TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

MAIJU TSOKKINEN

RISKIENHALLINTAJÄRJESTELMÄN KEHITTÄMINEN

Diplomityö

Tarkastaja: yliopistonlehtori Rainer Breite
Tarkastaja ja aihe hyväksytty 26. helmikuuta 2018

TIIVISTELMÄ

MAIJU TSOKKINEN: Riskienhallintajärjestelmän kehittäminen
Tampereen teknillinen yliopisto
Diplomityö, 57 sivua, 2 liitesivua
Marraskuu 2018
Johtamisen ja tietotekniikan diplomi-insinöörin tutkinto-ohjelma
Pääaine: Tuotantotalous
Tarkastaja: yliopistolehtori Rainer Breite

Avainsanat: riskienhallinta, riskiperusteinen ajattelu, strategia, kehittäminen

Tämä tutkimustyö käsittelee riskienhallinta järjestelmän kehittämistä pk-yrityksessä. Työn tarve sai alkunsa päivitetystä standardista SFS-ISO 9001:2015, jossa lähestymistapana on riskiperusteinen ajattelu. Standardi ei vaadi muodollisia riskienhallintatoimenpiteitä, mutta kohdeyrityksessä haluttiin lähteä kehittämään kattavampaa riskienhallintajärjestelmää. Työn tavoitteeksi asetettiin tunnistaa yrityksen toimintaan liittyviä riskejä sekä kehittää niiden hallintaan ja seurantaan toimiva järjestelmä. Lisäksi tavoitteeksi asetettiin löytää tapoja, joilla riskienhallinta saadaan osaksi yrityksen liiketoimintaa. Työn tutkimusongelmaksi muodostui kartoittaa mitä yrityksen johto asettaa riskienhallinnalle tarpeiksi ja vaatimuksiksi sekä miten yrityksen johto voi hyödyntää riskienhallinnasta syntyvää tietoa liiketoiminnassa.

Työn teoriaosuus käsittelee käsiteanalyysin menetelmin riskienhallinnan perusteita, miten yrityksen johto voi eri toiminnan tasoilla hyödyntää riskienhallintaa ja miten riskienhallinta integroidaan toimintaan parhaiten. Työn teoriaa on lähestytty tiedon tuottamisen näkökulmasta. Tutkimustyön empiiristä osuutta käsiteltiin tapaustutkimuksena. Aineisto ja analyysi osiossa käsitellään tämän hetkistä tilaa kohdeyrityksen riskienhallinnassa, koostetaan johdon tarpeista ja vaatimuksista yhteenveto sekä esitellään toteutettuja kehittämistoimenpiteitä ja jatkotoimenpiteitä kehittämisen osalta. Aineisto työhön kerättiin teemahaastatteluilla ja tutustumalla kohdeyrityksen toimintaan. Tutkimuksen lopussa on johtopäätökset ja yhteenveto, jossa esitellään työn tulokset. Tuloksissa tuodaan esiin, että riskienhallinnan kehittäminen vaatii yrityksen johdolta sitoutumista ja se tulee saada osaksi yrityksen kulttuuria.

ABSTRACT

MAIJU TSOKKINEN: Developing a risk management system
Tampere University of Technology
Master of Science Thesis, 57 pages, 2 Appendix pages
November 2018
Master's Degree Programme in Management and Information Technology
Major: Industrial Engineering and Management
Examiner: University Lecturer Rainer Breite

Keywords: risk management, risk-based thinking. Strategy, development

This Master's theses consider developing a risk management system in small and medium enterprise. The need for the work started from the updated standard, the SFS-ISO 9001:2015 in which the approach is risk-based thinking. The standard does not require formal risk handling methods, but in target company of thesis wanted to develop comprehensive risk management system. The objective of thesis was to identify risks which concern the target company and develop the methods how to manage and control these risks. Also, one objective was found the way how risk management can embed to the company. The research problem of the theses was what the management of the company sets on the risk control as needs and demands and how the management of the company can utilize in the business the information which is created from the risk control.

Theory of the theses consider the grounds of the risk management, how the management of the company can utilize risk management at the levels of the different operation and how the risk management is best integrated into the operation. The theory of the work has been approached the production of the information from the point of view and in this part, there is used the methods of the concept analysis. The empiric part of the theses work was processed as a case study. The material and the analysis are processed present situation in the risk management of the target company, a summary of the needs and demands of the management is put together and executed developing measures and further measures are shown for the developing. The material to the work was collected with theme interviews and by becoming acquainted with the operation of the target company. At the end of the theses, there will be conclusions and summary in which the results of the work are presented. In the results it is brought out that the developing of the risk management requires a commitment of the management of the company and it culture of the company has to be gained.

ALKUSANAT

Haluan kiittää kaikkia tämän työn haastatteluihin osallistuneita henkilöitä, diplomityön ohjaajaa sekä muita, jotka ovat auttaneet, tukeneet ja kannustaneet minua opiskeluiden aikana ja erityisesti tämän diplomityön aikana.

Raumalla, 12.11.2018

Maiju Tsokkinen

SISÄLLYSLUETTELO

KUVALUETTELO

LYHENTEET JA MERKINNÄT

COSO	The Committee of Sponsoring Organizations of the Treadway Commission
ERM	Enterprise Risk Management
IRM	Institute of Risk Management
ISO	International Organization for Standardization
KRI	Key risk indicator
PDCA sykli	Plan, Do, Check, Act-sykli
SMA	Statement on Management Accounting
SWOT	Strengths, Weaknesses, Opportunities, Threats-analyysi
VUCA	Volatility, Unsertainity, Complexity, Ambiguity

1. JOHDANTO

Diplomityö käsittelee kokonaisvaltaista riskienhallintaa ja riskienhallintajärjestelmän kehittämistä ja käyttöönottoa yritykselle joka päiväiseen toimintaan. Työ tehdään yritykselle, joka suunnittelee, valmistaa ja huoltaa laitteita meriteollisuuden sektorille. Työn tarve syntyi päivitetyn standardin ISO9001:2015 pohjalta, jossa korostetaan riskienhallintaa ja sen merkitystä jokaisessa liiketoiminnan osa-alueessa. Yritys haluaa varmistaa oman liiketoiminnan jatkuvuuden ja huomioida mahdolliset riskitekijät sekä pyrkiä hyödyntämään mahdollisuudet.

Laadunhallintajärjestelmän standardi ISO 9001 sai uuden päivitetyn version vuonna 2015 ja yksi merkittävä muutos verrattuna vanhaan ISO9001:2008 versioon on, että erillinen ennaltaehkäisevät toimet on korvattu riskiperusteisella ajattelulla. Tämä muutos perustuu siihen, että riskejä on kaikkialla systeemissä, prosesseissa ja toiminnoissa ja riskiajattelulla varmistetaan, että riskit tunnistetaan, huomioidaan ja kontrolloidaan kattavasti läpi koko systeemin. Se on kiinteä osa laadunhallintaa ja se muuttuu ennakoivaksi eikä vain estä tai vähennä ei-toivottuja vaikutuksia. (ISO/TC 176/SC2/N1284.) Vaikka standardissa ISO 9001:2015 määrätään, että organisaatiossa on suunniteltava toimenpiteet riskien käsittelyyn, se ei vaadi dokumentoitua riskienhallintaprosessia tai käyttämään muodollisia riskienhallintamenetelmiä. Organisaatio saa itse halutessaan kehittää kattavamman riskienhallintajärjestelmän kuin mitä ISO 9001 standardi vaatii hyödyntäen muita ohjeita tai standardeita. (ISO9001:2015.) Riskiperusteinen ajattelu ei ole uutta ja sitä tehdään yrityksissä jo jollakin tasolla, mutta ajattelulla varmistetaan riskien tuntemus ja parantaa valmiutta, lisää tavoitteiden saavuttamista sekä vähentää negatiivisten tulosten todennäköisyyttä (ISO/TC 176/SC2/N1284).

Riskienhallinta on pääosin vapaaehtoista toimintaa yrityksessä, jota toteuttaa yrityksen johto ja muu henkilöstö johtamiseen ja toimintaan sisältyvänä prosessina. Riskienhallintaa sovelletaan strategia valinnasta lähtien ja se on mukana kaikessa organisaation toiminnassa eri tasoilla, prosesseissa ja sidosryhmissä. Tavoitteena on tunnistaa ja hallita yrityksen toimintaan vaikuttavia mahdollisia tapahtumia, jotta varmistetaan yrityksen toiminnan jatkuvuus ja henkilöstön hyvinvoinnin turvaaminen. Riskienhallinnassa huomioidaan niin haitalliset tapahtumat kuin potentiaaliset mahdollisuudet, jotta yrityksen asetetut tavoitteet saavutetaan. (Riskikompassi 2017.)

1.1 Tutkimuksen tavoite, rajaus ja tutkimusongelma

Tutkimuksen tavoitteena on tunnistaa liiketoimintaan liittyviä riskejä yrityksessä ja kehittää systemaattinen ja toimiva riskienhallintajärjestelmä, jonka avulla tunnistettuja riskejä voidaan arvioida, hallita ja seurata kokonaisvaltaisesti. Tavoitteena on myös löytää tapoja, joilla riskienhallinta saadaan osaksi yrityksen liiketoimintaa sekä täyttää ISO9001:2015 vaatimukset riskien käsittelyn osalta osana riskienhallintajärjestelmää.

Tutkimus on rajattu koskemaan liiketoimintaan ja sen prosesseihin liittyviä riskejä ja mahdollisuuksia, joita syntyy pk-yrityksessä. Tutkimuksesta on rajattu pois työturvallisuus- ja ympäristöriskit, koska se on yrityksessä organisoitu systemaattisesti ja se ei vaadi muutoksia.

Tutkimusongelma liittyy yrityksen johdon vaatimuksiin riskienhallinnalle, koska tavoitteena on saada järjestelmä osaksi liiketoiminnan riskejä, joista vastaa yrityksen johto. Jotta riskienhallintajärjestelmä olisi toimiva sekä osa yrityksen toimintaa, muodostuu tutkimuksen päätutkimuskysymykseksi: *Mitä vaatimuksia yrityksen johdolla on riskienhallintajärjestelmälle?*

Vastausta on haettu seuraavilla apukysymyksillä:

1. Miten riskienhallintajärjestelmä integroidaan yrityksen toimintaan?
2. Miten riskeistä syntyvää tietoa käsitellään ja hyödynnetään?

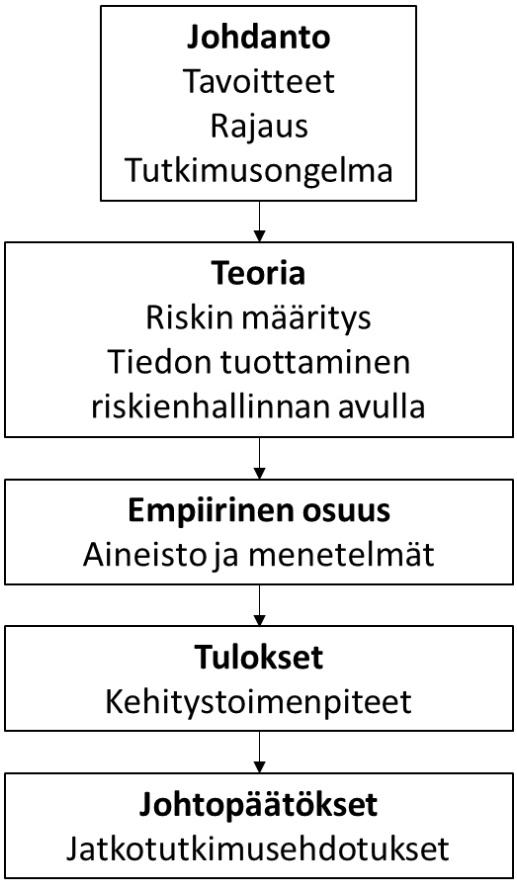
1.2 Tutkimusmenetelmät

Tutkimuksen teoreettiseksi viitekehykseksi on valittu tiedon tuottaminen yrityksen johdolle, jonka tavoitteena on muodostaa kokonaiskuva riskienhallinnasta ja korostaa siitä syntyvän tiedon merkitystä liiketoiminnassa. Tutkimuksen teoriaosuus pohjautuu riskienhallintaan käsittelevään kirjallisuuteen ja lehtiartikkeleihin. Teorian osalta on käytetty käsiteanalyysi menetelmää, jossa analyysin avulla on pyritty jäsentämään riskienhallinnan käsitettä sekä tunnistamaan siihen liittyvät kriittiset ominaispiirteet (Puusa 2008). Empiirisessä osuudessa tutkimusote on laadullinen case- eli tapaustutkimus, koska työssä tutkimuskohteena on yksi valittu tapaus, mikä on ominaista tapaustutkimukselle. Laadulliselle tutkimukselle tyypillisiä piirteitä ovat aineiston kokoaminen todellisista tilanteista, aineiston monitahoinen ja yksityiskohtainen tarkastelu, laadullisten metodien käyttö aineiston hankinnassa kuten teemahaastattelut ja tapausta käsitellään ainutlaatuisesti ja tutkimussuunnitelma muotoutuu tutkimuksen edetessä. (Hirsjärvi et al. 2007.) Tutkimusote on myös osittain toimintatutkimus, koska työn tutkija on työskennellyt kohdeyrityksessä ja ollut näin osa tutkittavaa kohdetta. Tutkimusaineistoa on kerätty haastatteluiden avulla ja tutustumalla yrityksen toimintatapoihin, organisaatiokulttuuriin ja prosesseihin. Haastattelut toteutettiin teemahaastatteluina, joille tyypillistä on, että aihepiiri on tiedossa, mutta tarkka muoto kysymyksille puuttuu (Hirsjärvi et al 2007). Haastattelut toteutettiin

yksilöhaastatteluina, koska haluttiin saada yksilöiden omat näkemykset paremmin esiin. Aineisto analysoitiin litteroimalla tallennetut haastattelut, jonka jälkeen aineistoa jaettiin teemoittain, joita haastatteluissa nousi esiin. Empiirisessä osuudessa kuvataan nykytilaa, yrityksen asettamia tarpeita riskienhallinnalle sekä kehitystoimenpiteitä, joita työn aikana toteutettiin ja mitä jatkotoimenpiteitä tarvitaan.

1.3 Työn rakenne

Työn rakenne koostuu johdannosta, teoreettisesta viitekehyksestä, aineiston keräämisestä ja analysoinnista empiirisessä osuudessa, työn tuloksista ja yhteenvedosta. Työssä on teoriaosuus, jossa käsitellään riskienhallintaa yrityksen johdolle tiedon tuottamisen näkökulmasta ja se toimii pohjana empiiriselle osuudelle. Teoriaosuuden jälkeen käsitellään yrityksen nykytilaa riskienhallinnan osalta ja seuraavassa luvussa esitellään tutkimuksen tulokset.



Kuva 1. *Työn rakenne*

2. RISKIENHALLINNAN LÄHTÖKOHDAT

Liiketoiminnan kaikkiin osa-alueisiin liittyy aina riskejä ja ajan kuluessa riskienhallinta on irrallisten vakuutuksien kautta kehittynyt kokonaisvaltaisemmaksi ja nykypäivänä se on integroitu toimintaan ja ajatteluun (Erola & Louto 2000). Luvussa on tarkoitus esittää riskienhallinnan peruskäsitteitä, riskienhallintaprosessi ja lähtökohtia eri viitekehyksien kautta. Määrittämällä perusteet ja ymmärtämällä erilaiset vaatimukset, muodostuu niiden kautta riskienhallinnalle tavoitteet ja toimintamallin kehittäminen saa puitteet, joita voi tarkastella ja kehittää erilaisten viitekehysten avulla. Riskienhallinnan avulla pyritään muodostamaan riskikuva, jota päivitetään säännöllisesti ja muodostetaan kokonaiskuva epävarmuuksista, joita yrityksen toiminnassa ilmenee. (Ilmonen et al. 2016.)

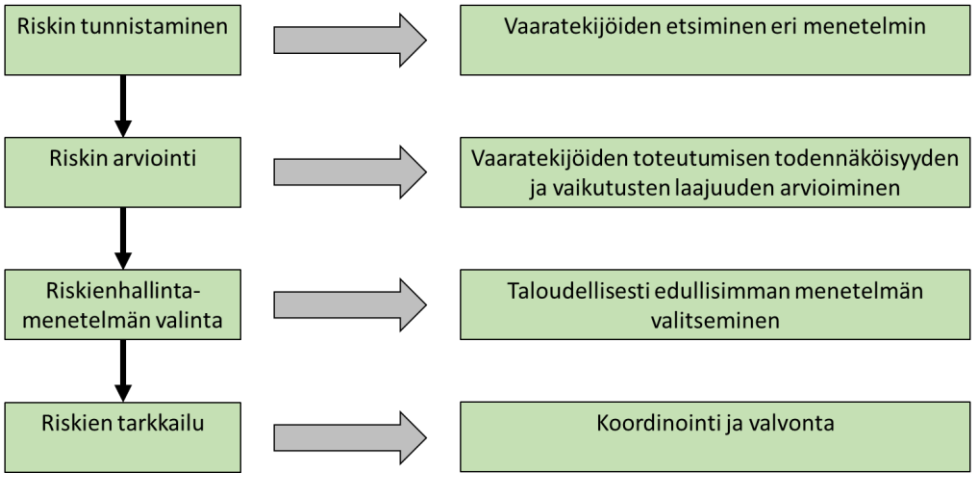
2.1 Riski ja riskienhallinnan määritelmät

Riskin määrittelyyn liittyen löytyy kirjallisuutta yhä enemmän ja enemmän, mutta yhteisymmärrystä, mitä riski tarkoittaa, ei löydy (Rosa 1998). Tapoja määrittelyyn on siis yhtä monta kuin tekijöitäkin ja ajansaatossa käsitystä on laajennettu niin ajallisilla, tilastollisilla kuin analyyttisillä ulottuvuuksilla, mutta yleensä riski mielletään äkillisen tapahtuman seurauksena jonkin mahdollisuuden menettämiseksi (Erola & Louto 2000). Rosa (1998) määrittelee riskin tilanteeksi tai tapahtumaksi, jossa jotain ihmiselle arvokasta on asetettu vaaraan ja jossa lopputulos on epävarma. ISO 31000 standardi määrittelee riskin epävarmuuden vaikutukseksi tavoitteisiin ja vaikutus voi olla niin myönteinen kuin kielteinenkin. ISO 31000 tuokin hyvin esiin sen, että riskiä ei pidä mieltää vain negatiivisena asiana, vaan pitää myös huomioida mahdollisuudet eli positiiviset riskit (Ilmonen et al. 2016). Juvonen (2005) esittääkin riskin määrityksen lähtökohdaksi, että tapahtumaan tulee liittyä epävarmuutta, koska jos tiedämme seuraukset tarkasti, tällöin se ei täytä riskin määritelmää. Aven&Renn (2009) ovat tutkimuksessaan todennut, että erilaisten riskimääritysten perusteella voidaan riskien ilmaisu jakaa kahden tyyppiseen kategoriaan:

1. Riski ilmaistaan todennäköisyyksien ja odotettujen arvojen avulla
2. Riski ilmaistaan tapahtuman / seurauksen ja epävarmuustekijän kautta.

Riskienhallinta on laajempi kokonaisuus, minkä avulla yritys pyrkii varautumaan tai estämään mahdolliset vahingot. Lyhyesti kuvattuna riskienhallinta on riskien tunnistamista, arvioimista, päätösten tekoa ja niiden toimeenpanemista. Kuvassa 2 on esitetty riskienhallinnan vaiheet yrityksessä ja näiden vaiheiden kautta riskienhallinnan tulisi vastata kysymyksiin: mitä, miksi, miten, millä eväin, milloin ja ketkä? Riskienhallinnassa syntyneen tiedon tavoitteena on jatkuvuuden varmistus, riskikustannusten optimointi ja liiketoimintamahdollisuuksien hyödyntäminen. (Juvonen 2005.) Itse riskienhallinnan tavoit-

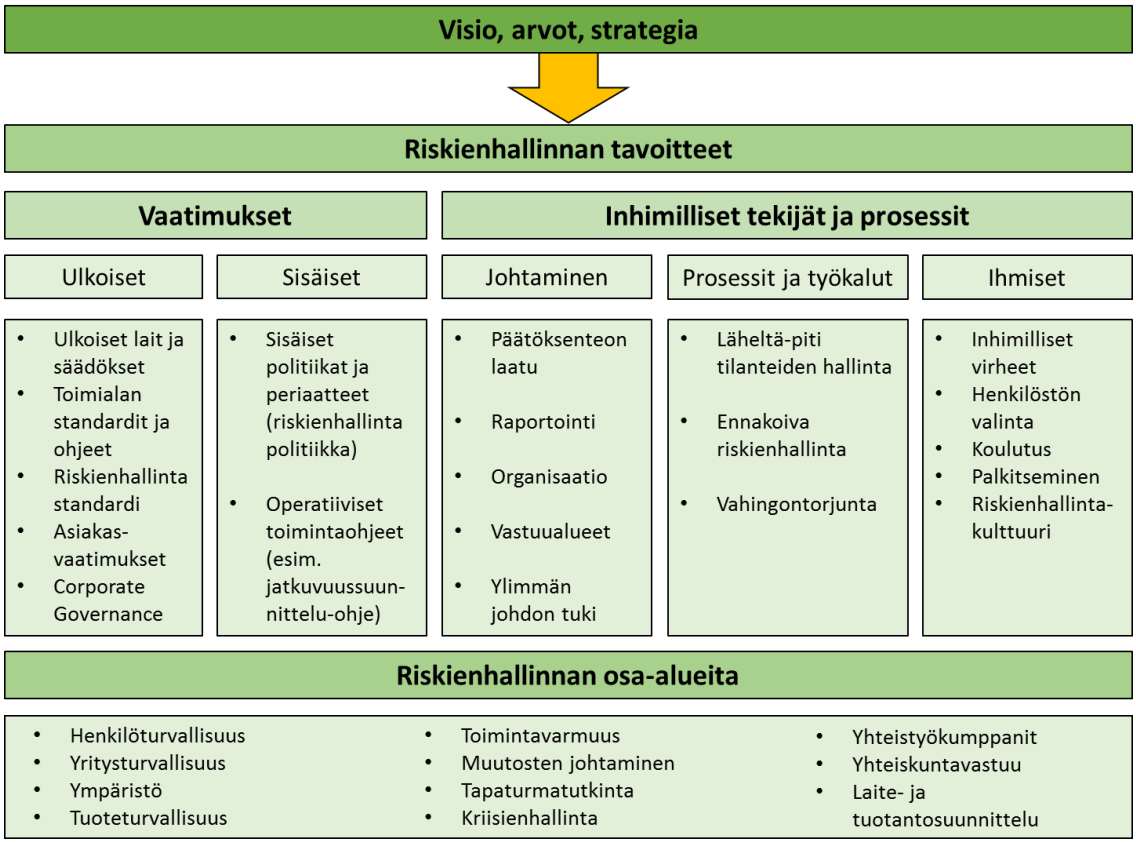
teisiin kuuluu löytää optimitaso riskienhallinnalle eli tavoiteltujen hyötyjen suhde käytettyihin kustannuksiin, pääomiin ja resursseihin (Ilmonen et al. 2016). ISO 31000 määrittelee riskienhallinnan koordinoiduksi toiminnaksi, jolla organisaatiota johdetaan ja ohjataan riskien osalta.



Kuva 2. *Riskienhallinnan vaiheet (mukaillen Juvonen, Korhonen et al. 2005).*

Riskienhallintaa on alun perin käytetty turvallisuus- sekä finanssialalla, josta liikkeenjohdon muutospaineesta näkökulmia on lähdetty laajentamaan kokonaisvaltaiseksi riskienhallinnaksi myös muilla aloilla (Erola & Louto 2000). Riskianalyysit ja riskienhallinta on tullut yhä enemmän kiinteäksi osaksi yleistä liiketoimintamallia ja nykyisin se on pakollinen vaatimus monissa rahoistussuunnittelu ja viranomaishyväksyntä tapauksissa. Myös monet asiakasorganisaatiot vaativat urakoitsijoiltaan mahdollisia riskejä sijoituksiin liittyen ja ilmoittamaan, että miten nämä riskit hoidetaan, jos niitä ilmenee. (Merna & Al-Thani 2008.) Shenkir&Walker (2011) ovat todenneet, että riskien ymmärtämisestä ja hallinnasta on tullut ehdoton tekijä onnistuneeseen johtamiseen tämän päivän maailmassa.

Riskienhallintaan vaikuttaa erilaiset vaatimukset niin ulkoisesti kuin sisäisestikin. Ulkoisia vaatimuksia ovat muun muassa lainsäädäntö, standardit, toimialan yleiset suositukset tai asiakkaalta tulleet mahdolliset vaatimukset. Sisäisiä vaatimuksia ohjaa yrityksen visio, strategia ja arvot, jotka muodostavat riskienhallinnalle perustan. Sisäisiin vaatimuksiin vaikuttaa myös yritys- ja riskienhallintakulttuuri sekä inhimilliset tekijät. (Ilmonen et al. 2016.) Kuvassa 3 on esitetty riskienhallinnan tavoitteisiin vaikuttavat tekijät sekä riskienhallinnan eri osa-alueita. Lähtökohtana on visio, arvot ja strategia ja siitä syystä hyvä lähtöasetelma on, että yrityksen ylin johto ja muut tärkeät osapuolet yrityksessä pyrkivät tunnistamaan riskejä (Riskit ja mahdollisuudet: käytännön neuvot riskien hallintaan, 2012). Määrittelemällä yrityksen toimintaympäristöön kuuluvien sidosryhmien vaatimukset ja odotukset sekä näihin liittyvät uhat ja mahdollisuudet, varmistetaan riskienhallinnan päämäärän ja arvioinnissa käytettävät kriteerien asettamiset tarkoituksenmukaisiksi yrityksen kannalta. (Kupi et al. 2009.)



