Tiina Ultamo

Hallinnon operatiivisten riskien hallinnan uudelleenorganisointi rahastoyhtiössä

Metropolia Ammattikorkeakoulu
Ylempi Ammattikorkeakoulututkinto
Yrittäjyyden ja liiketoimintaosaamisen koulutusohjelma (YAMK)
Opinnäytetyö
Lokakuu/2012

Metropolia

Tiivistelmä

Tekijä Otsikko Sivumäärä Aika	Tiina Ultamo Hallinnon operatiivisten riskien hallinnan uudelleenorganisointi rahastoyhtiössä 79 sivua + 1 liite 19.10.2012
Tutkinto	Ylempi Ammattikorkeakoulututkinto
Koulutusohjelma	Yrittäjyyden ja liiketoimintaosaamisen koulutusohjelma (YAMK)
Suuntautumisvaihtoehto	Liiketoiminnan kehittäminen
Ohjaaja	Yliopettaja Pia Koskenoja

Kehittämistehtävän tarkoituksena oli organisoida uudelleen Rahastoyhtiö X:n hallinnon operatiivisten riskien hallinta. Ongelmakohtana oli konkreettisen ja käytännön työssä luonnollisesti mukana seuraavan riskienhallintasuunnitelman sekä siihen liittyvän selkeän dokumentaation puuttuminen. Lisäksi tuli huomioida uusi EU-tason sijoitusrahastodirektiivi, joka asetti lisävelvoitteita rahastoyhtiöiden riskienhallinnalle.

Kehittämistehtävä toteutettiin kvalitatiivisena toimintatutkimuksena, joka jakautui kolmeen vaiheeseen: nykytila-analyysi ja suunnittelu (taustatietojen kartoitus ja tutkimusdatan keräyksen suunnittelu), toiminta ja havainnointi (uuden riskienhallintasuunnitelman luominen ja mittaaminen) sekä reflektointi (mukana koko projektin ajan painottuen loppuvaiheeseen).

Teoreettisessa viitekehyksessä sovellettiin erilaisia riskien luokittelumalleja sekä tarkasteltiin riskienhallintaa prosessina. Suunnitelma perustui kahdeksanportaiseen kokonaisvaltaiseen riskienhallintamalliin COSO ERM:ään. Lisäksi huomioon otettiin sovellettavat viranomaismääräykset. Valittu teoreettinen viitekehys tuki Rahastoyhtiön operatiivisten riskien hallinnan uudelleenorganisointia.

Työn konkreettisista tuloksista merkittävin oli riskijaottelutaulukko, joka käsitti 76 kartoitettua ja analysoitua riskiä. Kehittämisen kohteena olleista viidestä rahastoyhtiön hallinnon toiminnosta laadittiin prosessikuvaukset, työohjeet sekä tarkistuslistat.

Laadittua riskienhallintasuunnitelmaa seurattiin neljän kuukauden ajan alkuvuodesta 2012. Kokonaisuudessaan kehittämistehtävän tavoitteet saavutettiin hyvin, sillä projektin aikana luotiin niin yksityiskohtainen, kattava, selkeä ja käyttökelpoinen suunnitelma, että sen liittäminen osaksi yrityksen jokapäiväisiä rutiineja onnistui.

Avainsanat	riski, operatiivinen riski, riskienhallinta, COSO ERM

Metropolia

Abstract

Author Title Number of Pages Date	Tiina Ultamo Reorganization of the administrative operational risk management in Fund Management Company 79 pages + 1 appendix 19 October 2012
Degree	Master of Business Administration
Degree Programme	Business Administration
Specialisation option	Entrepreneurship and Business Competence
Instructor	Pia Koskenoja, Principal Lecturer

The purpose of this study was to reorganize the administrative operational risk management in Fund Management Company. The main problem was the lack of concrete risk management plan that would be a natural part of company's everyday work. There wasn't clear documentation of the risk management either. In addition the company was obliged to implement the new fund directive of the European Parliament.

The study was carried out as a qualitative action research which was divided into three phases: current state analysis and planning (surveying the background and planning the collection of the research data), action and observation (creating and measuring the new risk management plan) and reflection (present throughout the whole project but emphasized in the final phase).

Many risk classifying models were discussed in the theoretical framework. Risk management was examined as a process. Theory of the integrated framework for enterprise risk management, COSO ERM, was applied. In addition the applicable authority orders were taken into consideration. The selected theoretical framework was supporting the reorganization of the Fund Management Company's operational risks.

The most prominent of the study's concrete results was the risk classification table that included 76 analyzed risks. The process flow charts, working instructions and checkpoint lists were written out for the five functions of the company.

The finalized risk management plan was followed for four months in the beginning of 2012. In its entirety the goals of the study were achieved well. During the project the researcher was able to create so detailed, exhaustive, clear and practical risk management plan that the company was able to attach it to the part of the everyday routines.

Keywords	risk, operational risk, risk management, COSO ERM

Sisällys

1 JOHDANTO 1

2 YRITYKSEN TAUSTA 2

2.1 Yritys 2
2.2 Yrityksen riskienhallinnan nykytila-analyysi 2
2.2.1 Toiminnot 2
2.2.2 Nykytilan ongelmakohtia 3
2.2.3 Riskien lähteet 3
2.2.4 Tämänhetkinen riskienhallinta 4

3 KEHITTÄMISTEHTÄVÄN TAUSTA 4

3.1 Kehittämistehtävän tausta viranomaisvelvoitteiden näkökulmasta 4
3.2 Corporate governance ja sisäinen valvonta 5
3.3 Kehittämistehtävän tavoite 7
3.4 Kehittämistehtävän hyödyt 8
3.4.1 Riskienhallinnan hyöty yritykselle 8
3.4.2 Riskienhallintasuunnitelman laatimisen hyöty yritykselle 9

4 KEHITTÄMISTEHTÄVÄN KULKU 9

4.1 Aiheen rajaus ja aikataulu 9
4.2 Tutkimusmenetelmä 10
4.3 Mittarit, mittauksen toteutus ja seuranta 12
4.4 Validiteetti, reliabiliteetti ja verifiointi 13
4.5 Tutkijan ja muiden projektiin osallistuneiden roolit 14
4.6 Käsitteitä 15

5 TEOREETTINEN VIITEKEHYS 17

5.1 Riskien luokittelu 17
5.1.1 Gahinin riskimalli 17
5.1.2 Finanssivalvonnan jaottelu 19
5.1.3 Riskien kriteerit 19

5.1.4 Kolmikantajako Triage 20
5.2 Riskienhallintaprosessi 21
5.2.1 Historia 22
5.2.2 Riskienhallinnan suhde yrityksen tarpeisiin 23
5.2.3 Enterprise Risk Management eli kokonaisvaltainen riskienhallinta 23
5.3 COSO Enterprise Risk Management 24
5.3.1 Tausta 24
5.3.2 COSO ERM -malli 25
5.3.3 Mallin osatekijät 26
5.4 Vaihtoehtoiset teoriat 41
5.5 Sovellettava teoria 42
6 RAHASTOYHTIÖN RISKIENHALLINTAPROSESSI 43
6.1 Sisäinen toimintaympäristö 43
6.1.1 Riskienhallintafilosofia ja riskinottohalukkuus 44
6.1.2 Rehellisyys ja eettiset arvot 44
6.1.3 Organisaation rakenne sekä valtuudet ja velvollisuudet 44
6.2 Tavoitteiden asettaminen 44
6.3 Riskien tunnistaminen 44
6.3.1 Prosessit 46
6.3.2 Oikeudelliset riskit 53
6.3.3 Jatkuvuussuunnittelu 58
6.3.4 Varautuminen poikkeusoloihin 58
6.3.5 Tietojärjestelmät 59
6.3.6 Tietoturvallisuus 61
6.3.7 Rikosriskit 62
6.3.8 Muut 63
6.3.9 Jaottelu riskien kriteerien mukaan 64
6.4 Riskien arviointi 65
6.5 Riskeihin vastaaminen 66
6.6 Valvontatoimenpiteet 68

6.7 Informaatio ja tiedonkulku 68
6.8 Seuranta 69

7 KEHITTÄMISTEHTÄVÄN TULOKSET 70

7.1 Tehdyt toimenpiteet 70
7.2 Ulkopuolisten tahojen palaute 71
7.3 Mittaustulokset 71
7.3.1 Suunnitelman käyttöönoton onnistuminen ja sovellettavuus 71
7.3.2 Suunnitelman käyttökelpoisuus ja hyödyllisyys yritykselle 72
7.3.3 Riskienhallinnan laajuus 73
7.3.4 Riskienhallinnan tason optimaalisuus 73
7.3.5 Riskienhallintasuunnitelman mittaus 73
7.4 Vastaukset tutkimusongelmaan ja -kysymyksiin 74
7.5 Loppuanalyysi 75

8 JOHTOPÄÄTÖKSET JA JATKOTOIMENPITEET 76

8.1 Viitekehyksen soveltuvuus aiheeseen 76
8.2 Päättöreflektointi ja yhteenveto 77
8.3 Jatkotoimenpide-ehdotukset 78

Lähteet 80

Liitteet

Liite 1. *Riskijaottelu (Salainen)*

1 JOHDANTO

Tutkija työskentelee Rahastoyhtiössä back office -tehtävien parissa. Työtehtävien vahvan hallinnollisen luonteen vuoksi työnkuvaan kuuluvat myös riskiasiat ja siihen liittyen riskienhallinta on yksi oleellinen osakokonaisuus.

Tähänastinen yrityksen riskienhallinta on rajoittunut hyvin pitkälle viranomaismääräysten noudattamiseen. Konkreettista, operatiivisessa työssä mukana olevaa riskienhallintatoimintoa ei ole juurikaan ollut. Lisäksi riskienhallinnan dokumentaatio on toistaiseksi ollut melko niukkaa. Mikäli jokin vakava riski toteutuu, on siitä seurauksena rahallisten menetysten lisäksi mahdollisesti myös yrityksen maineen vahingoittuminen, mikä on sijoitusalalla useimmiten erittäin haitallista. Näistä lähtökohdista johdettuna kehittämistehtävän tutkimusongelma on, miten Rahastoyhtiön operatiivisen työn riskienhallintaa saadaan parannettua uudelleen organisoimalla niin, että se palvelee yritystä optimaalisella tavalla. Operatiivisella työllä tarkoitetaan tässä yhteydessä yrityksen toimintoihin liittyviä konkreettisia työtehtäviä. Se ei kata sellaisia toiminnan osa-alueita kuten suunnittelu, visiointi ja strategian määrittely. Operatiivisen työn riskienhallinta on edellä mainittujen työtehtävien suorituksen yhteydessä ilmenevien potentiaalisten riskien tunnistamista, kartoitusta ja niihin vastaamista.

Rahastoyhtiön haasteena on ollut hahmottaa riskikenttää kokonaisvaltaisesti. Riskit on nähty toimintolähtöisesti eikä niiden hallinta ole ollut luonnollisena osana yrityksen jokapäiväisiä rutiineja. Tämän vuoksi aiheeksi on valittu Rahastoyhtiön kokonaisvaltaisen riskienhallintasuunnitelman laatiminen ja dokumentointi. Erityisesti tarkoituksena on eritellä suunnitelmassa, miten operatiivisia riskejä kyetään tunnistamaan, määrittelemään sekä mittaamaan. Tarkemmat tutkimuskysymykset ovat: Mitkä ovat rahastoyhtiölle tyypilliset operatiiviset riskit, joilta halutaan suojautua? Miten suojautuminen hoidetaan käytännössä? Miten riskienhallintatoimintoa hyödynnetään ja kehitetään edelleen?

Suunnitelmassa on hyödynnetty Committee of Sponsoring Organisations of the Treadway Commissionin kehittämää COSO ERM-mallia soveltuvin osin. Sen perusajatuksena on luoda yhteys yrityksen tavoitteiden, toiminnallisen rakenteen sekä riskienhallinnan välille.

2 YRITYKSEN TAUSTA

2.1 Yritys

Tästä kappaleesta on salattu kohdeyrityksen yritysesittely.

Kuvio 1. Salattu.

Suomessa rahastosijoittaminen on melko tuoretta. Ensimmäinen versio sijoitusrahastolaista tuli voimaan 1987. Toimialalla on paljon erikokoisia yrityksiä suurten liikepankkien tytäryhtiöistä aina pieniin muutaman työntekijän ja yhden rahaston yhtiöihin. Suomessa oli rahastoyhtiöitä vuoden 2012 kesäkuun lopussa 33 kpl ja ne hallinnoivat yli 550 eri rahastoa. (Rahastoyhtiöiden markkinaosuudet.)

Toimialalla haasteita tuo alati muuttuva toimintaympäristö. Sovellettavat säädökset ja vallitseva markkinatilanne elävät vahvasti. Rahastoyhtiötoiminta on tarkoin säädeltyä ja luvanvaraista. Olosuhteet huomioon ottaen rahastoja tarjoavia yhtiöitä sekä yksittäisiä rahastoja on kuitenkin ilmestynyt viime vuosina Suomen markkinoille runsaasti.

2.2 Yrityksen riskienhallinnan nykytila-analyysi

Esittelen tässä Rahastoyhtiön riskienhallinnan nykytilaa hallinnollisesta näkökulmasta. Tarkastelu on jaoteltu toimintopohjaisesti. Se toimi lähtökohtana yrityksen riskien kartoituksen ja niiltä suojautumisen suunnittelussa.

2.2.1 Toiminnot

Rahastoyhtiössä perustoimintoja on kolme: salkunhoito, myynti ja hallinto. Näistä hallinnon alle luetaan kuuluvaksi rahastojen arvonlaskenta, asiakas- ja osuusrekisteri, asiakaspalvelu, taloushallinto sekä seuranta ja raportointi.

Tästä kappaleesta on salattu kohdeyrityksen toimintojen tarkemmat kuvaukset.

2.2.2 Nykytilan ongelmakohtia

Tähänastinen yrityksen riskienhallinta on rajoittunut pääasiassa viranomaismääräysten noudattamiseen. Konkreettista, operatiivisessa työssä mukana olevaa riskienhallinta-toimintoa ei ole juurikaan ollut. Kokonaisuutta ei ole lähestytty riskilähtöisesti vaan ennemmin toimintopohjaisesti, missä käytännön kautta ilmeneviä riskejä on tarpeen mukaan pyritty ennakoimaan tai ratkaisemaan. Lisäksi riskienhallinnan dokumentaatio on toistaiseksi ollut melko niukkaa.

Tästä kappaleesta on salattu kohdeyrityksen toimintojen ongelmakohtien tarkemmat kuvaukset.

2.2.3 Riskien lähteet

Edellä esitellyssä toimintopohjaisessa ajattelutavassa suurimmiksi riskilähteiksi muodostuvat henkilöstö, tietojärjestelmät ja toimintojen organisointi. Vaikka prosesseja on käytettävissä olevan teknisten ratkaisujen puitteissa pyritty automatisoimaan ja laatimaan luotettaviksi, on edelleen merkittävin riski inhimilliset virheet eli henkilöriskit. Nämä voivat liittyä huolimattomuuteen tai unohduksiin. Henkilöstöstä lähtöisin olevia mahdollisia riskejä ovat myös tahalliset väärinkäytökset, vilpillisyys ja muu rikollinen toiminta.

Huomattava riskilähde on tietotekniikka ja sen luotettavuus. Vaikka toiminta on suhteellisesti verrattuna melko pienimuotoista, on tietokoneiden käsittelemien tietojen oikeellisuuden tarkistaminen käsin mahdotonta. Lisäksi yrityksen sisältä ei löydy riittävää tietoteknistä asiantuntemusta. Sen vuoksi yritys on hyvin vahvasti ulkoisten palveluiden varassa.

Sitä vastoin kolmannen riskilähteen, toimintojen organisoinnin, toteutus on hyvin pitkälle yrityksen itsensä päätettävissä viranomaisten antamien rajoitusten puitteissa. Toistaiseksi toiminnot ovat melko pitkälle eriytetyt ja niillä on jokaisella erillinen vastuu- tai toimihenkilö. Toiminnot ovat hyvin itsenäisiä kokonaisuuksia ja niitä ei juuri hallita kokonaisvaltaisesti.

2.2.4 Tämänhetkinen riskienhallinta

Vaikka yrityksellä ei ole olemassa tarkkaa kirjallista kokonaisvaltaista riskienhallintasuunnitelmaa, riskejä luonnollisesti pyritään hallitsemaan. Yrityksellä on riskienhallintaan liittyen laadittuna kirjallisia muistioita sisäisen valvonnan periaatteista, arvonlaskennasta ja osuusrekisteristä sekä asiakkaan tunnistamisesta ja tuntemisesta. Ne sisältävät yleisluontoisia periaatteellisen tason ohjeita ja niissä on otettu kantaa viranomaismääräyksiin. Hallituksen rooli riskienhallintaan liittyen on vastata hallinnon luotettavasti järjestämisestä (Finanssivalvonnan standardi 1.3 2007, 14).

Yrityksen sisäisen riskienhallinnan seurannan lisäksi valvontaa on lakisääteisesti jaettu valvovalle viranomaiselle (Finanssivalvonta), säilytysyhteisölle sekä tilintarkastajalle. He kartoittavat yrityksen hallintoa säännöllisin väliajoin ja antavat palautetta myös riskienhallinnan tasosta. Tarkastuksia on tehty keskimäärin kerran vuodessa ja niissä on todettu yrityksen riskienhallinnan olevan riittävällä tasolla toiminnan laajuus huomioon ottaen.

Lakisääteisten vakuutusten lisäksi yrityksellä on toimitusjohtajan ja hallituksen vastuuvakuutus. Sen tarkoituksena on korvata ne varallisuusvahingot, jotka vakuutetut ovat aiheuttaneet toimiessaan vakuutuksenottajan hallintoelimen jäsenenä ja joista vakuutetut ovat voimassa olevan oikeuden mukaan korvausvastuussa (Toimitusjohtajan ja hallituksen vastuuvakuutus). Tämän lisäksi yrityksellä on henkilöstön matkavakuutus.

3 KEHITTÄMISTEHTÄVÄN TAUSTA

3.1 Kehittämistehtävän tausta viranomaisvelvoitteiden näkökulmasta

Viranomaismääräyksistä johtuen ja toiminnan luotettavan sujumisen vuoksi rahastoyhtiön tulee kartoittaa ja hallita liiketoiminnan riskejä. Tämä on viime kädessä yrityksen hallituksen vastuulla. Lisäksi sovellettavaksi tulee uusi EU-tason sijoitusrahastodirektiivi (UCITS IV) mikä asettaa lisävelvoitteita rahastoyhtiöiden riskienhallinnalle. Määräyksien vuoksi riskienhallinta tulee ottaa selkeämmin mukaan rahastoyhtiön päivittäisiin rutiineihin. Näistä lähtökohdista on johdettu kehittämistehtävän tavoite, riskienhallintasuunnitelman laatiminen Rahastoyhtiölle.

