prosessin toteutumiseen tai onnistumiseen yrityksissä, mikä voisi olla potentiaalinen jatkotutkimusehdotus. Tällainen tutkimus tulisi kuitenkin ajallisesti viemään runsaasti enemmän aikaa, sillä standardin mukaisen prosessin implementointi yritykseen ja riskienhallinnan toteuttaminen standardin mukaan vie ajallisesti kauemmin, kuin mitä tämän kyseisen pro gradu-tutkielman tekoon on varattu aikaa.

LÄHDELUETTELO

Alasuutari, P. (1999) Laadullinen tutkimus. Vastapaino. Tampere. 3.painos.

Anttila, P. (2014) Tutkimisen taito ja tiedonhankinta. Metodix. [Verkkodokumentti] [Viitattu 7.5.2019] Saatavilla: https://metodix.fi/2014/05/17/anttila-pirkko-tutkimisen-taito-ja-tiedon-hankinta/#10.1%20Tutkimuksen%20luotettavuus

Aon (2019) Global Risk Management Survey 2019 – Executive summary. *Aon.*

Aven, T. (2013) On the Meaning and Use of the Risk Appetite Concept. *Risk Analysis*. Vol. 33, No. 3, pp. 462-468.

Beasley, M., Branson, B. & Hancock, B. (2018) The State of Risk Oversight: an Overview of Enterprise Risk Management Practices. *Aicpa.*

Berlinger, E. & Váradi, K. (2015) Risk Appetite. *Public Finance Quarterly.* Vol. 60, Iss. 1, pp. 49-62

Butterfield, B. (2017) Traditional Risk Management vs. Enterprise Risk Management: Which Approach Is the Best Choice for Your Company? *Mondaq.* [Verkkodokumentti] [Viitattu 21.2.2019] Saatavilla: http://www.mondaq.com/unitedstates/x/636120/Securities/Traditional+Risk+Management+vs+Enterprise+Risk+Management+Which+Approach+Is+The+Best+Choice+For+Your+Company

Callahan, C. & Soileau, J. (2017) Does Enterprise Risk Management Enhance Operating Performance? *Advanced in Accounting*. Vol. 37.

Connolly, R. (2017) Toshiba faces fresh $400m lawsuit over historic accounting scandal. *The New Economy.* [Verkkodokumentti] [Viitattu 21.11.2018] Saatavilla: https://www.theneweconomy.com/business/toshiba-faces-fresh-400m-lawsuit-over-historic-accounting-scandal

COSO (2004) Enterprise Risk Management – Integrated Framework. *The Committee of Sponsoring Organizations of the Treadway Commission.*

COSO (2018) About us. *The Committee of Sponsoring Organizations of the Treadway Commission.* [Verkkodokumentti]. [Viitattu 6.12.2018]. Saatavilla: https://www.coso.org/Pages/aboutus.aspx

Daukant, R. & HIrst, A. (2009) 4 Steps to ERM. *Canadian Underwriter.* Vol. 78, Iss. 8, pp. 64-66.

Deloitte (2019) Global Risk Management Survey, 11th edition. *Deloitte.*

Ferdman, R. & Bhattarai, A. (2015) There's a crisis at Chipotle. *The Washington Post.* [Verkkodokumentti]. [Viitattu 21.11.2018]. Saatavilla: https://www.washingtonpost.com/news/wonk/wp/2015/12/09/chipotle-food-outbreak-ecoli-reputation/?noredirect=on&utm_term=.9d504c71709b

FERMA (2018) About FERMA. *The Federation of European Risk Management Associations.* [Verkkodokumentti] [Viitattu 6.12.2018] Saatavilla: https://www.ferma.eu/about/about-ferma

Fox, C. (2012) 10 Easy Steps to Implement Enterprise Risk Management. *Risk Management.* Vol. 59, Iss. 9, pp. 34-36.

Fox, C. (2018) Understanding the New ISO and COSO Updates. *Risk Management*. Vol. 65, Iss. 6. pp. 4,6-7.

Fraser, J. & Simkins, B. (2016) The Challenges of and Solutions for Implementing Enterprise Risk Management. *Business Horizons*. Vol. 59, Iss. 6, pp. 689-698.