Kuva 3. *Riskienhallinnan tavoitteet, vaatimukset ja osa-alueet (mukaillen Ilmonen 2016).*

Vaikka kiinnostus riittäisi vain yhteen osa-alueeseen tai tekijään, joita edellisessä kuvassa esitettiin, niin riskienhallinnan tulee silti pitää huoli, että tilannekuva päivitetään ennakoivana ja laaja-alaisena. Riskienhallinta on ennen kaikkea yrityksen johtamista ja kun sitä ajatellaan laajana käsitteenä, se kattaa koko yrityksen olemassaolon tarkoituksen. (Riskit ja mahdollisuudet: käytännön neuvot riskien hallintaan, 2012.) Kyse riskienhallinnassa on siis organisaation perusteellisesta analysoinnista eri tasoilla, epävarmuuden aiheuttamien tapahtumien kuvaamista ja päättämistä näiden riskien merkityksestä ja kehittämällä asianmukaisia toimenpiteitä niiden käsittelemiseksi. (MacLeod et al. 2012)

Mitä suurempi tai monimutkaisempi yritys on kyseessä, sitä enemmän se hyötyy riskiarvioinneista. Riskienhallinnan etuja on haastava määrittää, koska on vaikea väittää, että yrityksen riskienhallinta on estänyt esimerkiksi vakavan onnettomuuden tai tulipalon. Riskienhallinnalla avulla kuitenkin voi päättää mitä riskejä kannattaa ottaa ja mitä tulisi välttää. Kun riskienhallinta on mukautettu vastaamaan tarpeita, voidaan sitä hyödyntää henkilöstön kouluttamisessa ja muodostaa syvempi ymmärrys kohdistuvista riskeistä. Riskienhallinta auttaa yritystä välttämään kustannuksia, häiriöitä ja onnettomuuksia. (Sadgrove 2016.)

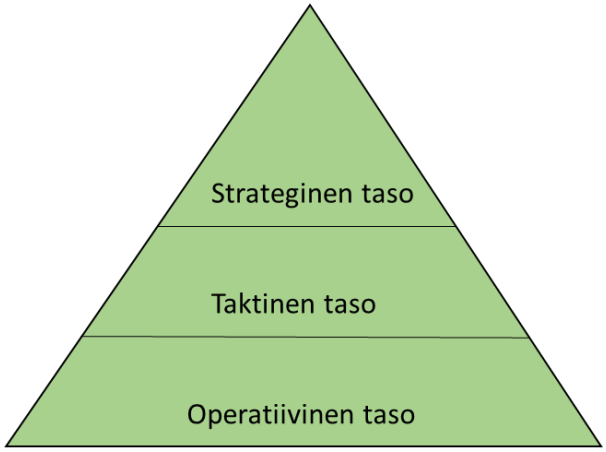
2.2 Kokonaisvaltainen riskienhallinta

Kokonaisvaltainen riskienhallinta on noussut modernin yrityksen johdon työkaluksi. Kaikki lähtee liikkeelle strategiasta ja arvoista, nämä luovat perustan kokonaisvaltaiselle riskienhallinnalle, jota toteutetaan koko liiketoiminnan laajuudessa ja usein tarkastelukohteena on strategisten tavoitteiden saavuttamisessa. Riskienhallinta ei ole turhaa hallinnollista harjoitusta, vaan tarkoituksena on tuottaa arvoa yrityksen eri sidosryhmille kuten omistajille, asiakkaille ja viranomaisille sekä lisätä markkinoilla luottamusta. (Ilmonen et al. 2016.) Statement on Management Accounting (SMA) onkin määritellyt kokonaisvaltaisen riskienhallinnan tavoitteeksi ”luoda, suojata ja parantaa osakkeenomistajan arvoa hallitsemalla epävarmuustekijöitä, jotka voisivat vaikuttaa negatiivisesti tai positiivisesti organisaation tavoitteiden saavuttamiseen”. Osakkeenomistajan sijaan osa saattaa käyttää ennemmin termiä sidosryhmä. (Shenkir & Walker 2011.)

Erolan ja Loudon (2000) mukaan kokonaisvaltaisella riskienhallinnalla pyritään yhdistämään eri näkökulmat organisaation liiketoimintojen välillä. Tyypillisesti yrityksissä riskienhallinta on järjestetty niin kutsutulla ”siilo” ajattelulla eli operatiivinen johto hoitaa erilaisia operatiivisia riskejä ja tietotekniikkaryhmä hoitaa turvallisuus- ja järjestelmäriskejä, jokaisella siilolla on selkeä oma tehtävänsä. Muuttuvassa maailmassa yritykseltä vaaditaan ymmärrystä, että miten näitä riskejä hallitaan monien yksittäisen siilojen sijaan kokonaisvaltaisesta ja integroidusta näkökulmasta. (Shenkir & Walker 2011.) Siilot useimmissa tapauksissa palastelevat tietoa ja vastuuta tehokkaasta riskienhallinnasta (Kaplan & Mikes 2012). Kokonaisvaltaisella riskienhallinnalla varmistetaan, että eri näkökulmista erotetaan oleelliset asiat epäoleellisista strategian kannalta. Tällöin johdolle saadaan tuotettua tietoa organisaation riskitilanteista ja tulevaisuudesta. (Erola & Louto 2000.) Saadun tiedon pohjalta taas voidaan hallita ja pienentää riskejä eri sidosryhmien eduksi ja tunnistaa organisaation avainriskit (Shenkir & Walker 2011). Tavoitteena on siis huomioida olennaisia vaikuttavuustekijöitä yrityksen toimintaan kaikilla yrityksen tasoilla ja tätä prosessia suorittaa ylin toimiva johto sekä kaikki työntekijät organisaatiossa (Ilmonen et al. 2016).

Yrityksen toiminnan tasot voidaan jakaa kolmeen eri osaan, joista muodostuu liiketoiminnan johtamiseen riskikehys. Tasot ovat strateginen, taktinen ja operatiivinen, joiden näkökulmasta riskejä tarkastellaan (kuva 4). Koko liiketoiminnalle kohtalokas on strategisen riskin toteutuminen. Strategisella tasolla riskit ovat suuria ja varsinkin jos strategiaa muutetaan, tällöin syntyy täysin uusia tuntemattomia riskejä. (Riskit ja mahdollisuudet: käytännön neuvot riskien hallintaan, 2012.) Taktisen tason riskit ovat juoksevan liiketoiminnan riskejä, jotka liittyvät strategian toteuttamiseen käytännössä (Riskiblogi 2017). Operatiivisen tason riskit syntyvät päivittäisen toiminnan työstä strategiaa ja suunnitelmia toteuttaessa ja tämän tason riskeissä korostuu kokemus ja aiemmat tehdyt virheet (Riskit ja mahdollisuudet: käytännön neuvot riskien hallintaan, 2012). Tärkeää on, että näiden

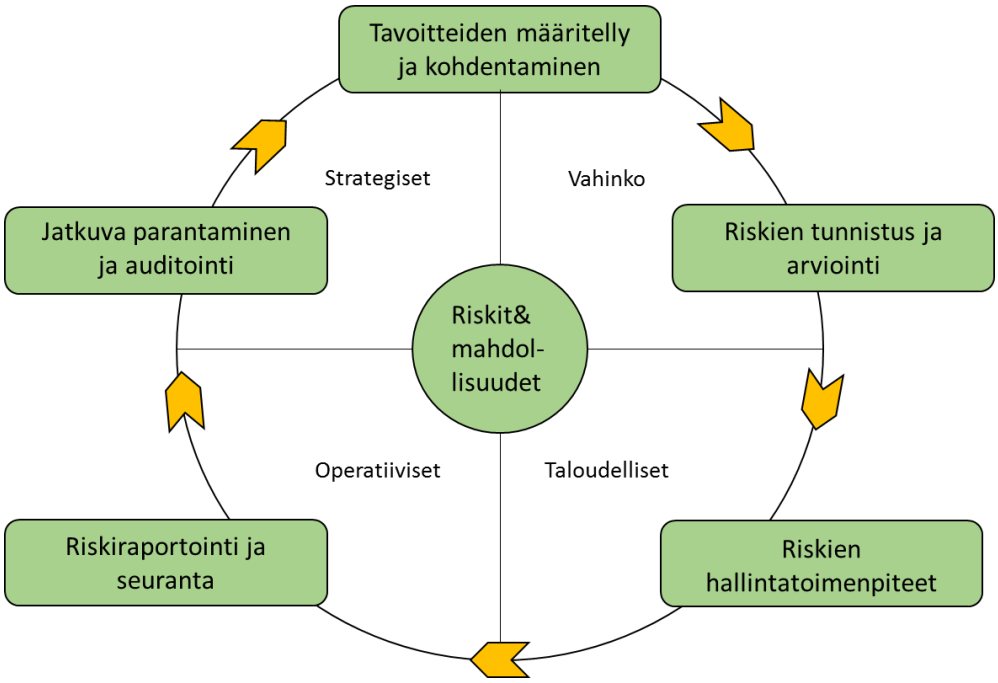
tasojen välillä on toimiva viestintä ja riskit huomioidaan kokonaisuutena. Operatiiviselta tasolta voi nousta strategisesti hyvinkin merkittäviä riskejä esiin. (Riskiblogi 2017.)



Kuva 4. *Yrityksen toiminnan tasot (mukaillen riskiblogi.fi 2017).*

2.2.1 Riskienhallintaprosessi

Kuvassa 5 on Ilmosen (2016) malli riskienhallintaprosessista, jossa on huomioitu karkeasti riskienhallintaprosessin eri vaiheet. Lähtökohta riskienhallintaprosessin luomiseen ja kehittämiseen on tavoitteiden määrittely esimerkiksi riskienhallintapolitiikan kautta. Riskienhallintapolitiikan määrittelee johto ja siinä kuvataan riskienhallinnan perusteet ja toimenpiteet. Riskienhallintapolitiikan avulla luodaan riskienhallinnalle tavoitteet sekä selkeät toimintaohjeet. (Juvonen 2005.) Riskienhallintapolitiikka yleensä sisältää tavoitteiden lisäksi määritelmät vastuista, tunnistamis-, arviointi- ja kontrollimenetelmistä sekä raportointiperiaatteista. Politiikkaa luotaessa on huomioitava, että se ei saa olla ristiriidassa muiden säännöstöjen ja toimintaa ohjaavien periaatteiden kanssa. (Kupi et al. 2009.)



Kuva 5. *Riskienhallintaprosessi (mukaillen Ilmonen 2016).*

Tavoitteiden määrittelystä siirrytään riskien tunnistamiseen ja arviointiin, joiden tuloksena syntyy lisätietoa ja kattava listaus yrityksistä löytyvistä riskeistä (Kupi et al. 2009). Tärkeintä onkin tunnistaa riskit, vaikka kaikkia niitä ei pystyisikään hallitsemaan, mutta riskin tunnistus mahdollistaa sen tarkkailun (Ilmonen et al. 2016). Arvioinnissa tulee selvittää riskin todennäköisyys ja seuraukset (Kupi et al. 2009). Tapahtuman todennäköisyys liiketoiminnassa on usein peräisin historiasta ja siitä kerätystä datasta, mutta se voi myös perustua asiantuntijoiden lausuntoon, jolloin riskin arviointiin vaikuttaa inhimilliset arvostelut sekä tilastollisten työkalujen soveltuvuus (Walker 2013). Jokainen hahmottaa riskit eri tavalla riippuen kokemuksesta, tilanneyhteydestä ja osaamisesta. Arviointiin vaikuttaa myös ihmisen sisäinen maailma, jolloin riskin arviointi ja esittämistapa riippuu korostaako henkilö todennäköisyyttä, vakavuutta vai molempia. Usein henkilöt, jotka painottavat vakavuutta, huomioivat merkittäviä uhkia ympäristössään ja näiden riskien todennäköisyys on pieni, mutta ihmiset haluavat välttää nämä riskit. (Juvonen 2005.) Seuraukset voidaan ilmaista aineellisina tai aineettomina yksikköinä ja yhdellä tunnistetulla riskillä voi olla monia erilaisia seurauksia ja vaikutusta tavoitteisiin. Riskin arviointi vaiheeseen kuuluu myös riskin merkityksen arviointi eli mitkä tunnistetuista riskeistä ovat oleellisia yrityksessä ja mikä on riskien tärkeysjärjestys siirryttäessä hallintatoimenpiteisiin. (Riskikompassi 2017.)

Arvioitujen riskien osalta niille määritellään hallintatoimenpiteet (Ilmonen et al. 2016). Hallintatoimenpiteitä voivat olla riskin välttäminen, poistaminen, todennäköisyyden tai seurauksen pienentäminen, jakaminen, seuranta tai riskin ottaminen mahdollisuuden hyödyntämiseksi. Hallintatoimenpiteen valintaan kuuluu myös valitun käsittelytavan vaikuttavuuden arvioiminen eli onko päätetyn hallintakeinon jälkeinen riskitaso hyväksyttä-

vissä. Hallintakeinon valintaan vaikuttaa myös kustannushyötysuhde eli mikä on toimenpiteen vaatima kustannus saatuun hyötyyn. Hallintatoimenpiteitä valittaessa tulee myös huomioida, että syntyykö siitä uusia riskejä niin kutsuttuja seurausriskejä, jolloin ne tulee käsitellä alkuperäisen riskin kanssa. (Riskikompassi 2017.)

Rautanen (2011) toteaa, että jälkiviisaus ei ota huomioon vallitsevaa ajankohtaa, tilannetta, toimintaympäristöä eikä tavoitteita, tästä syystä riskejä tulee raportoida ja seurata systemaattisesti. Seurannan tulisi kattaa koko riskienhallintaprosessin, jotta hallintakeinojen vaikuttavuutta voidaan seurata, havaita muutokset toimintaympäristössä, tunnistaa uusia riskejä ja uudelleen arvioida jo tunnistettuja riskejä (SFS-ISO 31000:2009). Seurannan tuloksia voidaan raportoida yrityksessä eri tasoille kuten hallitukselle, yrityksen johdolle tai operatiiviselle tasolle, raportoinnin taso vaikuttaa riskiraportin sisältöön ja laajuuteen. Hallitukselle raportoidaan usein kooste kriittisimmistä riskeistä ja niiden kehittymisestä, kun taas operatiivisella tasolla riskejä voidaan raportoida viikkopalavereissa käymällä läpi omia riskejä tai läheltä piti – tilanteita. (Ilmonen et al. 2016.) Seuranta mahdollistaa myös suorituskyvyn mittarin, kun riskienhallintaprosessin toteuttamista seurataan ja parhaimman hyödyn saa, kun mittarit yhdenmukaistetaan organisaation toimintamittariston kanssa (Riskikompassi 2017). Auditoimalla prosessia varmistetaan prosessin jatkuva kehittäminen. Jatkuvalle kehittämiselle voidaan asettaa tavoitteita kuten toimintojen yhdenmukaisuus, riskienhallinnan kattavuus ja varmistaa jatkuva kehittäminen. (Ilmonen et al. 2016.) Jatkuvaa kehittämistä ja riskienhallintaprosessin toimivuutta voidaan arvioida esimerkiksi toimintajärjestelmän auditoinnin yhteydessä (Kupi et al. 2009).

Ilmonen (2016) toteaa, että tärkeintä riskienhallintaprosessissa on se, että se etenee systemaattisesti ja tulee huomioida, että se on jatkuva silmukka (loop) eikä lineaarinen prosessi (Merna & Al-Thani 2008). Ehdoton edellytys riskienhallintaprosessille on, että yrityksen johto on aktiivisesti ja näkyvästi sitoutunut siihen sekä se on yhdistetty ja sovitettu yrityksen muuhun toimintaan, varsinkin hallintatoimet ja raportointi (Ilmonen et al. 2016). Näiden lisäksi riskienhallintaprosessin yhteydessä tulee tarkastella, että se ei muutu pelkäksi riskilistaukseksi vaan tehdään riskienhallintaa. Jos analyysissä ilmenneille riskeille ei ole tarkoitus mitään toimenpiteitä tehdä ja tarkoitus on lähinnä vain tuottaa tietoa kohdistuvista riskeistä, tällöin tehdään niin kutsuttua list managementia. (Riskit ja mahdollisuudet: käytännön neuvot riskien hallintaan, 2012.) Tähän tilanteeseen ajaudutaan melko helposti, jos riskienhallinnan tavoitteeksi on asetettu tunnistaa kaikki yritykseen liittyvät riskit. Riskien käsittelyyn ja hallintaan vaaditaan aikaa, joka jää tällöin vähemmälle. Riskien tarkastelutarkkuutta kannattaakin tarkentaa ja asettaa tavoite esimerkiksi strategiaa tai vuosi tavoitteitta hyödyntäen ja tunnistaa uhkaavia tekijöitä niitä vasten. (Ilmonen et al. 2016.) Lasse Väisäinen (2012) sanoo käytännön neuvot riskien hallintaan kirjan artikkelissa, että riskien arviointi ilman järjellistä asiaa vasten on vaikeaa ja turhaa. Tällöin arvioinnissa on haastava ymmärtää seuraukset, jos riski toteutuu. Riskienhallintaprosessin tavoitteena on kuitenkin tuottaa systemaattisesti tietoa johtamisen ja päätöksenteon tueksi eikä pelkästään listausta uhkaavista tekijöistä.

2.2.2 Viitekehykset riskienhallinnalle

Viitekehys helpottaa keskustelua keskeisistä periaatteista riskienhallinnan ja liikkeenjohdon välillä osana strategian suunnittelua ja toteuttamista. Tämä tuo riskienhallinnan toimintatapoihin ne tarkoituksenmukaiset ja aidosti arvoa tuottavat tekijät (Riskienhallinta modernisoituu - PwC:n Uutishuone 2018). Viitekehyksiä riskienhallintaan on luoto lukuisia ja lähestymistapoja on erilaisia soveltuen eri alojen organisaatioihin. Eroja viitekehyksissä löytyy myös tavasta esittää kehyksen toimintamalli, osa julkaisuista on pakottavia toimimaan tietyllä tapaa ja toiset taas ohjeistavia. Pääasiassa ERM viitekehykset ovat melko samanlaiset ja tietyt komponentit löytyvät melkein jokaisesta kehyksestä. Se millä tapaa organisaatio lähtee kehittämään omaa riskienhallintaan, kehyksen valintaan vaikuttavat, että se sopii yrityksen kulttuuriin, johtamisenfilosofiaan, tarpeisiin, kykyyn ja kokoon. (Shenkir & Walker 2011.) Tärkeintä valinnassa on varmistaa, että organisaatiossa ymmärretään termit samalla tavalla sekä jatkuva parantaminen ja toimivuus ovat toiminnan tavoitteena. Yleisimmin käytetyt viitekehykset ovat Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management (COSO ERM) ja ISO 31000 (Ilmonen et al. 2016). Muita viitekehyksiä ovat muun muassa Risk Management Standard by Federation of European Risk Management Association (FERMA), Basel II, Standard & Poor's and ERM. Kaksi viimeistä mainittua on kehitetty sopivammaksi finanssialan organisaatioille (Shenkir & Walker 2011).

ISO 31000 viitekehyksenä

Riskienhallinta ISO 31000 viitekehyksen on kehittänyt International Organization of Standardization (ISO) liiton tekninen riskienhallintatyöryhmä ja standardista julkaistiin päivitetty versio keväällä 2018. Standardin tarkoituksena ei ole edistää eri organisaatioiden yhdenmukaistavaa riskienhallintaa, määräämään johtamisjärjestelmän rakennetta tai käyttämään standardia sertifioinnin perustana. Se sisältää vaatimusten sijaan ohjeita, jotka antavat yritykselle joustavuutta toteuttaa riskienhallintaa omaan organisaatioon ja tavoitteisiin sopivaksi. (The new ISO 31000 keeps risk management simple 2018.)

Standardi korostaa arvon luomista ja säilyttämistä organisaatiossa riskien hallinnalla ja se nähdään apuna strategian määrittelyssä, tavoitteiden saavuttamisessa ja päätösten tekemisessä. Uusi versio standardista korostaa johtajuutta ja se on keskeinen tekijä kaikissa organisaation toiminnoissa sekä johtamisessa kaikilla tasoilla. Vaikuttavan ja tehokkaan riskienhallinnan ominaisuuksia on kuvattuna periaatteina, jotka toimivat perustana puitteille ja riskienhallintaprosessille. Periaatteilla pyritään hallitsemaan epävarmuuden vaikutusta tavoitteisiin ja niitä on kuvattu kahdeksan kappaletta:

- Sisällytetty organisaation johtamisjärjestelmään
- jäsennelty ja kattava toimintamalli
- räätälöity organisaatioon sopivaksi
- sidosryhmät huomioiva
- oikealla tavalla ja oikeaan aikaan muutoksiin reagoiva

- paras saatavilla oleva tieto
- inhimilliset ja kulttuuriset tekijät
- jatkuva kehittäminen. (SFS-ISO 31000:2018.)

Standardissa kuvataan myös puitteet, joiden avulla pyritään sisällyttämään riskienhallinta keskeisiin toimintoihin ja tehtäviin. Kaiken keskiössä on johtajuus ja johtajien sitoutuminen riskienhallintaan. Puitteita kehittäessä ylin johto on vastuussa riskienhallinnasta ja yrityksen hallitus taas sen valvonnasta. Hallitukselta usein odotetaan, että riskit huomioidaan asianmukaisesti, kun tavoitteita asetetaan, ymmärtää riskit jotka tavoitteita uhkaa ja varmistaa, että riskit ovat tarkoituksenmukaisia tavoitteisiin nähden. Standardin mukaan riskienhallinnan tulisi olla osa strategiaa, tavoitteita, hallintotapaa ja toimintoja sekä riskienhallinta on mukautettu kulttuuriin ja tarpeisiin sopivaksi. (SFS-ISO 31000:2018.)

Itse riskienhallintaprosessi tulisi olla osa johtamista, kulttuuriin ja käytäntöön sisällytetty sekä mukautettu sopivaksi liiketoimintaprosesseihin. Prosessi on jatkuva ja siihen kuuluu menettelyjen ja käytäntöjen soveltaminen tiedonvaihdossa, toimintaympäristön määrittelyssä, riskin arvioinnissa, seurannassa ja raportoinnissa. (SFS-ISO 31000:2018.)

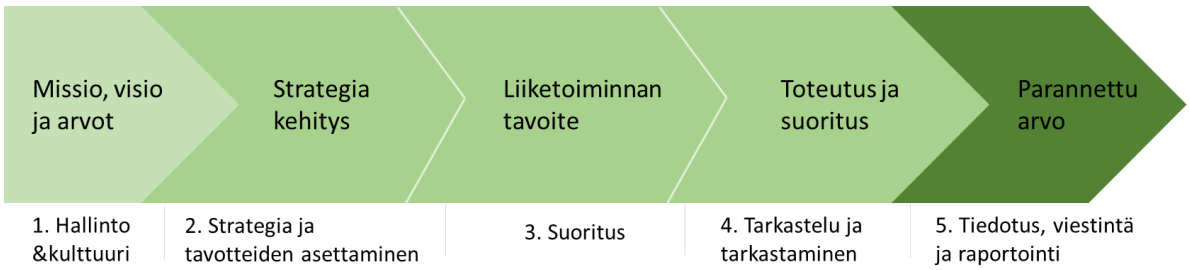
COSO ERM viitekehyksenä

COSO on riippumaton yksityisen sektorin toimija, joka on perustettu vuonna 1985. Alun perin viitekehys on luotu 2004, mutta päivitetty versio julkaistiin syksyllä 2017. Aiempi versio korosti sisäisen tarkistuksen roolia, mutta päivitetty versio tuo strategian merkitystä enemmän esiin ja strategian tulee tukea organisaation missiota ja visiota, jotka toimivat kokonaisuuden ja suorituskyvyn ohjaavina tekijöinä. COSO ERM tuokin mukaan kaksi lisänäkökulmaa, joilla voi tarkastella miten arvokehitykseen vaikuttavia riskejä syntyy strategiasta sen suunnitteluvaiheessa. Nämä näkökulmat ovat strategiavalinnan seuraukset ja strategian mahdollisuus, ettei se ole linjassa mission ja vision kanssa. Tämän jälkeen vasta siirrytään perinteiseen riskienhallintaan, jossa mietitään mitä riskejä liittyy jo valittuun strategiaan. (COSO 2017.)

Riskienhallinnan integrointi strategiaan ja tulokseen selventää yrityksen riskienhallinnan merkitystä strategisessa suunnittelussa ja sen sisällyttämisessä koko organisaatioon, koska riski vaikuttaa ja yhdenmukaistaa strategiaa ja suorituskykyä kaikilla osastoilla ja toiminnoilla. Viitekehys on esitetty kuvassa 6, se sisältää viisi eri osa-aluetta, jotka koostuvat eri periaatteista. Nämä periaatteet kattavat kaiken hallintotavasta seurantaan. Ne ovat helposti hallittavissa ja kuvaavat käytäntöjä, joita voidaan soveltaa eri tavoin eri organisaatioissa koosta tai toimialasta riippumatta. Näiden periaatteiden noudattaminen voi antaa johdolle ja hallitukselle järkevän odotuksen siitä, että organisaatio ymmärtää ja pyrkii hallitsemaan strategiansa ja liiketoiminnan tavoitteisiin liittyviä riskejä. (COSO 2017.)