Finanssivalvonta antaa finanssimarkkinoilla toimiville ohjeita ja määräyksiä, joilla ohjataan valvottavien toimintaa ja menettelytapoja. Käytännössä tämä tarkoittaa aihealueittaisten määräysten ja ohjeiden kokonaisuuksien eli standardien julkaisemista. Niiden tehtävänä on antaa suosituksia, tulkintoja sekä valvottavia toimijoita sitovia ohjeita. Standardien sisältö on kaiken laatuisille ja kokoisille valvottaville sama. Valvottavan vastuulle jää niiden tulkitseminen ja muokkaaminen omaan toimintaan riittävällä tasolla sopivaksi. Tällä hetkellä rahastoyhtiöiden toiminnassa sovelletaan Finanssivalvonnan standardeja 1.3 Luotettava hallinto ja toiminnan järjestäminen sekä 4.4b Operatiivisten riskien hallinta. Tämän lisäksi sovellettavaksi tulee myös Sijoitusrahastolaki (erityisesti 4 a luku).

Uudet viranomaismääräykset käsittävät riittävän ja dokumentoidun riskienhallintapolitiikan käytön ja ylläpidon, joihin kuuluu toimintaan suhteutettuna riskien tunnistus, määrittely sekä mittaus. Yrityksessä tulisi edelleen toiminnan laajuuteen suhteutettuna olla itsenäinen riskienhallintatoiminto. (Kirppu 2010.)

Laajemmin määritellen rahastoyhtiöllä tulee olla asianmukaiset ja dokumentoidut riskienhallintaperiaatteet, joilla voidaan tunnistaa toimintaan mahdollisesti tai tosiasiallisesti kohdistuvat riskit. Rahastoyhtiön on säännöllisesti arvioitava, valvottava ja tarkasteltava riskienhallintaperiaatteiden, menettelyjen sekä tekniikoiden asianmukaisuutta ja tehokkuutta, riskienhallintaperiaatteiden noudattamista sekä puutteiden korjaamista. Rahastoyhtiöllä on oltava järkevät hallintomenettelyt ja sen on luotava hyvin dokumentoitu organisaatiorakenne, jossa vastuualueet on jaettu selkeästi ja tiedonkulku on varmistettu. Rahastoyhtiön hallitus hyväksyy ja tarkistaa määräajoin riskienhallintaperiaatteet sekä niiden soveltamisen ja vastaa siitä, että rahastoyhtiöllä on pysyvä sisäisen valvonnan toiminto. (Örndahl 2011, 46 - 60.)

3.2 Corporate governance ja sisäinen valvonta

Corporate governance on järjestelmä, jolla yritystä johdetaan ja valvotaan. Se on oikeuksien, velvollisuuksien, sääntöjen ja menettelytapojen kokonaisuus, jonka kautta tehokkuuden sekä luotettavuuden ajatus yrityksessä konkretisoituu. Se sisältää yritykselle ja sen hallitukselle kuuluvat velvoitteet omistajilta, asiakkailta, sidosryhmiltä ja yh-

teiskunnalta. Sen mukaisesti määritellään miten ja millaista tietoa sidosryhmille annetaan. (Blumme ym. 2005, 11.)

Corporate governancelle ei ole vielä kehittynyt vakiintunutta suomennosta. Vaihtoehtoja ovat hyvä hallintotapa, hallintokulttuuri, johtamis- ja hallintojärjestelmä, omistajaohjaus ja yrityksen hallinta. Corporate governancen sisältö on myös vaihteleva painotuksesta riippuen (Blumme ym. 2005, 12).

Corporate governance muodostuu useista elementeistä, jotka käsittävät luotettavan hallinnon ja toiminnan järjestämisen periaatteet. Siihen kuuluvat hyvä johtamisjärjestelmä ja ilmapiiri, toimielimien (yhtiökokous, hallitus, toimitusjohtaja, tilintarkastus, sisäinen tarkastus) tehtävät ja suhteet, sidosryhmien tiedonsaanti- ja valvontaintressit sekä avoin ja luotettava raportointi. Yhden osan käsittävät ihmisresurssit: hyvä hallituksen kokoonpano ja hallintorakenne, osaava ja rehellinen johto sekä henkilöstö. Edelliseen liittyen huomioon tulee ottaa ylimmän ja toimivan johdon palkitsemistavat, jotka edistävät yrityksen ja sen omistajien etuja ilman epätoivottavia toimintatapoja tai hallitsematonta riskinottoa. Yksi osa-alue on yrityksen tavoitteiden asettaminen, niiden saavuttamiskeinoista päättäminen ja tavoitteiden saavuttamisen seuranta. Viimeisenä tärkeänä osatekijänä on myös oikein mitoitettu riskienhallinta ja tehokas sisäinen valvonta. (Blumme ym. 2005, 12 - 13, Finanssivalvonnan standardi 1.3 2007, 8.)

Sisäinen valvonta on corporate governancen osa, jonka avulla johto saa organisaation toimimaan halutulla tavalla ja joka tuottaa riittävästi tietoa organisaation tilasta sekä aikaansaannoksista. Yrityksen on järjestettävä tehokas ja kattava sisäinen valvonta. Käytännössä yrityksen tulee luoda riskienhallinnan arviointitoiminto, säännösten noudattamisen varmistamisesta vastaava toiminto ja sisäisen tarkastuksen toiminto tai nimettävä näistä toiminnoista vastaava henkilö. Normisto perustuu osakeyhtiö-, tilintarkastus- ja arvopaperimarkkinalakiin. Käytännössä relevantti ohjeistus tulee pääosin Finanssivalvonnalta. (Blumme ym. 2005, 15, 34, 44, Finanssivalvonnan standardi 4.1 2003, 14.)

Riskienhallinnan arviointitoiminto ylläpitää, kehittää ja valmistelee riskienhallinnan periaatteita hallituksen vahvistettaviksi sekä suunnittelee ja kehittää riskien ja riskienhallinnan kontrollointiin liittyviä menettelytapoja. Se valvoo, että jokainen riski pysyy vahvis-

tetuissa rajoissa. Lisäksi se varmistaa, että jokaista riskiä mittaavat menetelmät ovat asianmukaiset ja luotettavat. Säännösten noudattamisen varmistamisesta vastaava toiminto huolehtii siitä, että yritys noudattaa lainsäädäntöä, viranomaisten antamia ohjeita ja määräyksiä sekä markkinoiden itsesääntelyä. Näillä varmistutaan asiakkaiden ja markkinoiden luottamuksesta yrityksen toimintaan. Sitä tukee myös valvottavan omien sisäisten ohjeiden, henkilöstöä sitovien eettisten periaatteiden ja muiden ohjeiden noudattaminen. Sisäinen tarkastus on riippumatonta ja objektiivista arviointi- sekä varmennustoimintaa, jonka tehtävänä on tarkastaa sisäisen valvonnan riittävyyttä, toimivuutta ja tehokkuutta. (Finanssivalvonnan standardi 4.1 2003, 15.)

Sisäisen valvonnan ja riskienhallinnan yhteys on siinä, että organisaatioiden muuttuessa yhä monimutkaisemmiksi kasvaa riskien todennäköisyys, mikä lisää puutteellisen sisäisen valvonnan tuottamien epäonnistumisten mahdollisuuksia. Riskienhallinnan tehtävänä on varmistaa, että merkittävät riskit tunnistetaan, arvioidaan sekä mitataan ja että niitä seurataan osana päivittäistä liiketoimintojen johtamista. Riskienhallinnalla ja tarkastuksella parannetaan sisäistä valvontaa yrityksissä. Kansallisen corporate governance 2003 -suosituksen mukaan yrityksen on kirjattava periaatteet, joiden mukaan sen sisäinen valvonta ja riskienhallinta on järjestetty. Käytettävissä olevaa teoriaa on kehitetty, jotta pelisäännöt saataisiin yhteneväisiksi laajemmalla tasolla. Tämän perusteella on luotu muun muassa COSO-malli. (Blumme ym. 2005, 14, 17, 34, Finanssivalvonnan standardi 4.1 2003, 17.)

3.3 Kehittämistehtävän tavoite

Kehittämistehtävän tavoitteena oli organisoida ja toteuttaa operatiivisten riskien hallinta nykyistä kokonaisvaltaisemmasta lähtökohdasta. Yritys on hyötynyt tästä siten, että projektin jälkeen sillä on paremmat valmiudet pysyä tilanteensa tasalla ja olla siten ketterämmin vastaamassa sisäisen ja ulkoisen toimintaympäristön tuottamiin riskitekijöihin.

Työn konkreettisena tarkoituksena oli luoda riskienhallintasuunnitelma, jossa on esitelty operatiivisten riskien hallintaan liittyvät toimenpiteet. Tavoitteena oli saada luotua suunnitelma, joka on riittävän yksityiskohtainen ja kattava, mutta samalla niin selkeä ja käyttökelpoinen, että se liittyy osaksi yrityksen jokapäiväisiä rutiineja.

3.4 Kehittämistehtävän hyödyt

3.4.1 Riskienhallinnan hyöty yritykselle

Rahoitusmarkkinoilla toimivien yritysten menestyminen edellyttää, että niiden toiminnalla on asiakkaiden ja markkinoiden luottamus. Yksi tärkeimmistä asioista on hyvän maineen saavuttaminen ja sen säilyttäminen. Käytännössä tämä tarkoittaa, että asiakkaat voivat luottavaisin mielin asioida yrityksen kanssa ja tehdä sijoituspäätöksiä luotettavan informaation pohjalta. Markkinaosapuolilla tulee olla riittävästi tietoa päätöksenteon tueksi. Riskienhallinnan toimenpiteillä on tarkoitus varmistua siitä, että Rahastoyhtiö hoitaa oman osuutensa finanssimarkkinoiden avoimuutta sekä läpinäkyvyyttä ylläpitääkseen ja siitä, että yrityksen menettelytavat finanssimarkkinoilla ovat asialliset. Yrityksen tulee myös omalla toiminnallaan edistää asianmukaista corporate governancea.

Toimiva riskienhallintatoiminto varmistaa, että yritys ei ota toiminnassaan kohtuutonta riskiä, josta voisi aiheutua tarpeetonta vahinkoa asiakkaille. Tuolloin myös mahdollisten ongelmatilanteiden vaikutus pysyy hallittuna. Sen turvaamiseksi riskienhallintatoiminnon avulla tunnistetaan ja arvioidaan systemaattisesti sekä kattavasti kaikkia merkittäviä tavoitteiden saavuttamista uhkaavia riskejä. Sillä myös hyödynnetään optimaalisesti liiketoimintamahdollisuudet ja varmistetaan liiketoiminnan jatkuvuus. Näiden ohella riskienhallinnalla kyetään ennakoimaan ja tunnistamaan epävarmuustekijät ja siten kehittämään riskien ennakointia sekä riskien hallinnan edellyttämiä toimenpiteitä. Sen ansiosta otetaan vain tietoisia ja arvioituja riskejä sekä vältetään tai minimoidaan vahinkoriskejä, luodaan työntekijöille asiallinen työympäristö, minimoidaan epäterveiden ilmiöiden, rikosten tai väärinkäytösten mahdollisuudet sekä tiedotetaan riskeistä ja riskienhallinnasta sidosryhmille.

Kaiken kaikkiaan riskienhallinnan hyvä taso parantaa yrityksen menestymismahdollisuuksia siten, että häiriötilanteet ja katkokset vähenevät, toiminnan tehokkuus ja laatu paranevat sekä yllättäviä vahinkoja ja niiden aiheuttamia kustannuksia saadaan vähennettyä. Riskienhallinta voidaan nähdä myös kilpailuetuna siten, että riski voi olla mahdollisuus uusille liikeideoille tai toiminnan kehittymiselle.

Kun riskejä pyritään hallitsemaan kokonaisvaltaisesti, saadaan työnteon painopiste johdon kokonaislinjauksen mukaiseksi ja se tuo esille toiminnan kehityskohteet. Kunnollinen riskienhallintatoiminto tuottaa systemaattisesti tietoa yrityksen tilasta. Siitä yritys saa valmiuksia hyödyntää markkinatilanteiden ja muiden ulkoisten tekijöiden aikaansaamia muutoksia. Lisäksi se kehittää toimintaympäristön tarkkailua. (Erola & Louto 2000, 89 - 92.)

3.4.2 Riskienhallintasuunnitelman laatimisen hyöty yritykselle

Kun yritykselle tehdään kattava riskienhallintasuunnitelma, opitaan sen toimintaa ja siihen vaikuttavia tekijöitä ymmärtämään sekä tuntemaan paremmin. Tällöin saavutetaan kustannustehokkuutta riskienhallinnassa ja resurssit voidaan kohdentaa tärkeimpien ongelmien hallintaan. Henkilöstön osallistamisella prosessiin sen osaaminen paranee työn tuntemuksen ja ammattitaidon kasvun, työtehtävien kehittämisvalmiuksien parantumisen sekä tehtävien ja vastuiden selkeytymisen kautta. (Riskienhallinnan hyödyt 2009.)

Dokumentoidun riskienhallintasuunnitelman avulla voidaan riskien toteutuessa parantaa yrityksen toimintavalmiutta sekä varmistua toiminnan jatkuvuudesta. Näillä tekijöillä voidaan katsoa olevan välillinen vaikutus yrityksen imagon vahvistumiseen, asiakastyytyväisyyden kasvuun sekä työtyytyväisyyden parantumiseen. Konkreettisella tasolla riskienhallintasuunnitelman avulla voidaan myös osoittaa, että valvojalta tulleiden määräysten noudattamisvelvoite on täytetty. (Riskienhallinnan hyödyt 2009.)

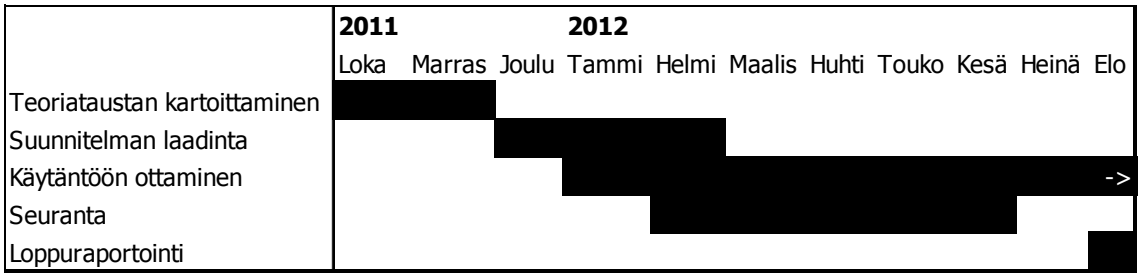
4 KEHITTÄMISTEHTÄVÄN KULKU

4.1 Aiheen rajaus ja aikataulu

Työssä on kartoitettu yrityksen operatiivisissa toiminnoissa ilmeneviä potentiaalisia ja relevantteja riskejä. Tarkoituksena ei ole ollut perehtyä strategisiin, taloudellisiin tai vahinkoriskeihin. Kehittämistehtävästä on rajattu pois yrityksen ydintoimintoja ajatellen rahastojen sijoituspäätöksiin sekä salkunhoitoon liittyvät asiat ja rahastojen myynti, koska nämä on toimintoina järjestetty yrityksessä hallinnosta erillisiksi. Lisäksi resurssi-

en vähyydestä johtuen taloushallinnollisen näkökulman tarkastelu on jätetty hieman muita osa-alueita pintapuolisemmaksi. Sinänsä hyödyllinen, mutta työläs benchmarkkaus- eli vertailuanalyysinäkökulma on jätetty työstä pois pääosin ajallisten resurssien niukkuuden vuoksi. Vertailutiedon kerääminen on myös osoittautunut alalla haastavaksi, sillä yritykset haluavat yleensä pitää riskienhallintaan liittyvät tiedot vain sisäisessä käytössä.

Opinnäytetyön aihe sai nykymuotonsa kevään 2011 aikana. Varsinainen kehittämistehtävän toteutus alkoi syksyllä 2011. Tarkemmat työvaiheet on eritelty kuviossa 2. Suunnitelma muotoutui lokakuun 2011 ja helmikuun 2012 välillä. Se otettiin käyttöön alkuvuodesta 2012 siten, että mittausdataa kerättiin väliltä helmi-kesäkuu. Nämä toimenpiteet esitellään tarkemmin alaluvussa 4.3 Mittarit, mittauksen toteutus ja seuranta. Loppuraportointi suoritettiin elokuussa 2012. Itse suunnitelman käyttöä jatkettiin myös mittausajanjakson jälkeen.



Kuvio 2. Projektin aikataulutus.

4.2 Tutkimusmenetelmä

Kehittämistehtävä on toteutettu kvalitatiivisena toimintatutkimuksena. Se jakautui kolmeen vaiheeseen: nykytila-analyysi ja suunnittelu, toiminta ja havainnointi sekä reflektointi.

Alkuvaiheessa kartoitettiin yrityksen sisäistä toimintaympäristöä nykytila-analyysin, tutkijan omien kokemusten, operatiivisessa työssä mukana olevien haastatteluiden ja yrityksestä saatavilla olevan kirjallisen materiaalin perusteella. Teoriapohjaa käytiin läpi kirjallisuuden ja artikkeleiden avulla. Datankeruuvaiheessa haastateltiin yrityksen perustajaa sekä toimitusjohtajaa (hallinnosta vastaava) ja muuta henkilöstöä, jotta saatiin

taustatietoa ja laajempaa perspektiiviä tutkimukselle. Lisäksi koottiin yrityksen olemassa oleva riskienhallintamateriaali.

Toimintavaiheessa käytiin läpi kerätty data ja sovellettiin sitä teoreettiseen viitekehykseen, minkä pohjalta tuotettiin uusi riskienhallintasuunnitelma. Siinä kartoitettiin eli tunnistettiin ja arvioitiin Gahinin riskimallin sekä Finanssivalvonnan standardi 4.4.b:n mukaisen jaottelun pohjalta yrityksen relevantit operatiiviset riskit siten, että ne luokiteltiin riskikriteerien (muodostumislokaatio, riskinoton tietoisuusaste, riskin vaikutustapa, vakuutettavuus) ja kolmikantajako Triagen perusteella. Tämän jälkeen päätettiin, miten riskeihin vastataan ja millä tavalla niiden toteutumista valvotaan. Kuuden kuukauden mittaisen seurantajakson aikana pyrittiin mittaamaan suunnitelman käyttökelpoisuutta ja sovellettavuutta sekä havainnoimaan sen tuottamaa hyötyä yritykselle.

Riskienhallintasuunnitelma sisältää tarkastuslistoja, joita käydään tapauskohtaisesti viikko- tai kuukausitasolla läpi. Näiden listojen perusteella kontrolloitiin suunnitelman toteuttamista ja niiden on tarkoitus myöhemminkin olla seurantatyökaluja siihen, onko suunnitelma aiotulla tavalla käytössä. Suunnitelmaa ja tarkastuslistoja voi päivittää tarpeen mukaan, mutta laajempi päivitys- ja tarkistuskierros on tarkoitus tehdä puolivuosittain.

Luotu riskienhallintasuunnitelma dokumentoitiin ja siitä johdettiin selkeät sekä yksinkertaistetut toimintaohjeet. Tavoitteena oli, että suunnitelmasta tulee niin selkeä ja yksiselitteinen, ettei se kohtuuttomasti lisää työtaakkaa vaan sen noudattamisesta saatava hyöty koetaan sen aiheuttamaa lisätyötä suuremmaksi.