Frijns, B., Gilbert, A., Lehnert, T. & Tourani-Rad, A. (2013) Uncertainty Advoidance, Risk Tolerance and Corporate Takeover Decisions. *Journal of Banking & Finance.* Vol. 37, Iss. 7, Pp. 2457-2471.

Gordon, L., Loeb, M. & Tseng, C-Y. (2009) Enterprise Risk Management and Firm Performance: A Contingency Perspective. *Journal of Accounting and Public Policy*. Vol. 28, No. 4, pp. 301-327.

Grace, M. F., Leverty J. T., Phillips, R. D. & Shimpi, P. (2015) The Value of Investing in Enterprise Risk Management. The *Journal of Risk and Insurance.* Vol. 82, No. 2, pp. 289-316.

Hirsjärvi, S, Remes, P. & Sajavaara (1997) Tutki ja kirjoita. Kustannusosakeyhtiö Tammi. Hämeenlinna. 15.-16. painos.

Hirsjärvi, S. & Hurme, H. (2008) Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö. Gaudeamus Helsinki University Press. Helsinki.

Hoyt, R. E. & Liebenberg, A. P. (2011) The Value of Enterprise Risk Management. *The Journal of Risk and Insurance.* Vol. 78, No. 4, pp. 795-822.

IRM (2002) A Risk Management Standard. *The Institute of Risk Management.*

IRM (2018a) A Risk Practioners Guide to ISO 31000: 2018. *Institute of Risk Management.*

IRM (2018b) IRM's Risk Management Standard. *Institute of Risk Management.* [Verkkodokumentti] [Viitattu 6.12.2018] Saatavilla: https://www.theirm.org/the-risk-profession/risk-management/irms-risk-management-standard.aspx

IRM (2018c) What is Risk Management? [Verkkodokumentti] [Viitattu 21.1.2019] Saatavilla: https://www.theirm.org/the-risk-profession/risk-management.aspx

ISO (2018a) ISO 31000:2009. *International Organization for Standardization.* [Verkkodokumentti] [Viitattu 6.12.2018] Saatavilla: https://www.iso.org/standard/43170.html

ISO (2018b) ISO 31000 – Risk Management. *International Organization for Standardization.* [Verkkodokumentti] [Viitattu 6.12.2018] Saatavilla: https://www.iso.org/iso-31000-risk-management.html

Kaplan, S., Garrick, B. J. & Apostolakis, G. (1981) Advances in Quantitative Risk Assessment – The Maturing of a Discipline. *IEEE Transactions on Nuclear Science.* Vol. 28, No. 1, pp. 944-946.

Kurkela, M. (2014) Yritystoiminnan riskeistä ja riskien hallintainstrumenteista. Edilex.

Louisot, J-P. & Ketcham, C. (2014) ERM – Enterprise Risk Management. *John Wiley & Sons.* Chicherser.

Malmén, Y. & Wessberg, N. (2004) Mitä tarkoitetaan riskillä, riskianalyysillä, riskin arvioinnilla ja riskienhallinnalla? *Teknologian tutkimuskeskus VTT Oy.* [Verkkodokumentti] [Viitattu 2.3.2019] Saatavilla: http://www.nbcsec.fi/sptry/arkisto/art-01.pdf

Malmén, Y. & Wessberg, N. (2005a) Mihin ennaltaehkäisevät toimenpiteet kannattaa kohdistaa? *Teknologian tutkimuskeskus VTT Oy.* [Verkkodokumentti] [Viitattu 2.3.2019] Saatavilla: http://www.nbcsec.fi/sptry/arkisto/art-04.pdf

Malmén, Y. & Wessberg, N. (2005b) Riskin arvioinnin kriteerit. *Teknologian tutkimuskeskus VTT Oy.* [Verkkodokumentti] [Viitattu 2.3.2019] Saatavilla: http://www.nbcsec.fi/sptry/arkisto/art-03.pdf

Meidell, A. & Kaarboe, K. (2017) How the Enterprise Risk Management Function Influences Decision-making in the organization – A Field Study of Large Global Oil and Gas Company. *The British Accounting Review*. Vol. 40, pp. 39-50.

Näpärä, L. (2017) Haastattelun lajityypit. [Verkkodokumentti] [Viitattu 9.12.2018] Saatavilla: https://www.spoken.fi/blogi/haastattelun-lajityypit

Oliva, F. (2016) A Maturity Model for Enterprise Risk Management. *International Journal of Production Economics*. Vol. 173, pp. 66-79.