Hallinnointi asettaa organisaation sävyn riskienhallinnalle vahvistamalla sen merkitystä ja asettamalla valvontavelvollisuudet. Kulttuuri liittyy eettisiin arvoihin, haluttuun käyt-

täytymiseen ja yhteisymmärrykseen liittyvistä riskeistä. Strategia ja tavoitteiden asettaminen toimivat yhdessä strategisen suunnitteluprosessin aikana. Riskihalukkuus luodaan ja yhdenmukaistetaan strategian kanssa. Liiketoimintatavoitteet asettavat strategian käytäntöön ja toimivat samalla pohjana riskin tunnistamiseksi, arvioimiseksi ja reagoimiseksi. Riskit on tunnistettava ja arvioitava, jotka voivat vaikuttaa strategian ja liiketoimintatavoitteiden saavuttamiseen. Riskit priorisoidaan riskinottohalun mukaan ja valitaan niille toimenpiteet. Tämän prosessin tulokset raportoidaan avainasemassa oleville sidosryhmille. Tarkastelemalla organisaation suorituskykyä organisaatio voi selvittää, kuinka hyvin yrityksen riskienhallinnan komponentit toimivat ajan myötä, merkittävien muutosten ilmetessä ja mitä uudistuksia tarvitaan. Yrityksen riskienhallinta edellyttää jatkuvaa prosessia hankkia ja jakaa tarvittavat tiedot sekä sisäisistä että ulkoisista lähteistä koko organisaatiossa. (COSO 2017.)



Kuva 6. *COSO ERM viitekehys mukaillen COSO (2017).*

Viitekehyksen tavoitteena on optimoida strategiaa ja suoritusta ja ERM:n avulla voidaan saavuttaa:

- Mahdollisuuksien määrään kasvattamista, kun huomioidaan riskin positiivinen ja negatiivinen puoli
- riskien tunnistus ja hallinta laaja-alaisesti
- kasvattaa positiivisia tuloksia ja hyötyjä sekä pienentää negatiivisia vaikutuksia
- suorituskyvyn parantumista, kun häiriöt minimoidaan
- edistää resurssien käyttöä
- joustavuuden parantuminen.

Nämä hyödyt korostavat sitä, että riskiä ei pidä tarkastella pelkästään mahdollisena rajoituksena tai haasteena strategian asettamisessa ja toteuttamisessa. Pikemminkin muutokset riskien taustalla luovat strategisia mahdollisuuksia ja keskeisiä kykeneväisyyksiä. (COSO 2017.)

Päivitetyillä viitekehyksillä on hyvin paljon samoja piirteitä, mutta eroavaisuuksia löytyy. Molemmat viitekehykset korostavat kulttuurin merkitystä riskienhallintaan sekä johtajuutta. COSO ERM tuo enemmän esiin riskienhallinnan näkyvyyttä strategiaprosessissa. Merkittävin ero on itse riskin määritelmässä. COSO ERM puhuu erikseen riskistä ja mahdollisuudesta kuin taas ISO 31000 määrittää riskin epävarmuuden vaikutuksesta tavoitteisiin eli sanassa riski on molemmat puolet mukana.

2.3 Riskiperusteinen ajattelu

Riskienhallintaa ja riskiperusteista lähestymistä velvoittavia lakeja ja säädöksiä on monia, mutta yrityksiä koskevia ovat esimerkiksi työturvallisuuslaki (738/2002), henkilötietolaki (523/1999) ja uusimpana EU:n tietosuoja-asetus (EU 679/2016). (VM 22/2017 Liitteet 1-6.) Lisäksi yritykset, jotka ovat laatusertifioituja, heitä koskevat uuden standardin (ISO 9001:2015) myötä riskiperusteisen ajattelutavan huomioiminen toiminnassa. Kuten jo aiemmin kuvattiin, että riskienhallinta on kehittynyt merkittävästi vuosien saatossa ja nyt osa syynä voi olla käytössä oleva uusi termi VUCA eli Epävakaus, Epävarmuus, Monimutkaisuus, Monimerkityksisyys. (**V**olatility, **U**nsertainity, **C**omplexity, **A**mbiguity). Termi kuvaa melko täydellisesti mitä globaalissa bisneksessä tapahtuu, koska mikään ei ole varmaa ja johtajien täytyy elää tämän kanssa (Bill George 2017). Riskit siis kasvavat ja uudistetussa standardissakin ennaltaehkäisevät toimet on muutettu ajattelulla riskit ja mahdollisuudet, jolloin ennakoidaan eikä muuteta toimintatapa vasta kun jotain tapahtuu.

Standardin asettamat vaatimukset ovat listattuna taulukossa 1. Kuten johdannossa jo todettiin, että uusin versio standardista ei vaadi muodollista riskienhallintajärjestelmää, mutta riskiperusteinen ajattelu tulee ottaa lähestymistavaksi organisaatiossa. Riskit esiintyvät monessa kohtaa standardia, mutta tiivistetysti riskeille ja mahdollisuuksille, joilla on olennainen vaikutus strategian kannalta tai kykyyn täyttää järjestelmän tavoitteet, tulee määrittää toimenpiteet riskien käsittelyyn sekä tarkastella niiden vaikuttavuutta eri yhteyksissä kuten johdon katselmuksessa ja poikkeaman tapahtuessa. Uusi standardi ei pelkästään käsittele riskiä vaan vaatii myös tunnistamaan mahdollisuuksia. Tällöin yrityksen tulee myös miettiä, että voidaanko ongelma muuttaa tilaisuudeksi. (BSI 2015b.) Organisaatioiden on ymmärrettävä riskien kokonaisvaltainen taso niiden prosessien ja toimintojen sisällä. Riskin käsite ISO 9001 -standardin yhteydessä liittyy järjestelmien tavoitteiden saavuttamiseen liittyvästä epävarmuudesta, joka on asiakkaiden vaatimusten mukaisten tuotteiden ja palveluiden tuottaminen (BSI 2015a).

Taulukko 1. *ISO 9001:2015 vaatimukset riskien käsittelyyn laadunhallintajärjestelmässä.*

ISO 9001:2015 vaatimukset riskiperusteiselle laadunhallintajärjestelmälle	
Kohta 4	Organisaation on määriteltävä riskit, jotka voivat vaikuttaa sen kykyyn täyttää järjestelmän tavoitteet
Kohta 5	Ylimmän johdon on osoitettava johtajuutta ja sitouduttava varmistamaan, että tuotteen tai palvelun vaatimustenmukaisuuteen vaikuttavat riskit ja mahdollisuudet määritetään ja käsitellään.
Kohta 6	Organisaation on ryhdyttävä toimiin riskien ja mahdollisuuksien tunnistamiseksi ja suunniteltava, miten käsitellä tunnistetut riskit ja mahdollisuudet
Kohta 8	Organisaation on suunniteltava, toteutettava ja ohjattava prosessit käsittelemään kohdassa 6 määritettyjä toimia.
Kohta 9	Organisaation on valvottava, mitattava, analysoitava ja arvioitava riskejä ja mahdollisuuksia.
Kohta 10	Organisaation on parannettava jatkuvasti soveltuvuutta vastaamalla riskien muutoksiin

Tässä luvussa tuotiin esiin riskienhallinnan kehittymistä yhden toimialan tarpeista kokonaisvaltaiseksi näkemykseksi kaikille toimialoille. Yksi iso tekijä riskienhallinnan laajentumisesta monille toimialoille on ISO standardien päivittyminen riskiperusteiseksi. Muutos ei näy pelkästään ISO 9001 standardissa vaan myös ympäristöjärjestelmä ISO 14001 sekä keväällä 2018 tullut uusi työterveys- ja työturvallisuusjärjestelmät ISO 45001 standardit vaativat huomioimaan riskit, jotta voidaan taata haluttujen tulosten saavuttaminen, estää tai vähentää ei-toivottuja vaikutuksia sekä saada aikaan jatkuvaa parantamista. Standardit vaativat tarkastelemaan riskejä ja mahdollisuuksia nimenomaan organisaation toimintaympäristön ja sidosryhmien tarpeiden ja vaatimusten näkökulmasta. (SFS-EN ISO 9001:2015; SFS-EN ISO 14001:2015; SFS-ISO 45001:2018.) Tässä luvussa tuotiin esiin myös sanan “riski” monet muodot. Pelkästään jo viitekehykset määrittävät riski sanan eri tavalla ja tämän lisäksi jokainen henkilö kokee riskin ja siihen liittyvät tekijät eri tavalla. Tärkeää onkin muodostaa yrityksessä yhteinen mielikuva riskistä ja sisällyttää tämä johtamiseen ja kulttuuriin.

3. TIEDON TUOTTAMINEN YRITYKSEN JOHDOLLE RISKIENHALLINNAN AVULLA

Kun useampi yrityksen työntekijä tai omistaja käy keskustelua perusteista päätöksenteolla ja niihin liittyvistä olettamuksista, tarvitsevat he tietoa mahdollisista riskeistä (Ilmonen et al. 2016). Jotta yrityksen johto voi ymmärtää ja hallita riskejä, tulee sen saada tietoa niistä. Tässä kohtaa riskienhallinta on kommunikoinnin ja vuorovaikutukset väline, jolla tuotetaan tietoa päätöksenteontueksi, arvioidaan päätöksiä ja kehitysaskelia ja tuodaan lisäarvoa toimintaan. Tietoa mitä riskienhallinnan työkalut tuottavat, ovat riippuvaisia yrityksen kulttuurista ja hallituksen puheenjohtajan sekä toimitusjohtajan johtamisideologiasta. (Ilmonen et al. 2016.)

Riskienhallinnan avulla luodaan näkökulmia johtamiseen, tulevaisuuteen ja sen avulla voidaan parantaa laatua sekä vahinkoja ja tappioita pystytään vähentämään. Riskienhallinnan prosessia ei kuitenkaan tule hienosäätää liian paljon vaan pitää se yksinkertaisena ja organisaatioon soveltuvana. Riskienhallinnalla luodaan tietoa, joka tarjoaa organisaatioon kehittämisvälineet ja vaihtoehdoille voidaan antaa painoarvoa ja lisäulottuvuuksia. (Rautanen 2011.) Pitkänajan tähtäimeksi tulee asettaa, että riskienhallinta on tehokkaasti hyödynnetty päätöksenteonprosessissa ja työntekijöillä on ymmärrys riskienhallinnan tiedon tuomasta lisäarvosta yritykselle (Ilmonen et al. 2016).

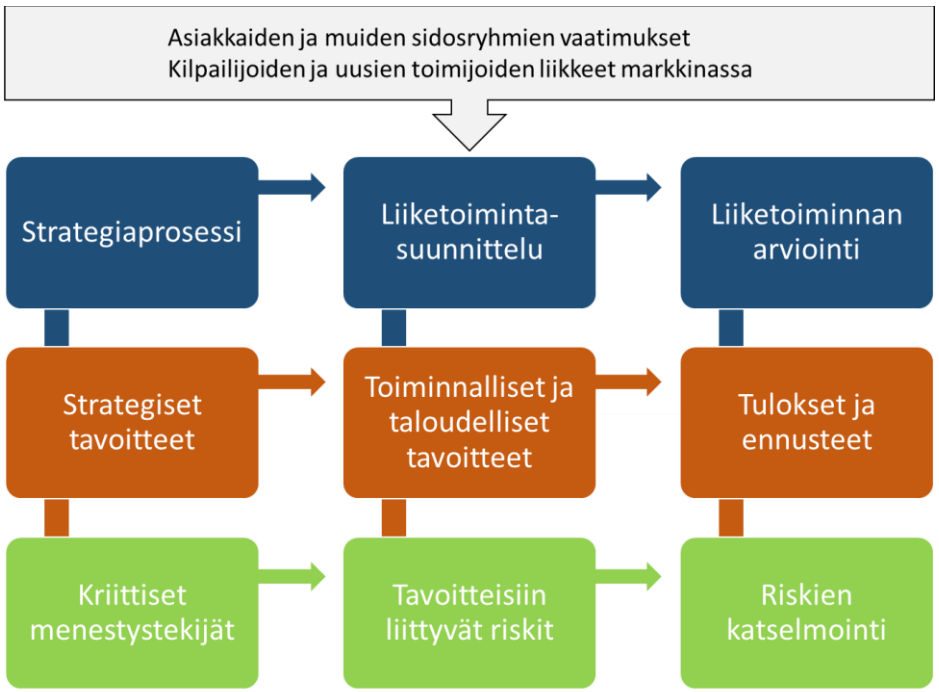
AON (2007) on tutkimuksessaan todennut, että toimivan kokonaisvaltaisen riskienhallinnan taustalla on kolme keskeistä osa-aluetta: strategia, kulttuuri ja resurssit. Nämä kolme tekijää aiheuttavat myös haasteita, kun yritykset pyrkivät ottamaan kokonaisvaltaisen riskienhallinnan käyttöön organisaatiossaan. Seuraavassa luvussa on tarkoitus esitellä toimivan ja tehokkaan riskienhallintajärjestelmän malli, jonka pohjalta voidaan lähteä tarkastelemaan ja kehittämään yritykseen riskienhallintaa. Malli tuodaan esiin tiedon tuottamisen ja hyödyntämisen näkökulmasta, mikä vaikutus yrityksen johdolla tässä kohtaa on ja miten johto voi tätä tietoa hyödyntää.

3.1 Kokonaisvaltaisen ja toimivan riskienhallintajärjestelmän malli

Kun yritys päättää aloittaa hallitsemaan riskejä, on selvää, että riskienhallinta on toteutettava jäsennetyllä tavalla ja integroitava koko yritykseen. Tämä edellyttää huomioida useita tekijöitä kuten riskin määrittely, riskienhallinnan roolin määritys, määriteltyjä toleransseja, toimintatapoja ja ohjeita riskien käsittelemiseksi, riskien sisällyttämisen liiketoimintaan ja päätöksentekoon sekä johdonmukaisen raportoinnin. Riskienhallinnan tulee

olla kattavaa ja kommunikoivaa, jotta ymmärretään riskien kytkökset ja seuraukset muihin tekijöihin. Pitää myös osata hallita riskiä liiketoimintastrategian näkökulmasta ja ymmärtää, että kaikki riskit eivät ole huonoja. (Abrams et al. 2007.)

Kuvassa 7 on esitettynä riskienhallinnan kytkökset liiketoimintaprosessiin. Liiketoiminnan riskit syntyvät joko sisäisistä prosesseista tai sidosryhmiltä ja markkinoilta tulevasta toimintaympäristöstä. Kun riskienhallintaa tarkastellaan osana johtamista ja liiketoimintaa, se ulottuu strategiaprosessista arkirutiineihin. Riskien kytkentä liiketoimintaprosessiin onnistuneesti antaa johdolle ennakoivan ohjausvälineen ja luo heille tiedon mitä uhkia ja mahdollisuuksia liiketoiminnassa esiintyy. (Juvonen et al. 2014.) Liittämällä riskienhallinnan liiketoiminnanprosesseihin saavuttaa se hyötyjä kuten vähentää riskien kokonaiskustannuksia, parantaa organisaation suorituskykyä ja kestävyyttä, turvaa kasvumahdollisuudet ja antaa strategisia etuja. (AON 2007.) Näitä hyötyjä vahvistaa AONin tutkimus vuodelta 2010, jolloin tuloksia on verrattu vuoden 2007 tutkimuksiin ja tuloksissaan toteavat, että yritysten määrä on kasvanut dramaattisesti, jotka pyrkivät parempaan suorituskykyyn. Yritykset, jotka ovat integroineet ERM:n paremmin toimintaansa, raportoivat voivansa tuoda merkittävää arvoa ERM:n kautta liiketoimintaan.



Kuva 7. *Riskienhallinta ja liiketoimintaprosessin kytkökset (mukaillen Riskikompassi 2017).*

Kokonaisvaltaisen riskienhallinnan kehittämiselle nähdään ja käytetään perusteluna usein hyvää hallintotapaa eli corporate governancea (Kuusela & Ollikainen 2005). Myös AONin (2010) tutkimukseen vastanneet osoittavat, että ERM-investointeihin liittyvät ensisijaiset tekijät parantavat hallintoa ja avoimuutta sekä parantaa parhaita käytäntöjä ja nämä

toimivat täytäntöönpanon tekijöinä. Corporate governance on OECD:n tuoma käsite yritysjohdon käyttöön. Sen tarkoituksena on selkeyttää ja määritellä yrityksen hallituksen toiminnalle ja valvonnalle vaatimukset, joiden avulla turvataan ja nostetaan luottamusta sekä arvostusta. (Erola & Louto 2000.) Corporate governance on yleisesti käytössä lähes kaikissa pörssiyhtiöissä ja suurissa yrityksissä ja jokainen yhteisö ja maa on luonut myös omia suosituksia. (Erma et al. 2010.) Myös Keskuskauppakamari (2016) on valmistellut asialuettelon listaamattomien yhtiöiden hallinnoinnin kehittämiseksi, joka perustuu vapaaehtoisuuteen ja voidaan hyödyntää esimerkiksi pk-yrityksissä. Yksi asialuetteloon kuuluvista kohdista on riskienhallinta osana yrityksen valvontajärjestelmää. Tällä pyritään varmistamaan, että yhtiön toiminta on tehokasta ja liiketoiminnan jatkuvuus voidaan turvata. Valtaosa suosituksista on yleispäteviä, mutta jokainen yritys voi hyödyntää niitä parhaalla katsomalla tavalla (Erma et al. 2010).

3.1.1 Riskikulttuuri

ERM ei tuota optimaalista ja vaikuttavaa tasoa ilman, että se on täysin integroitu organisaation käytäntöön ja kulttuuriin. Kun kulttuuri huomioidaan koko ERM-toteutusprosessin aikana, sillä on paljon suurempi mahdollisuus onnistua ja auttaa yritystoimintaa positiivisella tavalla myös tulevaisuudessa. (AON 2007.) Organisaatiokulttuuri on monitahoinen termi, mutta käsitteellä halutaan korostaa, että organisaatio on yhteisö, jolla on omat tapansa, käsitykset ja vuorovaikutus. Se on toiminnallinen kehys, joka luo mahdollisuudet ja rajoitukset organisaatioon. Organisaatiokulttuuri muodostuu yksilöiden jakamista käsityksistä, olettamuksista, arvoista, normeista, käytännöistä, teknologiasta ja työvälineistä. (Flink et al. 2007.)

Kuten jo todettiin, että organisaatiokulttuuri on monimutkainen termi ja sille on vaikea määrittää yhtä selkeää selitystä. Schein (2001) määrittää yrityskulttuurin kolmeen eri tasoon, näkyvästä näkymättömään. Ensimmäinen taso on nimetty artefaktiksi, joka on näkyvin osa eli mitä näemme, kuulemme ja havaitsemme liikkuessa ympäriinsä. Tähän tasoon kuuluvat esimerkiksi organisaation rakenne ja prosessit. Toinen taso on ilmaistut arvot, joita strategia ja päämäärät edustavat. Tämä taso ohjaa ajattelulla ja käsityksillä näkyvää käyttäytymistä vastaamalla kysymykseen miksi teemme tätä? Kolmas syvin taso on pohjimmaiset perusoletukset eli tiedostamattomia käsityksiä ja ajatuksia, joka on arvojen perimmäinen lähde. Organisaatiokulttuurin elementit määrittävät ja ohjaavat strategiaa, päämääriä ja toimintatapoja, tästä syystä kulttuurilla on erityistä merkitystä yrityksissä.

Organisaatiokulttuurista voidaan tarkentaa myös erillinen riskikulttuuri, jossa keskitytään yhteiseen kykyyn hallita riskejä. Termi kuvaa yhteisten tavoitteiden mukaisten ihmisten, etenkin organisaation työntekijöiden tai organisaatioiden tiimien tai ryhmien, arvoja, uskomuksia, tietämystä ja ymmärrystä riskeistä. Riskiasenne on yksilön tai ryhmän omaksuma, mihin vaikuttaa riskin havaitseminen ja ennakointi. Riskikäyttäytyminen sisältää

ulkoisesti havaittavia toimia riskiin liittyen kuten riskipohjainen päätöksenteko, riskiprosessit, riskiviestintä ja niin edelleen. Jokaisessa yrityksessä on riskikulttuuri, mutta kysymys on lähinnä siinä, että edesauttaako kulttuuri vai heikentääkö se pitkänajan suunnitelmia. Vallitseva riskikulttuuri vaikuttaa merkittävästi kykyyn tehdä strategisia päätöksiä ja suorituskyvyn lupauksiin. Heikko riskikulttuuri merkitsee sitä, että tietyt henkilöt tai ryhmät tekevät näitä toimintoja, mutta muut organisaatiossa jättävät huomiotta, epäröivät tai eivät näe, mitä tapahtuu. Pahimmillaan tämä vaikeuttaa strategisten, taktisten ja operatiivisten tavoitteiden saavuttamista. Pahimmassa tapauksessa se johtaa vakavaan maineeseen ja taloudelliseen vahinkoon. Tästä syystä yrityksen johdolla on velvollisuus asettaa, viestiä ja valvoa riskikulttuuria, joka johdonmukaisesti vaikuttaa, ohjaa ja yhdenmukaistaa liiketoiminnan strategiaa ja tavoitteita ja tukee siten riskienhallintakehyksiensä ja -prosessiensa sisällyttämistä. Tämä alkaa itse riskiasenteista, käyttäytymisestä ja kulttuurista ja ulottuu koko organisaatioon. (The Institute of Risk Management 2012.)

Riskienhallintaa voidaan integroida monella eri tapaa olemassa olevaan kulttuuriin ja edistää riskikulttuuria esimerkiksi johdon asettamalla politiikka ja toiminta riskienhallintaosaamisen lisäämiseksi. (FERMA 2003) Financial Stability Board on määrittänyt hyvän riskikulttuurin merkeiksi seuraavat kolme kohtaa:

- tukee tehokasta riskinhallintaa,
- edistää järkevää riskinottoa,
- varmistaa, että uudet riskit ja liialliset riskinottotoimet arvioidaan ja käsitellään ajoissa. (EY 2015.)

Tehokkaan riskienhallinnan avain onkin siinä, että se on osa kulttuuria ja tämän kautta saadaan yrityksessä työskentelevät henkilöt hallitsemaan riskejä ja olemaan riskinomistajia, myös edistämään yrityksen tavoitteiden saavuttamista. (Louisot & Ketcham 2014.) Yritysten täytyy ottaa riskejä, jotta tavoitteet voidaan saavuttaa. Vaikka ajan kuluessa onkin kehitetty erilaisia sääntöjä, kehyksiä, prosesseja ja standardeja hallitsemaan riskejä, eivät ne yksinään riitä tekemään organisaatiosta menestyvää tai epäonnistujaa. Näiden lisäksi tarvitaan riskikulttuuria organisaatiossa, mikä on puuttuva osa toiminnassa ymmärtää kuinka tasapainottaa riskit ja näiden avulla tehdä onnistuneita päätöksiä. (The Institute of Risk Management 2012.) Myös COSO (2017) korostaa, että kokonaisvaltainen riskienhallinta ei ole vain toiminto tai osasto, vaan se on kulttuuria ja käytäntöjä strategia asetannan ja sen toteuttamisen yhteydessä, minkä tarkoitus on hallita riskejä arvon luomisessa, säilyttämisessä ja toteuttamisessa.

3.1.2 Riskienhallinnan lähtökohdat tiedon tuottamiseen

Riskienhallinnan onnistumiseen vaikuttaa moni eri tekijä, mutta taustalle luodut puitteet auttavat hallitsemaan riskejä ja puitteet varmistavat, että saadut tiedot riskeistä raportoidaan oikealla tavalla ja niitä käytetään päätöksenteon perustana. (SFS-EN ISO

31000:2018). Riskienhallinnan perustana toimii ulkoisten ja sisäisten toimintaympäristöjen tunnistaminen ja määrittely, joilla on vaikutusta riskienhallintaprosessin toteuttamiseen ja ne tulee huomioida tässä yhteydessä. Oleellista on huomioida myös, että riskienhallintaprosessi ei ole erillinen liiketoiminnasta, vaan tarkoitus on kuvata toimenpiteitä, joita tarvitaan päätöksenteon tukena eri tasoilla (Riskikompassi 2017).

Riskienhallinnan tuottaman tiedon hyödyntämiseen oleellista on määrittää vastuualueet, kuka vastaa riskienhallinnasta ja kenelle niihin liittyvistä asioista raportoidaan? Vastuuta riskeistä ei voi ulkoistaa, vaikka käsittelyyn liittyviä tehtäviä kuten riskirekisterin ylläpito voidaan keskittää muille toimijoille. Periaatteisiin kuuluu, että hallitus ja toimitusjohtaja vastaavat riskienhallinnan järjestämisestä luomalla esimerkiksi riskienhallintapolitiikan ja operatiivisella tasolla henkilö, joka muutenkin on vastuussa kyseisestä prosessista, yksiköstä, toiminnasta tai tavoitteesta. Johdon vastuulla on lisäksi vahvistaa riskienhallintakulttuuria organisaatiossa ja saattaa se vallitsevaksi käytännöksi yritykseen, jolloin jokainen työntekijä on vastuussa oman toimintaympäristön riskienhallinnasta sekä riskejä tunnistetaan ja niitä raportoidaan relevanteissa yhteyksissä. (Ilmonen et al. 2016.) Pk-yrityksissä vastuu ja osaaminen on usein jaettu muutaman henkilön kanssa eivätkä he ole välttämättä asiantuntijoita riskienhallinnassa. Suuryrityksissä taas usein palkataan oma riskienhallintapäällikkö, joka vastaa riskienhallinnasta ja sen tiedon tuottamisesta. (Juvonen 2005.) Mutta tilanteita tulee välttää, joissa toiminta muuttuu oletukseksi, että riskienhallintapäällikkö tai muu riskienhallinnasta vastuussa oleva vastaa yksin yhtiön riskeistä ja huolehtii, että riskejä ei synny (Ilmonen et al. 2016).