Reflektointi eli arviointi kulki mukana koko prosessin läpi siten, että organisaation oppimiselle ja jatkuvalle kehittymiselle luotiin otolliset olosuhteet. Käytännössä reflektointivaiheessa analysoitiin, miten tutkimukselle asetetut tavoitteet saavutettiin, olivatko tavoitteet oikeat ja miten tavoitteiden saavuttaminen edisti tutkimusongelman ratkaisua. Lisäksi arvioitiin, miten tutkimus on kehittänyt tutkimuskohdetta ja projektiin osallistuvia. Sen perusteella hahmoteltiin, miten toimintaa pitäisi edelleen kehittää. (Suojanen 1992, 62.)

Koko henkilöstö osallistettiin suunnitteluun mukaan riskien kartoitusvaiheessa. Tarkoituksena oli, että jokaisen päästessä osallistumaan prosessiin kasvaa halukkuus sitoutua suunnitelmaan. Käytännössä kuitenkin kävi niin, että suurin osa hallinnon henkilöstöstä vaihtui projektin aikana, jonka vuoksi jatkuvuuden toteuttaminen osoittautui haasteelliseksi. Tilanne vaikutti hyvin paljon yrityksen toimintaan kaikkiaan. Tämän projektin kannalta asialla oli hyviäkin puolia, joihin palataan päättöreflektoinnin yhteydessä alaluvussa 8.2.

4.3 Mittarit, mittauksen toteutus ja seuranta

Koko kehitystehtävän onnistumista mitattiin neljällä eri mittarilla. Ensimmäinen mittauksen kohde oli suunnitelman käyttöönoton onnistuminen ja sovellettavuus eli millä tasolla sitä pystyttiin yrityksessä soveltamaan. Tätä varten laadittiin tarkistuslistat (lista suoritetuista toimenpiteistä, jotka kuitataan tarkastetuksi läpi käymisen jälkeen). Niiden avulla käytiin läpi riskiprosessien yksityiskohdat ja dokumentoitiin ne. Tavoitteena oli, että listoista tulee täytetyksi vähintään 90 %.

Konkreettisten toimenpiteiden mittaamista varten kaikista viidestä toiminnosta luotiin prosessikuvaus (suoritettavat toimenpiteet, niiden järjestys ja lopputulos), työohje (vaiheittaiset ja yksityiskohtaiset ohjeet prosessin suorittamiseksi) sekä tarkistuslista (yksityiskohtainen lista prosessiin liittyvistä tarkistettavista asioista). Uutta riskienhallintasuunnitelmaa seurattiin viikoilla 9-26 (27.2.2012 - 28.6.12). Analysoitujen riskien ilmenemismäärä mitattiin kyseisellä ajanjaksolla.

Seuranta järjestettiin toiminnoittain siten, että rahastojen arvonlaskennan tarkisti viikoittain se henkilö, joka ei kyseisen rahaston arvonlaskentaa muina päivinä pääsääntöisesti tee (yhteensä 18 tarkastusta). Asiakas- ja osuusrekisteri käytiin läpi rahastojen merkintäpäivää edeltävänä päivänä (neljä tarkastusta). Asiakaspalvelu tarkastettiin joka kuukauden ensimmäisenä maanantaina (neljä tarkastusta). Seurantaan ja raportointiin liittyvät asiat kartoitettiin joka kuukauden 22. päivänä (neljä tarkastusta). Mikäli tarkistuspäivä osui viikonlopulle tai arkipyhälle, siirtyi se seuraavaan työpäivään.

Toisena mittauskohteena oli suunnitelman käyttökelpoisuus ja hyödyllisyys yritykselle. Tämä toteutettiin tarkoituksenmukaisilla nykytila- ja loppuanalyyseillä. Näistä saatuja

tuloksia verrattiin keskenään ja sen perusteella subjektiivisella yrityksen sisäisellä arvioinnilla mitattiin kuinka paljon riskienhallintaprosessi on parantunut. Käytännössä laskettiin kuinka moni erikseen määritelty riskienhallinnan osa-alue katsottiin parantuneeksi. Tavoitearvo oli yli 50 %.

Kolmas mittauskohde oli riskienhallinnan laajuus, jota mitattiin tunnistettujen riskien lukumäärällä. Tässä laskettiin riskien lukumäärä ja sitä verrattiin alkutilanteeseen. Tavoitteena oli, että tunnistettujen riskien määrä on suurempi kuin lähtöarvo.

Neljäntenä mitattiin riskienhallinnan tason optimaalisuutta. Se määriteltiin siten, että riskienhallinnan katsottiin olevan optimaalinen kun operatiivisessa toiminnassa ei ilmene sellaisia virheitä, joiden vuoksi yritys joutuisi korvausvastuuseen ulkopuolisten tahojen suuntaan. Tätä mitattiin toteutuneen korvausvastuun suuruudella. Mikäli korvausvastuuta olisi realisoitunut, olisi sen euromäärä suhteutettu yrityksen taseeseen. Tavoitteena oli, että missään tapauksessa euromäärä ei ylittäisi 1 % edellisen tilikauden taseen arvosta.

Lisäksi jokaiselle kartoitetulle riskille määriteltiin erikseen oma mittarinsa ja tavoitearvonsa. Ne on eritelty riskijaottelu-taulukossa (liite 1).

4.4 Validiteetti, reliabiliteetti ja verifiointi

Laadullisen tutkimuksen validiteetti on sen uskottavuutta ja vakuuttavuutta. Haasteena on, että tutkimuksella voidaan aina vain raapaista tutkittavan ilmiön pintaa eikä sitä kyetä koskaan kuvaamaan raportissa täysin sellaisena kuin se todellisuudessa ilmenee. (KvaliMOTV: Validiteetti.) Tämän kehittämistehtävän validiteettia pyrittiin vahvistamaan riittävän perusteellisella nykytilan kartoituksella ja sen lähtökohdista johdetuilla kehittämistoimenpiteillä sekä raportoimalla tutkimuksen kulku ja johtopäätösten teko niin, että lukija voi itsenäisesti arvioida tutkimuksen pätevyyttä. Näiden perusteella erityisesti tutkimuksen sisäisen validiteetin katsotaan olevan hyvä, sillä toimintatutkimuksen luonne muutoksen toteuttajana tuki kehitystehtävän tavoitteiden saavuttamista. Käytetyt mittarit ja tapahtumien mittaukset olivat selkeitä ja sellaisenaan toistettavissa.

Sisäistä validiteettia heikentäviä tekijöitä voivat olla ajassa ja olosuhteissa tapahtuneet muutokset. Koska mittausperiodin täytyy olla rajallinen, on lähinnä sattumasta kyse, millaisia ulkoisten vaikutusten mukaisia tapahtumia kyseiselle ajanjaksolle sattuu. Lisäksi se, että kaikkia tavoitteena olleita tarkistuslistoja ei saatu täytettyä suunnitellusti, saattoi aiheuttaa pientä vääristymää tuloksiin. Tällä ei pitäisi olla merkittävää vaikutusta, sillä täytettyjen listojen prosentuaalinen osuus oli kuitenkin merkittävä. Näistä lisää alaluvussa 7.3.1 Suunnitelman käyttöönoton onnistuminen ja sovellettavuus. Ulkoinen validiteetti kehittämistehtävässä jäi todennäköisesti melko heikoksi tutkimuksen ainutkertaisuuden ja organisaatiosidonnaisuuden vuoksi. Kehittämistehtävä käsitti lähtökohtaisesti kertaluonteisia ja kohdeorganisaatioon räätälöityjä toimintojen parannusehdotuksia.

Kirk ja Miller erittelevät laadullisen tutkimuksen reliabiliteetin arvioimisen kolme ulottuvuutta: ajallinen reliaabelius, metodin reliaabeliuden arviointi ja johdonmukaisuus tuloksissa (KvaliMOTV: Reliabiliteetti). Näistä näkökulmista tarkastellen tämän tutkimuksen reliabiliteetti on hyvä. Yrityksen sisäinen toimintaympäristö, eli henkilöstö, puitteet ja liikeidea, on historiallisesti tarkastellen melko stabiili, joten ajallinen reliaabelius on sen vuoksi hyvällä tasolla. Tutkimusmenetelmät, haastattelut ja kirjallisen aineiston analysointi tukivat toisiaan siten, että odotettavissa ei ollut näistä lähteistä saatavan datan epäjohdonmukaisuutta. Tutkimuksen kokonaisreliabiliteettia pyrittiin vahvistamaan tutkimusprosessin huolellisella raportoinnilla siten, että selvityksestä käy ilmi mitä tehtiin ja miten toimenpiteet toteutettiin. Lisäksi tutkimustuloksia peilattiin käytettyyn teoriaan, tutkimusongelmaan ja -kysymyksiin. Täten pyrittiin myös verifioimaan tutkimus.

4.5 Tutkijan ja muiden projektiin osallistuneiden roolit

Toimintatutkimuksessa tutkijan rooli on verrattavissa konsultin rooliin tavoitteena auttaa kohdeyritystä tiedostamaan ja ratkaisemaan kehittämisen kohteen ongelmia ja selviytymään ratkaisemattomien ongelmien parissa. Hänen roolinsa on kaksinainen: yhtäältä hän tutkii, toisaalta käyttää saamiaan tietoja suoraan hankkeen hyväksi. (Toimintatutkimus.)

Kehittämistehtävän ajan tutkija työskenteli kohdeyrityksessä ja suoritti tutkimuksen pääosin itsenäisesti työpaikkaohjaajan valvonnassa. Käytännössä hän teki kohdeyrityksen nykytila- sekä loppuanalyysit, tunnisti ja arvioi riskit, kirjasi riskeihin vastaamisen käytänteet, laati valvontatoimenpiteitä ja varmisti tiedonkulun sekä seurannan. Vastuullinen rooli yrityksen koko toiminnan ja myös tämän kehittämistehtävän osalla korostui henkilöstömuutosten myötä.

Yrityksen koko muu henkilöstö osallistui myös omien toimiensa ohella projektiin. Näkyvimmin he olivat mukana laatimassa riskeihin vastaamisen käytänteitä sekä valvontatoimenpiteitä. Pääasiassa tämä tarkoitti toimintokohtaisten tarkistuslistojen laatimista, kehittämistä ja testausta sekä työohjeiden tarkastuksia. Yrityksen perustajan haastatteluiden perusteella saatiin merkittävää taustatietoa yrityksen historiasta sekä toimintaperiaatteista.

4.6 Käsitteitä

Sijoitusrahasto (myöh. rahasto) on arvopaperisalkku, jonka omistavat rahasto-osuudenomistajat tekemiensä sijoitusten suuruisessa suhteessa. Rahastot tarjoavat mahdollisuuden parempaan tuottoon alhaisemmalla riskillä ja alhaisemmilla kuluilla kuin minkä yksittäinen sijoittaja voi saada aikaan omalla aktiivisella arvopaperikaupankäynnillään. (Puttonen & Repo 2003, 25 - 29.) Rahasto-osuuksien ostoa kutsutaan rahastomerkinnäksi ja myyntiä rahastolunastukseksi.

Salkunhoitaja on rahastojen sijoituspäätöksistä vastaava. Hänen tulee noudattaa rahaston toimintaperiaatteita, jotka on määritelty Finanssivalvonnan vahvistamissa rahastokohtaisissa säännöissä.

Rahastoyhtiö vastaa rahastojen hallinnoinnista ja toiminnasta, mikä on luvanvaraista. Luvan myöntää sekä toimintaa valvoo Finanssivalvonta. (Rahastoyhtiöt 2010.)

Finanssivalvonta on hallinnollisesti Suomen Pankin yhteydessä toimiva valvoja, joka on rahoitus- ja vakuutusvalvontaviranomainen. Sen tehtävänä on edistää hyvien menettelytapojen noudattamista finanssimarkkinoilla ja yleisön tietämystä finanssimarkki-

noista. Finanssivalvonta toimii pankki-, vakuutus- ja sijoituspalveluiden käyttäjien hyväksi. (Tietoa Finanssivalvonnasta. 2011.)

Sijoitusrahastolaki säätelee sijoitusrahastojen toimintaa. Siinä on määräykset sijoitusrahastotoiminnasta. Laki sisältää myös säännökset rahastoyhtiöstä, säilytysyhteisöstä sekä rahastojen markkinoinnista ja tiedonantovelvollisuudesta. (Sijoitusrahasto-opas 2009.)

UCITS IV on sijoitusrahastodirektiivin muutos, jonka tarkoituksena on uudistaa sijoitusrahastojen sääntelyä. Muutos on tullut Eurooppatasolla voimaan heinäkuussa 2011. Kansallinen implementointiprosessi on vielä kesken. (Kirppu 2010.)

Riskienhallinta kattaa kaiken toiminnan, mikä liittyy tavoitteiden asettamiseen, riskien tunnistamiseen, mittaamiseen, arvioimiseen, käsittelyyn, raportointiin, seurantaan, valvontaan ja riskeihin reagoimiseen (Sisäinen valvonta ja riskienhallinta 2012).

Riski tarkoittaa vahingonvaaraa tai vahingonuhkaa. Tilastotieteellinen tulkinta riskistä on tappion tai voiton todennäköisyys. Matemaattisen määritelmän mukaan riski = todennäköisyys x riskin laajuus/vakavuus. (Suominen 2003, 9 - 10.) Riskiin liittyvät tekijät, jotka vaikuttavat riskin kokemiseen, ovat tapahtumaan liittyvä epävarmuus, tapahtumaan liittyvät odotukset sekä tapahtuman laajuus ja vakavuus. (Juvonen ym. 2005, 7.)

Operatiivinen riski tarkoittaa haitallisten seuraamusten vaaraa tai tappionvaaraa, joka aiheutuu riittämättömistä tai epäonnistuneista sisäisistä prosesseista, henkilöstöstä, järjestelmistä tai ulkoisista tekijöistä sisältäen myös oikeudelliset riskit. Operatiiviset riskit ovat useimmiten laadullisia eikä niiden aiheuttama tappio ei ole kaikissa tapauksissa mitattavissa. Riski voi toteutua viiveellä ja ilmetä välillisesti esimerkiksi valvottavan maineen ja arvostuksen heikkenemisenä. Operatiivisten riskien hallinta on yleensä riskien minimoimista. (Finanssivalvonnan standardi 4.4.b 2004, 12.)

5 TEOREETTINEN VIITEKEHYS

Teoreettisessa viitekehyksessä käsitellään riskien luokittelua erilaisten luokittelumallien pohjalta sekä riskienhallintaa prosessina. Lisäksi huomioidaan sovellettavat viranomaismääräykset eli Finanssivalvonnan standardi 4.4.b Operatiivisten riskien hallinta sekä sijoitusrahastodirektiivi UCITS IV.

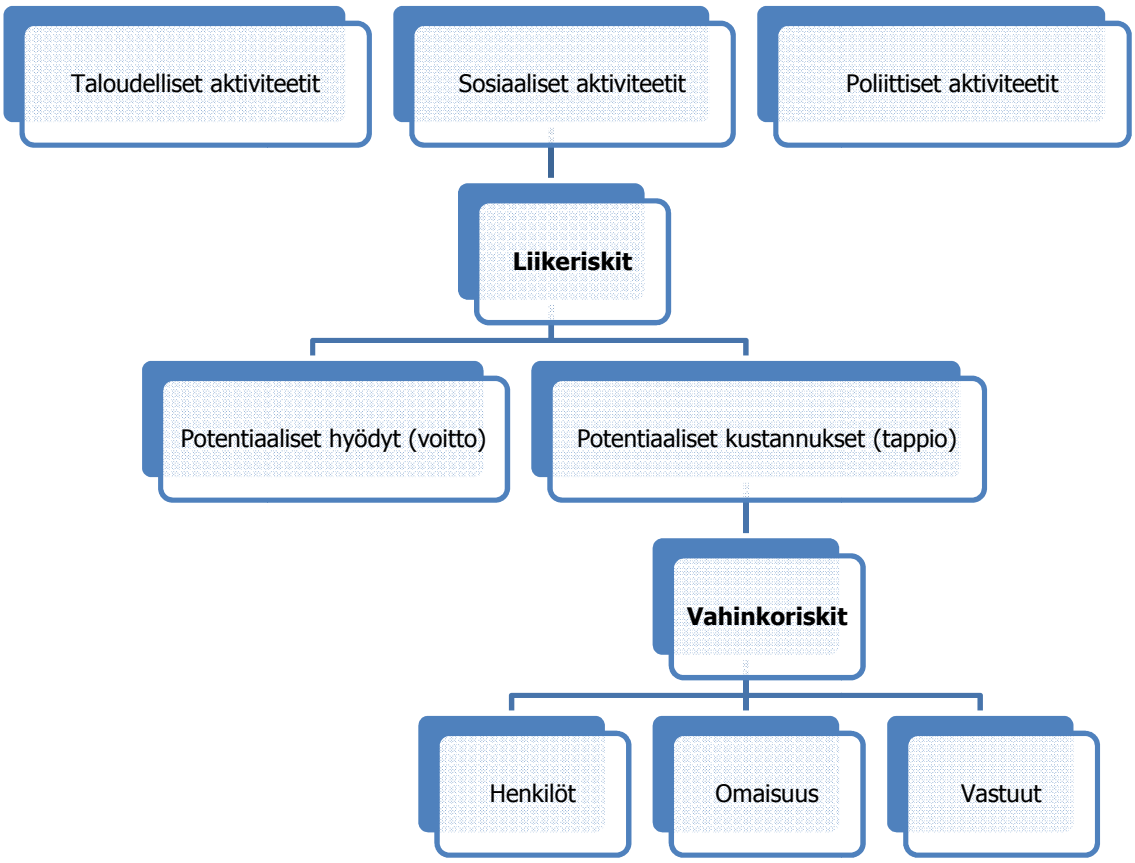
5.1 Riskien luokittelu

Riskien luokittelu on riskienhallinnan keskeisin teema, sillä siten ne saadaan yhteismitallisiksi ja niiden vertailtavuus paranee. Lisäksi näin parannetaan yrityksen riskitietoisuutta sekä lisätään ymmärrystä eri riskien keskinäisistä suhteista. Riskien luokittelu on riippuvainen toimialasta, organisaatiosta, arvioijasta sekä kontekstista. (Ilmonen & Kallio & Koskinen & Rajamäki 2010, 70.)

5.1.1 Gahinin riskimalli

Fikry Gahinin klassista riskifilosofiaa on havainnollistettu kuviossa 3. Teoriassa lähdetään luokittelemaan riskejä yrityksen toiminnoista: taloudellisista, sosiaalisista ja poliittisista aktiviteeteistä. Nämä muodostavat yrityksen liikeriskien kentän. Niille on tyypillistä sekä voiton että tappion mahdollisuus ja niiden katsotaan olevan oleellinen osa yritystoimintaa. Liikeriskit liittyvät yrityksen tekemiin päätöksiin ja niiltä ei useimmiten pysty suojautumaan vakuuttamisella. (Suominen 2003, 12.)