Osbich, L. (2018) The Updated International Risk Management Standard ISO 31000 – The Changes You Need to Know About. *School Governance.* [verkkodokumentti] [viitattu 9.2.2019] Saatavilla: http://www.schoolgovernance.net.au/2018/03/15/the-updated-international-risk-management-standard-iso-31000-the-changes-you-need-to-know-about/

Pagach, D. & Warr, R. (2011) The Characteristics of Firms That Hire Chief Risk Officers. *Journal of Risk and Insurance*. Vol. 78, No. 1.

Preda, C. (2013) Implementig a Risk Management Standard. *Journal of Defence Resources Management.* Vol. 4, Iss. 1, pp. 111-120.

Purdy, G. (2010) ISO 31000:2009 - Setting a New Standard for Risk Management. *Risk Analysis*. Vol. 30, No. 6, pp. 881-886

SFS-OPAS 73 (2011) Riskienhallinta. Sanasto. Suomen standardoimisliitto SFS ry.

SFS-FI ISO 31000 (2018) Riskienhallinta. Ohjeet. Suomen standardoimisliitto SFS ry.

SFS ry (2018) Riskit hallintaan – SFS-ISO 31000. Suomen standardoimisliitto SFS ry. [verkkodokumentti] [viitattu 9.2.2019] Saatavilla: https://www.sfs.fi/files/8535/31000_riskienhallinta_esite_A4_web.pdf.pdf

Shah, J.N., & Moosemiller, M.D. (2012) Understanding and Developing Quantitative Risk Criteria. *Process Safety Progres.* Vol. 31, Iss. 4, pp. 369-372.

Thun, J-H. & Hoenig, D. (2011) An Empirical Analysis of Supply Chain Risk Management in German Automotive Industry. *International Journal of Production Economics.* Vol. 131, No. 1, pp. 242-249.

Tranchard, S. (2018) The New ISO 31000 Keeps Risk Management Simple. *International Organization of Standardization.* [Verkkodokumentti] [Viitattu 9.2.2019] Saatavilla: https://www.iso.org/news/ref2263.html

University of Cambridge (2019) Set risk criteria. *University of Cambridge*. [Verkkodokumentti] [Viitattu 10.3.2019] Saatavilla: http://www.ssatoolkit.com/ssatoolkit/examine4setcriteria/

Vehviläinen, M. (2016) Skandaali jättipankissa: asiakkaille luotiin miljoonia valetilejä. *Kauppalehti.* [Verkkodokumentti]. [Viitattu: 21.11.2018]. Saatavilla: https://www.kauppalehti.fi/uutiset/skandaali-jattipankissa-asiakkaille-luotiin-miljoonia-valetileja/ee8a34aa-8398-328b-ab91-1e432ab39d16

Vilkka, H. (2015) Tutki ja kehitä. PS-Kustannus, Jyväskylä. 4. uudistettu painos. [E-kirja]

Viscelli, T., Hermanson, D. & Beasley, M. (2017) The Integration of ERM and Strategy: Implications for Corporate Governance. *Accounting Horizons.* Vol. 32, No. 2, pp. 69-82.

AINEISTOLUETTELO

Yritys 1 (2019) Selvitys hallinto- ja ohjausjärjestelmästä.

Yritys 2 (2017) Taloudellinen katsaus.

Yritys 3 (2017) Corporate Social Responsibility Report.

LIITTEET

Liite 1. Haastattelurunko

Nro.	Kysymys
1	Onko riskienhallinnassa määritetty selkeä toimintasuunnitelma siitä, miten riskienhallintaprosessi etenee ja jos on, niin mitä se sisältää?
2	Onko roolit, vastuut ja valtuuden riskienhallinnassa määritetty ja dokumentoitu?
3	Miten organisaatiossa on järjestetty riskienhallintaan tarvittavat resurssit?
4	Miten riskejä tunnistetaan?
5	Miten riskejä analysoidaan?
6	Miten riskien merkityksen arviointia tehdään?
7	Miten riskejä käsitellään?
8	Miten riskienhallinnan seurantaa ja arviointia toteutetaan?
9	Millä tavalla riskienhallintaa raportoidaan?
10	Millä tavoin riskienhallinnan tuloksista, hyödyistä ja arvosta viestitään organisaatiossa?