Aiemmin toisessa luvussa esitettiin, että kokonaisvaltaisessa riskienhallinnassa riskejä tulee käsitellä yrityksen kaikilla tasoilla ja tasoja on kolme; strateginen, taktinen ja operatiivinen. Riskit voidaan myös luokitella, jotta riskit saadaan yhteismitallistettua ja niitä voidaan vertailla paremmin. Luokittelulla lisätään myös ymmärrystä riskien keskinäisistä riippuvaisuuksista sekä lisätään riskitietoisuutta organisaatiossa (Ilmonen et al. 2016). Luokittelun avulla voidaan myös varmistaa, että yrityksessä on pyritty tunnistamaan kattavasti kaikki riskit ja kuvaamaan riskin syntymisen taustat ja ilmenemismuodot (Riskikompassi 2017). Perinteinen tapa on jakaa riskit kahteen luokkaan (taulukko 2) eli vahinko- ja liikeriskeihin, joista voidaan erottaa muita ja osittain päällekkäisiä riskilajeja kuten henkilö- ja tuoteriskit. Vahinkoriskit ovat negatiivisia ja toteutuessaan ne ovat yrityksen toiminnalle haitallisia. Vahinkoriskit ovat hallittavissa usein vakuuttamalla ja ne ovat lähempänä operatiivista tasoa. Liikeriskillä taas voi olla niin negatiivisia kuin positiivisia vaikutuksia ja usein riskit liittyvät osaamiseen, työkykyyn ja kykyyn tehdä oikeita päätöksiä strategisella tasolla. Liikeriski syntyy usein, kun liiketoiminnassa tehdään päätöksiä, joilla yritys ottaa riskin liikevoiton maksimoimiseksi. (Flink et al. 2007.)

Taulukko 2. *Perinteinen riskiluokittelu (mukaillen Flink et al .2007).*

RISKIT	
Vahinkoriskit: • Omaisuusriski • Henkilöstöriski • Vastuuriski • Tietoriski • Jne.	Liikeriskit: • Verotus • Markkinat • Kilpailijat • Resurssit • Jne.

Toinen tapa, melko vakiintunut sellainen, on jakaa riskit neljään luokkaan; strategiset riskit, taloudelliset riskit, operatiiviset riskit sekä vahinkoriskit. Näihin kaikkiin luokkiin voidaan sisällyttää niin ulkoiset kuin sisäisetkin riskit. (Ilmonen et al. 2016.)

Strategiset riskit

Strategiset riskit ovat pitkän aikavälin riskejä yrityksessä ja ne liittyvät strategian tavoitteisiin (Ilmonen et al. 2016). Ne voidaan jakaa myös strategian laadintaan ja toteuttamiseen liittyviin riskeihin. Laadinta vaiheessa riskejä syntyy puutteellisen ja väärän taustatiedon pohjalta ja toteuttamisvaiheessa riskejä muodostuu esteistä, joita yrityksen toiminnassa aiheutuu. (Juvonen 2005.) Strategisia riskejä voi olla niin ulkoisia kuin sisäisiäkin, ulkoisia riskejä ovat esimerkiksi kilpailijoihin tai muihin liiketoimintaympäristön muutoksiin liittyviä kuten lainsäädäntö tai yllättävä markkinatilanteen muutos. Sisäiset riskit voivat taas liittyä strategian toimeenpanon epäonnistumiseen tai tuotteet eivät vastaakaan asiakkaiden odotuksia ja tarpeita eikä ne vastaa strategisten tavoitteiden tarpeita. (Ilmonen et al. 2016.)

Operatiiviset riskit

Operatiiviset riskit ovat yrityksen jokapäiväisiin toimintoihin liittyviä ja ne voivat olla joko välillisiä tai välittömiä. Riskit syntyvät sisäisistä prosesseista, järjestelmistä, henkilöstöstä tai ulkoisista tapahtumista. (Riskikompassi.) Riskien määrä on suurempi operatiivisella tasolla ja usein myös riskien tunnistamiseen ja arviointiin osallistuu useampi henkilö (Riskiblogi) (Riskiblogi 2017). Operatiiviseen riskiluokkaan sisällytetään usein myös projektiriskit, joita syntyy esimerkiksi projektin aikataulun ja budjetin ylittymisestä, projektihenkilöstön osaamisesta ja resurssien riittävyydestä (Ilmonen et al. 2016).

Taloudelliset riskit

Taloudelliset riskit liittyvät maksuvalmiuteen, korkoihin, veroihin tai valuuttariskeihin eli yrityksen rahaprosessiin vaikuttaviin epävarmuustekijöihin. Taloudelliset riskit voivat syntyä esimerkiksi pääomien saatavuuden tai valuuttakurssien muutoksista. (Riskikompassi 2017.) Taloudellisilla tilanteella ja sen riskeillä on vaikutusta yrityksen riskinkan-

tokykyyn ja riskinottokykyyn. Riskinkantokyvyllä on vaikutusta, että kuinka yritys pystyy uudistumaan ja voiko yritys tavoitella kasvua vai pelkästään kannattavuutta. (Juvonen et al. 2014.)

Vahinkoriskit

Vahinkoriskit voivat liittyä henkilöstöön sekä ympäristöön, vahinkoriskeiksi luetaan esimerkiksi työkyvyttömyys, työtapaturmat, vaarallisten aineiden käsittely, saastuttaminen ja ympäristövastuun hoito. Vahinkoriskit mielletään usein riskeiksi ja ne ovat tutuimpia melkein jokaiselle ihmisille, koska vahinkoriskejä on tunnistettu yrityksissä jo vuosia erillisenä toimintona. (Ilmonen et al. 2016.)

Luokittelutapoja on monia, näiden kahden aiemmin esitetyn luokitustavan lisäksi riskejä voidaan luokittaa yrityksen toimintojen mukaan kuten Gahin riskifilosofiassa eli riskit ilmenevät taloudellisen, sosiaalisen ja poliittisen toiminnan pohjalta ja riskit ovat riippuvaisia toisistaan (Suominen 2003). Riskit voidaan jakaa myös tietoisiin ja tiedostamattomiin riskeihin, välillisiin ja välittömiin riskeihin sekä vakuutettaviin ja ei-vakuutettaviin riskeihin. Oleellista on löytää malli, jonka avulla luokittelu tukee parhaiten oman organisaation tapaa mieltää riskit ja ottaa huomioon toimintaympäristön ominaispiirteet (Riskikompassi 2017).

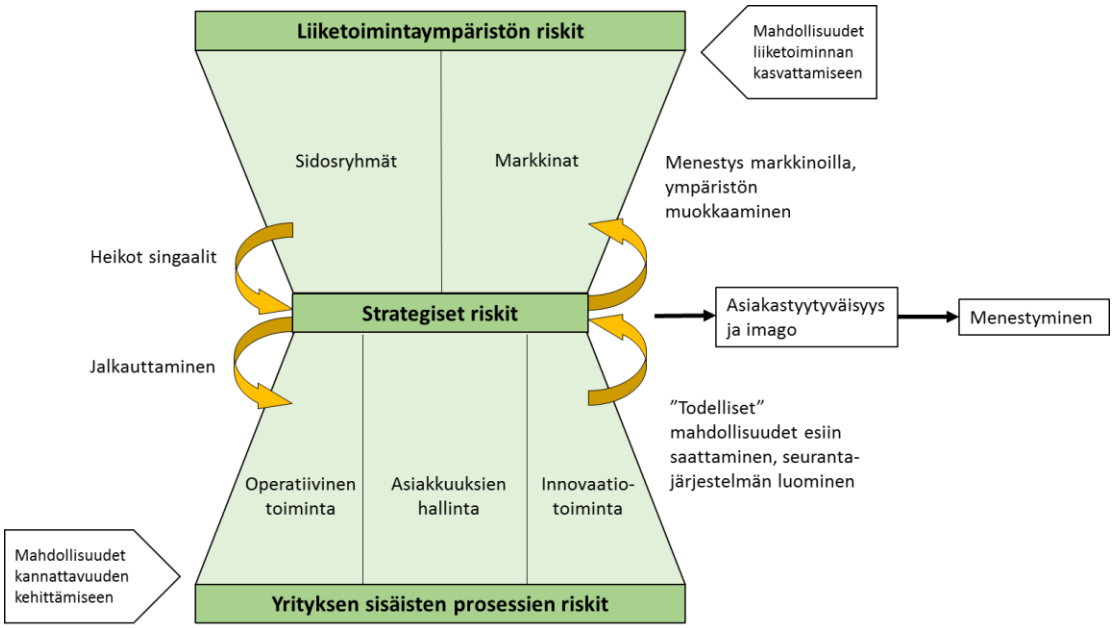
3.1.3 Riskienhallinta ja strategiatyö

Riskienhallinnassa ei tule olla kysymys irrallisesta prosessista, vaan se tulee olla kytketty suoraan yrityksen strategiaan ja arvoihin (Ilmonen et al. 2016). Strategian tarkoitus on kuvata yrityksen tavoitetila ja keinot, kuinka se saavutetaan. Keskeisiä kysymyksiä strategiassa on, missä ollaan mukana ja missä ei ja kuinka saadaan aikaan pysyvää kilpailuetua. (Hiltunen 2015.) Aiemmin esitetyt viitekehykset korostavat riskienhallinnan kytkemistä strategiaan ja tavoitteisiin ja tätä kautta johtamiseen. Myös Ilmonen (2016) kirjoittaa, että yrityksen aloittaessa systemaattista riskienhallintaa, kannattaa fokus keskittää strategisten tavoitteiden ja vuositavoitteiden saavuttamista uhkaaviin tekijöihin.

Kaplan ja Mikes (2012) ovat kirjoittaneet, että riski näkökulmaa koko yrityksen laajuudelta voidaan kehittää strategiasuunnittelun yhteydessä. Riskienhallinta on enemmänkin strateginen työkalu, jolla tuodaan yrityksen johdolle lisää näkökantoja ja keinoja jatkuvuuden varmistamiseksi. Riskienhallinnasta syntyvällä tiedolla yrityksen johto voi vertailla vaihtoehtostrategioita pohtiessaan esimerkiksi laajentumista tai suurempaa suunnanmuutosta liiketoiminnassa. Sen avulla yritys saa tietoa strategian tavoitteita uhkaavista tekijöistä, jolloin se voi ennakoida ja torjua niitä, koska riskienhallinta pakottaa ajattelemaan tulevaisuuden skenaarioita paljon aiemmin kuin muutoksen jo tapahduttua. (Rautanen 2011.) Ratkaisevaa strategian valinnassa ja prosessin, jolla sitä kehitetään, on yrityksen liiketoiminnassa ilmenevät epävarmuudet ja niiden taso toiminnassa. (Courtney et al. 1997).

Riskienhallinta toimii tukena strategiaprosessissa ja sen kytkentä prosessiin tulee ajallisesti miettiä sopivaksi, milloin saatava tieto on hyödynnettävissä parhaimmalla tavalla. Jos riskienhallinta tulee mukaan liian myöhäisessä vaiheessa, riskinä on että siinä tehdyt havainnot jäävät puuttumaan ja huomioimatta tehtäessä valintaa lopullisesta strategiavaihtoehdoista. Mutta myöskään liian aikaisessa vaiheessa riskien tunnistamista ei tule tehdä, jotta arvioinnin taustalle saadaan luonnosteltua strategiset tavoitteet. (Ilmonen et al. 2016.) Jos strategia on muodostettu siten, ettei riskejä ole tunnistettu, se on puutteellinen ja alttiimpi riskeille. Tilanne on myös sama, jos riskejä ei ole tunnistettu kokonaisvaltaisesti ja merkittävimpiä riskejä ei ole tunnistettu. (Shenkir & Walker 2011.)

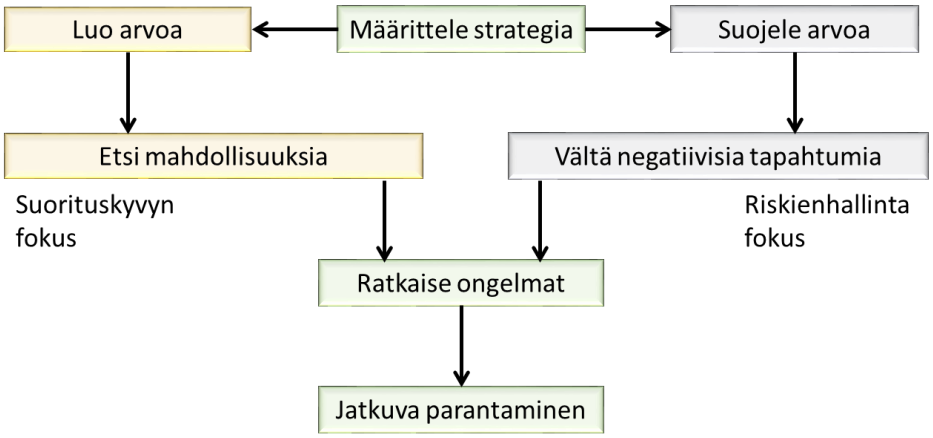
Kuvassa 8 on esitetty strategian ja sen riskien kytkös koko liiketoimintaan vaikuttaviin tekijöihin. Markkinoilla menestymistä voi edesauttaa kokonaisvaltaisella riskienhallinnalla, jolloin tunnistetaan liiketoimintaympäristöstä mahdollisuudet ja riskit. Toimintaympäristön sosiaaliset, poliittiset ja taloudelliset olot ovat suurimpia uhkia, esimerkiksi markkinoiden muutokset, teknologian kehitys, globalisaatio, nopeat poliittiset muutokset ja työvoiman saatavuus. Tästä syystä strategiasuunnittelun yhteydessä on tärkeää tunnistaa sidosryhmiin liittyvät riskit ja tarkkailla toimintaympäristöä ja sen heikkoja signaaleja. (Juvonen 2005.) Strategian luomisen jälkeen johdon tulee vielä varmistaa, että yrityksen sisäisten prosessien osalta riskit eivät uhkaa strategian toteutumista (Juvonen et al. 2014).



Kuva 8. *Riskienhallinta ja liiketoiminta (mukaillen Juvonen et al. 2014).*

Ensisijainen hyöty riskiin perustuvaan strategia lähestymiseen on se, että sen avulla voidaan keskittyä suunnitelmiin sisältyviin mahdollisuuksiin ja samalla minimoida uhkien mahdolliset vaikutukset (Sheehan 2010). EY (2013) on tutkimuksessaan todennut, että yhä enemmissä määrin yrityksen keskittyvät riskienhallinnan strategisiin ja liiketoimin-

nallisiin mahdollisuuksiin, kun ennen fokus oli riskien lieventämisessä, kustannusten hallinnassa, liiketoiminnan pois pitämisessä vaikeuksista ja brändin suojaamisesta. Riskienhallinta käytäntönä tulisi olla, että liiketoiminnan suunnitteluun sisällytetään olemassa oleva tietoa riskeistä, joka raportoidaan ja päivitetään säännöllisesti. Kuvassa 9 on esitetty strategian kaksi puolta, jossa on suorituskyky sekä riskienhallinta näkökulmat huomioitu strategian ja arvon luomisen näkökulmasta. Riskienhallinnan jakaminen lähes erillisiin johtamisjärjestelmiin vähentää merkittävästi sen tehokkuutta ja sillä voi olla dramaattisia seurauksia. (EY 2017.) Mutta huomioimalla riskienhallinnan osana johtamista ja strategiaa, mahdollistaa se johtajien nopean ja luotettavan reagoinnin tilanteisiin joko mahdollisuuksien tai uhkien osalta (Sheehan 2010). Painopisteen tulisi olla sellaisissa tapahtumissa, jotka voivat vaikuttaa strategian ja liiketoiminnan tavoitteiden saavuttamiseen. Kun keskitytään riskeihin eikä strategioihin ja tavoitteisiin, ERMista tulee ohjelma. Arvon lisäämiseksi ERM: n täytyy aina olla strategioiden ja tavoitteiden toteuttamisessa. Johto ei ajattele ensin riskeistä, vaan suorituskyvyn tuottamisesta ja siitä, mikä voi vaikuttaa tähän suorituskykyyn. (Anderson 2017.)



Kuva 9. *Strategian kaksi puolta (mukaillen EY 2017).*

Strategiaan liittyvien epävarmuuksien huomioimiseen Sheehan (2010) esittää kehyksen, jossa hyödynnetään Kaplan ja Nortonin strategiakarttaa. Strategiakartan avulla yritys havainnollistaa strategiansa neljästä eri näkökulmasta; talous, asiakas, prosessi ja oppiminen. Tunnistamalla menestystekijät ja vaatimukset eri osa-alueilla, voi niiden pohjalta tunnistaa avainriskit, jotka uhkaavat strategian toteutumista. Tunnistetuille riskeille määritetään toimenpiteet sekä niiden seurantaan vaadittava kontrolli. Näin kriittisistä menestystekijöistä saadaan johdettua riskit ja kytkettyä ne liiketoimintaprosessiin sekä huomioitua strategian molemmat puolet kuten kuvassa 9.

Huomioitavaa kuitenkin on, että liiketoiminta itsessään on jo riski. Mikään lähestymistapa ei poista epävarmuutta ja sen haasteita strategiassa, mutta se antaa käytännön ohjeita, jotka johtavat tietoisempiin ja luotettavimpiin strategisiin päätöksiin (Courtney et al. 1997). Lisäksi olettamuksilla on syvät vaikutukset riskipäätöksiin ja riskin ottamiseen lii-

ketoiminnassa (Walker 2013). Päätöksillä tulee olla vahvaa näyttöä, että valittu toimintalinja on turvallinen, erityisesti jos tehdään peruuttamattomia päätöksiä, joilla on kielteinen seuraus (Collins 2010). Päättäjille keskeisempää on mahdollisen epäonnistumisen suuruus kuin todennäköisyys (Temmes & Välikangas 2010).

3.1.4 Riskienhallinta ja päätöksenteko

Toimintaympäristö ja olosuhteet ovat muutoksessa jatkuvasti, siksi yrityksen johdon tulee tunnistaa ja hallita riskejä (Rautanen 2011). Hyvän johtamisen merkkinä pidetään myös, että riskienhallintaosaaminen on luontevasti kytketty yrityksen johdon työhön ja päätöksentekoon (Kuusela & Ollikainen 2005). Riskienhallinta tulisikin nähdä ja tapahtua osana johtamista ilman sanaa riskienhallinta (Rautanen 2011).

Menestymiseen markkinoilla yrityksen tulee kyetä ennustamaan oikein muutokset, joita liiketoimintaympäristössä tapahtuu (Juvonen 2005). Riskien ennustaminen ja kuvaaminen tosin ovat hankalaa, mutta johtajan vastuulla ovat aiheutuneet vahingot. Riskienhallinnassa tärkeää onkin asennoituminen, jos johto vähättelee ja kieltää riskit, otetaan tällöin suurempi riski. Samalla unohdetaan, että riskienhallinta on enemmänkin mahdollisuus ja kehittämisen työkalu kuin esimerkiksi johtamisen kritiikkiä tunnistetuilla riskeillä. (Rautanen 2011.) Riskien ollessa integroituna osaksi johtamista ja päätöksentekoa, helpottaa se keskittymistä olennaiseen ja panostaminen oikeisiin asioihin auttaa saavuttamaan parhaan mahdollisen lopputuloksen (Juvonen et al. 2014). Riskien integroimiseen osaksi johtamista vaikuttaa hyvin paljon yrityksen johdon johtamis- ja ajattelutapa sekä kokemus sekä halu nähdä riskienhallinta osana johtamista. Lisäksi arvomaailma heijastuu riskienhallintaan ohjaavana tekijänä lähes kaikissa valinnoissa ja päätöksissä. (Rautanen 2011.) Riskiperusteisella lähestymistavalla päättäjät saavat tukea päätökseen, tarkoitus ei ole kyseenalaistaa johtajien taitoa vaan saada epävarmuus hallintaan. (Ilmonen et al. 2016).

Temmes ja Välikangas (2010) toteavat, että johtajien tehtävä on tehdä päätöksiä ja panna ne toimeen. Tässä kohtaa toimivalla riskienhallinnalla tarkoituksena on päätöksenteon tukeminen epävarmuudet huomioiden (Ilmonen et al. 2016). Päätös määritellään yleisemmin sitoutumiseksi toimenpiteeseen ja strateginen päätös on suuri päätös, jolla on vaikutusta yrityksen tulevaisuuteen. Strategisiin päätöksiin liittyy epävarmuutta, riskejä ja sivuvaikutuksia, koska emme tiedä varmaksi mitä tapahtuu päätöksenteon jälkeen. Strategisten päätösten riskeissä pitäisi osata myös huomioida, että strategiat harvoin menevät suunnitelmien mukaan, koska osa jää toteutumatta ja myös ulkopuolelta ilmestyy suunnittelemattomia toimenpiteitä. (Temmes & Välikangas 2010.) Päätöksiä tehdään myös kahdella muulla tasolla, taktisella ja operatiivisella. Operatiivisen tason päätökset ovat lyhyen tähtäimen päätöksiä ja taktisella tasolla ajallinen jakso on hieman pidempi kuin operatiivisessa. Pienissä ja keskisuurissa yrityksissä päätöksenteon tasot eivät välttämättä erotu selkeäsi toisistaan ja sama päätöksentekijä voi olla tekemässä jokaisella päätöksentekotasolla päätöksiä. Strategisiin päätöksiin liittyy vähiten historiatietoa, jolloin siihen

liittyvän riskin epävarmuus on suurin ja sama esiintyy ulkopuolelta syntyviin riskeihin. (Engblom 2003.) Päätöksen toimeenpanovaiheessa on luotettava siihen, että sivuvaikutukset on arvioitu sekä niitä on pienennetty riittävästi eri riskienhallintatoimenpiteillä (Temmes & Välikangas 2010). Päätöksenteossa vaarallisinta on se, että olemassa oleva tieto on epäselvää ja se tulkitaan väärin. Tämän seurauksen aletaan toimimaan sen mukaisesti ja myöhemmässä vaiheessa tilanne voikin osoittautua yritykselle vaikeaksi. (Collins 2010.)

3.1.5 Riskienhallinta osana prosessia ja organisaatiota

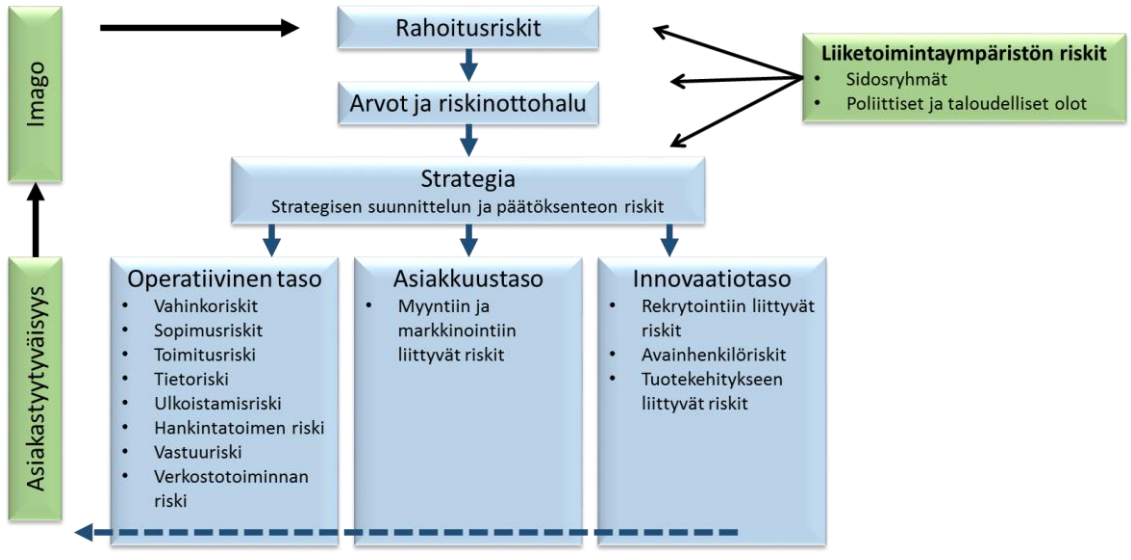
Linjaorganisaatiot ovat muuttuneet kehittyvissä organisaatioissa prosessimaiseen toimintamalliin, joilla toimintaa mallinnetaan ja johdetaan prosesseilla (Ilmonen 2016). Prosessin käsite sisältää toiminnan lisäksi resurssit, tuotokset ja niihin liittyvät suorituskyvyt. Prosessien tehtävä on kuvata ja auttaa ymmärtämään kriittisiä tekijöitä organisaatiossa, joilla on vaikutusta keskeisten tavoitteiden saavuttamiseksi. Näitä kriittisiä tekijöitä voidaan mitata ja prosessit toimivat kehittämisen perustana toimintajärjestelmässä. Vahingollinen tapa lähestyä järjestelmien rakentamista on kehittää jokaiselle tärkeälle asialle oma järjestelmä kuten laatu-, ympäristö ja riskienhallintajärjestelmä. Riskienhallinta tulee sisällyttää prosessiin toimintaperiaatteina, joihin on kiteytetty tärkeimmät uskomukset johtamiseen ja toimintaan liittyen. (Laamanen 2012.) Prosessien tunnistamisen avulla saadaan määritettyä, millaista tietoa prosessin vaiheista voidaan kerätä johtamisen tueksi. Kun riskienhallinta näkökulma sisällytetään tähän, saadaan kerättyä mahdollisesti myös tietoa riskeistä ja prosessin sujuvoittamista asiakkaan, että omien tarpeiden pohjalta. (Kupi et al. 2009.)