Vahinkoriskit sijoittuvat Gahinin mallissa potentiaalisten kustannusten eli tappion uhan alle. Nämä ovat seurausvaikutuksiltaan pelkästään vahinkoa aiheuttavia, mutta ne ovat tyypillisesti vakuuttamiskelpoisia. Vahinkoriskien alakategorioihin Gahin jakaa henkilö-, omaisuus- ja vastuuriskit. Mallissa liike- ja vahinkoriskit eivät ole erillisiä riskejä, vaan toisistaan riippuvaisia. Niiden välille ei ole myöskään tarkoitus tehdä jakoa. (Suominen 2003, 12–13.)



Kuvio 3. Gahinin riskimalli (Suominen 2003, 13).

Riskien jakaminen liike- ja vahinkoriskeihin on periaatteessa yksinkertaista. Liikeriskit ovat kuitenkin nopeasti muuttuvia, mikä aiheuttaa haasteita niiden listaamiseen ja riskienhallintaan. Vahinkoriskit ovat staattisempia luonteeltaan ja suhteellisen hyvin tunnettuja sekä tunnistettuja. (Suominen 2003, 14.) Lisäksi liikeriskejä leimaa myös tuntematon elementti. Siinä missä vahinkoriskien toteutumistodennäköisyyttä voi arvioida vakuutus- ja muiden tilastojen perusteella, liikeriskeistä ei vastaavaa kattavaa dataa ole saatavissa vaan niiden arviointiin vaikuttavat ennen kaikkea johdon kyky arvioida yrityksen voimavarat ja tehdä yrityksen kannalta onnistuneita ratkaisuja. (Suominen 2003, 51.)

Liikeriskit liittyvät läheisesti strategiseen päätöksentekoon ja investointeihin sekä odotettavissa oleviin tuottoihin ja kustannuksiin. Vahinkoriskit puolestaan sijoittuvat lähelle yrityksen jokapäiväistä operatiivista toimintaa. Ne liittyvät odottamattomien ja haitallisten tapahtumien todennäköisyyteen. (Flink & Reiman & Hiltunen 2007, 23.) Tässä kehittämistehtävässä käsiteltävät operatiiviset riskit sijoittuvat Gahinin riskimallissa vahinkoriskeihin.

5.1.2 Finanssivalvonnan jaottelu

Finanssivalvonnan standardit ovat aihealueittaisia määräysten ja ohjeiden kokonaisuuksia, jotka osoittavat valvojan haluaman laatutason ja perustelevat sääntelyä (Rahoitussektorin määräyskokoelma). Finanssivalvonta on laatinut valvottavilleen vuonna 2004 standardin 4.4.b Operatiivisten riskien hallinta, jossa käsitellään operatiivisten riskien hallinnan periaatteita ja järjestämistä (Finanssivalvonnan standardi 4.4b 2004, 7). Standardi sijoittuu rahoitussektorin määräyskokoelmassa pääjakson Vakavaraisuus ja riskien hallinta alle. Operatiiviset riskit ovat yksi riskialue luotto-, markkina- ja likviditeettiriskien hallinnan ohella.

4.4b-standardissa operatiiviset riskit jaotellaan kahdeksaan osa-alueeseen: prosessit, oikeudelliset riskit, henkilöstö, jatkuvuussuunnittelu, varautuminen poikkeusoloihin, tietojärjestelmät, tietoturvallisuus sekä rikosriskit. Tämä jaottelu on myös kehittämistehtävän perustana.

5.1.3 Riskien kriteerit

Riskejä voi luokitella eri kriteerein, esim. riskin muodostumislokaation, riskinoton tietoisuusasteen, riskin vaikutustavan tai vakuutettavuuden perusteella. Lisäksi riskejä voi ryhmitellä kohteiden, seurausten vakavuuden sekä toteutumisen todennäköisyyden mukaan. (Erola & Louto 2000, 24; Ilmonen ym. 2010, 75–76.)

Muodostumislokaatio tarkoittaa yrityksen riskien toteutumispaikkaa eli tapahtuvatko riskit yrityksen sisäisessä vai ulkoisessa toimintaympäristössä. Toimintojen ulkoistaminen ja globalisoituminen lisäävät yrityksen ulkoisten riskien todennäköisyyttä. Ne ovat luonnollinen osa joka tapauksessa yrityksen riskienhallintaa, sillä yksikään yritys ei kykene toimimaan yhteisöstä tai ulkopuolisesta ympäristöstä itsenäisenä yksikkönä. Toiminnan turvaamisen varmistamiseksi oleellista on varmistaa toiminnan jatkuvuus, jos riskien verkkoon (toimintakumppaneiden riippuvuus ulkoisista tekijöistä) tulee toimintahäiriöitä. (Erola & Louto 2000, 25 - 27)

Ulkoiset riskit uhkaavat yritystä ulkoapäin siten, että yrityksen vaikutusmahdollisuudet niihin ovat rajalliset. Sisäiset riskit liittyvät yrityksen toimintoihin ja niihin liittyviin häiri-

öihin. Riskin lähteenä on useimmiten yrityksen toiminnan häiriö, työntekijän tekemä virhe tai toimintasuunnitelman epäloogisuus. (Erola & Louto 2000, 26.)

Riskinoton **tietoisuusaste** tarkoittaa sitä, ovatko käsillä olevat riskit tiedostettuja vai tiedostamattomia. Liiketoiminta kokonaisuudessaan on riskinottamista. Riskien tiedostaminen on yrityksen riskienhallintatoiminnon ensisijainen tehtävä, sillä vain tiedostettuja riskejä voi pyrkiä hallitsemaan. Menestyvä yritys kykenee ottamaan riskejä hallitusti. (Ilmonen ym. 2010, 76.) Tietoisen riskin ottamiseen liittyy hyötymismotiivi, jossa punnitaan panos-tuottosuhdetta. Tiedostamattomia riskejä yritys joutuu ottamaan silloin, kun tilanteeseen ei voida tai osata varautua. Tämä voi liittyä esim. toimintaympäristön radikaaliin muutokseen. (Erola & Louto 2000, 28.)

Riskien **vaikutustavalla** tarkoitetaan sitä, onko riskeillä välitön vai välillinen vaikutus yrityksen toimintaan. Välittömät tapahtumat toteutuvat usein nopeasti. Välilliset taas voivat itää pitkään ja vääristää toiminnan tuloksia kauan ennen kuin ne havaitaan. Usein näiden löytäminen ja eliminointi on haastavaa. Sen vuoksi niiden vaikutukset voivat muodostua merkittäviksi. Riskien mahdollisimman aikaisen vaiheen havainnointi on ensisijaista. Niiden kartoittamisessa riskien toteutumista ennakoivat merkit ja mittaustulokset on selvitettävä perusteellisesti ja varmistettava niiden merkityksen ymmärtäminen. (Erola & Louto 2000, 29.)

Riskienhallinnan keinoja ja toimenpiteitä suunnitellessa riskien **vakuutettavuus** on oleellinen seikka. Jotta riski ylipäätään olisi vakuutettavissa, sen tulee olla toistuva ja ennustettava jollain tasolla. Vakuutettavia riskejä voidaan kutsua staattisiksi tai vahinkoriskeiksi ja niille on tyypillistä, että toteutuminen aiheuttaa rahallisia tai aineellisia menetyksiä. Vakuutettavien riskien ulkopuolelle jäävät ovat dynaamisia eli liikeriskejä tai liiketaloudellisia riskejä, joihin liittyy myös voiton mahdollisuus. (Ilmonen ym. 2010, 75 - 76.)

5.1.4 Kolmikantajako Triage

Riskien ominaisuustarkastelu on tärkeä osa riskin ja sen vaikutusten analysointia. Riskien hallinnan kannalta relevantti jaottelu on kolmikantajako Triage. Siinä riskit on jaoteltu kolmeen luokkaan niiden haitallisuusasteen mukaan. Triage 1:een kuuluvat henkilö-

riskit tai muuten vakavat riskit, joiden seurausvaikutukset ovat erittäin haitallisia. Triage 2 käsittää muut riskit, jotka häiritsevät normaalia toimintaa. Triage 3 -ryhmään luetaan vähäiset ja merkityksettömät riskit, joiden ehkäisemiseksi ei ole välttämätöntä tehdä akuutisti mitään. (Erola & Louto 2000, 37.)

Riskejä voidaan luokitella niiden haitallisuuden lisäksi myös toteutumistodennäköisyyden mukaan. Nämä kaksi ulottuvuutta yhdistämällä saadaan luotua riskikartta, josta lisää seuraavassa luvussa riskienhallintaprosessin kuvauksen yhteydessä.

5.2 Riskienhallintaprosessi

Riskienhallintaprosessi on systemaattinen tapa arvioida, hallita ja raportoida yrityksen riskejä. Tällöin riskejä ei nähdä yrityksen toiminnasta irrallisina, vaan niitä kyetään suhteuttamaan poikkeamiin normaalioloista sekä tapahtuneisiin vahinkoihin. (Ilmonen ym. 2010, 91.)

Riskienhallintatyö on loogisinta aloittaa riskienhallintapolitiikan laatimisesta, jonka tavoitteena on luoda selkeät toimintatavat riskien tunnistamiseen ja hallintaan. Tuolloin tulee määritellä riskienhallinnan perusteet (perusperiaatteet, riskienhallintaorganisaatio, riskien tunnistamis- ja arviointiperiaatteet), toimenpiteet (kontrollointi, rahoittaminen) sekä johtaminen (seuranta ja tulosten raportointi). (Juvonen & Korhonen & Ojala & Salonen & Vuori 2005, 7.)

On hyvä mieltää eri riskienhallinnan vaiheet osiksi liiketoimintaprosesseja eikä irrottaa niitä erillisiksi keinotekoisiksi osa-alueikseen. Siten ne saadaan mukaan yrityksen jokapäiväiseen toimintaan, ajatteluun ja konkreettisiin työvälineisiin. Prosessimaisen riskienhallinnan perusedellytyksiä on riippuvuusnäkökulma, jossa selvitetään toimintojen riippuvuudet toisistaan. (Flink ym. 2007, 130; Erola & Louto 2000, 108 - 112.)

Riskienhallintaprosessin konkreettisena tuloksena voi olla riskikartta, joka on konkreettinen dokumentaatio koko liiketoiminnan vallitsevasta riskiympäristöstä. Sen avulla kuvataan usean riskin aiheuttajan suhteellista asemaa kahden ulottuvuuden, todennäköisyyden ja merkittävyyden, avulla. Riskikartan tarkoituksena on tuoda esiin erot riskien

jakautumisesta ja keskinäisistä suhteista. Niiden perusteella riskit jaetaan hyväksyttäviin, merkittäviin ja erittäin merkittäviin. (Flink ym. 2007, 152.)

5.2.1 Historia

Riskienhallinta on perinteisesti ymmärretty vahinkoriskilähtöiseksi prosessiksi, jonka avulla pyritään torjumaan organisaatiota uhkaavia vaaroja ja minimoimaan niistä aiheutuvat menetykset. Tämän ajattelutavan juuret ovat 1930-luvun Yhdysvalloissa. Suomessa aihepiiri tuli ajankohtaiseksi 1980-luvulla pankkikriisien aikaan. Tähän olivat vaikuttamassa vakuutusyhtiöt, joiden markkinointi liittyi riskien hallitsemiseen. 1990-luvun lopulla laajennuksena tuli mukaan Enterprise Risk Management (ERM) eli kokonaisvaltaisen riskienhallinnan käsite. (Flink ym. 2007, 125 - 126.)

Kehityssuunta on kulkenut viime vuosina perinteisestä riskilähtöisestä ajattelusta kohti kokonaisvaltaista riskienhallintaa. Riskien vakuuttamisen ja välttämisen sijaan keskitytään strategialähtöisyyteen; riskienhallinta suunnitellaan ja toteutetaan palvelemaan liiketoimintatavoitteiden toteutumista. (Flink ym. 2007, 129.) Näkökulma on laajentunut yritysten eri elementtien keskinäisten riippuvuussuhteiden tarkasteluun. Riskienhallintaa ajatellen keskitytään yksittäisten toimintojen ja niistä aiheutuvien riskien tarkastelun sijasta yrityksen taloudellisen ja toiminnallisen kokonaishyödyn maksimointiin riskienhallinnan keinoin. (Blumme ym. 2005, 83 - 84.)

Vuosituhannen alussa talousmaailmaa järkyttivät useat ilmitulleet tilinpäätösskandaalit, joiden johdosta sijoittajat menettivät luottamuksensa yhtiöitä ja niiden kirjanpitojärjestelmiä kohtaan. Tällaisia tapauksia olivat mm. energiayhtiö Enron, teleyhtiö WorldCom ja italialainen elintarvikeyhtiö Parmalat. (Ahokas 2009.)

Tapahtumien seurauksena asetettiin voimaan Sarbanes-Oxley -laki (SOx) Yhdysvalloissa 2002. Lain on arvioitu olevan merkittävin arvopaperimarkkinoihin vaikuttava laki sitten 1930-luvun. Sen tavoitteena on parantaa yrityksen julkistamien tietojen oikeellisuutta ja luotettavuutta. Laki vaatii yhdysvaltalaisissa pörsseissä noteerattavien yritysten johtamis- ja hallintojärjestelmiltä entistä suurempaa tehokkuutta. Sen antamat määräykset koskevat muun muassa johdon raportointia, tilinpäätöstietojen julkistamista, tilintarkastajien vastuuta ja sisäisen valvonnan järjestämistä. Erityistä huomiota SOx

kiinnittää yrityksen sisäiseen valvontajärjestelmään. Yrityksen tulee myös arvioida sisäisen valvonnan ja menettelytapojen tehokkuutta vertaamalla omaa sisäisen valvonnan järjestelmää sopivaan viitekehykseen, joista yleisesti käytetyin on COSO-malli. Myös tilintarkastajien tulee ottaa kantaa johdon arviointiprosessiin sekä sisäisten valvontajärjestelmien tehokkuuteen. (Ahokas 2009.)

5.2.2 Riskienhallinnan suhde yrityksen tarpeisiin

Edellä esitettyä taustaa vasten yrityksissä on lähtökohtaisesti tarve organisoida riskienhallinta, saada prosessi määrämuotoiseksi ja tietyin ajoin päivitettäväksi sekä hyödyntää riskienhallintaa liiketoiminnallisesti (Erola & Louto 2000, 95). Riskienhallinnan rooli voidaan nähdä koko yritystoimintaa palvelevana, suunnitelman mukaisena ja vaiheittain etenevänä toimintaprosessina. Se tulisi nähdä yrityksessä jatkuvana monimuotoisena prosessina, jota seurataan ja arvioidaan tasaisin väliajoin. Yksittäisenä kertaprojektina suoritettuna sen merkitys heikkenee eikä se pysty vastaamaan yrityksen alati muuttuviin tarpeisiin. (Suominen 2003, 31.)

Riskienhallinnan toteuttaminen tekemisen vuoksi ei ole itseisarvo, vaan tavoitteiden tulee pohjautua yrityksen liiketoiminnallisiin tavoitteisiin. Jatkuvuus, tavoitteellisuus, mitattavuus ja vastuunjako tyypittävät riskienhallintatyötä. Onnistuakseen prosessin tulee tuottaa hyötyä eli johdon tulee nähdä toiminnan tuovan lisäarvoa yritykselle. (Flink ym. 2007, 128.)

5.2.3 Enterprise Risk Management eli kokonaisvaltainen riskienhallinta

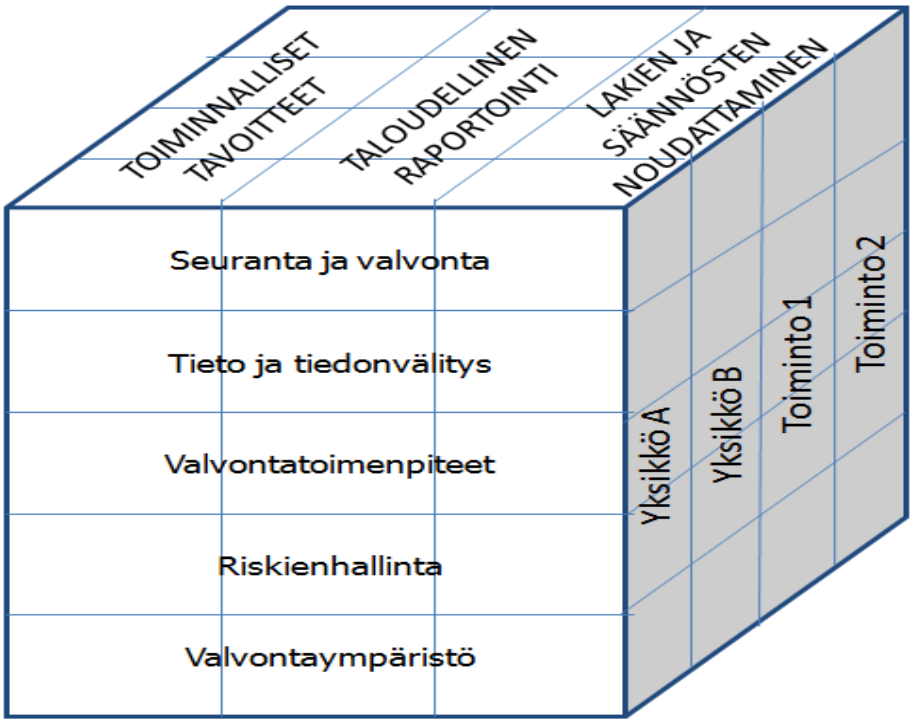
Kiristyvä kilpailutilanne ja tiukentuvat viranomaisvaatimukset muokkaavat yritysten toimintaympäristöä. Tämä johtaa siihen, että yrityksen johtamis- ja hallintojärjestelmän, riskienhallinnan sekä toiminnan tuloksellisuuden riippuvuussuhteita tulee pohtia entistä tarkemmin. Johdon tulee hallita yhä laajempia kokonaisuuksia luodakseen lisäarvoa omistajille ja maksimoidakseen yrityksen tuoton. Tämän vuoksi riskeistä puhuttaessa tarkastelu kääntyy yksittäisistä toiminnoista ja niiden riskeistä koko yrityksen tasolle. Päämääräksi tulee yrityksen taloudellisen ja toiminnallisen kokonaishyödyn maksimointi riskienhallinnan keinoin. (Blumme ym. 2005, 83 - 84.)

Enterprise Risk Management (ERM) tarkoittaa kokonaisvaltaista riskienhallintaa. Se pyrkii yhdistämään yrityksen eri liiketoimintojen näkökulmat riskienhallintaan erotellen strategian kannalta oleelliset asiat epäolennaisista. Näin prosessi tuottaa johdolle tietoa yrityksen riskitilanteesta ja tulevaisuudesta. (Flink ym. 2007, 282.)