Prosessien kautta riskit kytkeytyvät liiketoimintaan ja suurimmillaan riskit ovat prosessien rajapinnoilla. Pääprosessien osalta keskitytään kartoittamaan riskejä liiketoimintaan ja riippuvuuksiin kuten asiakkaaseen ja investointeihin liittyen. Pääprosessin oikeellisuus, painoarvot ja kytkösvaikutukset varmistetaan kartoittamalla tukiprosessien riskit. Tärkeimpiä asioita prosessiriskien osalta onkin keskittyä vain suurimpiin ja painoarvoltaan tärkeimpiin riskikokonaisuuksiin. (Rautanen 2011.) Kun jokainen prosessi hallitsee omat kriittiset ja erityisriskit ja arvioinnissa on huomioitu riskiä aiheuttavat ja lisäävät tekijät, tällöin ylimmän johdon tarvitsee keskittyä vain yritystason riskienhallintaan (Ratsula 2016). Sisäisten prosessien riskit tunnistamalla ja hallitsemalla eri tasoilta kuten innovaatio, asiakkuus ja operatiivinen taso, yritykselle syntyy mahdollisuus kehittää omaa kannattavuuttaan (Juvonen 2005). Prosessiriskejä kartoitetaan toimintojen kuvauksista, konseptista, kilpailijoista, kannattavuudesta ja tuloksista ja kartoituksen fokuksessa on prosessien ongelmakohdat, ongelmien syntyyn vaikuttavat tekijät ja niiden rahallinen arvo ja merkitys (Rautanen 2011).

Prosesseille asetetaan mittareita ja niille tavoitteet, joita seuraamalla saadaan tietoa yrityksen toiminnasta ja prosessien toimivuudesta (Ilmonen 2016). Usein liiketoiminnassa hallitaan prosessit hyvin, mutta prosessien riskejä ei niin hyvin (Rautanen 2011). Luotuja

mittareita hyödyntämällä ja pohtimalla niiden tavoitteisiin liittyviä riskejä, saadaan prosessien omistajat hahmottamaan riskin toteutumisen seurauksia paremmin. Tätä kautta myös riskienhallinnan käytäntöjä on helpompi integroida olemassa olevaan johtamisjärjestelmään. (Ilmonen 2016.) Yhdistämällä eri analyyseihin kuten asiakastyytyväisyyteen, henkilöstökyselyihin ja kilpailija-analyyseihin riskienhallinnan, saa yritys ja sen prosessit lisäävät tietoa mahdollisten toimenpiteiden tehostamiseksi ja prosessin toimivuuden parantamiseksi (Rautanen 2011).

Riskien ollessa osana organisaatiota ja prosesseja, parantaa se strategian ymmärrettävyyttä, soveltuvuutta ja implementointia (Rautanen 2011). Strategian ymmärrettävyyttä lisää luotettava ja kokonaisuutena huomioitava tieto riskeistä. Strategian ollessa valmis, tulee sitä soveltaa ja implementoida organisaatiossa ja tässä vaiheessa prosessien osalta tunnistetut riskit helpottavat tunnistamaan strategian toteutumista uhkaavat tekijät. (Juvonen 2005.) Riskien kautta pystytään myös pohtimaan organisaation tulevaisuutta, sen uhkakuvia ja kuinka niihin voidaan varautua omalla toiminnallaan. Tästä syystä riskienhallinnan tulisi olla osa jokapäiväistä toimintaa organisaatiossa eikä vasta siinä vaiheessa, kun lama, huonot ajat tai suuret vahingot tapahtuvat. (Rautanen 2011.) Kuvassa 10 on kuvattu, kuinka riskienhallinta kulkeutuu organisaatiossa koko johtamisprosessin läpi kaikilla eri tasoilla luoden tietoa riskeistä liiketoiminnassa. Käytännön riskienhallinta tapahtuukin operatiivisella tasolla ja siksi toimiva riskienhallinta vaatii selkeät vastuualueet ja aktiivista kommunikointia (Ilmonen 2016). Prosesseissa tapahtuva toiminta heijastuu suoraan asiakastyytyväisyyteen ja imagoon markkinoilla.



Kuva 10. *Riskienhallinta johtamisprosessin läpi (mukaillen Juvonen et al. 2014).*

Prosessimainen työskentely lisää vuoropuhelua eri osastojen välillä ja tämä palvelee riskienhallintaa erinomaisesti. Näissä keskusteluissa tunnistetaan epäkohtia ja uhkia, joita

arvioimalla voidaan tunnistaa riskejä. (Ilmonen 2016.) Kommunikaation merkitys organisaation riskienhallinnassa nousee esiin myös Stulzin (2009) HBR artikkelissa, jossa on listattu kuusi tapaa, kuinka hallita harhaanjohtavasti riskejä ja yksi näistä on kommunikaatio, koska tieto voi olla liian vaikeaselkoista tai tieto riskeistä tulee liian myöhään tai on vääristynyt välikäsien kautta. Tästä syystä kommunikaatio päättäjien suuntaan on hyvin tärkeää. (Stulz 2009.) Kommunikointi on tärkeää, kun seurataan esimerkiksi hiljaisia signaaleja sidosryhmissä ja omissa prosesseissa. Riskienhallinnan tulisi luoda matala kynnys henkilöstölle informoida ja viestiä huomioiduista toistuvista pienistä tapahtumista tai huolenaiheista. Hiljainen tieto henkilöstöllä on riskienhallinnalle merkittävä tekijä. (Ilmonen 2016.) AON (2007) on tutkimuksessaan todennut, että kommunikoinnilla ERM:n sisällyttäminen keskeisiin liiketoimintaprosesseihin helpottuu ja koko organisaatiossa tapahtuu johdonmukainen ja mielekäs ERM-tiedonvaihto. Kommunikointi on keskeinen tekijä ERM:n toteuttamisen kannalta. (AON 2007.) Riskienhallinta edellyttää kommunikaatiota, jotta saatu tieto saadaan hyödynnettyä parhaalla mahdollisella tavalla. Se tuottaa tietoa, jonka avulla voidaan esimerkiksi parantaa oman toiminnan laatua ja tarkastella johtamista laajemmin ja perusteellisemmin. (Rautanen 2011.) Myös sisäiset ja ulkoiset sidosryhmät tarvitsevat lisätietoa riskeistä omien päätöstensä tukemiseksi siitä, miten he voivat hallita riskejä ja ymmärtää, miten riski koko arvoketjussa voi vaikuttaa liiketoiminnan tavoitteisiin ja loppujen lopuksi suorituskykyyn. (AON 2010.)

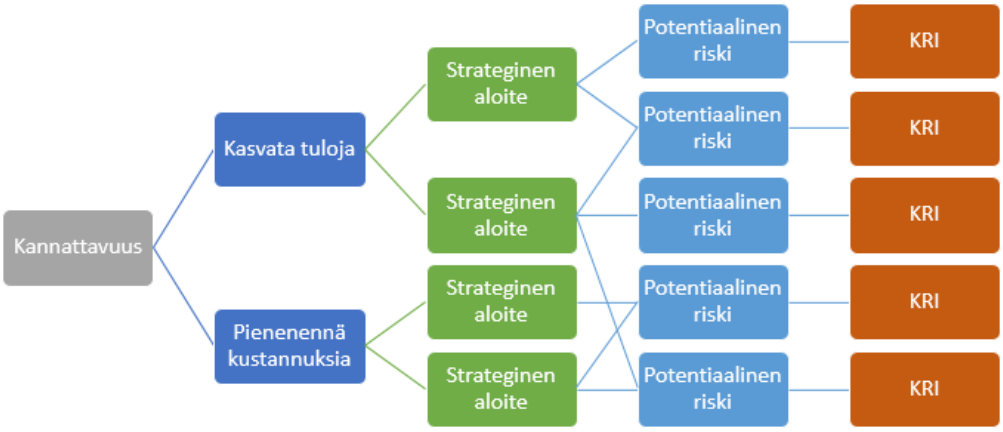
3.1.6 Seuranta ja jatkuva parantaminen

Seurannan yksi tarkoituksista on tarkistaa ja arvioida yrityksen edistymistä tavoitteiden ja suunnitelmien osalta. Katselmusten lähtökohtana on yrityksen strategia ja tarkoitus on saada mahdollisimman kattava kuvaus kokonaisuudesta. Seurannan yhteydessä tulee käsitellä myös uudet mahdollisuudet ja niiden hyödyntäminen sekä tulevaisuuden riskit ja niihin varautuminen. (Laamanen 2012.) Seurannan tapa riippuu riskistä, koska osa riskeistä ovat muuttuvia ja vaativat jatkuvaa seurantaa ja arviointia. Toiset riskit taas pysyvät samantyyppisinä ja vaativat vain uudelleenarvioinnin säännöllisin väliajoin, mutta muuttuneet olosuhteet saattavat laukaista jatkuvan seurannan tarpeen. (Curtis & Carey 2012.) Se mitä riskejä seurataan, riippuu yrityksen painotuksesta ja koosta. Pienille yrityksille jokin operatiivisista riskeistä voi olla merkittävämpi kuin muut riskit. Myös jos yritys päättää riskienhallinnan kohdistamisen strategisiin riskeihin, tällöin niitä on enemmän seurannassa. (Ilmonen 2016.) Ilmonen (2016) suosittelee, että riskit kiinnitetään strategisiin tavoiteisiin, tällöin saadaan riskin seurannan yhteydessä päivitetty kuva siitä, että mikä on esteenä tai hidasteena analysoiduissa riskeissä ja niiden vaikutus tavoitteisiin. Lisäksi yhdistämällä riskiraportointi johtamis- tai strategiaprosessin yhteyteen, riskiraportointi ja seuranta tapahtuvat tietyin väliajoin esimerkiksi neljännesvuosittain ja riskikuva pysyy päivitettynä. Mutta riskien seuranta on hyvin riippuvainen siitä, että kuinka vahvasti yritys haluaa integroida riskienhallinnan osaksi johtamisjärjestelmää. Tällöin tulee pohtia, että riittääkö riskiseurannaksi raportti kerran vuodessa toteutuneista riskeistä ja suurimmista uhista vai halutaanko päätöksenteon tueksi luotettavampaa tietoa riskeistä.

(Juvonen et al. 2005.) Raportointia kuitenkin pidetään hyvin tärkeänä osana riskienhallintaa ja erityisesti tulee seurata hallintatoimenpiteiden toteutumista ja vaikuttavuutta. Näiden seuraamisella ja raportoinnilla yritys pystyy arvioimaan oman riskienhallinnan toimivuutta ja onnistuvuutta. (Rautanen 2011.)

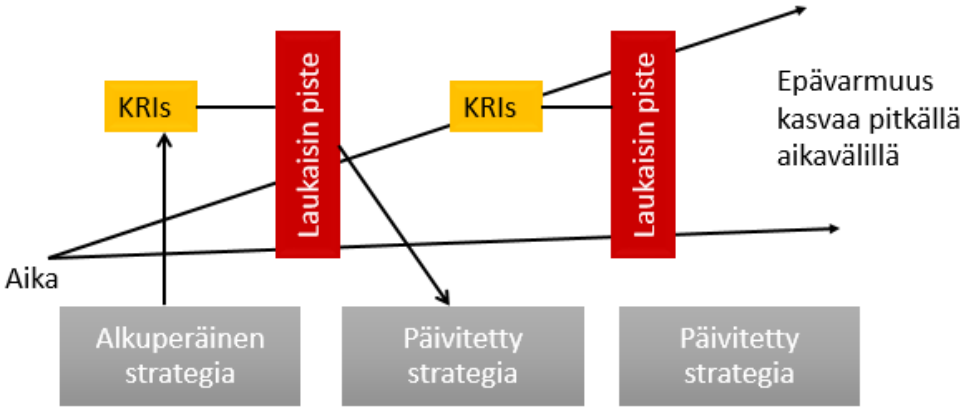
Useimmiten merkittävämmät riskit tai niiden syyt eivät muutu, mutta vaikutus ja näkymät voi muuttua (Ilmonen 2016). Tästä syystä raportointiin ja seurantaan liittyvä aineisto syntyy riskikartoituksessa, jonka yhteydessä on tärkeää kerätä riskitietoa järjestelemällisesti ja huolellisesti. Tällöin kyetään paremmin löytämään oikeat ja riittävät toimenpiteet, joita raportoinnissa seurataan. (Rautanen 2011.) Kattavan tiedon valossa voidaan myös tarkastella tarvittavia toimenpiteitä uudelleen muuttuneessa tilanteessa (Ilmonen 2016).

Hyvin suunniteltu kokonaisvaltainen riskienhallintajärjestelmä tarjoaa tietoja, joiden avulla johdolla on mahdollisuus ymmärtää, täyttävätkö keskeiset strategiset tavoitteet ja mitkä ovat mahdollisuudet sopeuttaa strategioita ja taktiikoita hyödyntämällä toimintaympäristön muutoksia organisaation ja sen sidosryhmien eduksi. Riskienhallinnan voi ottaa mukaan strategian seurantaan, jolloin organisaatiota herätellään aiheesta ja saadaan käsitys riskeistä, joita mahdolliset muutokset strategiassa aiheuttavat. (Ilmonen et al. 2016.) Aiemmin esitetty Sheehanin tapa tunnistaa tavoitteet ja niihin liittyvät riskit strategiakartan avulla, voidaan strategia seurannassa yhdistää nämä tiedot ja liittää niihin kriittinen riskimittari eli key risk indicator (KRI). KRI:n pitäisi antaa kvantitatiiviset tiedot riskialttiudesta sekä varhaisen varoituksen riskin toteutumisesta kuten kuvassa 11. KRI:n tarkoitus on seurata merkittävimpiä riskejä ja pohtia niihin sopivat seuranta yksiköt. Operatiivisella tasolla esimerkiksi käsittelyvirheet, asiakasreklamaatiot tai järjestelmien katkoaika. (Lam 2014.) KRI:lle voidaan määrittää erilaisia tasoja, joiden ylittäessä tai alittaessa tilanne otetaan tarkasteluun johtoryhmässä ja mietitään mahdollisia lisätoimia (Ilmonen 2016). Johto voi käynnistää toimenpiteitä esimerkiksi sopeuttaakseen strategiat ennakoivasti riskin hallitsemiseksi. (Beasley et al. 2010.)



Kuva 11. *Strategiatavoitteista johdettu riskimittari (mukaillen Beasley et al. 2010).*

Kuvasta 12 näkyy, kuinka ajan myötä epävarmuus vaihtelee valittujen strategioiden kohdalla ja mikä uhkaa näiden strategioiden onnistumista. Epävarmuuden vuoksi ilmenevien riskien seurantaa varten johto voi tunnistaa erilaisia kriittisiä riskejä, joita he tarkkailevat suorittaessaan valittua strategiaa. (Beasley et al. 2010.) Yksi keino yhdistää riskit ja strategia on tunnetun strategiatyökalun Balanced score cardin avulla. Yhdistämällä riski-indikaattorit tärkeimpiin tulosindikaattoreihin tasapainotetussa tuloskortissa, yritys pystyy välttämään epätasapainoisen analyysin yrityksen kehityksestä. (EY 2017.) Kun strategioita tarkistetaan, uusia KRI-käynnistyspisteitä laaditaan etukäteen suunnitelluilla toimintasuunnitelmilla. KRI:n strateginen käyttö lisää todennäköisyyttä, että johdon asettamat tavoitteet saavutetaan, koska riskejä ja niihin liittyviä strategioita hallitaan entistä ennakoivammin, kun asiaankuuluvat KRI:t on tunnistettu. (Beasley et al. 2010.)



Kuva 12. *KRI ja strategia (mukaillen Beasley et al. 2010).*

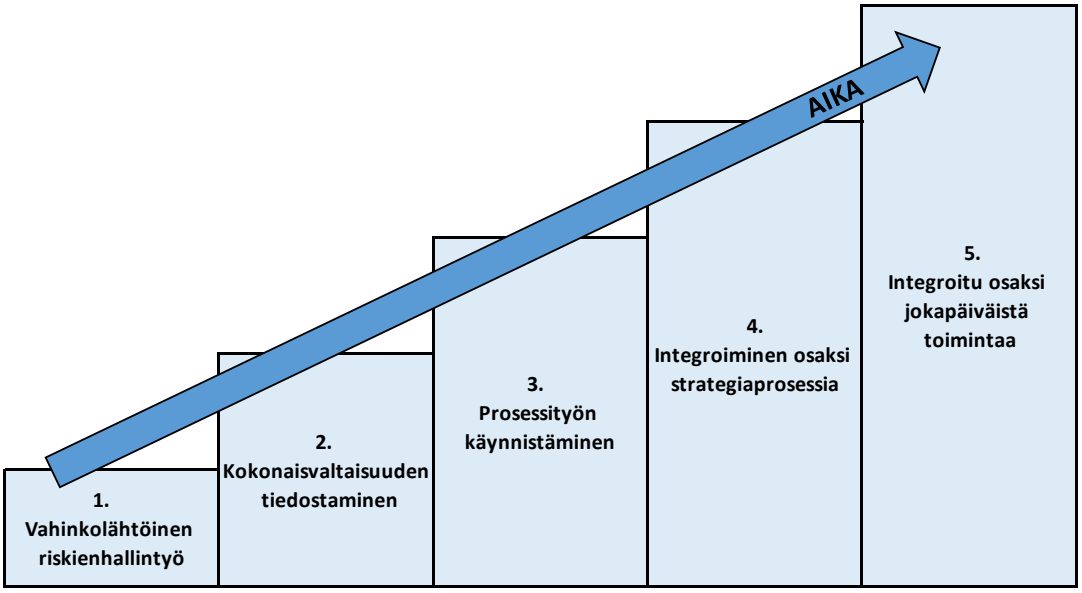
Jatkuvassa parantamisessa tulee huomioida poikkeamista ja vahingoista oppiminen. Tärkeää onkin, että poikkeaman jälkeen ei lähde etsimään syyllistä vaan tilanne tulee analysoida ja ottaa oppia tapahtuneesta ja miettiä toimenpiteet, joilla jatkossa vastaavia vahinkoja estetään. Tämä työskentely vaatii luoda kulttuurin ja systeemin, jolla analyysi tehdään. (Ilmonen 2016.) Riskiperusteisena ajatteluna tämä tulee tehdä tarkastelemalla, että onko riski kirjattu ja siinä olevat toimenpiteet olleet kuinka vaikuttavia.

3.2 Riskienhallintajärjestelmän integroiminen osaksi toimintaa

Riskienhallinnan integroiminen onnistuneesti edellyttää, että asiat riskienhallinnan osalta tehdään mahdollisimman yksinkertaisesti, selkeät ja yksinkertaiset mittarit sekä arvioinnin keinot (Rautanen 2011). Melko paljon järjestelmän integroiminen on riippuvainen yrityksen johdosta eli sen tavasta johtaa ja kiinnostuksesta riskienhallintaa kohtaa. Tekemisen täytyy lähteä johdosta ja heidän tulee asettaa tavoitteet riskienhallinnalle. (Ilmonen 2016.) Lisäksi integroituminen on riippuvainen yrityskulttuurista, organisoinnista, tavoitteista, aikataulusta ja käytetystä johtamisjärjestelmästä (Juvonen, Korhonen et al. 2005). Tästä syystä yksinkertaisuus riskienhallinnassa korostuu, kokonaisuus ei saa olla liian

suuri ja vaikeaselkoinen, tällöin se on helpompi omaksua ja se ei jää irralliseksi prosessiksi muusta johtamisesta (Ilmonen 2016). Juvonen ja Korhonen (2005) toteaa, että riskienhallinta antaa sitä enemmän informaatiota päätöksenteon tueksi, mitä paremmin se on integroituna toimintaa.

Integroituminen tapahtuu vaiheittain riippuen yrityksen kypsyydestä. Ilmonen (2016) esittää viisi eri vaihetta, kuinka riskienhallinnan kehittyminen ja integroituminen tapahtuvat (kuva 13). Ensimmäinen vaihe on vahinkokeskeinen riskienhallinta, joka syntyy yrityksille pelkästään laki- ja viranomaisperusteisista vaatimuksista kuten työturvallisuuslaista, työterveyshuoltolaista ja kemikaalilaista. Toinen vaihe on kokonaisvaltaisuuden tiedostaminen eli yrityksen johto tiedostaa tarpeen aloittaa kattavan riskienhallinnan eri toiminnoissa ja tässä vaiheessa usein luodaan riskienhallintapolitiikat ja ohjeistukset sekä pyritään muodostamaan tukitoimintoja, jotta riskienhallinnasta saadaan jatkuva eikä projektiluontoista. Kolmas vaihe on prosessityön käynnistäminen, jolloin tukitoimintoja selkeytetään ja prosesseihin liitetään riskien tunnistaminen ja kontrollien laatiminen. Neljäs vaihe on riskienhallinnan integroiminen toiminnan suunnitteluun eli yrityksessä on ymmärretty ennaltaehkäisevän riskienhallinnan merkitys. Riskiarvioinnit tulee mukaan strategiaprosessiin ja riskienhallintakulttuuri on vahvistunut. Se toimii alhaalta ylös ja toisin päin sekä raportit ja mittarit ovat aktiivisessa käytössä. Viimeinen viides vaihe on, että riskienhallinta on integroitu osaksi jokapäiväistä toimintaa, jolloin jatkuva riskienotto on perusteltua sekä tietoista ja riskienhallintakulttuuri on vahvana tekijänä koko organisaatiossa. Riskienhallinnan perustehtävä on edelleen tavoitteiden saavuttamisen tukena, mutta negatiivissävytteinen hallinta alkaa muuttumaan enemmän mahdollisuuksien hallinnaksi. Riskienhallinta on täydellisesti integroitu osaksi johtamista ja toimintaympäristön muuttuessa myös riskienhallintajärjestelmää kehitetään eteenpäin.



Kuva 13. *Riskienhallinnan integroitumisen vaiheet (mukaillen Ilmonen 2016).*

Ilmonen (2016) toteaa, että integroimista helpottaa, kun riskitietoisuutta lisätään yrityksessä. Riskienhallinnan osalta pitää tiedostaa myös sen haasteet, jotka voivat estää sen sulautumista jokapäiväisen toimintaan. Hiltunen (2015) on listannut neljä erilaista riskienhallintaan liittyvää haastetta. Ensimmäinen on samojen riskien käsittely, vaikka riskienhallinta olisikin systemaattista, se saattaa johtaa kyvyttömyyteen tunnistaa uusia riskejä maailman muuttuessa. Toinen haaste on valmis riskiluettelo eli riskikartoitus muodostuu rutiiniksi, joka pohjautuu valmiiseen riskiluetteloon. Kolmas haaste on rutinoituminen eli kartoitus tehdään rutiininomaisesti vuosikellon niin vaatiessa ja toimenpiteet eivät johda todellisiin tekemisiin, ollaan vain tyytyväisiä, kun listat ovat taas esittelykunnossa. Neljännen haasteen muodostaa johdon ja hallituksen epäonnistuneiden päätösten puuttuminen riskiluettelosta. (Hiltunen 2015.) Myös Temmes ja Välikangas (2010) luettelee samantyyppisiä asioita riskinä riskienhallinnassa, kun riskien kanssa aletaan elämään tottuneesti, niin se ei paranna kokonaistilannetta ja jäännösriskit jäävät huomiotta, jolloin ne alkavat kasaantua ja seurauksena strategia voi pettää. Mutta riskejä on otettava ja tästä syystä avoimuus riskejä läpikäydessä on hyvin oleellista, se mahdollistaa selviytymisen riskeistä. Yksi esteistä riskienhallinnan integroitumiseen saattaa olla myös, että hallitukselta puuttuu tietämys riskienhallinnassa ja hallitus on yksimielinen, jolloin perusteellisia ja avoimia keskusteluja riskeistä saattaa jäädä käymättä (Andersen 2006).

Tehokkaan koko yrityksen riskienhallintajärjestelmän luominen on johdon keskeinen velvollisuus (MacLeod et al. 2012). Kuten monesti jo todettu, että ratkaisevaa riskienhallinnassa on ylimmän johdon, mukaan lukien hallituksen, täydellinen sitoutuminen. Hallituksen on muun muassa osoitettava suuntaa määrittämällä riskinottohalukkuus organisaatiossa. (Andersen 2006.) Hallitukset ja johto vastaavat kokonaisvaltaisesta lähestymistavasta organisaatioriskien tunnistamiseen, riskien lieventämiseen, havaittujen riskien ja

valvonnan seurantaan ja tarkasteluun sekä riskienhallinnan integrointiin organisaatiossa - sekä strategisissa että operatiivisissa riskeissä. (MacLeod et al. 2012.) Johtajat ovat lopulta vastuussa ja heidän on omaksuttava riskienhallintaprosessiin sitoutuminen varmistaakseen, että henkilöstö omaksuu sen ja asettaa sävyn positiiviselle riskikulttuurille. Asenteiden on läpäistävä organisaatio, joka pyrkii luomaan vahvan ja positiivisen riskienhallintakulttuurin, joka lopulta onnistuessaan johtaa asianmukaiseen rakenteeseen. (Andersen 2006.) Yritys tietää tekevänsä oikein riskienhallintaa, kun johtajat kaikilla eri tasoilla käyttävät syntyvää tietoa päätöksenteon tukena (Curtis & Carey 2012).

Riskienhallinta on enemmän taitoa ja asennetta kuin prosessi. Ei ole mahdollista asettaa riskinottohalukkuutta ilman, että kulttuuri ei ole tietoinen; ei voida valita riskirajoituksia ilmoittamatta riskejä organisaatiossa; ei voi olla suurta riskinarviointiin perustuvaa lähestymistapaa ilman, että palautepiiri tarkastelee ja parantaa oppimiseen perustuvaa prosessia. (Anderson 2017.)

Luvussa käsiteltiin hyvin laajasti tiedon tuottamista riskienhallinnan avulla. Se kuinka paljon tietoa riskeistä kerätään ja hyödynnetään, riippuu yrityksen johdosta, mutta riskienhallinta lähtee liikkeelle jo strategiaprosessista ja kulkee johtamisprosessin avulla eri tasoille organisaatioon. Lopulta riskienhallinnalla on vaikutusta asiakastyytyväisyyten, koska mitä paremmin yritys tunnistaa mahdollisuuksia ja hallitsee riskejä, tuottaa se arvoa niin omalle toiminnalle kuin asiakkaallekin. Tärkeäksi tekijäksi tässä kohtaa nousee riskikulttuuri, joka on näkymätön osa liiketoiminnassa, mutta hyvin hallitseva onnistuneessa riskienhallinnassa. Kuten Anderson toteaa, että riskienhallinta on enemmän taitoa ja asennetta kuin prosessi, jota vain toteutetaan pakosta. Riskien seurannalla voidaan ennakoida ja tarvittaessa muuttaa esimerkiksi strategiaa ja liiketoimintasuunnitelmaa, tällöin päätösten tukena on riskeistä kerätty tieto.

4. AINEISTO JA MENETELMÄT

Tässä kappaleessa kuvataan yrityksen nykytilaa riskienhallinnan osalta ja tehdään havaintoja ISO 31000 viitekehyksen ja aiemmin teoriassa esitetyn teoreettisen mallin pohjalta. Näiden pohjalta tehdään yhteenveto nykytilasta ja kootaan tarvittavat toimenpiteet, joiden avulla yritykseen kehitetään systemaattinen ja toimiva riskienhallintajärjestelmä, joka täyttää yrityksen johdon asettamat vaatimuksen järjestelmälle. Aineistoa on kerätty haastattelemalla yrityksen laatupäällikköä ja johtoryhmän jäseniä, tekemällä havaintoja riskien tunnistus tilaisuuksissa ja tutustumalla yrityksen toimintatapoihin, järjestelmiin ja olemassa olevaan tietoon.

Haastattelut olivat yksilöhaastatteluja ja haastatteluiden teemana oli riskienhallinta yrityksessä eli haastateltavien kanssa käsiteltiin yleisesti riskien määritelmää ja miten yrityksen riskeistä saa tietoa, nykytilaa riskienhallinnasta yrityksessä, kuinka riskit ovat mukana strategiassa ja päätöksenteossa sekä näkemyksiä, kuinka riskienhallintaa tulisi organisoida ja integroida yrityksen toimintaan. Haastattelut olivat puolistrukturoituja, koska haastateltaville annettiin etukäteen tietoon aiemmin luetellut käsiteltävät aiheet. Vaikka työstä on rajattu vahinkoriskit pois, käsitellään niitä seuraavassa luvussa, koska se kuuluu osana kerättyä aineistoa.

4.1 Riskienhallinnan nykytila yrityksessä

Luvussa 3.3 kuvattiin riskienhallinnan eri vaiheet yrityksen toimintaan integroitumisessa (kuva 13). Kohdeyrityksen tilaa kuvastaa vaihe kaksi eli vahinkolähtöinen riskienhallintatyö on yrityksessä toimivaa ja systemaattista, mutta kokonaisvaltaisuus muiden riskien osalta yrityksessä on tiedostettu. Riskienhallintaan liittyvää seurantaa ja toimenpiteitä on toteutettu työturvallisuus- ja kemikaaliriskien osalta useita vuosia sekä vuonna 2017 on pilotoitu riskienhallintaprosessia myynti- ja toimitusprojektien osalta. Tietoturvariskit on kartoitettu ulkopuolisen tahon toimesta muutamia vuosia sitten ja toimenpiteitä on tehty niiden pohjalta, lisäksi EU:n tuoma tietosuoja-asetus edellytti riskiperusteista lähestymistä ja tunnistamaan henkilötietojen käsittelyyn kohdistuvia riskejä. Strategian ja sidosryhmien osalta uhkia ei ole tunnistettu, muuta kuin vuonna 2014 tehdyssä SWOT -analyysissä strategiasuunnittelun yhteydessä, jota ei tämän jälkeen ole käsitelty tai tarkasteltu tarkemmin uudelleen. Liiketoimintaan ja prosesseihin liittyvien riskien tunnistusta on nostettu esiin useissa toimintajärjestelmän sisäisissä auditoinneissa, mutta prosessi ei ole lähtenyt kunnolla liikkeelle.

Riskienhallinta kuitenkin koetaan merkitykselliseksi ja hyödylliseksi, erityisesti markkinoihin ja kilpailijoihin liittyvät riskit koetaan uhkaavimmiksi. Haastatteluissa tuotiin esiin, että liiketoimintaa ei voida tehdä ilman riskejä ja niitä kyllä tiedostetaan, mutta tieto

riskeistä jää hyvin paljon kommunikaation varaan käytävillä ja palavereissa sekä omaan päähän. Yrityksen johdossa on kauan työelämässä ja toimialalla olleita henkilöitä, joilla riskitietoisuus on selkärangassa ja esille tuotiin myös, että tekniikkaan liittyviin riskeihin kuuluu tietyntyyppinen ammattietiikka pohtia mahdollisia riskejä ja seurauksia, mutta systemaattisuus ja tarkempi analyysi puuttuvat erityisesti liiketoimintaan yleisesti liittyvistä riskeistä. Vaikka riskienhallintaa kuvaillaan olevan vielä alkutekijöissä, riski ja riskienhallinnan käsitteet kuitenkin nähdään samansuuntaisina. Riskienhallinnasta tosin tiedetään vähän kokonaisuutena henkilöstön kesken ja se saatetaan kokea helposti ylimääräisenä työnä. Yrityksessä ei voida puhua kokonaisvaltaisesta riskienhallinnasta, mutta elementtejä siihen löytyy kuten ennakoivana toimintana ovat toimittajapalaverit ja auditoinnit säännöllisesti, joissa seurataan toimittajia ja pohditaan, että aiheuttavatko nämä riskiä omaan toimintaan. Myös päätöksenteossa on riskienhallinnallisia elementtejä, mutta niitä ei systemaattisesti arvioida tai seurata.

Riskienhallinnan tavoitteet ovat tällä hetkellä täyttää viranomaisvaatimukset kuten työturvallisuus ja kemikaaliriskien osalta, joiden kartoitus perustuu työturvallisuuslakiin 738/2002. Riskienhallinnan periaatteita ja tavoitteita ei ole kirjattu yhteiseen riskienhallintapolitiikkaan, mutta yrityksen toimintakäsikirjaan on määritetty toimintamalliin riskiperusteinen ajattelu sekä yrityksen johdon sitoutuminen riskien ja mahdollisuuksien tunnistamiseen ja käsittelyyn.

Riskejä ei ole varsinaisesti luokiteltu muulla tapaa kuin puhumalla työturvallisuusriskeistä, projektiriskeistä ja tietoturvariskeistä, joissa riskien tunnistusta on jo tehty. Riskienhallinnassa tulee jakaa vastuut ja roolit, vahinkoriskien osalta prosessista ja havaittujen riskien viestimisestä vastaa yrityksen laatupäällikkö. Muiden riskiluokkien osalta vastuita ja rooleja ei ole määritetty.

Riskienhallinnassa on toteutettu systemaattista toimintatapaa ja riskienhallintatoimenpiteitä vain vahinkoriskien osalta. Niiden osalta on tehty selkeä ohjeistus, prosessi ja riskien tunnistuksessa on käytössä valmis dokumenttipohja, jota päivitetään vuosittain ja joka kolmas vuosi riskit kartoitetaan uudelleen. Taulukossa 3 on esitetty nykyinen arviointitaulukko vahinkoriskien osalta. Arviointi perustuu riskin todennäköisyyteen ja sen seurausten suuruuteen. Riskin arvioinnissa käytettävässä dokumenttipohjassa on sarakkeet vaaratilanteen kuvaukselle, riskin suuruudelle, mahdolliselle toimenpide määritykselle sekä vastuu ja aikataulu määritykselle. Arvioinnissa on käytössä periaate, että jos riskiluokka on suurempi kuin kolme, tälle tulee määrittää toimenpiteet. Vahinkoriskien osalta raportointi tapahtuu vuosittain tuotannon koulutustilaisuuksissa, koko organisaation tilinpäätöstilaisuudessa sekä riskien toimenpiteiden vaikuttavuuden arviointi käsitellään, jos tapahtuu läheltä piti-tilanne tai sisäinen poikkeaman.

Taulukko 3. *Vahinkoriskeissä käytettävä arviointitaulukko.*

Riskien luokittelu tehdään seuraavan taulukon mukaisesti:

Esiintymisen todennäköisyys	**Seuraukset**		
	VÄHÄISET	HAITALLISET	VAKAVAT
EPÄTODENNÄKÖINEN	**1 Merkityksetön riski**	**2 Vähäinen riski**	**3 Kohtalainen riski**
MAHDOLLINEN	**2 Vähäinen riski**	**3 Kohtalainen riski**	**4 Merkittävä riski**
TODENNÄKÖINEN	**3 Kohtalainen riski**	**4 Merkittävä riski**	**5 Sietämätön riski**

Riskien arvioinnin perusteella tulee ryhtyä toimenpiteisiin seuraavasti:

Riski	**Toimenpiteet ja aikajänne**
1 - MERKITYKSETÖN	Ei tarvita toimenpiteitä.
2 - VÄHÄINEN	Ennalta ehkäiseviä toimenpiteitä ei tarvita. Pitäisi kuitenkin harkita parannuksia, jotka eivät aiheuta lisäkustannuksia. Tarvitaan seurantaa, jolla varmistetaan, että riski pysyy hallinnassa.
3 - KOHTALAINEN	Riskin pienentämiseksi on ryhdyttävä toimiin, mutta ennaltaehkäisyn kustannukset on mitoitettava ja rajattava tarkasti. Toimenpiteet on toteutettava määrätyn ajan kuluessa.
4 - MERKITTÄVÄ	Työtä ei pidä aloittaa ennen kuin riskiä on pienennetty. Jos riski liittyy meneillään olevaan työhön, ongelma pitäisi korjata lyhyemmässä aikataulussa kuin kohtalaisen riskin ollessa kyseessä.
5 - SIETÄMÄTÖN	Työtä ei pidä aloittaa eikä jatkaa ennen kuin riskiä on pienennetty. Jos riskin pienentäminen ei ole mahdollista edes rajoittamattomilla resursseilla, työ täytyy olla pysyvästi kielletty.

Yrityksessä on otettu käyttöön vuoden 2017 keväällä projektiriskien kartoitus, johon on määritetty selkeä ohjeistus, vastuut ja prosessi. Tarkoituksena on tehdä tarkempi riskien tunnistus, kun kyseessä ei ole budjettitarjous tai myyntipäällikkö kokee tarpeelliseksi kartoittaa riskit tarjouksen ollessa poikkeava esimerkiksi tuotteen osalta. Jos tarjous muuttuu toimitusprojektiksi, tarjousvaiheessa tunnistetut riskit päivitetään ja täydennetään projektin aloituspalaverissa. Riskejä seurataan projektin kuluessa ja projektin päätyttyä arvioidaan, toteutuiko riskit, oliko toimenpiteet riittävät ja mitä tulee huomioida tulevissa projekteissa.

4.2 Riskien kartoitus yrityksessä

Tutkimustyön aikana riskien kartoitusta ei oltu tehty kuin muutamasta tarjouksesta ja projektipalaverin asialistalla oli kirjattuna muutama riski. Haastatteluissa kuitenkin tuotiin esiin, että ideaalitilanne olisi, että riskit kulkisivat tarjousvaiheesta projektin loppuun saakka. Tällöin jokaisessa prosessissa oltaisiin tietoisia mahdollisista riskeistä ja niiden kytköksistä sekä tarjousvaiheessa ilmenneeseen uhkaan osattaisiin varautua etukäteen. Riskienhallinta tarjouksissa ja projekteissa nähdään myönteisenä asiana, haastatteluissa tuotiin esiin, että se mahdollistaisi valitsemaan hyvät projektit ja projektit pystyttäisiin hoitamaan mahdollisimman pienin ongelmin. Tärkeäksi havaittiin lisäksi se, että projektin loppupalaverissa käytäisiin läpi toteutuneiden riskien lisäksi onnistumiset, joista voitaisiin oppia, hyödyntää toisissa projekteissa ja löytää uusia mahdollisuuksia tätä kautta.

Projektiriskien pilotoinnin yhteydessä luotiin olemassa olevaan tiedonhallintajärjestelmään ”SP possible risk” niminen luokka, jonka alle kirjaamalla tunnistetut riskit tallen-

tuvat järjestelmään ja tätä kautta syntyy automaattinen riskirekisteri, josta jokainen organisaatiossa näkee analysoidut riskit ja niitä voidaan lisätä esimerkiksi johtoryhmän tai projektipalaverin asialistalle. Riskirekisteriä voidaan päivittää helposti ja siihen jää historiatieto tehdyistä toimista ja analyyseistä. Riskirekisteriin on luotu erilaisia näkymiä, joiden kautta voidaan tarkastella tiettyihin projekteihin tai tarjouksiin liitettyjä riskejä. Kun esimerkiksi tarjousprojektien riskejä tunnistetaan jatkossa enemmän, voidaan aiemmin käsiteltyjä riskejä hyödyntää samantyyppisissä projekteissa.

5. TULOKSET JA TULOSTEN TULKINTA

Tässä luvussa on tarkoitus esitellä työn tulokset, joita kerätyn aineiston pohjalta on tulkittu. Tuloksissa käydään läpi haastatteluiden pohjalta nousseet tarpeet ja vaatimukset sekä niiden pohjalta haivatut tarpeet kehittämistoimenpiteille.

5.1 Kohdeyrityksen asettamat tarpeet ja vaatimukset riskienhallinnalle

Haastatteluissa pyrittiin saamaan mahdollisimman kattava kuvaus eri näkemyksistä riskienhallinnasta yrityksessä, kuinka se toimii nyt, miten omassa työssä näkyy ja kuinka riskienhallinta nähdään ylipäätänsä. Riskiperusteista ajattelua perustellaan standardeissa (ISO 9001 ja ISO 31000) lisäarvon tuomisella yrityksen toimintaan. Kerätyn haastatteludatan pohjalta voidaan todeta, että kohdeyrityksessä riskienhallinta nähdään lisäarvoa tuottavana tekijänä, kunhan se on sopivalla tavalla toteutettu yrityksen toimintaan. Myös DNV-GL:n tekemän tutkimuksen (2016) mukaan 80 prosenttia vastanneista ajattelee, että johtamisjärjestelmään sisällytetty strukturoitu riskienhallintajärjestelmä tuo lisäarvoa organisaatiolle ja sen sidosryhmille ja erityisesti kyselyyn vastanneet johtajat (noin 95 %) ajattelevat näin.

Gustafsson (2001) on tehnyt tutkimuksen, jossa tutkittiin ISO 9000 standardin implementointia pienyrityksiin. Tuloksissa tulee selkeästi esiin, että jos järjestelmä hankitaan ja implementoidaan puhtaasti ulkoisten vaatimusten tähden, on todennäköisempää, että sen implementointi epäonnistuu. Oli kyse mistä tahansa järjestelmästä, asenne ja halu ovat ratkaisevia tekijöitä implementoinnin onnistumiseen. Myös uudet versiot ISO 9001 ja ISO 31000 standardeista korostavat johtajuutta, jotta järjestelmä on tehokas ja sisällytetty toimintaan. Tämän tutkimustyön tarve syntyi ulkopuolisten tahojen toimesta, erityisesti päivitetty laadunhallintajärjestelmän standardi ja sen korostama riskiperusteinen ajattelu. Tämä tuotiin myös esiin haastatteluissa, kun kysyttiin merkittävimpiä syitä riskienhallinnan kehittämiseen kohdeyrityksessä. Vaikka standardi ei vaadi käyttämään muodollisia riskienhallintamenetelmiä tai dokumentoimaan niitä, mutta haastatteluissa tuotiin esiin myös tarvetta kehittää riskienhallintaa kattavammaksi liiketoiminnan tueksi.

Riskienhallinnan halutaan olevan ennakoivaa eikä vain riskilistauksen luomista, josta todetaan jälkikäteen, että täällä olikin tällainen riski tunnistettu. Riskiperusteisen ajattelun tarkoitus on olla ennakoivaa eikä vain estää tai vähentää ei-toivottuja vaikutuksia (ISO/TC 176/SC2/N1284).

Riskit ja mahdollisuudet: käytännön neuvot riskien hallintaa (2012) kirjassa Juha Pietarinen toteaa, että riskejä ei kannata edes kartoittaa, jos tarkoituksena on vain tehdä listaus riskeistä, tämä ei hyödytä ketään ja saattaa luoda vain pelotteita tekemiselle. Näin myös

muutama haastateltavakin totesi, että riskienhallinnasta ei saa tulla pääagenda eikä luoda turhia pelotteita liiketoimintaan, vaan sen tulee olla jokaisen tietoisuudessa ja tekemisessä mukana sopivalla tavalla kuormittamatta liikaa. Kuten Rautanen (2011) ja Ilmonen (2016) molemmat toteavat, että yksinkertaisuus on riskienhallinnassa olennaista. Kokonaisuus ei saa olla liian suuri ja vaikeaselkoinen, tällöin se on helpompi omaksua ja se ei jää irralliseksi prosessiksi muusta johtamisesta (Ilmonen 2016). Eri viitekehykset korostavat, että riskienhallinta tulee sisällyttää kulttuuriin ja esimerkiksi Louisot ja Ketcham (2014) ovat todenneet, että tehokkaan riskienhallinnan avain onkin siinä, että se on osa kulttuuria ja tämän kautta saadaan yrityksessä työskentelevät henkilöt hallitsemaan riskejä. Johdolla on tässä merkittävä rooli, että asenteet läpäisevät organisaation, kun pyritään luomaan vahva ja positiivinen riskienhallintakulttuuri. Kun riskienhallinta on integroitu osaksi johtamisjärjestelmää ja kulttuuria, on se luontevasti mukana päätöksenteossa eikä kuormita liikaa.

Kuten jo aiemmin tuotiin esiin, että vahinkoriskit koetaan toimivaksi ja systemaattiseksi riskienhallinnan osalta, mutta systemaattisuus puuttuu liiketoiminnan, prosessien ja strategiaan liittyvien riskien osalta. Seurannan puute ilmeni haastatteluissa ja yleisesti toimintaa seuratessa. Projektiriskeille on sovittu, että seurantaa tehdään projektipalavereissa ja muutama riski palavereissa on ollutkin esillä jo toimitetuista projekteista. Diplomityön aikana aloitettiin yhden tarjousprojektin riskien kartoitus, mutta tarjousprosessin ollessa vielä niin alkutekijöissä, ei diplomityöhön saatu täydellistä aineistoa projektiriskien hallintaprosessista. Liiketoimintaan yleisesti ja prosesseihin liittyen ei yrityksessä ole tehty riskien tunnistusta ennen diplomityötä eikä näille ole sovittu seurantaa tai vastuuhenkilöitä. Haastateltavat kertoivat, että strategisia riskejä on aiemman strategiaprosessin yhteydessä pohdittu SWOT -analyysin yhteydessä, mutta niiden systemaattinen seuranta puuttuu. Vaikka kulttuuria ja organisaatiota kuvailtiin asiantuntijaorganisaatioksi, joka ei ole jäykkä ja siilomainen, vaan prosessit keskustelevat keskenään, nähtiin silti mahdollisena, että luomalla systemaattisemman tavan riskienhallintaan lisäisi se avoimuutta ja riskejä pystyttäisiin tuomaan helpommin esiin. Tällöin riskeistä voidaan keskustella ja riskinkantokyky jakautuu eikä jää yhden henkilön harteille tai riskitieto jää yhden henkilön taakse. Myös luomalla systemaattisemman tavan riskienhallintaan nähtiin sen helpommin tulevan tavaksi ja osaksi yrityskulttuuria.

Osa systemaattisuutta ja seurantaa on myös dokumentointi. Tällä hetkellä dokumentaatiota ei juuri ole, vaan kaikki tieto riskeistä perustuu kommunikaatioon ja otetuista tai havaituista riskeistä ei ole tarkempaa analyysiä olemassa. Dokumentointi saatetaan nähdä liian työläänä ja ettei se välttämättä suoraan hyödytä omaa työtä. Yksi tunnistettu riski oli, että tietoa on liian paljon yhden ihmisen päässä ja tämä on pienessä yrityksessä melko vakava, erityisesti jos avainhenkilölle tapahtuukin jotain ja joutuu olemaan työelämästä pois pidemmän aikaa. Riskeistä kuitenkin kommunikoidaan, vaikkakin se tapahtuu usein kahvihuoneessa tai käytävillä jo riskin tapahduttua. Haastatteluissa keskusteltiin kuinka riski ovat mukana päätöksenteossa ja kaikkien haastateltavien mielestä ne ovat mukana

päätöksissä, näkyvästi tai huomaamatta. Haastatteluissa nousi esiin, että riskit ovat mukana päätöksenteossa riippumatta tasosta, jolla se tehdään. Riskejä haluttiin myös mukaan päätöksentekoon näkyvämmin, jotta tehdyistä päätöksistä ja varsinkin niihin liittyvistä riskeistä jää jälki. Tällöin on tiedossa millainen riski tai mahdollisuus on otettu, miksi ja mitä toimenpiteitä sille on tehty. Merkittävistä ja isoista riskeistä ainakin osa haastateltavista halusi saada enemmän tietoa.

Riskit tulisi huomioida koko johtamisprosessin läpi, jolloin huomioidaan liiketoimintaympäristö, strategia ja operatiivinen taso. Johtamisprosessiin lukeutuu myös kaikki päätökset, joita tehdään eri tasoilla. EY (2013) on tutkimuksessaan todennut, että yhä enemmissä määrin yrityksen keskittyvät riskienhallinnan strategisiin ja liiketoiminnallisiin mahdollisuuksiin, kun ennen fokus oli riskien lieventämisessä, kustannusten hallinnassa, liiketoiminnan pois pitämisessä vaikeuksista ja brändin suojaamisesta.

Riskienhallinta strategiaprosessin yhteydessä nähtiin hyvin tärkeänä ja oleellisena osana sitä. Työn aikana yrityksessä aloitettiin uuden strategian prosessi, mutta se oli hyvin lähtökuopissa ja kukaan ei osannut vielä sanoa tarkkaan, kuinka edetään. Shenkir ja Walker (2011) korostavat, että jos strategia on muodostettu siten, ettei riskejä ole tunnistettu, se on puutteellinen ja alttiimpi riskeille. Tilanne on myös sama, jos riskejä ei ole tunnistettu kokonaisvaltaisesti ja merkittävimpiä riskejä ei ole tunnistettu. Tästä syystä uuden strategian luomisen yhteydessä on tärkeää tunnistaa merkittävimmät uhat ja ottaa seurantaan riskit, jotka voivat estää tavoitteiden saavuttamisen. Sheehan (2010) toteaa, että ensisijainen hyöty riskiin perustuvaan strategia lähestymiseen on se, että sen avulla voidaan keskittyä suunnitelmiin sisältyviin mahdollisuuksiin. Haastatteluiden pohjalta kuitenkin voidaan todeta, että strategisten riskien seuranta nähtiin mahdollisena normaalin strategiaprosessin ja tavoitteiden toteutumisen seurannan yhteydessä. Luomalla skenaarioita mahdollisista tapahtumista strategiaan liittyen suurempien kriittisten uhkien kohdalta, voidaan tilanteita ennakoida. Vaikka riskit olisivatkin jokaiselle itsestäänselvyyksiä, mutta tunnistamalla riskejä yhdessä, saadaan luotua keskustelua, näkemyksiä ja jaettua hiljaista tietoa.

Positiivinen asenne ja kulttuuri riskeille ovat avainasemassa kaikessa ja IRM on raportissaan todennut, että yrityksen johdolla on velvollisuus asettaa, viestiä ja valvoa riskikulttuuria. Asenteelliset tekijät nousivat myös haastatteluissa esiin. Selkeänä nähtiin, että johdolla on iso rooli siihen, kuinka riskit nähdään ja niihin asennoidutaan koko organisaatiossa. Kuten aiemmin jo tullut useasti esiin, että asenteet, johdon rooli ja olemassa oleva kulttuuri vaikuttavat siihen, kuinka riskienhallinta nähdään yrityksessä. Jo se, että riskienhallinta integroidaan muista syistä kuin ulkopuolisesta paineesta ja sillä on johdon sitoutuminen, on hyvä lähtökohta riskienhallintajärjestelmän kehittämiselle. Haastatteluissa tuotiin myös esiin se, että jokaisella on vastuu riskeistä ja riskienhallinnasta, mutta sen läpiviemisestä organisaatioon on johdon vastuulla. Yritys on aloittanut vaiheittain tuomaan riskienhallintaa eri toimintoihin ja pienin askelin se saadaan mukaan toimintaan,

jonka jälkeen sitä pystytään tehokkaammin hyödyntämään päätöksissä ja yrityksen strategisissa linjauksissa.