5.3 COSO Enterprise Risk Management

5.3.1 Tausta

Committee of Sponsoring Organisations of the Treadway Commission (myöh. COSO) on viidestä yhdysvaltalaisesta järjestöstä koottu yhteisyritys, jonka tarkoituksena on tarjota työkaluja yritysten riskienhallintaan, sisäiseen valvontaan sekä väärinkäytösten ennaltaehkäisyyn (COSO: About us). Vuonna 1992 julkaistiin raportti, jossa esiteltiin ensimmäisen kerran sisäisen valvonnan määritelmä ja osatekijöiden kuvaukset. Tätä kutsutaan COSO-malliksi. Siinä on eritelty sisäisen valvonnan prosessin tavoitteet, jotka nivoutuvat eri osatekijöiden kautta yksikkö- ja toimintokohtaiselle tasolle. Tämä on esitelty kuvan muodossa kuviossa 4. (Blumme ym. 2005, 34 - 35.)



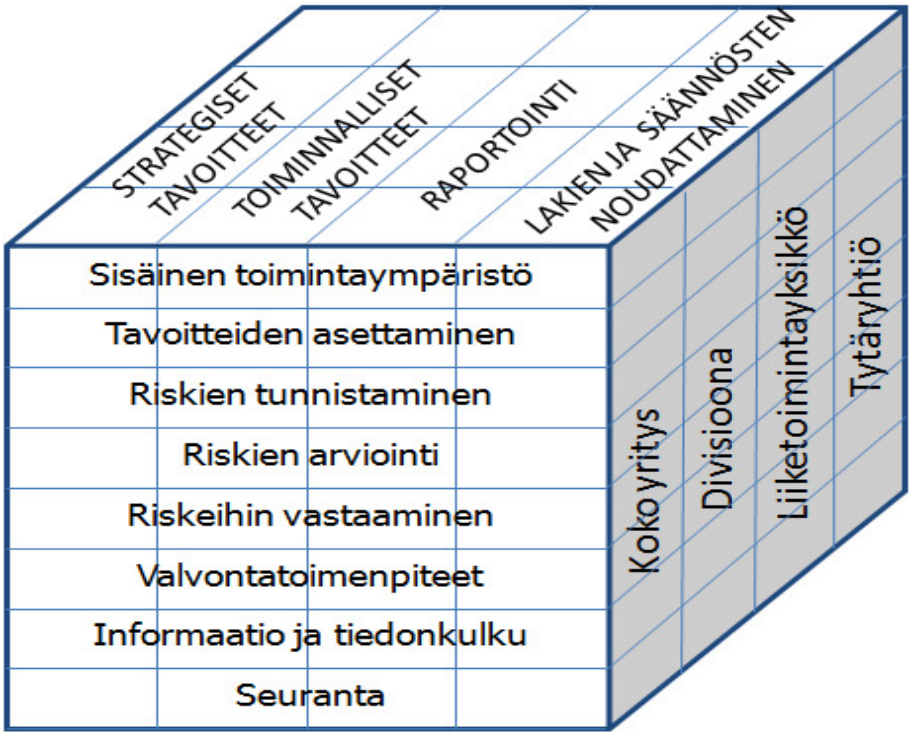
Kuvio 4. COSO-mallin osatekijät (Blumme ym. 2005, 35).

COSO-mallissa sisäinen valvonta on prosessi, johon osallistuvat hallitus, johto sekä henkilöstö. Se pyrkii varmistamaan, että saavutetaan toimintojen tehokkuus ja tarkoituksenmukaisuus, taloudellisen tiedon ja raportoinnin luotettavuus sekä lakien ja säännösten noudattaminen. Sisäinen valvonta muodostuu viidestä toisiinsa vaikuttavasta osatekijästä: valvonnasta, tiedonvälityksestä, valvontatoimenpiteistä, riskienhallinnasta sekä valvontaympäristöstä. Näiden ulottuvuuksien lisäksi kolmas osatekijä on yrityksen eri toiminnot tai yksiköt, joihin edellä esiteltyjä tekijöitä sovelletaan. (Blumme ym. 2005, 35.)

Valvontaympäristö on organisaatiossa vallitseva valvontakulttuuri, joka on perusta kaikille muille sisäisen valvonnan osatekijöille. Riskienhallinta tässä yhteydessä tarkoittaa, että yrityksen toimintaympäristön jatkuva muutos asettaa velvoitteita tunnistaa, arvioida ja hallita muutokseen liittyviä sisäisiä ja ulkopuolelta tulevia riskejä, jotka uhkaavat yrityksen tavoitteiden saavuttamista. Valvontatoimenpiteet ovat toimintaperiaatteita ja -tapoja, jotka auttavat varmistamaan, että yrityksen toiminta on johdon ohjeiden mukaista ja että yrityksessä ryhdytään tarvittaviin toimenpiteisiin tavoitteita uhkaavien riskien hallitsemiseksi. Tieto ja tiedonvälitys käsittävät sen, että asiaankuuluva informaatio välitetään muodossa, jonka avulla henkilöstö voi suoriutua velvollisuuksistaan. Seuranta ja valvonta käsittävät sisäisen valvonnan toimivuuden ja laaduntarkkailun. Arviointien laajuus ja tarkkuus linkitetään riskiarviointien tuloksiin ja jatkuvan seurannan tehokkuuteen. (Blumme ym. 2005, 36 - 37.)

5.3.2 COSO ERM -malli

COSO julkaisi vuonna 2004 kokonaisvaltaisen riskienhallinnan mallin (COSO ERM), joka perustuu edellä esiteltyyn COSO-malliin. COSO ERM keskittyy näistä lähtökohdista yrityksen riskienhallintaan. Malli määrittelee riskienhallinnan prosessiksi, jota yritys toteuttaa strategiansa mukaisesti ja jonka tarkoituksena on tunnistaa mahdolliset yritykseen haitallisesti vaikuttavat tapahtumat. Lisäksi mallin avulla hallitaan ja rajataan riskejä siten, että yrityksen tavoitteiden toteutuminen voidaan riittävässä laajuudessa varmistaa riskinottohalukkuuden puitteissa. Perusajatus on, että luodaan yhteys yrityksen tavoitteiden, toiminnallisen rakenteen sekä riskienhallinnan välille. Tämä kokonaisuus on esitetty kuviossa 5. (Blumme ym. 2005, 84 - 85.)



Kuvio 5. COSO ERM -malli (Blumme ym. 2005, 84).

COSO ERM -mallissa kokonaisvaltaisen riskienhallinnan tavoitteet jaetaan neljään osa-alueeseen: strategiseen, toiminnalliseen, raportointiin sekä lakeihin ja asetuksiin liittyviin. Jotta tavoitteet saavutetaan, malli määrittelee kahdeksan sen mahdollistavaa johtamisprosessin osatekijää: sisäinen toimintaympäristö, tavoitteiden asettaminen, riskien tunnistaminen, riskien arviointi, riskeihin vastaaminen, valvontatoimenpiteet, informaatio ja tiedonkulku sekä seuranta. (Flink ym. 2007, 282.) Kolmantena ulottuvuutena ovat yrityksen eri osakokonaisuudet tytäryhtiöistä yksikkötasolle. Yrityksestä riippuen näitä osia voi olla yksi tai useita. (Moeller 2011, 55.)

5.3.3 Mallin osatekijät

COSO ERM -mallin mukaisen riskienhallinnan pyrkimyksenä on riskinottohalukkuuden ja strategian yhdenmukaistaminen, riskienhallinnan keinoja koskevien päätösten parantaminen, toiminnallisten yllätysten ja tappioiden vähentäminen, kertautuvien sekä yrityksenlaajuisten riskien havaitseminen ja hallinta, mahdollisuuksien hyödyntäminen sekä pääoman käytön tehostaminen. (Blumme ym. 2005, 85.) Seuraavassa esitellään

mallin kahdeksan eri horisontaalisen osatekijän perusperiaatteet. Samalla tuodaan esiin viranomaismääräyksiä, joita rahastoyhtiön toiminnassa tulee ottaa huomioon.

Sisäinen toimintaympäristö muodostaa COSO ERM -mallin perustan. Sen avulla määritellään yrityksen strategia ja päämäärät, miten liiketoimintasuunnitelma jäsennellään sekä miten riskejä tunnistetaan ja hallitaan. Sisäinen toimintaympäristö koostuu kahdeksasta eri elementistä. (Moeller 2011, 56.)

Riskienhallintafilosofia on yrityksen tapa suhtautua riskipitoisiin suunnitelmiin. Se koostuu yhteisistä uskomuksista sekä asenteista ja määrittelee, miten riskinäkökulma otetaan huomioon yrityksen kaikessa tekemisessä. (Moeller 2011, 56.)

Riskinottohalukkuus määrittelee, minkä verran yritys on valmis ottamaan riskiä pyrkiessään tavoitteisiinsa. Sitä voidaan mitata sekä määrällisesti että laadullisesti. Oleellista on, että koko johdolla on samansuuntainen käsitys yrityksen yleisestä riskinottohalukkuudesta. (Moeller 2011, 57.)

Hallitus on yleensä yrityksen johdosta riippumaton hallintoelin, jolla on tärkeä rooli valvoa ja johtaa yritystä myös riskienhallintanäkökulmasta. Sen tehtävänä on seurata johdon toimintaa, esittää myös hankalia kysymyksiä sekä kontrolloida yrityksen liiketoimintaa. Hallituksen suhtautumistavalla ja asennoitumisella toimintaan on usein iso merkitys yritykselle. (Moeller 2011, 57.)

Rehellisyys ja eettiset arvot määrittelevät johtamiskäytäntöjen ohella yrityksen koko henkilöstön käyttäytymisnormistoa. Tässä kohdin yrityskulttuurin tulisi olla vahvasti ohjaamassa yrityksen kaikkien tasojen toimintaa mahdollisissa riskipitoisissa tilanteissa. Niihin voivat liittyä yrityksen tekemät virheet, väärinkäytösepäilyt, vastuukysymykset jne. (Moeller 2011, 57 - 58.)

Johdon valvontaperiaatteet tarkoittavat johdon velvollisuutta etsiä jokaiseen tehtävään osaava ja pätevä henkilö siten, että hän omalla työpanoksellaan on viemässä yritystä kohti sen strategisia tavoitteita. (Moeller 2011, 58.)

Organisaation rakenne tulisi olla järjestetty niin, että se tukee yrityksen toimintaa optimaalisesti. Tällöin rakenne vastaa yrityksen tarpeita ja mahdollistaa tavoitteiden saavuttamisen. Tähän liittyy valta- ja vastuunäkökulmien ohella selkeä raportointi ja kommunikaatio. (Moeller 2011, 58.)

Finanssivalvonta on määritellyt organisaatiota niin, että hallituksen tehtävänä on hyväksyä operatiivisten riskien hallinnan periaatteet ja arvioida niitä määräajoin uudelleen siten, että muutokset yrityksen toimintaympäristössä ja liiketoiminnassa otetaan huomioon. Periaatteet kattavat operatiivisten riskien tunnistamisen sekä riskien arvioinnissa, valvonnassa ja rajoittamisessa käytettävät menettelyt sekä tärkeimmät operatiivisten riskien hallintaprosessit. (Finanssivalvonnan standardi 4.4.b 2004, 13.)

Toimitusjohtajan vastuulla on huolehtiminen operatiivisten riskien hallinnan periaatteiden käytännön toteuttamisesta ja siitä varmistuminen, että jokainen työntekijä tunnistaa omaan toimintaansa liittyvät operatiiviset riskit ja niiden hallintaan liittyvät menettelytavat. Hän vastaa myös yrityksen tuotteisiin, toimintoihin, prosesseihin sekä järjestelmiin liittyvien operatiivisten riskien hallinnan menettelytapojen kehittämisestä ja ylläpidosta. (Finanssivalvonnan standardi 4.4.b 2004, 13.)

Valtuudet ja velvollisuudet jaetaan yrityksissä tätä nykyä usein siten, että organisaatiosta pyritään tekemään matala ja päätäntävaltaa viedään niille tahoille, jotka ovat lähellä ydinliiketoimintaa. Oleellista on, että kaikki organisaatiossa ovat tietoisia näistä käytännöistä ja siitä, miten heidän omat tekemisensä vaikuttavat yrityksen tavoitteiden saavuttamiseen. (Moeller 2011, 59.)

Henkilöstö on yrityksen suurin voimavara. Jotta se edesauttaisi yritystä menestymään, tulee jokaisella työntekijällä olla selkeä kuva siitä, mikä on toivottavaa, sallittua ja kiellettyä. Nämä käytännöt tulee viestiä selkeästi henkilöstölle ja niistä tulee pitää kiinni. (Moeller 2011, 59.)

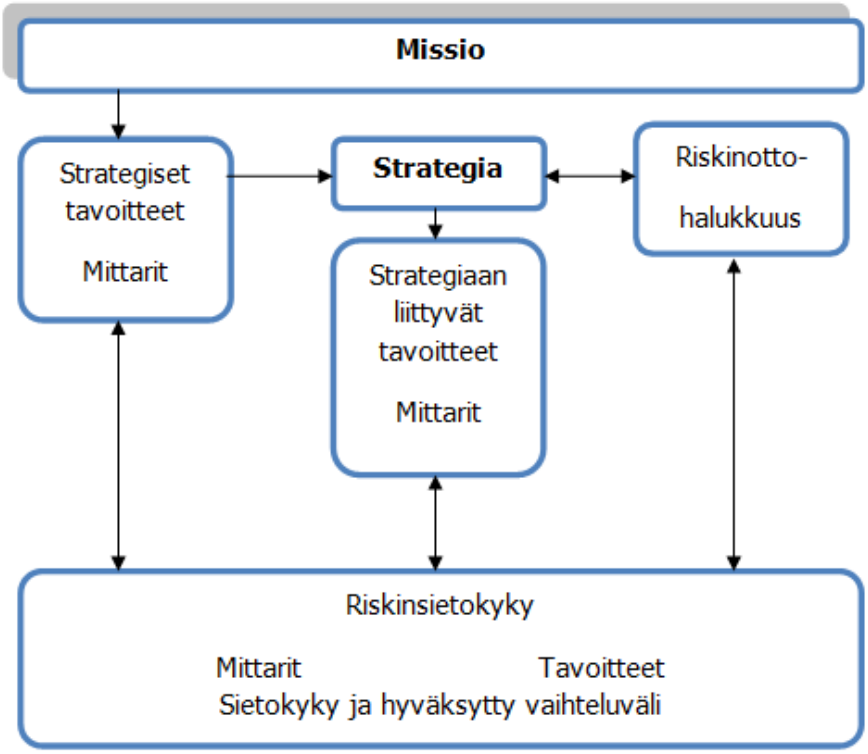
Esitellyt sisäisen toimintaympäristön elementit ovat yrityksen riskienhallinnan lähtökohtia muodostaen riskienhallinnan perustan. Erityisen merkityksellisiä ovat riskienhallintafilosofia ja riskinottohalukkuus. Niistä informointi yrityksen sidosryhmille tulisi olla ensisijaisen tärkeää. (Moeller 2011, 61.)

Tavoitteiden asettaminen tulee tehdä ennen kuin yrityksen riskienhallintaprosessi voidaan aloittaa. Toiminnan suunnittelu, seuranta ja ohjaus sekä näihin liittyvä tavoitteiden määrittely ovat edellytyksiä tavoitteita uhkaavien riskien tunnistamiselle (Blumme ym. 2005, 65). Strategisen suunnittelun kannalta yrityksen mission eli perustehtävän tai toiminta-ajatuksen määrittely on ensimmäinen vaihe, sillä sen avulla saadaan kiteytettyä yrityksen toiminta-ajatus ja olemassaolon syy. Oikein toteutettuna se tuottaa strategisia tavoitteita, jotka tähtäävät mission saavuttamiseen. Tämän jälkeen voidaan valita, kehittää sekä implementoida sopiviksi katsotut toimenpiteet. Näitä ovat yrityksen kannattavuuteen ja menestykseen liittyvät operatiiviset tavoitteet, raportointiin liittyvät tavoitteet ja lakien sekä säännösten noudattamiseen liittyvät hyvät hallintotavat. (Moeller 2011, 62.)

COSO ERM -malli ei itsessään tarjoa toimintaohjeita tai -ehdotuksia edellä mainittujen tavoitteiden saavuttamiseksi. Ennemmin kyse on siitä, että jokaisen yrityksen tulisi ensin määritellä missionsa ja sen jälkeen muodolliset tavoitteet, joiden avulla se saavutetaan. Lisäksi tähän yhteyteen tulisi luoda mittaristo, jolla edistymistä mitataan. (Moeller 2011, 65.)

Sisäisen toimintaympäristön kahden pääasiallisen elementin, riskienhallintafilosofian ja riskinottohalukkuuden, avulla tavoitteiden asettaminen helpottuu. Yrityksen tulee määritellä riskistrategia ja riskienhallinnan tavoitteet. Niiden asettamissa rajoissa tulee mitata riskinottohalukkuus ja riskinsietokyky eli minkä suuruisia riskejä ollaan valmiita ottamaan ja kantamaan sekä minkä verran asetetuista arvoista voidaan poiketa. Sitä varten yrityksellä tulee olla selkeät toimintaohjeet. (Moeller 2011, 65.)

Periaatetta on selvennetty kuviossa 6. Kun liikkeelle lähdetään yrityksen missiosta, määritellään ensin strategiset tavoitteet, jotka tukevat mission saavuttamista. Sen jälkeen luodaan strategia tavoitteiden saavuttamiseksi ja määritellään siihen liittyvät tavoitteet. Lopuksi määritetään riskinottohalukkuus strategian viimeistelyksi. Tavoitteille myös muokataan tarkoituksenmukaiset mittarit. Jotta riskejä kyetään kaikissa vaiheissa asianmukaisesti hallitsemaan ja kontrolloimaan, on oleellista myös tunnistaa ja määritellä yrityksen riskinsietokyky. (Moeller 2011, 65.)



Kuvio 6. COSO ERM riskitavoitteiden asettamisen komponentit (Moeller 2011, 64).

Tavoitteiden asettaminen on edellytys COSO ERM -mallin seuraaville osa-alueille eli riskien tunnistamiselle, arvioinnille ja niihin vastaamiselle, joista muodostuu riskienhallintaprosessin ydin. Loput osatekijät muodostavat riskienhallintaprosessin kontekstin ja taustan, jossa riskienhallintaprosessi toimii.

Riskien tunnistaminen tai riskien lähteiden tunnistaminen (inventointi) jää usein yrityksen muiden jatkuvan tarkkailun alla olevien asioiden, kuten kulujen tai laadun, jalkoihin, sillä se on osittain tulevaisuuteen suuntautuvaa haastavaa suunnittelua. Siitä huolimatta yrityksen tulee määritellä, mitkä se katsoo olevan selkeästi riskejä aiheuttavia tapahtumia ja löytää mittarit, joilla se pystyy ennustamaan riskien ilmenemistä. (Moeller 2011, 67 - 68.)

Riskien inventointi on keskeisten elementtien tunnistamista yrityksen liiketoiminnasta. Kun käännetään tilanne päinvastaiseksi, on käsillä liiketoimintaa uhkaavat potentiaaliset riskit. (Erola & Louto 2000, 129.) Riskien tunnistaminen on kaiken toiminnan alkupiste, sillä tunnistamattomia riskejä ei voi hallita (Flink ym. 2007, 131). Tässä vaiheessa inventoidaan riskit, pyritään tunnistamaan kriittiset prosessit sekä luokittelemaan ne Triage-periaatteen mukaisesti ja viedään tulokset mukaan päätöksentekoprosessiin.

Prosessi myös rajataan asianmukaisesti. (Erola & Louto 2000, 97, 135.) Finanssivalvonnan standardin 4.4b mukaan yrityksen tulee tunnistaa tuotteisiin, toimintoihin, prosesseihin ja järjestelmiin liittyvät operatiiviset riskit. Tämä luo perustan niiden valvonnalle ja niitä koskevien kontrollien suunnittelulle. (Finanssivalvonnan standardi 4.4.b 2004, 14.)

Riskien tunnistamiseen on olemassa erilaisia työkaluja. *Tapahtumien inventointi* tarkoittaa menneiden tapahtumien analysointia ja niistä oppimista. *Työryhmätyöskentely* tuo yhteen eri toimintojen osaajia. Usein tämän tyyppinen työskentely todetaan kuitenkin aikaa vieväksi. *Haastattelut, kyselyt ja tutkimukset* voivat tuottaa yllättävistäkin lähteistä kumpuavaa käyttökelpoista informaatiota. *Prosessikaavioiden analysointi* voi auttaa potentiaalisten riskilähteiden hahmottamisessa. *Tappioihin johtaneiden tapahtumien seuranta* edesauttaa virheistä oppimista. Kaikki nämä voivat tuottaa yritykselle käyttökelpoista dataa, joka edesauttaa riskeiltä suojautumista, mahdollisuuksien tunnistamista tai molempia. (Moeller 2011, 69 - 70.)

Riskien tunnistamismenetelmiä voidaan jakaa kahteen eri kategoriaan: vaarojen tunnistamismenetelmiin sekä toteutuneiden ja potentiaalisten onnettomuuksien mallintamismenetelmiin. Ensin mainitut ovat rajattujen kohteiden yksityiskohtaista tutkimista varten. Niihin kuuluvat toimintovirheanalyysi (action error analysis tai TVA) sekä potentiaalisten ongelmien analyysi (potential problems analysis tai POA). Jälkimmäiset ovat tapahtumien kulkuun keskittyviä, riskien todennäköisyyksien arviointiin tarkoitettuja menetelmiä. Näitä ovat vikapuuanalyysi (fault tree analysis), tapahtumapuuanalyysi (event tree analysis) ja syy-seurauskaavio (cause consequence diagram tai SSK). (Flink ym. 2007, 139 - 144.)

Toimintovirheanalyysi on menetelmä, jolla tunnistetaan työtehtävän eri työnosiin eli toimintoihin liittyviä ihmisen toiminnan virhemahdollisuuksia ja näiden aiheuttamia riskitilanteita. Se soveltuu parhaiten sellaisten työtehtävien tarkasteluun, jotka voidaan määritellä selvinä toimintosarjoina ja joita tehdään toistuvasti. Toimintovirheanalyysin tavoitteena ei ole virheen tekijän tai syyllisen etsiminen, vaan ihmiselle luonteenomaisten virhesuoritusmahdollisuuksien ja niiden vaikutusten tunnistaminen. Analyysi aloitetaan jakamalla tarkasteltava työtehtävä työn osiin eli työvaiheisiin. Jokainen työvaihe analysoidaan ja arvioidaan siihen mahdollisesti liittyviä toimintovirheitä. Tunnistetuille

vaaratilanteille arvioidaan riski. Tarvittaessa kehitetään parannustoimenpide-ehdotuksia. (Toimintovirheanalyysi.)

Potentiaalisten ongelmien analyysi on menetelmä, jonka avulla voidaan nopeasti tutkia järjestelmiin liittyviä riskejä. Siinä lähdetään liikkeelle toiminnan häiriöiden ja riskien tunnistamisesta aivoriihi-tyyppisellä työskentelyllä, jonka jälkeen tunnistetut tekijät arvioidaan. Sen jälkeen kehitetään toimenpide-ehdotuksia näiden varalle sekä raportoidaan analyysi. (Potentiaalisten ongelmien analyysi.)

Vikapuuanalyysin tavoitteena on löytää valittuihin järjestelmävikoihin vaikuttavat viat ja vikayhdistelmät mukaan lukien ihmisen toimintovirheet. Periaatteena on, että järjestelmäviasta lähtien etsitään sen toteutumisen mahdollistavia tekijöitä. Tapahtumapuu-analyysin tavoitteena on löytää valittuihin alkutapahtumiin liittyvät onnettomuusmekanismit siten, että määritellystä alkutapahtumasta lähtien etsitään graafisen puun avulla erilaisiin seurauksiin johtavia tapahtumaketjuja. Näitä kahta puumenetelmää soveltaen syy-seurauskaavioilla etsitään kriittisen alkutapahtuman syitä ja niistä aiheutuvia seurauksia. Lopullisena tavoitteena on löytää valittujen kriittisten tapahtumien mahdolliset seuraukset. (Menetelmät.)

Riskien arviointi (evaluointi) on COSO ERM -mallin ydin. Siinä yritys arvioi potentiaalisten riskitapahtumien vaikutusten laajuutta yrityksen tavoitteiden saavuttamiseen. Olennaisiksi luokitellut riskit tulee arvioida kattavasti. Tarkastelussa on kaksi ulottuvuutta: riskin toteutumistodennäköisyys sekä sen potentiaalinen vaikutus. Ensin mainittua arvioidaan usein sanallisesti asteikolla korkea-keskimääräinen-matala. Potentiaalista vaikutusta voidaan mitata rahassa tai sanallisella asteikolla (vakava-keskimääräinen-matala). (Moeller 2011, 71.)

Riskianalyysi voidaan määritellä suppeasti tai laajasti. Suppean määritelmän mukaan se on teknispainotteinen tarkastelutapa, jossa systemaattisen prosessin avulla tunnistetaan ja arvioidaan yrityksen vahinkotapahtumien todennäköisyydet ja seuraukset. Laajemmin tarkastellen riskianalyysi käsittää riskin määrittämiseen, arviointiin, kokemiseen ja hallintaan liittyviä asioita. (Suominen 2003, 9 - 10.) Yhtä kaikki sen tarkoituksena on säännöllisesti tunnistaa valitun kohteen riskit ja arvioida vahinkotapahtuman todennä-

köisyydet sekä odotettavissa olevat vahingot. Myös arvioitujen riskien hallintatoimenpiteisiin otetaan yleensä kantaa. (Flink ym. 2007, 136.)

Riskien arvioinnissa tarkoituksena on evaluoida kaikki tunnistetut riskit ja jaotella ne toteutumistodennäköisyyksien ja vaikutuksien perusteella. Oleellista on tunnistaa todennäköisimmät riskit, joiden vaikutukset ovat merkittävimmät. Tärkeää on myös, että riskejä on arvioimassa useampi henkilö, jotta näkökulma on riittävän laaja ja että relevantit riskien väliset yhteydet löydetään. Kokonaisuutena prosessi eroaa perinteisestä riskienhallinnasta siten, että COSO ERM -mallissa korostuu yrityksen riskienhallinnan kokonaisvaltaisuus. Siinä pyritään kattamaan kaikkien yksiköiden strategiset huolenaiheet, jotta riskit saadaan tunnistettua johdonmukaisesti ja perusteellisesti. (Moeller 2011, 74.)

Finanssivalvonnan ehdottamia sovellettavia riskienarviointimenetelmiä ovat määrämuotoiset itsearviointilomakkeistot, vahinkotilastointi sekä itselle tai muille sattuneiden vahinkojen läpikäynti. Kun tarkastellaan muille osapuolille sattuneita vahinkoja vertaamalla niitä yrityksen omaan toimintaan, on mahdollista selvittää, olisiko jossain yrityksen omassa yksikössä voinut tapahtua vastaavaa, mitä siitä olisi voinut aiheutua sekä miten vahinkoja voitaisiin estää. (Finanssivalvonnan standardi 4.4.b 2004, 14 - 15.)

Riskeistä aiheutuvia tappioita voidaan vähentää pienentämällä riskin toteutumisen todennäköisyyttä sekä pienentämällä yrityksen haavoittuvuutta riskin toteutuessa. Riskien arvioinnissa on toiminnoittain otettava huomioon riskien toteutumisen todennäköisyys ja vaikutukset vahingon sattuessa. (Finanssivalvonnan standardi 4.4.b 2004, 14.)

Riskeihin vastaaminen tarkoittaa strategisia päätöksiä sen suhteen, miten edellisissä vaiheissa kartoitettuihin riskeihin halutaan varautua ja missä laajuudessa. Prosessi on johdon vastuulla. Sen tulee laatia suojautumistapa jokaiselle tunnistetulle riskille yrityksen riskinsietokyky huomioiden. Prosessissa tulee arvioida kulujen sekä tuottojen suhdetta ja peilata sitä potentiaalisiin suojautumiskeinoihin. Riskeihin voidaan vastata pääpiirteissään neljällä tavalla, jotka esitellään seuraavissa kappaleissa. (Moeller 2011, 74 - 75; Erola & Louto 2000, 137.)

Välttäminen tai *poistaminen tarkoittaa* hankkiutumista eroon riskikkäistä kohteista tai liiketoimintayksiköistä. Ongelmana on, että yritykset eivät usein irrottaudu riskikohteista ennen kuin riski toteutuu. Jollei yrityksen riskinsietokyky ole poikkeuksellisen matala, on vaikeaa luopua kohteesta tai yksiköstä vain sillä perusteella, että tulevaisuudessa siinä saattaa piillä riski. Etenkin jos tämänhetkinen tilanne vaikuttaa hyvältä. Välttäminen on usein kallis strategia. (Moeller 2011, 74.) Samalla poistetaan myös tuoton mahdollisuus (Flink ym. 2007, 148).

Jos yrityksellä on historiassaan epäonnistumisia, joissa riskit ovat toteutuneet, voi näistä virheistä oppia. Usein toistuvat organisaatiomuutokset ja lyhyet työsuhteet tosin johtavat helposti siihen, että tämäntyyppinen arvokas tieto katoaa matkan varrelle. Tässä yhteydessä huolellisesti laadittu ja dokumentoitu riskinsietokykyraportti on hyödyllinen työkalu. (Moeller 2011, 74 - 75.)

Pienentäminen voidaan toteuttaa monella tavalla siten, että riskin todennäköisyyttä tai seurauksia pienennetään. Käytännössä tämä tarkoittaa toimintojen hajauttamista. (Moeller 2011, 75; Flink ym. 2007, 148; Finanssivalvonnan standardi 4.4.b 2004, 15.)

Jakaminen tai *siirtäminen* on peruspiirteissään vakuutuksien hankkimista riskien varalta. Tämä on yksi konkreettisimmista suojautumiskeinoista. Yrityksen tulee huolehtia siitä, että vakuutusturvan riittävyyttä ja kustannuksia arvioidaan säännöllisesti niin, että huomioon otetaan liiketoiminnan muutokset. Myös muita tapoja jakaa riskejä on olemassa. Taloudellisten riskien varalta voi suojautua. Riskiä voi jakaa yhteisyrityksen avulla tai toimintoja voi ulkoistaa. (Finanssivalvonnan standardi 4.4.b 2004, 15; Moeller 2011, 75.)

Hyväksyminen tai *pitäminen* tarkoittaa riskin ottoa ilman erityistä suojautumista eli lisätoimenpiteitä. Se on välttämisen tai poistamisen vastakohta. Tässä kohdin tulisi tutkia riskien todennäköisyyksiä ja vaikutuksia riskinkantokyvyn valossa, minkä perusteella päätös tulisi tehdä riskin hyväksymisestä tai siltä suojautumisesta. (Moeller 2011, 75.)

Tässä vaiheessa yrityksen tulee palata potentiaalisiksi katsomiinsa riskeihin ja niihin liittyvään sietokykyynsä. Tämän jälkeen tulee jokaisen tunnistetun riskin todennäköi-

syys ja vaikutus määrittää, jotta voidaan arvioida sekä riskikategoriat että kokonaisvaltainen riskeihin vastaamistapa kuten myös miten ne suhtautuvat yrityksen kokonaisvaltaiseen riskinsietoon. Yritys on tässä kohdin arvioinut jokaisen tavoitteeseensa liittyvän riskin todennäköisyyden ja peilannut niitä kaikkia samoja potentiaalisia vaikutuksia vastaan. Tämän jälkeen tulee päättää, miten kuhunkin riskiin vastataan. Prioriteettilistan kärkipäässä tulee olla riskit, joilla on suurin toteutumistodennäköisyys ja merkittävimmät vaikutukset. (Moeller 2011, 75 - 76.)

Prosessi vaatii paljon suunnittelua ja strategista pohdintaa. Yrityksen tulisi pyrkiä kartoittamaan kaikki mahdolliset riskit johdonmukaisesti ja miettiä useampi strategia millä vastata niihin. Kartoittamalla potentiaaliset riskit, niiden esiintymistodennäköisyydet ja vaikutukset huolellisella analyysillä, päästään käsiksi merkittävimpiin riskeihin. (Moeller 2011, 76 - 77.)

COSO ERM -mallissa riskejä kartoitetaan yritystasolla ja kootaan ne riskiportfolioksi. Tähän päästäkseen tulee tehdä ensin riskikartoitus. (Moeller 2011, 78.) Oleellista on määritellä toiminnan vastuuhenkilöt erityisesti sitä ajatellen, kenen vastuulla on seurata dokumentoituja ennusmerkkejä riskien mahdollisesta toteutumisesta. Riskin aktualisoituessa tulee olla selkeä toimintaohjeistus valmiina. On tärkeää listata vahinkojen estämiseen, tiedottamiseen sekä toiminnan vakiinnuttamiseen liittyvät ohjeet. Tämän lisäksi pitää tehdä toiminnan palautumis- ja jatkuvuussuunnitelma. Tulee suunnitella, miten normaalin toiminnan taso saavutetaan ja miten olosuhteet huomioiden toiminta saadaan mahdollisimman tarkoituksenmukaiseksi vaihtoehtoisten toimintamallien avulla. (Erola & Louto 2000, 144 - 147.)

Valvontatoimenpiteet ovat menettelytapoja, joilla varmistutaan siitä, että potentiaalisiksi katsottuihin riskeihin on vastattu aiotulla tavalla. Siten tämä vaihe linkittyy tiiviisti edellisen kanssa. Valvontatoimenpiteiden tehtävänä on tuottaa kohtuullinen varmuus siitä, että yrityksen tavoitteet saavutetaan halutulla tavalla (Blumme ym. 2005, 66). Se sisältää neljä vaihetta:

1) Merkittävien riskien huolellinen kartoitus ja valvontatoimenpiteistä päättäminen näiden riskien havainnointiin tai korjaamiseen.
2) Testikäytäntöjen kehittäminen näiden valvontatoimenpiteiden toiminnan kontrollointiin.

3) Valvontatoimenpiteiden testaus sen varalta, että ne toimivat tehokkaasti ja odotetulla tavalla.
4) Tarkistuksien ja parannuksien tekeminen tarvittaessa riskien valvontaprosessin kehittämiseksi.

Valvonta käsittää kaikki toimenpiteet, jotka lisäävät asetettujen tavoitteiden ja päämäärien saavuttamisen todennäköisyyttä tai pienentävät riskejä. Se voi olla ennakoivaa ja ehkäisevää, todentavaa tai ohjaavaa. Ryhmittely perustuu siihen, kuinka ne vaikuttavat riskeihin. Ennakoiva ja ehkäisevä valvonta pyrkii estämään epätoivottuja tapahtumia ja riskejä realisoitumasta. Todentava valvonta tuo esiin ja korjaa epätoivottuja tapahtumia. Ohjaava valvonta eli kontrollointi saa aikaan tai edistää toivottuja tapahtumia eli saavat henkilöstön toimimaan halutulla tavalla. (Blumme ym. 2005, 52, 66.)

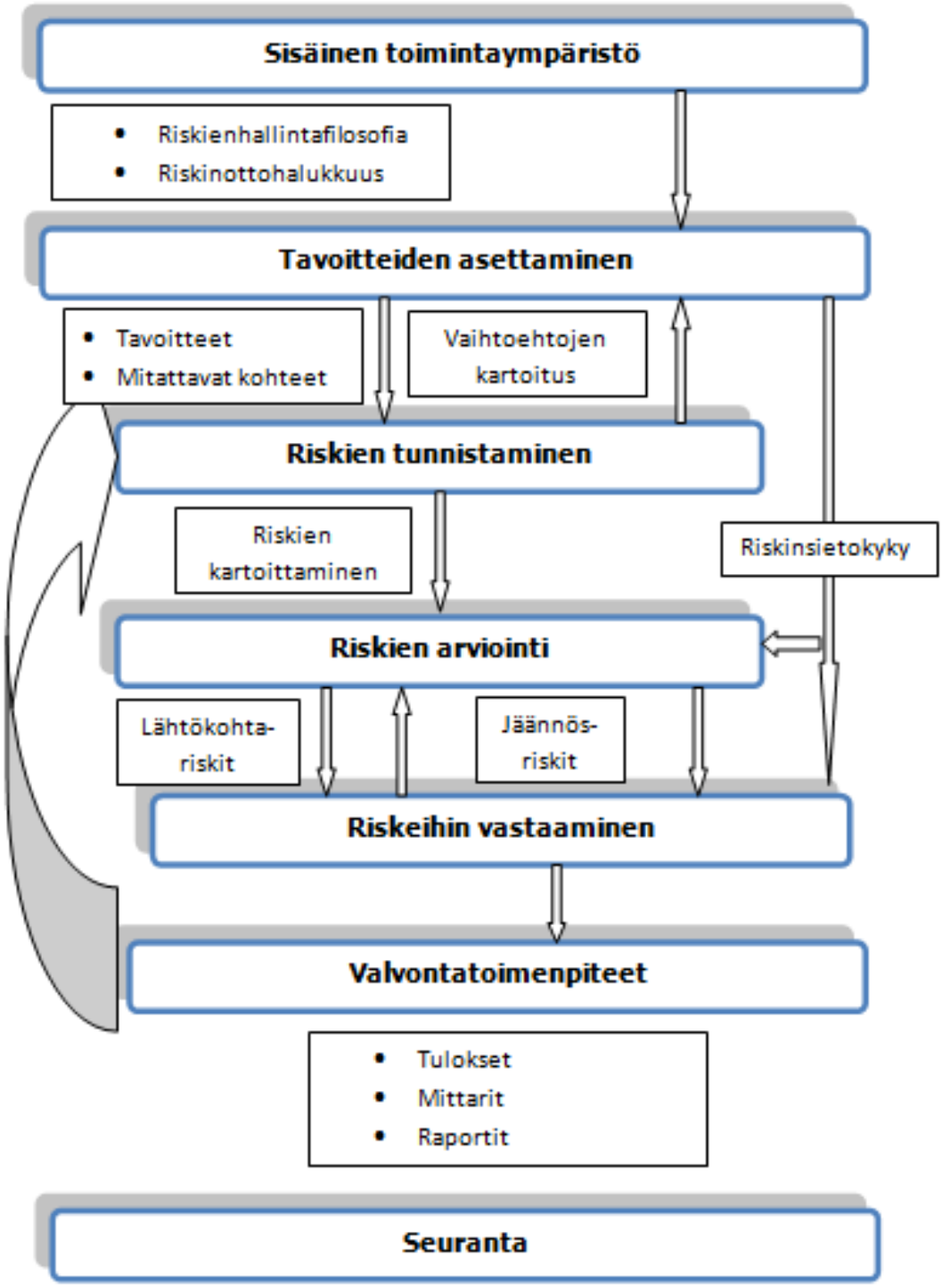
Sisäisessä valvonnassa tulee ottaa huomioon, että toimintaa suorittava taho ei ole sama kuin sitä valvova, kirjausketjut ovat katkeamattomia, valvontatoimenpiteet suoritetaan asianmukaisesti ja toimenpiteet dokumentoidaan. Itse valvontatoimenpiteitä on lukuisia. *Ylemmän johdon tarkistukset* varmistavat, että he ovat tietoisia tunnistetuista riskeistä ja miten niihin vastataan. Säännölliset tarkistukset yhdistettynä korjaustoimenpiteisiin ovat oleellisimpia valvontatoimenpiteitä. *Operatiivinen johto* on myös oleellisessa valvontaroolissa. *Tiedon prosessointi* on avainroolissa. *Konkreettiset tarkastukset* ovat oleellisia siinä tapauksessa, kun yrityksellä on paljon fyysisiä tuotannontekijöitä kuten koneita, laitteita tai tehtaita. *Suoritusmittareita* on yleensä yrityksessä jo olemassa. Näitä taloudellisia ja operatiivisia raportointityökaluja voi hyödyntää sellaisenaan tai muokattuina riskienhallinnan raportoinnissa. *Tehtävien erillään pito* on klassinen valvontatoimenpide. Sen tarkoituksena on varmistaa, että toimintaa suorittava taho ei ole sama kuin sitä valvova. Tämä on myös yksi edellä esiteltyjä sisäisen valvonnan periaatteita. (Moeller 2011, 78 - 81.)