Asenteet ja olettamukset ovat osa kulttuuria, jos näitä halutaan muuttaa, niin Schein (2001) kuvaa, että toissijaisia tekijöitä kulttuurin istuttamiseen on organisaation järjestelmät ja menettelytavat, ensisijaisena on johtajan käyttäytyminen. Se miten johtaja reagoi kriittisiin tapahtumiin ja mihin hän kiinnittää huomiota, mitä he mittaavat ja kontrolloivat säännöllisesti. Näillä on suurin merkitys siihen, mihin muut organisaation jäsenet kiinnittävät enemmän huomiota. Myös kulttuuri, oletukset ja asenne vaikuttavat siihen, että millaista informaatiota kerätään ja miten sitä tulkitaan. Varsinkin se mikä määritetään poikkeamaksi tai virheeksi, upotetaan kulttuurisiin oletuksiin. Virheiden havaitsemiseen useimmat yritykset käyttävät taloudellista suorituskykyä, mutta kulttuuriset oletukset hallitsevat sitä. (Schein 2001.) Tällä on siis vaikutusta siihen, että mitä tietoa riskeistä halutaan kerätä. Tärkeimmäksi dataksi koettiin yrityksessä se, että mitä riskille on jo tehty ja mitä pitäisi tehdä. Tällä hetkellä yrityksessä on oletus, että jokaisella pitäisi olla selkärangassa riskit.

Haastatteluista nousseista asioista, mitä riskienhallinnan tulisi olla haastateltavien mielestä, on koottu taulukkoon 4.

Taulukko 4. *Kohdeyrityksen asettamat tarpeet ja vaatimukset.*

Kohdeyrityksen tarpeet ja vaatimukset	Täyttää ulkopuolisen tahon vaatimukset (ISO 9001:2015)
	Ennakoiva riskienhallinta
	Ei liian kuormittava
	Systemaattinen toimintatapa myös liiketoiminnan riskeihin
	Seurannan puute listatuille riskeille
	Paljon hiljaista tietoa: Tarpeellisen tiedon dokumentointi ja raportointi riskeihin ja mahdollisuuksiin liittyen
	Strategiasuunnittelun ja seurannan yhteyteen riskit
	Positiivinen asenne riskienhallintaa kohtaan
	Yhteinen tiedottaminen yleisistä riskeistä/kokonaiskuvan muodostus

Kohdeyrityksen johdon tarpeet ja vaatimukset kohtaavat melko hyvin teoriassa esitetyn toimivan riskienhallintajärjestelmän piirteitä.

5.2 Riskienhallinnan kehittäminen

Aiemmissa luvuissa tarkasteltiin nykytilaa ja haastatteluiden avulla kartoitettiin kohdeyrityksen tarpeita ja vaatimuksia riskienhallinnalle. Riskienhallinnan kehittämistyössä huomioidaan myös ISO 9001:2015 asettamat vaatimukset riskeille ja niiden käsittelyyn, koska tämä oli yksi tarpeista ja vaatimuksista, joka nousi haastatteluissa esiin.

Puitteiden osalta työn aloitusvaiheessa riskit päätettiin jakaa strategisiin, taloudellisiin, operatiivisiin, projekti ja vahinkoriskeihin. Luokittelun koettiin olevan selkeämpi ja helpompi hallinnoida ja varmistaa, että riskit on tunnistettu jokaisesta luokasta. Luokittelun avulla kyetään myös käsittelemään ja seuramaan riskejä eri yhteyksissä. Yrityksessä ei ole luotu riskienhallintapolitiikkaa, mutta työn aikana tämä luotiin, johon määritettiin yhteiset riskienhallinnan periaatteet, vastuut ja menetelmät ja tämä annettiin tiedoksi koko organisaatiolle.

Haastatteluiden perusteella voidaan tulkita, että riskienhallinnalla on ainakin johtoryhmän tuki ja nykyisessä strategiassa on huomioitu uhkia ja mahdollisuuksia SWOT-analyysin avulla, vielä oli epäselvää, kuinka uudessa strategiassa nämä huomioidaan. Työn puitteissa tätä ei voitu kehittää konkreettisesti ja testata toimivuutta, mutta kehitysehdotus strategisten riskien osalta on esitetty seuraavassa luvussa.

Liiketoiminnan riskejä lähdettiin tunnistamaan aluksi yrityksen prosesseista, koska strategiaprosessi oli vasta alkamassa, joten liiketoimintaympäristön ja tulevien tavoitteiden

riskejä ei päästy tarkastelemaan diplomityön aikana. Prosessien kautta kuitenkin riskit kytkeytyvät liiketoimintaan ja Juvonen (2005) toteaa, että strategian ollessa valmis, tulee sitä soveltaa ja implementoida organisaatiossa ja tässä vaiheessa prosessien osalta tunnistetut riskit helpottavat tunnistamaan strategian toteutumista uhkaavat tekijät. Lisäksi uuden ISO 9001 vaatimuksiin lukeutuu käsitellä laadunhallintajärjestelmän prosesseihin liittyviä riskejä ja mahdollisuuksia.

Prosessiriskejä tunnistettiin siihen kuuluvien henkilöiden kanssa aivoriihenä ja riskit kirjattiin tiedonhallintajärjestelmään. Arvioinnissa käytettiin aluksi vahinkoriskeissä käytettävää taulukkoa riskiluokan määrittämiseksi, mutta se todettiin hyvin nopeasti liian suppeaksi, joten taulukkoa laajennettiin toimimaan asteikolla 1-5 (taulukko 5). Prosessiriskien tunnistamisen yhteydessä ilmeni havaintoja, että arviointi perustuu hyvin paljon henkilön omaan ajatteluun ja näkemykseen seurausten vakavuuksista ja hyvin paljon tunnistetut riskit perustuivat jo tapahtuneisiin tapauksiin.

Taulukko 5. *Uusi arviointitaulukko riskiluokan määrittämiseksi.*

Tapahtuma	**Seuraukset**				
Todennäköisyys	Merkityksetön	Vähäinen	Kohtalainen	Suuri	Sietämätön
Erittäin epätodennäköinen	1	1	2	3	4
Epätodennäköinen	1	2	2	3	4
Mahdollinen	1	2	3	4	5
Todennäköinen	1	3	3	5	5
Erittäin todennäköinen	2	3	4	5	5

Riskejä tunnistettiin yhteensä 50 kappaletta, joita ensin työn tutkija analysoi ja yhdisti päällekkäisiä riskejä. Riskejä myös jaettiin ryhmiin kokonaiskuvan muodostamiseksi, koska esiin nousi selkeästi toimitukseen, henkilöstöön, imagoon ja tuotteisiin liittyviä riskejä. Vakavat ja sietämättömät riskit käytiin vielä yhdessä johtoryhmän kanssa läpi, jossa päätettiin riskit, jotka todellisuudessa vaativat toimenpiteitä ja seurantaa. Seurantaan ja toimenpiteitä vaativia riskejä jäi yhteensä viisi kappaletta. Parhaimmaksi koettiin, että riskienhallinta sisällytetään olemassa oleviin järjestelmiin ja toimintatapoihin eikä luoda omaa yksittäistä järjestelmää. Jatkossa siis prosesseihin liittyviä riskejä tullaan käymään läpi neljännesvuosittain laajennetulla johtoryhmällä, jolloin mukana on myös laatupäällikkö. Näissä tilaisuuksissa käydään läpi, onko toimenpiteitä toteutettu, onko riski mahdollisesti pienentynyt ja onko uusia riskejä tullut esiin, jotka vaativat toimenpiteitä johtoryhmältä. Lisäksi jatkossa prosessien riskejä päivitetään vuosittain sisäisten auditointien yhteydessä, jolloin saadaan systemaattisuutta riskien seurantaan kuten vahinkoriskeissä ja toiminta saadaan sisällytettyä olemassa olevaan tapaan. Myös johdon katselmuksessa käydään yhteenvetona läpi suurimmat muutokset riskien osalta.

Osan haastateltavien kanssa keskusteltiin, että arviointiin voisi määrittää yhteiset rajakriteerit ja ainakin aluksi riskien tunnistuksia olisi hyvä tehdä yhdessä porukalla. Käytännössä osoittautui haasteelliseksi kuvata riskiä ja sen seurauksia kattavasti, nyt riskien tun-

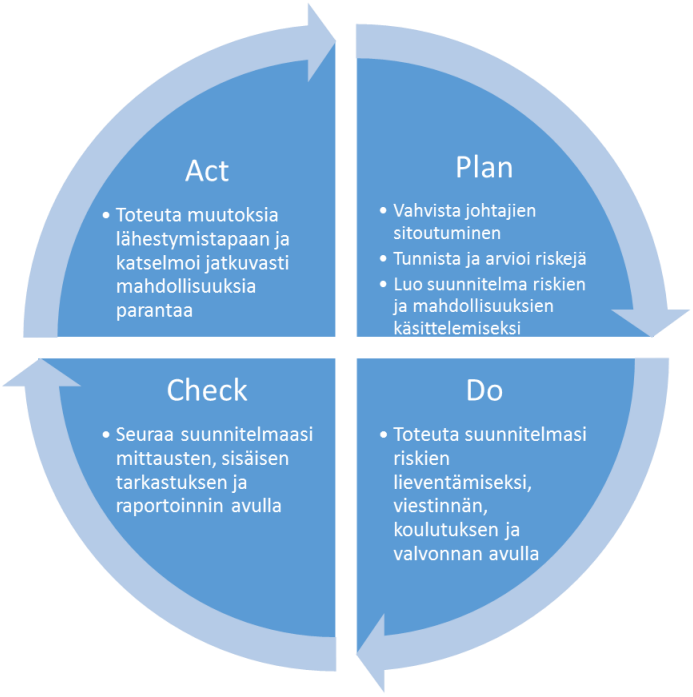
nistuksesta jäi paljon jälkijättöisiä riskejä eli analyyseistä jäi uupumaan, esimerkiksi pohdinta, että mitä jos riski toteutuukin, kuinka siinä vaiheessa tulee mahdollisesti toimia tai onko tapahtuessa mahdollisia seuraus- tai jälkiriskejä. Tästä syystä yksi vaihtoehto on ottaa jokin teema riskien tunnistukseen prosesseissa esimerkiksi asiakkaalle arvon luominen tai tavoitteisiin heijastettava arviointi. Jotta riskien kirjaamisesta saataisiin kattavampi, luotiin ohjeistus ja ohjeisiin lisättiin seuraavia näkökulmia avustamaan riskin tai mahdollisuuden kuvailua ja sen vaikutuksia toimintaan:

- Vaikutus toiminnalle (välitön operatiivinen)
- asiakkaalle
- koko organisaatiolle.

Ohjeisiin lisättiin myös yhteiset arviointikriteerit riskin seurauksille ja todennäköisyyksille, jolloin on yhtenäisempi linja riskin suuruus luokasta.

5.3 Jatkotoimenpiteet kehittämistyöhön

Riskienhallinta vaatii aikaa ja halua integroida se. Riskienhallinnan kehittäminen on jatkuva prosessi ja vasta käytännön toimissa sen tarpeet ja toimivuuden huomaa, siksi jatkossa voi hyödyntää PDCA sykliä (kuva 14) sekä työn aikana kehitettyä kypsyysmallia, jossa voidaan valita painoalue riskienhallinnan kehittämisessä (liite A). Frigon ja Andersonin (2011) mukaan riski on luonteeltaan dynaaminen, joten riskienhallinnan ja arvioinnin on kehityttävä tapahtumasta prosessiksi - ja siihen on sisällyttävä säännöllinen analyysi ja kriittiset riskitiedot päivitetään.



Kuva 14. *PDCA- sykli riskienhallinnan näkökulmasta.*

Liitteenä olevaan kypsyysmalliin on koottu eri osa-alueita ja kuinka niitä tulisi toteuttaa aiemmin esitetyn teorian ja viitekehysten pohjalta. Tämä voisi toimia tarkempana arviointi työkaluna riskienhallinnan tilasta yrityksessä ja löytää tärkeimmät painopiste alueet, joita halutaan kehittää puitteiden tai prosessin osalta.

Sidosryhmä riskit

Päivitetyt standardit ja teoreettisessa mallissakin korostuu se, että kaikki lähtee liikkeelle strategiasta ja arvoista, nämä luovat perustan kokonaisvaltaiselle riskienhallinnalle, jota toteutetaan koko liiketoiminnan laajuudessa. Riskienhallinnalla luodaan arvoa sidosryhmille, omistajille ja niin edelleen. Tarkoitus ei ole enää vain välttää riskejä, vaan pyrkiä hyödyntämään mahdollisuuksia ja ennakoimaan aiemmin. Näistä syistä tulee myös ymmärtää toimintaympäristöä ja sen sisäisiä sekä ulkoisia sidosryhmiä ja niihin liittyviä riskejä ja mahdollisuuksia. Näitä yrityksessä ei ole vielä käsitelty ja myös tämä asia nostettiin esiin ulkopuolisen auditoijan toimesta. Sidosryhmien tarpeiden ja vaatimusten avulla varmistetaan riskienhallinnan päämäärän ja arvioinnissa käytettävät kriteerien asettamiset tarkoituksenmukaisiksi yrityksen kannalta. (Kupi et al. 2009.) Joitakin sidosryhmiin liittyviä riskejä nousi esiin prosessiriskejä tunnistaessa, mutta ainakin tärkeimmiksi koettujen sidosryhmien kohdalla voisi tehdä työpajan, jossa käytäisiin systemaattisesti läpi sidosryhmien odotukset ja tarpeet. Riskejä tulee tarkastella, kun sidosryhmissä tai toimintaympäristössä tapahtuu muutoksia.

SFS ry:n tekemä kalvosarja oppilaitoksille (Johdanto laadunhallinnan ISO 9000 -standardeihin 2016) kiteyttää hyvin sidosryhmät ja niihin liittyvä riskiperusteisen ajattelun ”Si-

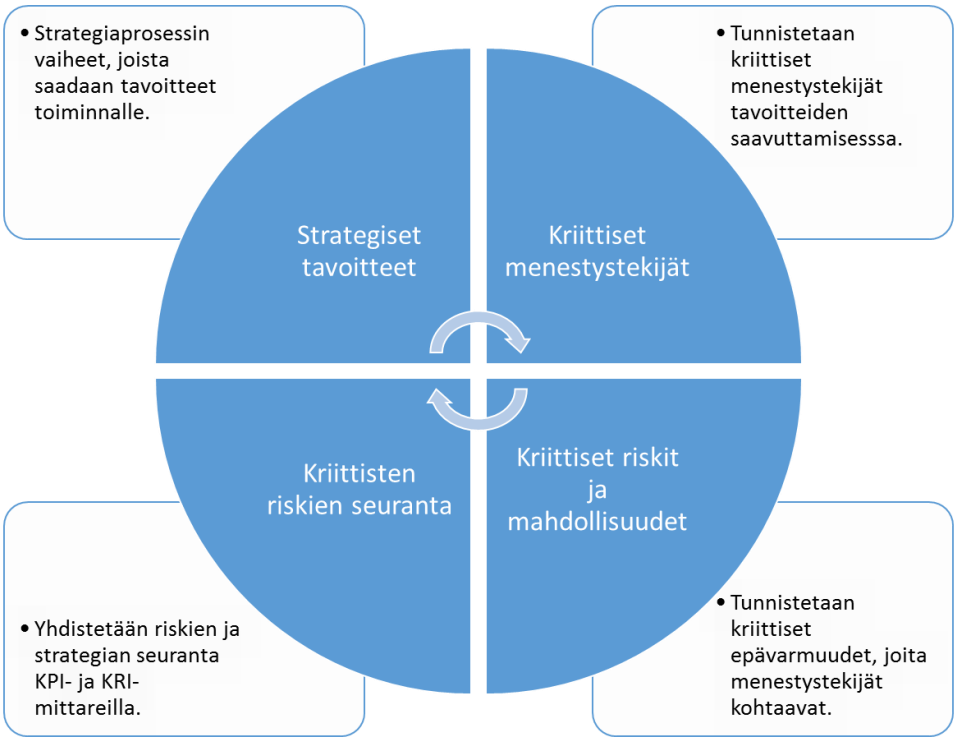
dosryhmiä ovat ne, jotka aiheuttavat merkittävän riskin organisaation kestävälle kehitykselle, jos niiden odotukset ja tarpeet eivät täyty – organisaatiot määrittelevät, mitä tuloksia tarvitaan, jotta kyseinen riski vähenee”

Sidosryhmien tarpeilla ja vaatimuksilla on myös vaikutusta strategian suunnitteluun ja toteuttamiseen. Tästä syystä on tärkeää tunnistaa ja analysoida sidosryhmiin liittyvät riskit, jolloin niitä voidaan hyödyntää myös strategiaprosessin yhteydessä.

Strategiset riskit

Tutkimustyön aika oli melko lyhyt ja erityisesti kun yrityksessä oli uuden strategian aloitusvalmistelut käynnissä, joten strategisia riskejä ei koettu vielä tarpeelliseksi aloittaa tunnistamaan ja sille tuleekin miettiä oikea hetki strategiaprosessissa. Ilmonen (2016) on kirjoittanut, että strategiaan liittyvien riskien tunnistus tulee ajoittaa oikeaan kohtaan, kun tavoitteita on saatu hahmoteltua, mutta ei liian tarkasti, jolloin voidaan tuoda esiin vertailevia vaihtoehto strategioiden uhkia ja mahdollisuuksia esiin. Sheehan (2010) toteaa, että ensisijainen hyöty riskiin perustuvaan strategia lähestymiseen on se, että sen avulla voidaan keskittyä suunnitelmiin sisältyviin mahdollisuuksiin. Mutta alustavasti tulee huomioida riskienhallintasuunnitelmassa, että miten riskien arviointi ja riskienhallinta voidaan integroida strategian toteutusprosesseihin. Tämä käsittäisi riskienhallinnan integroinnin strategisiin suunnittelu- ja suoritusmittausjärjestelmiin. (Frigo & Anderson 2011.)

Frigo ja Anderson (2011) toteavat artikkelissaan, että monissa yrityksissä strateginen riskienhallinta on usein epäkypsätoiminto. Kohdeyrityksessä on nyt tunnistettu ja luotu systemaattisempi tapa prosessien riskeihin, projekti riskeihin sekä vahinkoriskeihin. Jotta riskienhallinta olisi kokonaisvaltaisempi ja huomioisi vielä paremmin strategiset tavoitteet sekä liiketoimintaympäristön, riskit voisi liittää itse strategiaprosessiin. Frigo ja Anderson (2011) kirjoittavat myös artikkelissaan, että strategiset riskienhallintatutkimukset olisi tehtävä osana säännöllisiä strategia-arviointeja. Riskien tunnistamisessa voisi hyödyntää Sheehanin luomaa prosessia (kuva 15), jossa ensin tunnistetaan strategisesti kriittiset menestystekijät, jonka jälkeen näihin liittyviä kriittisiä riskejä. Riskien seurannassa voidaan hyödyntää joko KRI-mittaria, jolloin mittarin mentäessä tiettyjen rajojen yli tai ali, otetaan riski tarkasteluun johtoryhmässä tai yhdistää olemassa olevaan KPI (Key performance indicator) mittariin tietyt raja-arvot. Tärkeää kuitenkin on, että riskit huomioidaan jo strategian luomisen yhteydessä, jolloin voidaan siirtyä keskittymään strategisiin mahdollisuuksiin enemmän. Frigo ja Anderson (2011) ohjeistavat, että tee strateginen riskienhallinta, kuten itse strategian hallinta eli jatkuvana prosessina.



Kuva 15. *Strategisten riskien riskienhallintaprosessi.*

Se kuinka riskit otetaan mukaan strategiaprosessiin, riippuu yrityksen johdosta ja yrityksen kulttuurista. Frigo ja Anderson (2011) kirjoittavat artikkelissaan, että strategisten riskienhallintaprosessien ja -ominaisuuksien kehittäminen voi olla vahva perusta riskienhallinnan ja hallinnon parantamiselle, tällöin myös keskitytään tärkeisiin riskeihin eli strategisiin riskeihin. Kun riskit otetaan huomioon johdon toimesta esimerkiksi strategiassa, luo se positiivista riskikulttuuria yritykseen ja riskeistä voidaan keskustella avoimemmin. Edistämällä kulttuuria riskiperusteiseksi, tapahtuu riskienhallinta ilman sanaa riskienhallinta. Asenteet nostettiin esiin myös tarpeissa ja tärkeää onkin, että johto sitoutuu järjestelmän integroimiseen.

Yksi tunnistustyökalu liiketoiminnan ja strategisiin riskeihin on yrityksessä jo aiemmin tuttu SWOT-analyysi. Analyysi on yksinkertainen ja sen avulla voidaan selvittää yrityksen nykyiset vahvuudet ja heikkoudet sekä tulevaisuuden näkökulmasta mahdollisuudet ja uhat. Nelikenttään kirjatuista asioista voidaan tarkemman keskustelun jälkeen nostaa strategiaa varten kriittisiä tekijöitä ja niiden avulla löytää toimenpiteitä joko mahdollisuuksien vahvistamiseksi, heikkouksien korjaamiseksi tai uhkien pienentämiseksi tai torjumiseksi.

Kun uusi strategia valmistuu, tulee prosessien riskit myös uudelleen arvioida, jotta niiden riskiluokat saadaan vastaamaan strategisia tavoitteita ja niille saadaan selkeä kohde, jota vasten niitä arvioidaan. Nyt riskejä arvioitiin lähinnä yleisestä näkökulmasta, että mikä prosessissa voi epäonnistua ja aiheuttaa toiminnalle riskin.

Projektiriskit

Yrityksessä on tuotekehitys-, myynti- ja toimitusprojekteja. Erityisesti tuotekehitys ja myyntiprojektien yhteyteen voisi sisällyttää riskiperusteista ajattelua enemmän esimerkiksi luomalla yksinkertaisen lomakepohjan (liite B), johon voisi lisätä projektin riskit ja mahdollisuudet, varsinkin, jos projekti on liiketoiminnalle kriittinen, tehtäisiin tarkempi analyysi päätöksenteon tueksi. Päätökset perustuvat sen hetkisiin olemassa oleviin tietoihin ja yksi kohta päätökseen voisi olla kriittisten riskien tunnistaminen. Riskit ja mahdollisuudet huomioitaisiin päätöksenteon yhteydessä, kun päätetään, jatketaanko projektia vai ei. Jos riskit on tunnistettu ja ne koetaan hyväksyttäviksi sellaisenaan tai toimenpiteiden kanssa, saisi se siltä osin ”jatkoon” päätöksen. Jatkoon päätöksen jälkeen ainakin määritetyille toimenpiteille määritettäisiin vastuut ja aikataulu sekä niitä seurattaisiin projektin kuluessa. Myös muilta osin riskiperusteinen ajattelu olisi taustalla jatkuvasti, että voidaanko projektia jatkaa nyt olemassa olevan tiedon valossa vai ei. Dokumentoimalla sen hetkisen tiedon valossa projektiin liittyviä epävarmuuksia, voi niitä hyödyntää myöhemmin ja dokumenttiarkistoon jää myös tieto millä perusteella ja mistä näkökulmasta päätös on tehty.

Tärkeää on saada riskeistä syntyvää tietoa hyödynnettyä ja osaksi päätöksentekoa. Tärkeää jatkotoimenpiteiden osalta on myös saada johto sitoutumaan ja tuomaan riskiperusteista ajattelua näkyvämmin osaksi kulttuuria. Taulukkoon 6 on koottu ehdotetuista toimenpiteistä yhteenveto. Aluksi yrityksessä joudutaan tekemään kertatoimenpiteenä isompi riskien tunnistus sidosryhmien osalta, mutta tarkemman analyysin jälkeen niitä voidaan seurata ja päivittää tarvittaessa muutosten yhteydessä. Myös strategiatyön pohjalle voidaan tehdä SWOT – analyysi ja tästä voidaan analysoida strategian kannalta merkittävämmät uhat ja mahdollisuudet, joita seurata normaalin strategiaprosessin yhteydessä ja päivittää myös tarvittaessa, jos toimintaympäristössä tapahtuu muutoksia. Yksi kehittämistoimenpiteistä on saada riskienhallinnasta systemaattisempaa, jonka jälkeen sitä voidaan kehittää lisää ja muuttaa ennakoivammaksi sekä saada se rutiiniksi erityisesti projekteihin liittyviin riskeihin.

Taulukko 6. *Toimenpiteet riskienhallinnan kehittämiseen*

Toistuvuus	**Toimenpide**	**Sisältö**
Kertaluonteiset toimenpiteet	Sidosryhmä riskien tunnistus	Käydään läpi sisäiset ja ulkoiset sidosryhmät ja heidän vaatimuksiin ja odotuksiin liittyvät riskit ja mahdollisuudet.
	SWOT -analyysi liiketoiminnan riskeistä	Tunnistetaan riskit ja mahdollisuudet tämän hetkisessä toimintaympäristössä.

Toistuvat toimenpiteet	Riskianalyysien päivittäminen	Säännöllisesti päivitetään prosesseissa ja strategiassa tunnistettuja riskejä ja mahdollisuuksia.
	Viestintä riskeistä	Viestitään riskienhallinnasta ja riskeistä henkilöstölle sekä tarvittaessa ulkoisille sidosryhmille.
	Järjestelmän analysointi	Analysoidaan toimenpiteiden vaikuttavuutta ja riskienhallinnan toimivuutta.
	Myynti-, toimitus- ja tuotekehitysprojektien riskianalyysien kehittäminen	Analysoidaan säännöllisesti myyntitarjousten riskejä ja päivitetään toimitusprosessin aikana. Tunnistetaan myös uusiin tuotekehitysprojekteihin liittyvät riskit ja mahdollisuudet.