Informaatio ja tiedonkulku ei varsinaisesti ole itsenäinen osatekijä COSO ERM -mallissa vaan ennemmin prosessi, joka linkittää muut tekijät toisiinsa. Näitä yhteyksiä ja informaatiovirtoja on havainnollistettu kuviossa 7. Esimerkinomaisesti tavoitteiden asettamisvaihe tuottaa informaatiota riskinsietokyvystä riskeihin vastaamista silmälläpitäen. Se puolestaan tarjoaa otollisia kohteita valvontatoimenpiteille kuten myös vastapalautetta riskien arviointiin. (Moeller 2011, 82.)

Vaikka periaatteessa kuvio vaikuttaa yksinkertaiselta, kokonaisuus on linkkeineen ja informaatiopolkuineen todellisuudessa usein melko monimutkainen. Näitä valvonta- ja tiedotustoimenpiteitä voidaan sisällyttää useissa yrityksissä käytössä oleviin toiminnanohjaus- eli ERP-järjestelmiin. Internet-pohjaisella sovelluksella voidaan mukaan saada vielä muita yrityksen sidosryhmiä, kuten asiakkaita, toimittajia ja yhteistyökumppaneita. (Moeller 2011, 83.)

Oleellinen merkitys on itse kommunikaatiolla. Kaikilla yrityksen sidosryhmillä tulisi olla tietämys yhteisestä riskienhallinnan kielestä ja käsitteistöstä kuten myös rooleista sekä vastuualueista. Riskienhallinnan merkitys ja tärkeys tulee saattaa koko yrityksen tietoon selkeästi ja yksiselitteisesti, jotta se palvelee yritystä optimaalisella tavalla. (Moeller 2011, 85.)

Viranomaisen ohjeistuksen mukaan yrityksen johdon tulee hyväksyä sisäisen tiedottamisen periaatteet ja määritellä tiedottamisvastuut. Toimintatavoista päätettäessä tulee huomioida liiketoiminnan laatu, laajuus ja monimuotoisuus. Johdon tulee myös varmistaa, että kaikki yrityksen henkilöt saavat tehtäviensä suorittamisessa tarvitsemansa tiedot. (Finanssivalvonnan standardi 1.3, 2007, 26.)



Kuvio 7. Informaatio- ja kommunikaatiovirrat COSO ERM -mallin komponenttien välillä (Moeller 2011, 82).

Seuranta on kokonaisvaltaisen riskienhallinnan jatkuvuuden turvaamiseksi oleellista. Koska yrityksen henkilöstö ja toimintaympäristö ovat jatkuvan muutoksen kohteena, voidaan suunnitelluilla seurantatoimenpiteillä varmistua siitä, että kaikki riskienhallinta-komponentit toimivat suunnitellusti. Viitaten kuvioon 7, vaikka seurantakomponentilla

ja muiden osa-alueiden välillä ei ole suoria informaatiovirtoja, on seuranta mukana kaikkien toimintojen tarkkailussa. (Moeller 2011, 83, 84.)

Tämän vaiheen tehtävä on varmistaa riskienhallintaprosessin jatkuvuus tarkkailun ja ylläpidon keinoin. Siinä tunnistetaan riskien havaitsemiseen liittyvät tunnusmerkit, toteutetaan varautumissuunnitelma sekä laaditaan seurantamenettely. Lisäksi varmistutaan liiketoiminnan jatkuvuudesta. Yleisin syy suunnitelmien vanhenemiseen on, ettei riskienhallintaa ole mielletty jatkuvaksi prosessiksi. Tämä kyetään estämään prosessiin liitetyllä päivitysvaiheella, jossa suunnitelmia päivitetään muuttuneiden tietojen osalta. (Erola & Louto 2000, 98, 152.)

Niin kuin useilla muillakin osa-alueilla, myös seurannan osalta kokonaisvastuu tulisi olla johdolla. Rutiininomaisia valvontavastuita tulisi laajentaa niin, että ne kattavat myös riskienhallinnan osatekijät. Toteutettavia toimenpiteitä ovat jatkuvan ja toimivan raportointijärjestelmän kehittäminen etenkin riskien hälytysrajoja ajatellen, riskeihin liittyvien havaintojen ja suositusten säännöllinen statustarkastus sekä riskeihin liittyvän ulkopuolisen informaation säännöllinen seuraaminen. (Moeller 2011, 85.)

Seuranta voidaan toteuttaa sisäisen valvonnan, ulkopuolisen konsultin tai koulutetun henkilöstön voimin. Heillä kaikilla on käytössään samat seurantatyökalut. *Prosessikuvaukset* tulisi olla saatavilla kaikista yrityksen prosesseista. Näitä kaavioita voidaan hyödyntää myös yksittäisten prosessien riskienhallinnan tilan seurannassa. Tuolloin pitäisi varmistua siitä, että prosessikuvaus on ajan tasalla. Jos tässä kohdin tulee esille uusia riskejä tai vanhoja todetaan poistuneen, tarvittavat päivitykset tulee toteuttaa. *Riski- ja kontrollimateriaalin tarkastelu* säännöllisin väliajoin auttaa erottamaan hyödyllisen materiaalin epäolennaisesta, sillä riskienhallintaprosessin sivutuotteena tulee usein paljon ylimääräisiä muistioita, ehdotuksia ja lomakkeita. *Benchmarkkaus* on hyödyllinen, mutta melko vähän käytetty tapa seurata yrityksen riskienhallinnan tilaa. Usein tämä johtuu siitä, että yritykset eivät ole halukkaita jakamaan tietojaan. *Kyselyt* ovat tehokkaita tiedon keräämisessä isoilta tai laajalle levinneiltä joukoilta. *Pienryhmäsessiot* voivat tuottaa arvokasta tietoa yrityksen riskienhallinnan tilasta kun kerätään yhteen eri yksiköissä tai tehtävissä työskenteleviä henkilöitä ja annetaan heille mahdollisuus kertoa näkemyksiään. (Moeller 2011, 85 - 86.)

Seurantaprosessin tavoitteena on arvioida, miten kokonaisvaltainen riskienhallinta toimii yrityksessä, ei siis vain etsiä virheitä ja puutteita. Tulokset tulee raportoida säännöllisesti vastuuhenkilöille, jotta prosesseihin voidaan tehdä tarvittavia muutoksia ja parannuksia. Kuitenkin siitä huolimatta, että riskienhallinta on pyritty tekemään aukottomaksi, inhimillisten erehdysten tai odottamattomien tapahtumien vuoksi yllätyksiä voi tulla esiin. (Moeller 2011, 86 - 87.)

Finanssivalvonnan määräysten perusteella yrityksen tulee säännöllisesti seurata ja arvioida havaitsemiensa operatiivisten riskien luonnetta, riskien toteutumisen todennäköisyyksiä ja tappion määrää riskien mahdollisesti toteutuessa. Lisäksi on luotava ennakoivat menettelyt ja mittarit operatiivisten riskien havaitsemiseksi. On hyvä myös arvioida operatiivisten riskien kasvua ennakoivia tekijöitä. Näitä ovat esimerkiksi merkittävä muutos liiketoiminnan laajuudessa, uusien tuotteiden tai palveluiden käyttöönotto, työntekijöiden suuri vaihtuvuus, avoimien paikkojen vaikea tai hidas täyttäminen, asiakasvalitukset sekä lisääntyneet toiminta tai palvelukatkokset. Laskentajärjestelmistä ja muista tietojärjestelmistä saatavaa informaatiota on syytä hyödyntää, kun arvioidaan operatiivisten riskien kasvua ennakoivia tekijöitä. (Finanssivalvonnan standardi 4.4.b 2004, 16.)

Sisäisen raportoinnin tulee toimia niin, että saatavilla on taloudellista informaatiota, laadullisia analyysejä, arvioita sisäisten ja ulkoisten ohjeiden noudattamisesta sekä tietoa päätöksenteon kannalta merkittävistä ulkoisista tapahtumista ja toimintaympäristön muutoksista. Raporteista tulee ilmetä todetut ongelma-alueet, niiden perusteella tulee voida arvioida muutoksia operatiivisten riskien määrässä sekä niiden tulee tukea ennakoivaa riskienhallintaa. Säännöllisesti on arvioitava käytettyjen menetelmien ja raportointijärjestelmien ajanmukaisuutta, tarkkuutta sekä tarkoituksenmukaisuutta, raportoinnin sisällön laajuutta ja yksityiskohtaisuutta sekä raporttien jakelua ja raportointitiheyttä. (Finanssivalvonnan standardi 4.4.b 2004, 16.)

Finanssivalvonta suosittelee, että operatiivisten riskien aiheuttamia tappioita seurataan siten, että kirjataan kuvaus tapahtumasta, tapahtumaan johtaneet syyt, arvio suorista ja epäsuorista kustannuksista, mahdolliset vakuutuskorvaukset sekä toimenpiteet vahingon ennaltaehkäisemiseksi jatkossa. Lisäksi on hyvä raportoida, mihin toimenpiteisiin on vahingon vuoksi ryhdytty sekä kuka on vastuussa korjaavista toimista ja mikä

on niiden aikataulu. On syytä määritellä rahamääräinen taso, jota suuremmat tapahtumat raportoidaan. Pienistäkin vahingoista on raportoitava, jos niillä on periaatteellista merkitystä. (Finanssivalvonnan standardi 4.4.b 2004, 17.)

5.4 Vaihtoehtoiset teoriat

On olemassa myös muita riskienhallinnan viitekehyksiä tai standardeja, joiden tarkoitus on tukea organisaatioita riskienhallinnan kehittämisessä sekä riskeihin liittyvissä päätöksissä. Ne ovat yleensä riskienhallinnan asiantuntijoiden, organisaatioita valvovien ja ohjaavien elinten tai erilaisten yhdistysten ja komiteoiden laatimia. Viitekehykset ja standardit noudattavat useimmiten samaa perusrunkoa lähtien riskienhallinnan tavoitteista ja päätyen jatkuvaan seurantaan. Tunnettuja riskienhallintamalleja ovat edellä esitellyn COSO ERM -mallin lisäksi esimerkiksi Federation of European Risk Management Associations (FERMA) -yhdistyksen Risk Management Standard, Joint Standards Australia/Standards New Zealand Committeen Risk Management Standard, James DeLoachin Enterprise-Wide Risk Management sekä International Organization for Standardizationin ISO/IEC-standardit. (Juvonen ym. 2005, 31.)

FERMA on 21 maan kansallisen riskienhallintayhdistyksen muodostama eurooppalainen riskienhallintajärjestö, joka perustettiin vuonna 1974. Siihen on liittynyt myös Suomen Riskienhallintayhdistys ry. (What is FERMA? 2011.) FERMA:n vuonna 2002 ensimmäistä kertaa julkaisema A Risk Management Standard on kokonaisvaltainen kuvaus riskienhallinnan roolista organisaatiossa sekä itse riskienhallintaprosessista. (A Risk Management Standard 2003.)

Australia (AS) ja Uusi-Seelanti (NZS) ovat aktiivisia riskienhallinnan kehittäjämaita, jotka ovat yhdessä julkaisseet lukuisia standardeja ja ohjeita riskienhallintaan liittyen. AS/NZS 4360:2004 on Joint Standards Australia/Standards New Zealand Committeen laatima kokonaisvaltaisen riskienhallinnan standardi, josta on johdettu myös tuorein AS/NZS-riskienhallintastandardi AS/NZS ISO 31000:2009. Nämä standardit toimivat riskienhallinnan yleisoppaina, joita voidaan soveltaa kaiken tyyppisten toimintojen tai yritysten riskien kartoittamiseen sekä riskienhallinnan toteuttamiseen ja ylläpitämiseen. (AS/NZS 4360:2004 Risk management 2004.)

James W. DeLoachin Enterprise-Wide Risk Management on riskienhallinnan yleisteos, jossa esitellään Business Risk Model -malli. Sen DeLoach kehitti Arthur Andersen -tilintarkastusyhteisölle. Malli ja teos käsittelevät erityisesti liiketoimintariskien hallintaa ja painottaa riskeihin liittyvien hyötyjen hallintaa osana yrityksen riskienhallintastrategiaa. (Wesanko 2010, 9.)

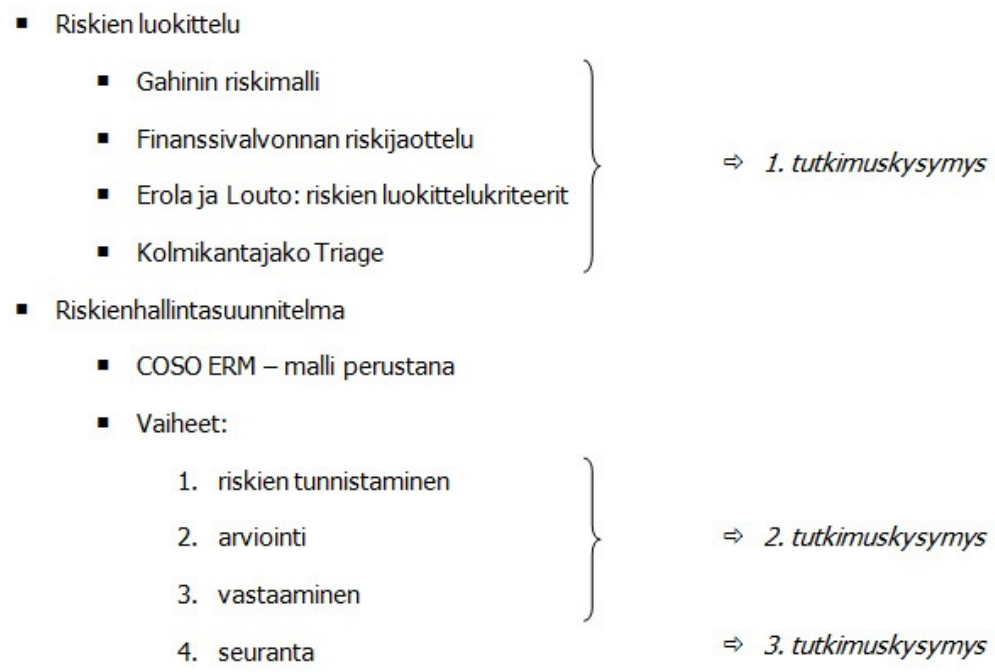
Kansainvälinen standardisoimisjärjestö ISO on maailman suurin standardien kehittäjä ja julkaisija. Se on 163 maan standardisoimisjärjestöjen muodostama verkosto, joka tuottaa suositusluonteisia standardeja sekä julkisen että yksityisen sektorin käyttöön. (About ISO 2011.) Riskienhallintaan liittyen on kehitetty useita standardeja. ISO 31000:2009 ja IEC/ISO 31010:2009 ovat riskienhallinnan yleisstandardeja, jotka tarjoavat työkaluja riskien systemaattiseen arviointiin. (ISO/IEC 31010:2009 2011.) Tietoturva-asioihin on keskitytty standardeissa IEC/ISO 27005 (tietoturvariskien hallinta) ja IEC/ISO 27001 (tietoturvallisuuden hallintajärjestelmä).

Kaikkia edellä esiteltyjä malleja voisi käyttää sovellettuna tämän tutkimuksen kohteeseen. COSO ERM -riskienhallintamallia päädyttiin käyttämään sen loogisuuden ja käytännönläheisyyden vuoksi. Vaikka malli on lähtökohtaisesti suunniteltu tutkimuskohdetta selkeästi suurempien ja toiminnaltaan laajempien yritysten tarpeisiin, katsottiin sen olevan yksinkertaistetussa muodossa käyttökelpoinen Rahastoyhtiön operatiivisen riskienhallintasuunnitelman viitekehykseksi. COSO ERM -mallin teoriassa on kattavasti vaiheistettu riskienhallinnan prosessin kulku ja ohjeistettu periaatteiden vieminen käytännön tasolle.

5.5 Sovellettava teoria

Seuraavassa luvussa esiteltävä riskienhallintasuunnitelma rakentuu Gahinin riskimallin ja Finanssivalvonnan standardissa 4.4.b Operatiivisten riskien hallinta esitellyn riskijaottelun pohjalle. Tarkastelun kohteeksi otetaan rahastoyhtiön operatiiviset riskit, joita eritellään Erolan ja Loudon (2002) esittelemien riskien kriteerien perusteella sekä kolmikantajako Triagen jaotteluperiaatteiden mukaan. Tämän tarkoituksena on vastata ensimmäiseen tutkimuskysymykseeni eli mitkä ovat rahastoyhtiölle tyypilliset hallinnon operatiiviset riskit, joilta halutaan suojautua.

Toiseen tutkimuskysymykseen suojautumisen käytännön hoidosta pyrin vastaamaan luotavalla riskienhallintasuunnitelmalla. Sen tarkoitus on pääpiirteissään rakentua COSO ERM -mallin kahdeksan osatekijän pohjalle. Pääpiirteissään prosessin vaiheet ovat riskien tunnistaminen, arviointi, riskeihin vastaaminen sekä seurantavaihe. Viimeiseen vaiheeseen yhdistän myös kolmannen tutkimuskysymykseni eli miten riskienhallintatoimintoa hyödynnetään ja kehitetään edelleen. Teorioiden ja tutkimuskysymysten välistä suhdetta on havainnollistettu kuviossa 8.