Toivottavaa on, että tunnistettuja riskejä ja niille määritetyt toimenpiteet eivät jää ajatusten taakse, että katsotaan seuraavalla kerralla ja tätä kertaa ei ikinä enää tulekaan. Tällöin vaaditaan hyvää dokumentaatiota sekä vastuiden jakamista.

6. JOHTOPÄÄTÖKSET

Tutkimustyön tavoitteena oli kehittää kohdeyritykseen riskienhallintajärjestelmä, joka on systemaattisempi ja huomioi paremmin liiketoiminnan riskejä. Tutkimustyössä käytiin läpi teoriassa toimivan riskienhallintajärjestelmän malli tiedontuottamisen näkökulmasta, jota heijastettiin työn empiirisessä osuudessa, kun analysoitiin riskienhallinnan nykytilaa kohdeyrityksessä ja esiteltiin kehittämistoimenpiteitä. Käytetty tutkimusaineisto toi hyvin esiin nykytilassa ilmenevät epäkohdat ja mitä yrityksen johto vaatii riskienhallinnalta, joiden pohjalta lähdettiin kehittämistoimenpiteitä suunnittelemaan.

Riskienhallinta on kehittynyt hyvin laajaksi kokonaisuudeksi vuosien aikana ja erityisesti riskiperusteista ajattelua on tuotu esiin enemmän nykyhetkessä. Epävarmuus kasvaa jatkuvasti ja yritysten tulee osata ennakoida paremmin. Työn lähtökohta oli ISO 9001:2015 standardin tuomat muutokset riskienhallinnan osalta ja työssä todettiinkin, että standardi ei vaadi muodollisia riskienhallintatoimia tai järjestelmiä, mutta seuraavan standardi päivityksen tullessa voi vaatimukset tämän osalta muuttua. Tästä syystä työ oli hyvä lähtökartoitus sille, että miten riskienhallinta nähdään tällä hetkellä ja mihin suuntaan sitä mahdollisesti tulisi viedä, jotta riskit ja mahdollisuudet voidaan ottaa paremmin huomioon liiketoiminnassa sekä kuinka niihin liittyvää seurantaa voidaan toiminnassa lisätä ilman erillistä omaa järjestelmää.

Tutkimustyön teoriassa tuotiin myös esiin, että mitä riskienhallinnasta syntyvällä tiedolla voidaan tehdä ja hyödyntää liiketoiminnassa. Paljon korostetaan, että se on nykypäivän johdon työkalu ja riskienhallinnalla saadaan lisäarvoa omaan toimintaan. Kohdeyrityksen haastatteluiden pohjalta voidaan todeta, että lisäarvo syntyy, kun riskienhallinta toteutetaan sopivalla tavalla yrityksen toimintaan. Vaikka riskienhallinnalle on monenlaisia viitekehyksiä ja ohjeita, tulee näitä soveltaa omaan toimintaan sopivaksi. Tutkimustyössä viitekehykset toimivat hyvänä runkona huomioimaan eri osa-alueita riskienhallinnassa.

Tutkimustyön aikana esiin nousi selkeästi kulttuurin merkitys riskienhallintaan. Kulttuuri on toiminnassa mukana jokaisessa osa-alueessa ja eri tasoilla näkyvästä toiminnasta ajatusmaailmaan. Riskiperusteisen ajattelu tulee sisällyttää olemassa olevaan kulttuuriin tai muuttaa kulttuuria riskiperusteiseen suuntaan. Tässä kohtaan johtajan merkitys ja vaikutus korostuu eli miten kriittisiin tilanteisiin reagoidaan ja mitä mitataan. Jos johtajaa ei kiinnosta asettaa ja seurata esimerkiksi kriittisiä rajoja mittareissa, ei näin tee myöskään kukaan muu. Positiivinen riskienhallintakulttuuri voi myös edistää sitä, että organisaatiossa työskentelevät henkilöt seuraavat hiljaisia signaaleja enemmän ja tuovat näitä helpommin esiin, erityisesti sidosryhmiltä tulevia signaaleja. Tärkeää on myös asettaa riskienhallintaan selkeät ohjeet, mitä pitää tehdä, kuka tekee ja miksi näin tehdään. Tällöin riskienhallintaa voidaan saada systemaattisemmaksi ja se saadaan yrityksen jokapäiväiseen toimitaan paremmin käytännöksi. Kohdeyrityksessä puuttui systemaattinen seuranta

riskeistä ja tähän esitettiin ratkaisuksi, että sisällytetään riskien seuranta olemassa oleviin järjestelmiin, jolloin se ei kuormita toimintaa ja se ei tällöin vaadi omaa tietoteknistäjärjestelmää sekä riskit tulee katselmoitua olemassa olevissa toimintatavoissa kuten osana sisäistä auditointia. Teoriassa tuotiin esiin, että riskienhallinnan tulee olla yksinkertainen tapa ja myös kohdeyrityksessä työskentelevät toivoivat, että järjestelmä ei kuormita liikaa. Menestyvässä yrityksessä riskejä ei vain tunnisteta selkärangasta tarjousta tehdessä, vaan sille on oma ohjeistettu systemaattinen tapa ja sille on määritetty vastuuhenkilöt sekä toimintatapa.

Riskienhallinta kulkeutuu johtamisprosessin läpi koko organisaatioon ja se lähtee liikkeelle yrityksen visiosta, strategiasta ja toimintaympäristöstä. Tästä syystä työssä esiin tuli myös strategisten riskien merkitys ja strategian kautta tavoitteet heijastuu operatiiviselle tasolle, jossa riskejä tulee heijastaa asetettuihin tavoitteisiin. Tällöin varmistetaan, että operatiivisella tasolla ei ole esteitä strategian toteutumiselle tai tunnistetaan mahdollisuuksia, joilla voidaan vahvistaa strategian tavoitteiden saavuttamista. Haastateltavatkin toivat vahvasti esiin, että riskienhallinta tulisi olla osana strategiaa systemaattisemmin ja toimintatavalle nähtiin mahdollisuus tulla osaksi strategian seurantaa.

Yksi iso osa riskienhallintaa on sen vaikuttavuuden arvioiminen ja tätä tulee tehdä koko prosessin ajan. Riskienhallinnan tulisi olla vaikuttavaa, jotta varmistetaan siitä saatava hyöty ja lisäarvo yritykselle kuten tavoitteiden saavuttaminen sen avulla, epävarmuuksiin varautuminen tai estäminen sekä jatkuvan parantamisen. Vaikuttavuutta voidaan arvioida monella tapaa esimerkiksi kuinka valitut toimenpiteet ovat vaikuttaneet tavoitteen saavuttamiseen tai onko riskienhallinnan avulla kyetty tunnistamaan uusia uhkia, joihin ei olla osattu varautua. Riskienhallinta on myös jatkuvaa oppimista. Erityisesti kohdeyrityksessä, jossa projektit ovat hyvin erilaisia ja jokaisesta voi huomata uusia mahdollisuuksia tai riskejä, joita ei aiemmin ole edes ajateltu. Näitä tulee käydä läpi ja heijastaa niitä nykyiseen toimintaympäristöön, onko jokin mahdollisuus vahvistunut toimintaympäristön muutosten kautta tai jonkin negatiivisen riskin todennäköisyys tai seuraus kasvanut. Tunnistettavien mahdollisuuksien kautta riskienhallinnan vaikuttavuutta tulisi myös tarkastella ja arvioida.

Kuten teoriassa ja myös haastateltavien kanssa tuli esiin, että riskienhallinnan tulisi tapahtua ilman sanaa riskienhallinta. Tämä on tavoitetila, vaikka aluksi se vaatiikin paljon näkyvää työtä ja erityisesti viestintää aiheen osalta, jotta se saadaan henkilöstö ymmärtämään riskienhallinnan merkitys osana normaalia liiketoimintaa. Riskienhallintajärjestelmän kehittäminen vie ajallisesti myös aikaa ja vasta käytännössä sen toimivuus ja vaikuttavuus voidaan arvioida. Myös kohdeyritys käytännön työssä huomaa, onko ehdotetut toimenpiteet käyttökelpoisia ja mihin suuntaan niitä tulee edelleen kehittää. Kehittämistä ei tule unohtaa, jotta riskienhallinta saadaan sopimaan kohdeyritykseen paremmin ja tulee todellisia esimerkkejä, että riskienhallinnasta on oikeasti hyötyä eikä vain sanahelinänä tutkimustyön teoriassa. Käytännön hyödyt edistävät myös sitoutumista riskienhallintaan.

Tutkimusaiheena riskienhallinta on hyvin yleinen aihe ja erityisesti perinteinen riskienhallinta, mutta aiheena tämä on hyvin ajankohtainen, koska toimintaympäristöt ovat monimutkaisempia ja muuttuvimpia kuin ennen ja riskiperusteinen ajattelu on haluttu nostaa standardeissa ja uusissa säädöksissä näkyvämmäksi osaksi. Tämä tutkimus oli tapaustutkimus pk-yritykselle, mutta teoriassa esitetty malli tiedon tuottamisen näkökulmasta on validi kaikille organisaatioille. Tapaustutkimuksessa ominaista on, että sitä ei voida yleistää ja sitä käsitellään ainutlaatuisesti kuten tässä työssä. Työssä pyrittiin kehittämään nimenomaan kohdeyritykseen sopivaa järjestelmää ja huomioimaan sen tarpeet ja vaatimukset. Jatkotutkimuksen aiheena voisi olla riskienhallinnan vaikuttavuuden arvioiminen kohdeyrityksessä ja kuinka esimerkiksi strateginen riskienhallinta on saatu integroitua osaksi toimintaa ja miten sen vaikuttavuus näkyy yrityksen tuloksessa ja tavoitteiden saavuttamisessa.

LÄHTEET

Abrams, C., Känel, Müller, S., Pfitzmann, B., Ruschka- & Taylor, S. (2007). Optimized enterprise risk management, Systems Journal, Vol. 46(2), https://search.proquest.com/docview/222427462/fulltextPDF/83B4B13E15194D91PQ/1?accountid=27303.

Andersen, T.J. (2006). Perspectives on Strategic Risk Management, Copenhagen Business School Press, Frederiksberg, Denmark.

Anderson, D. (2017). COSO ERM: Getting risk management right, Internal Auditor, Vol. 74(5), pp. 38-43. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=128494760&site=ehost-live&scope=site.

AON (2010). Enterprise risk management, Aon Corporation, Chicago, Financial engineering and risk management. Saatavilla: http://www.aon.com/attachments/2010_Global_ERM_Survey.pdf.

AON (2007). Enterprise Risk Management - The full picture, AON, USA, Saatavilla: http://secure.eloqua.com/web/AON/Enterprise Risk Management - The full picture_0.pdf?elq_mid=&elq_cid=3012454.

Aven, T. & Renn, O. (2009). On risk defined as an event where the outcome is uncertain, Journal of Risk Research, Vol. 12(1), pp. 1-11. http://www.tandfonline.com/doi/abs/10.1080/13669870802488883.

Beasley, M.S., Branson, B.C. & Hancock, B.V. (2010). Developing Key Risk Indicators to Strengthen Enterprise Risk Management, pp. 20. Saatavilla: https://www.coso.org/Documents/COSO-KRI-Paper-Full-FINAL-for-Web-Posting-Dec110-000.pdf.

Bill George VUCA 2.0: A Strategy For Steady Leadership In An Unsteady World, Forbes, web page. Saatavilla (viitattu 17.4.2018): https://www.forbes.com/sites/hbsworkingknowledge/2017/02/17/vuca-2-0-a-strategy-for-steady-leadership-in-an-unsteady-world/#4074b68613d8.

BSI (2015a). ISO 9001 Whitepaper The importance of risk in quality management. Saatavilla (viitattu 4.6.2018): https://www.bsigroup.com/LocalFiles/en-IN/Resources/ISO%209001/ISO-9001-Whitepaper-Risk-in-quality-management.pdf

BSI (2015b). Why ISO 9001:2015 is better for your business. Saatavilla (viitattu 4.6.2018): https://www.bsigroup.com/Global/revisions/Why-ISO-9001-is-better-for-your-business-FINAL-Dec-2015.pdf

Collins, J. (2010). Parhaasta pohjalle vai vahvana eteenpäin? Talentum, Helsinki.

COSO (2017). Enterprise Risk Management Integrating with Strategy and Performance, Committee of Sponsoring Organizations of the Treadway Commission. Saatavilla: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf.

Courtney, H., Kirkland, J. & Viguerie, P. (1997). Strategy Under Uncertainty, Harvard Business Review, https://hbr.org/1997/11/strategy-under-uncertainty.

Curtis, P. & Carey, M. (2012). Risk assessment in practice, Committee of Sponsoring Organizations of the Treadway Commission, Saatavilla: https://www.coso.org/Documents/COSO-ERM-Risk-Assessment-in-Practice-Thought-Paper-October-2012.pdf.

DNV-GL (2016). VIEWPOINT REPORT;Where are you on the risk management journey? DNV-GL, 44 p.

Engblom, J. (2003). Liikeriskit : luonne, lajit ja riskikentän mallintaminen, Turun kauppakorkeakoulu.

Erma, J., Rasila, T. & Virtanen, O.V. (2010). Hyvä hallitustyö, 3. uud. p. ed. Kauppakamari : Hallitusammattilaiset, Helsinki.

Erola, E. & Louto, P. (2000). Riskit voimavaraksi: liiketoimintariskien hallinta yrityksessä, Edita, Helsinki.

EY A new balanced scorecard--measuring performance and risk, EY, web page. Saatavilla (viitattu 1.11.2017): http://www.ey.com/gl/en/services/advisory/a-new-balanced-scorecard--measuring-performance-and-risk.

EY (2015). Risk Culture — how can you create a sound risk culture? pp. 8. Saatavilla: http://www.ey.com/Publication/vwLUAssets/Risk_culture_-_How_can_you_create_a_sound_risk_culture/$FILE/EY-risk-culture-model-brochure.pdf.

EY (2013). Turning to risk for results. Saatavilla: http://www.ey.com/Publication/vwLUAssets/Turning_risk_into_results/$FILE/Turning%20risk%20into%20results_AU1082_1%20Feb%202012.pdf.

FERMA A Risk Management Standard. Saatavilla (viitattu 12.1.2018): https://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-english-version.pdf.

Flink, A., Reiman, T., Hiltunen, M. & Prima, E. (2007). Heikoin lenkki? riskienhallinnan inhimilliset tekijät Anna-Liisa Flink, Teemu Reiman, Mika Hiltunen, Edita.

Frigo, M.L. & Anderson, R.J. (2011). Strategic Risk Management: A Foundation for Improving Enterprise Risk Management and Governance, The Journal of Corporate Accounting & Finance, pp. 81-88. https://onlinelibrary-wiley-com.libproxy.tut.fi/doi/epdf/10.1002/jcaf.20677.

Gustafsson, R., Klefsjö, B., Berggren, E. & Granfors-Wellemets, U. (2001). Experiences from implementing ISO 9000 in small enterprises – a study of Swedish organisations The TQM Magazine, Vol. 13(4), pp. 232-246. https://www.emeraldinsight.com/doi/pdfplus/10.1108/09544780110366088.

Hiltunen, A. (2015). Johtamisesta, Talentum, Helsinki.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2007). Tutki ja kirjoita, 13. osin uud. laitos ed. Tammi, Helsinki, 448 sivua p.

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. (2016). Johda riskejä: käytännön opas yrityksen riskienhallintaan, 2. laitos ed. Finva, Helsinki.

Juvonen, M. (2005). Yrityksen riskienhallinta, Suomen vakuutusalan koulutus ja kustannus, Helsinki.

Juvonen, M., Koskensyrjä, M., Kuhanen, L., Ojala, V., Pentti, A., Porvari, P. & Talala, T. (2014). Yrityksen riskienhallinta, Finanssi ja vakuutuskustannus FINVA, Helsinki.

Kaplan, R.S. & Mikes, A. (2012). Managing Risks: a New Framework, Harvard business review, Vol. 90(6), pp. 48-60. https://hbr.org/2009/03/six-ways-companies-mismanage-risk.

Keskuskauppakamari (2016). Asialuettelo listaamattomien yhtiöiden hallinnoinnin kehittämiseksi: Corporate governance, Helsinki. Saatavilla: https://cgfinland.fi/wp-content/uploads/sites/6/2012/01/asialuettelo-listaamattomien-yhtioiden-hallinnoinin-kehittamiseksifinal.pdf.

Kupi, E., Keränen, J. & Lanne, M. (2009). Riskienhallinta osana pk-yritysten strategista johtamista, VTT Working Papers 137, VTT.

Kuusela, H. & Ollikainen, R. (2005). Riskit ja riskienhallinta, Tampere University Press, Tampere.

Laamanen, K. (2012). Johda liiketoimintaa prosessien verkkona : ideasta käytäntöön, 9th ed. Laatukeskus, Helsinki.

Lam, J. (2014). Enterprise Risk Management: From Incentives to Controls, John Wiley & Sons, Incorporated, Somerset, UNITED STATES.

Louisot, J. & Ketcham, C.H. (2014). ERM - Enterprise Risk Management: Issues and Cases, Wiley, Somerset.

MacLeod, A., Foster, B., Macdonald, P., Robertson, A., Stokka, T. & Ybarra, B. (2012). Coordinating Risk Management and Assurance. International Professional Practice Framework - Practice Guide, The Institute of Internal Auditors, pp. 12. https://na.theiia.org/certification/Public%20Documents/Coordinating%20Risk%20Management%20and%20Assurance.pdf.

Merna, T. & Al-Thani, F.F. (2008). Corporate Risk Management, John Wiley & Sons, Incorporated, New York.

The new ISO 31000 keeps risk management simple Saatavilla (viitattu 1..6.2018): https://www.iso.org/news/ref2263.html.

Puusa, A. (2008). Käsiteanalyysi tutkimusmenetelmänä, Premissi, pp. 36. Saatavilla (viitattu 12.11.2018): http://www.academia.edu/3310906/K%C3%A4siteanalyysi_tutkimusmenetelm%C3%A4n%C3%A4.

Ratsula, N. (2016). Yrityksen sisäinen valvonta, 2., uudistettu painos ed. Edita Publishing Oy, Helsinki.

Rautanen, K. (2011). Aineettomien riskien hallinta johdon työkaluna, WSOYpro, Helsinki.

Riskiblogi. Saatavilla (viitattu 6.3.2018): https://riskiblogi.fi/.

Riskienhallinta modernisoituu - PwC:n Uutishuone. Saatavilla (viitattu 12.12.2017): https://uutishuone.pwc.fi/riskienhallinta-muuttuu-ja-viitekehykset-sen-mukana/.

Riskikompassi. Saatavilla (viitattu 12.12.2017): https://riskikompassi.fi/.

Riskit ja mahdollisuudet: käytännön neuvot riskien hallintaan (2012). Suomen riskienhallintayhdistys: Finnsecurity; Turvallisuuden ja riskienhallinnan tietopalvelu, Helsinki: Vantaa.

Rosa, E.A. (1998). Metatheoretical foundations for post-normal risk, Journal of Risk Research, Vol. 1(1), pp. 15-44.

Sadgrove, K. (2016). The Complete Guide to Business Risk Management, Taylor & Francis Group, London.

Schein, E.H. (2001). Yrityskulttuuri: selviytymisopas : tietoa ja luuloja kulttuurimuutoksesta, Laatukeskus, Helsinki.

SFS-EN ISO 14001:2015 (2015). Ympäristöjärjestelmät. Vaatimukset ja niiden soveltamisohjeita, Suomen Standardisoimisliitto SFS ry, Helsinki.

SFS-EN ISO 31000:2018 (2018). Riskienhallinta. Ohjeet, Suomen Standardisoimisliitto SFS ry, Helsinki.

SFS-EN ISO 9001:2015 (2015). Laadunhallinjärjestelmät.Vaatimukset, Suomen Standardisoimisliitto SFS ry, Helsinki.

SFS-ISO 45001:2018 (2018). Työterveys- ja työturvallisuusjärjestelmät. Vaatimukset ja niiden soveltamisohjeita, Suomen Standardisoimisliitto SFS ry, Helsinki.

Sheehan, N.T. (2010). A risk-based approach to strategy execution, Journal of Business Strategy, Vol. 31(5), pp. 25-37. http://www.emeraldinsight.com/doi/abs/10.1108/02756661011076291.

Shenkir, W.G. & Walker, P.L. (2011). Enterprise Risk Management: Frameworks, Elements, and Integration Statement on Management Accounting, http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan050722.pdf.

Stulz, R.M. (2009). 6 Ways Companies Mismanage Risk, Harvard Business Review, Vol. 87(3), pp. 86-94. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=36589942&site=ehost-live&scope=site.

Suomen Standardisoimisliitto SFS ry (2016). Johdanto laadunhallinnan ISO 9000 -standardeihin, Suomen Standardisoimisliitto SFS ry.

Suominen, A. (2003). Riskienhallinta, 3. uud. p. ed. WSOY, Helsinki.

Temmes, A. & Välikangas, L. (2010). Strateginen ajautuminen, WSOYpro, Helsinki.

The Institute of Risk Management (2012). Risk culture, The Institute of Risk Management, Saatavilla: https://www.theirm.org/media/885907/Risk_Culture_A5_WEB15_Oct_2012.pdf.

Walker, R. (2013). Winning with risk management, World Scientific, Hackensack, NJ.

LIITE A: RISKIENHALLINNAN ARVIOINTI

PUITTEET		1	2	3	4	5	Tila	Tavoite
Johtajuus ja sitoutuminen	Riskienhallinnalla on yrityksen johdon ja henkilöstön tuki	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
	Johto ja hallitus huomioi riskit asianmukaisesti, kun organisaation tavoitteita asetetaan	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
	Ylin johto vastaa, hallitus valvoo	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
	Ymmärtää kohdistuvat riskit, kun tavoitteita pyritään saavuttamaan	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
Johtamisjärjestelmään sisällyttäminen	Jokaisessa osassa riskienhallinta mukana ja jokaisella vastuu riskienhallinnasta	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
	Riskienhallina on tehokkaasti ja tarkoituksenmukaisesti sisällytetty organisaation käytäntöihin ja kulttuuriin	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
Suunnittelu	Toimintaympäristö (sisäinen ja ulkoinen) on määritetty ja ymmärretty	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
	Riskienhallintapolitiikka on määritetty ja vahvistettu johdon toimesta ja se on samansuuntainen organisaation kulttuurin ja muun toiminnan kanssa	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
	Roolit, vastuut ja valtuudet jaettu	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
	Riskeistä viestitään sisäisesti ja ulkoisesti tarkoituksenmukaisella tavalla ja riittävästi. Sisäisellä viestinnällä vahvistetaan vastuuta ja riskien omistajuutta.	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
Toteuttaminen ja arvioiminen	Puitteet ovat kunnossa ja toteutettu oikein	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
	Riskienhallinnan toimivuuden arviointi säännöllisesti	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
Kehittäminen	Riskienhallinnan muokkaantuminen muutosten sattuessa	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
	Puitteiden jatkuva kehittäminen	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
RISKIENHALLINTAPROSESSI		**1**	**2**	**3**	**4**	**5**		
Riskikriteerit	Riskikriteerit ja termit on määritetty yhtenäisesti ja selkeästi	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
Riskien arviointi	Riskien arviointi on systemaattista ja arvioinnissa on yhteiset todennäköisyys ja seuraus näkemykset. Arviointi tehdään tavoitteita vasten.	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
Riskien käsittely	Riskin käsittely on systemaattista, riskeille on määritetty tarvittava toimenpide, jäännösriskit on huomioitu ja käsittelyn vaikuttavuutta arvioidaan	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
Riskien seuranta	Seuranta on systemaattista, huomioidaan toimintaympäristön muutokset, analysoidaan onnistumisia ja epäonnistumisia, uusia riskejä tunnistetaan	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
Riskien raportointi	Riskienhallinnasta raportoidaan avoimesti ja säännöllisesti	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
Prosessin dokumentointi	Prosessin dokumentointi on jatkuvaa, keskitettyä ja riskille tehdyt mahdolliset toimenpiteet on jäljitettävissä	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
TOTEUTTAMINEN		**1**	**2**	**3**	**4**	**5**		
Osana strategiaa	Riskit ovat mukana strategiaprosessin eri vaiheissa ja riskeissä tapahtuneita muutoksia seurataan strategian kannalta. Strategiasta johdetaan tavoitteet, joita vasten riski arviointia tehdään jokaisella tasolla.	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
Osana prosesseja	Riskit ovat osa prosessien toimintaa, riskejä tunnistetaan ja niiden seuranta ja raportointi on systemaattista.	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
Osana sidosryhmiä	Sidosryhmiin liityvät riskit on tunnistettu ja riskien muuttumista seurataan toimintaympäristön muuttuessa	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5
Osana projekteja	Riskit ovat mukana projektien tarjousvaiheesta niiden loppumiseen. Riskejä päivitetään ja seurataan projektin aikana.	Ei näyttöä tai puhetasolla	Jonkin verran näyttöä	Näyttöä	Selvää näyttöä	Laaja-alaista näyttöä		5

LIITE B: PROJEKTIRISKIEN ARVIOINTI

PROJEKTIN RISKIT

Projektin numero:	**Projektin kuvaus:**
Pvm:	**Tekijä(t):**

Projekti sisältää:

Strateginen riski		Kustannusriski	
Taloudellinen riski		Tietoturvariski	
Operatiivinen riski		Mahdollisuus	
Aikatauluriski		Muu riski	
Tekninen riski			
Ulkoinen riski			

Projektin mahdollisuudet:	**Projektin uhat:**