Kuvio 8. Teorioiden ja tutkimuskysymyksien suhde

6 RAHASTOYHTIÖN RISKIENHALLINTAPROSESSI

Tässä pääluvussa kuvataan kehittämistehtävän mukainen Rahastoyhtiön riskienhallintaprosessi, joka pohjautuu teoriatasolla alaluvussa 5.3 esiteltyyn COSO ERM -malliin. Prosessi koostuu teorian kuvaamista kahdeksasta vaiheesta, joita peilataan Finanssivalvonnan antamiin määräyksiin ja suosituksiin.

6.1 Sisäinen toimintaympäristö

Tästä kappaleesta on salattu kohdeyrityksen toimintaympäristön kuvaus.

6.1.1 Riskienhallintafilosofia ja riskinottohalukkuus

Tästä kappaleesta on salattu kohdeyrityksen riskienhallintafilosofian ja riskinottohalukkuuden kuvaus.

6.1.2 Rehellisyys ja eettiset arvot

Tästä kappaleesta on salattu kohdeyrityksen arvojen kuvaus.

6.1.3 Organisaation rakenne sekä valtuudet ja velvollisuudet

Tästä kappaleesta on salattu kohdeyrityksen organisaatiokuvaus.

6.2 Tavoitteiden asettaminen

Tästä kappaleesta on salattu kohdeyrityksen liiketoimintatavoitteiden kuvaus.

6.3 Riskien tunnistaminen

Yrityksen keskeiset toiminnot ovat salkunhoito, myynti ja hallinto. Näistä viimeksi mainittu jakaantuu viiteen eri osa-alueeseen (rahastojen arvonlaskenta, asiakasrekisteri, asiakaspalvelu, taloushallinto sekä seuranta ja raportointi) joihin tässä kehittämistehtävässä keskitytään. Näihin liittyen arvonlaskennan sekä osuudenomistajarekisterin tietojen oikeellisuus ovat toiminnan kannalta kriittisimpiä asioita ja niihin liittyvien riskien hallinta on siten oleellisinta.

Yrityksen operatiiviset riskit on inventoitu siten, että Finanssivalvonnan operatiivisten riskien jaottelun perusteella jokainen osa-alue on kartoitettu rahastojen arvonlaskennan, asiakasrekisterin, asiakaspalvelun, taloushallinnon sekä seurannan ja raportoinnin osalta. Näin on laadittu laaja riskikartta, jossa on listattu potentiaaliset riskitekijät, mahdollinen käytännön esimerkki, riskin toteutumiseen johtavat syyt, seuraukset, ennaltaehkäisyvaihtoehdot sekä keinot varmistaa yrityksen toiminnan jatkuvuus riskitilanteessa. Tämän jälkeen riskeistä on analysoitu muodostumislokaatio, tietoisuusaste, vaikutustapa ja vakuutettavuus. Sitten riskit on luokiteltu Triage-periaatteiden mukaan

riskin toteutumistodennäköisyyden sekä vaikutuksen perusteella, molemmat kolmiportaisella asteikolla. Lopuksi jokaiselle riskille on määritelty ensisijaisesti määrällinen mittari ja selostettu mittarin käyttötapa sekä tavoitearvo. Kokonaiskuvaa ajatellen riskeistä on myös poimittu oleellisimmat.

Kaiken kaikkiaan operatiivisia riskejä saatiin tunnistettua 76 kappaletta. Niiden tunnistamiseksi käytettiin riskianalyysin menetelmistä vaarojen tunnistusmenetelmien osalta potentiaalisten ongelmien analyysiä karkean tason ongelmakohtien kartoittamiseen sekä toimintovirheanalyysiä. Tarkoituksena oli löytää ihmisten tekemistä toimintovirheistä aiheutuvia uhkia siten, että tietty työtehtävä tai prosessi jaettiin yksityiskohtaisiin toimintoihin ja analysoitiin näiden toimintojen merkittävimpiä virhemahdollisuuksia sekä niistä aiheutuvia riskitekijöitä. Toteutuneiden ja potentiaalisten onnettomuuksien mallintamismenetelmistä käyttöön otettiin yhdistettynä vika- ja tapahtumapuuanalyysit siten, että etsittiin syy-seuraussuhteita. Molempia puumenetelmiä käyttäen pyrittiin löytämään kriittisten alkutapahtumien syitä ja niistä aiheutuvia seurauksia.

Riskien tunnistamiseen käytettiin useita työkaluja. Kaikki yrityksen työntekijät osallistettiin prosessiin henkilökohtaisilla haastatteluilla heidän omaan työhönsä liittyvistä riskeistä. Lisäksi asioista keskusteltiin aivoriihi-tyyppisesti. Toteutuneita ja dokumentoituja riskejä käytiin erityisen tarkasti läpi siten, että pureuduttiin yksityiskohtaisesti tapahtumien syihin, lähtökohtatilanteisiin sekä vaikuttaneisiin tekijöihin. Lisäksi toiminnoista laadittiin prosessikaavioita, joita analysoitiin riskinäkökulmasta.

Tarkasteltuja operatiivisten riskien hallinnan osa-alueita ovat prosessit, oikeudelliset riskit, henkilöstö, jatkuvuussuunnittelu, varautuminen poikkeusoloihin, tietojärjestelmät sekä tietoturvallisuus. Seuraavassa esitellään jokainen osa-alue ja sen osalta tunnistetut riskit eroteltuna jokainen omalla järjestysnumerollaan, mahdollinen käytännön esimerkki, riskin toteutumiseen johtavat todennäköisimmät syyt, sen toteutumisen seuraukset, ennaltaehkäisevät toimenpiteet sekä yrityksen toiminnan jatkuvuuden varmistaminen riskin toteuduttua. Lopuksi kartoitetaan myös riskien muodostumislokaatiot, tietoisuusasteet sekä vaikutustavat yhteenvedonomaisesti.

Alan vahvan sääntelyn vuoksi Finanssivalvonnalla on tarpeellisiksi katsomissaan tilanteissa oikeus määrätä valvottavalleen hallinnollinen seuraamus eli sanktio. Näitä ovat

uhkasakko, rikemaksu, julkinen huomautus, julkinen varoitus ja seuraamusmaksu. Lisäksi valvova viranomainen voi myös tehdä tutkintapyynnön poliisille ja rajoittaa johdon toimintaa määräaikaisesti sekä rajoittaa toimiluvan mukaista toimintaa. (Hallinnolliset seuraamukset 2011.)

6.3.1 Prosessit

Prosessilla tarkoitetaan palvelun tai suoritteen tuottamiseksi muodostettua toimintojen ja resurssien kokonaisuutta. Prosessien hallintaan liittyvät asiakastyytyväisyys, tehokkuus, kannattavuus ja laatunäkökohdat. Prosessien analysointi ja eri vaiheisiin liittyvien operatiivisten riskien arviointi auttavat operatiivisten riskien tunnistamisessa ja rajoittamisessa. (Finanssivalvonnan standardi 4.4.b 2004, 19.)

Tarkasteltavista osa-alueista prosessit ovat selkeimmin mukana päivittäisessä operatiivisessa työssä. Niihin sisältyy eniten työvaiheita ja sitä myöten myös potentiaalisten riskien toteutumismahdollisuuksia on eniten. Prosessien osalta tunnistettiin 20 riskiä, jotka jakaantuivat seuraavasti:

Rahastojen arvonlaskenta

1 Arvonlaskennassa on virhe.
Käytännön esimerkkejä arvonlaskennan virheestä voivat olla osakkeiden arvojen poimiminen väärin kohdemaiden pörssien internet-sivuilta (syynä virheellinen lähtödata), tilitapahtumien päivittämättä jättäminen (syynä maksuliikenneohjelman virhe tai huolimattomuus) tai inhimillinen näppäilyvirhe tietojen syöttövaiheessa (syynä huolimattomuus tai tarkistuksen puuttuminen). Kaikkien seurauksena on virheellinen rahastoosuuden arvo, mistä voi seurata korvausvastuu, mikäli virhe on suuruudeltaan olennainen ja ajoitukseltaan merkittävä. Rahastojen arvonlaskennan virheen olennaisuus määräytyy rahaston volatiliteetin mukaan. Ajoituksen puolesta kriittisiä hetkiä ovat rahastojen merkintä- ja lunastuspäivät, joiden arvojen perusteella toteutetaan rahastomerkinnät ja -lunastukset.

Ennaltaehkäiseviä toimenpiteitä ovat datan lähteistä ja prosessien toimivuudesta varmistuminen, tarkistuslistojen laatiminen sekä seuraaminen, arvonlaskentaan varattava

riittävä aika ja tarkkaavaisuus sekä arvonlaskentojen ristiintarkistus siten, että kriittisinä ajankohtina vähintään kaksi henkilöä suorittaa toisistaan erillisinä arvonlaskennan alusta loppuun. Mikäli virhe arvonlaskennassa toteutuu, tulee virhe korjata välittömästi ja ottaa yhteyttä tarvittaessa vahinkoa kärsineisiin asiakkaisiin sekä korvata virheen johdosta aiheutunut rahallinen menetys. Lisäksi virheestä tulee raportoida hallinnosta vastaavalle, joka vie asian hallituksen tietoon. Jatkuvuutta ajatellen myös virheen aiheuttaneet tekijät tulee kartoittaa ja tehdä tältä osin tarkennuksia arvonlaskentaprosessiin.

2 Sijoitusrajat ylittyvät/sääntörikkomus.

Rahastojen säännöissä eritellään sijoituskohteiden suhteellisen osuuksien maksimiosuudet. Markkinatilanteiden vaihdellessa ja suurista arvopaperikohtaisista painotuksista johtuen Finanssivalvonta on ohjeistanut, että osakkeiden suhteellisten osuuksien ylittäessä sääntöjen sallimat rajat tilanne on korjattava viipymättä osuudenomistajan etua ajatellen. Käytännössä näitä tilanteita ilmenee silloin kun yksittäisten osakkeiden painoarvot kasvavat rahaston arvopaperisalkussa liian suuriksi. Tämä johtuu yllättävien markkinatilanteiden ohella salkunhoidon virheestä, tietoisesta riskinotosta tai siitä, että informaatio salkun ajankohtaisesti sijoitustilanteesta ei tavoita salkunhoitajaa. Mikäli virhettä ei annetussa kahdessa viikossa korjata, voi seurauksena olla Finanssivalvonnan hallinnollinen seuraamus. Tilanteen jatkuminen voi myös heijastua rahasto-osuuden arvoon negatiivisesti. Ennaltaehkäisynä on salkun sijoitustilanteen raportointi salkunhoidolle päivittäin ja siinä yhteydessä osuuksien ylityksestä informointi. Jatkuvuus varmistetaan siten, että virhe korjataan mahdollisimman pian sen huomaamisesta.

3 Puutteellinen dokumentointi.

Arvonlaskennan oikeellisuutta ajatellen käytetyn materiaalin dokumentointi on oleellista. Mikäli esim. päivittäisiä tiliotteita tai valuuttakursseja ei tulosteta yleensä unohduksesta johtuen, on riski arvonlaskennan virheelle suuri. Tätä ehkäistäkseen arvonlaskentaan tulee varata riittävästi aikaa ja se tulee tehdä tarkkaavaisesti kaikki vaiheet huolellisesti läpikäyden. Myös arvonlaskentojen ristiintarkistus tulee suorittaa siten, että kriittisinä ajankohtina vähintään kaksi henkilöä tekee toisistaan erillisinä arvonlaskennan alusta loppuun. Mikäli dokumentoinnissa ilmenee puutteita, tulee mahdollinen aiheutunut virhe korjata ja prosessiin tehdä tarkennuksia vastaavan tilanteen toistumisen ehkäisemiseksi.

4 Arvopaperikauppojen selvityksessä on virhe.

Tyypillisimmillään arvopaperikauppojen ohjeistuksessa tulee virheitä huolimattomuudesta näppäilyvirheen tai myöhästymisen muodossa. Seurauksena voi vakavimmillaan olla rahallinen sanktio mikäli kaupat eivät selviä (vastapuoli saa varoja tai osakkeita) ajallaan. Ennaltaehkäisynä arvopaperikaupat käydään läpi kahteen kertaan kahden eri henkilön toimesta. Myös arvopaperikaupoissa pääosin käytettävät välittäjät seuraavat kaupan ohjeistuksen etenemistä ja lähettävät muistutusviestin pikaisesti jos ohjeissa on virheitä tai viivettä. Mikäli arvopaperikaupan selvityksessä ilmenee virhe, tulee se korjata välittömästi ja tarkistaa yhtiön sisäistä selvitysprosessia virheiden välttämiseksi tulevaisuudessa.

Asiakas- ja osuusrekisteri

5 Virhe tiedoissa.

Todennäköisin asiakasrekisteriin liittyvä riski on virheen joutuminen asiakaskohtaisiin tietoihin. Tämä voi johtua esimerkiksi siitä, että asiakkaan uusia yhteystietoja ei päivitetä järjestelmään, asiakas ilmoittaa virheelliset yhteystiedot, tiedot syötetään järjestelmään väärin tai osuusrekisteriin asiakkaan rahasto-omistuksiin pääsee tulemaan virhe. Pääasiallinen syy näihin virheisiin on huolimattomuus tai unohdus. Syynä voi olla myös virheellinen lähtödata. Virheestä on seurauksena se, että asiakkaan yksityisyyden suoja tai oikeusturva on uhattuna. Virheen joutumista asiakas- tai osuusrekisteriin voi ehkäistä tekemällä useampia tarkistuksia, varmistumalla tiedon lähteistä ja prosessin toimivuudesta sekä keskittymällä käsiteltäviin tietoihin rauhassa ja ajan kanssa. Jatkuvuus virheen jälkeen varmistetaan sillä, että asiakkaiden tietoja päivitetään tasaisesti heti tiedon saavuttaessa rahastoyhtiön, havaitut virheet korjataan välittömästi ja prosessiin tehdään tarvittavat muutokset.

6 Rekisteristä ei saa tietoa ulos.

Joskus voi käydä niin, että asiakas- tai osuusrekisteristä ei saa ulos relevantteja tietoja. Tämä voi johtua esimerkiksi siitä, että käyttötarkoitukseen sopiva dataraportti puuttuu ja kyseistä raporttia ei osata laatia koulutuksen tai perehdytyksen puutteen vuoksi. Seurauksena tällaisen riskin toteutumisesta voi olla asiakkaan oikeuksien toteutumatta jättäminen tai huono asiakaspalvelukokemus. Tilannetta voi ennaltaehkäistä perehdyttämällä työntekijöitä tarpeeksi järjestelmiin. Jatkuvuutta ajatellen lisäkoulutus sekä

osaamisen seuranta varmistavat, ettei virhe toistu ainakaan samanlaisena tulevaisuudessa.

7 Asiakirjan katoaminen.

Vakavimmillaan asiakirjan katoaminen tarkoittaa sitä, että asiakkaan lähettämä rahastolunastusilmoitus hukataan ja lunastustoimeksianto jää sen vuoksi toteutumatta. Syynä tähän on huolimattomuus ja seurauksena asiakkaan rahastojen säännöissä sekä sijoitusrahastolaissa määritelty oikeus lunastaa rahasto-osuutensa toteutumatta jääminen. Ennaltaehkäisynä tulee korostaa vastaanotettujen lunastusilmoitusten huolellista käsittelyä ja arkistointia. Mikäli riski asiakirjan katoamisesta realisoituu, tulee virhe korjata välittömästi sekä tehdä prosessiin tarvittavat muutokset.

Asiakaspalvelu

8 Yhteydenottoihin ei vastata.

Ilmeisin asiakaspalveluun liittyvä riski on, että asiakkaan yhteydenottoon ei vastata. Todennäköisimmin tämä johtuu unohduksesta tai siitä, että kukaan ei tartu asiaan vaikka asiakkaan lähestymisyritys noteerataan. Tästä on seurauksena epämieluisa asiakaskokemus ja sitä myöten mahdollinen mainehaitta. Ennaltaehkäisynä toimivat tarkat asiakaspalvelullisten vastuualueiden määrittelyt. Mikäli vastaamaton yhteydenottopyyntö havaitaan, tulee asiakkaaseen ottaa yhteyttä välittömästi.

9 Asiakkaan toimeksiannon epäonnistunut tai virheellinen toteutus rahastoyhtiöstä johtuvasta syystä.

Käytännössä on kyse asiakkaan lähettämän lunastustoimeksiannon katoamisesta (ks. edellä no 7 Asiakirjan katoaminen) tai väärän osuusmäärän lunastamisesta. Näiden syynä on huolimattomuus. Seurauksena vakavimmillaan on rahallinen korvausvelvollisuus asiakkaalle tai vähintäänkin epämieluisa asiakaskokemus ja sitä myöten aiheutettu mainehaitta. Ennaltaehkäisy liittyy tarkkoihin vastuualueiden määrittelyihin sekä huolellisuuden korostamiseen rahastolunastusten ja merkintöjen osalta. Jatkuvuutta ajatellen virhe tulee välittömästi korjata tai toimeksianto toteuttaa seuraavana mahdollisena hetkenä.

10 Asiakkaan toimeksiannon epäonnistunut toteutus asiakkaasta johtuvasta syystä.

Edellä kuvattu tilanne voi myös toteutua asiakkaasta johtuvasta syystä eli käytännössä siitä, että hän lähettää rahastolunastuksensa myöhässä. Toimeksianto voi myös epäonnistua merkintämaksun myöhästymisestä tai asianmukaisen luvan puuttumisesta jos sijoittajana on vajaavaltainen henkilö. Syynä tähän tilanteeseen on se, että asiakas ei ole ajan tasalla käytännöistä tai että häntä on ohjeistettu puutteellisesti. Seurauksena on epämieluisa asiakaskokemus ja mahdollinen mainehaitta. Ennaltaehkäisyä ajatellen informaatiota tulee antaa riittävästi kirjallisessa muodossa (rahastoesitteet, kotisivut) sekä suullisesti (asiakkaiden yhteydenotot) siten, että se on selkeästi ja yksiselitteisesti esitetty. Jatkuvuus varmistetaan sillä, että asiakasta ohjeistetaan puutteen korjaamiseksi.

11 Asiakasta ei osata auttaa.

Voi myös käydä niin, että asiakkaan tiedusteluun tai kysymykseen ei osata vastata, mikä johtuu tiedon tai kokemuksen puutteesta. Seurauksena voi olla epämieluisa asiakaskokemus. Tätä voidaan ennaltaehkäistä kouluttamalla ja perusteellisella perehdyttämisellä. Jatkuvuus varmistetaan sillä, että asia luvataan selvittää mahdollisimman pian.

12 Asiakas ei ole tyytyväinen saamaansa palveluun.

Tyypillisin asiakaspalvelun riski on asiakkaan tyytymättömyys johonkin asiaan. Syynä on se, että asiakkaan odotukset tai toiveet eivät kohtaa asiakaspalvelijan tai yrityksen panoksen kanssa. Seurauksena voi olla mainehaitta ja taloudelliset menetykset mikäli asiakkuus päätetään. Jos kyseessä on asiakaspalvelun laatu, tulee ennaltaehkäisevään koulutukseen ja perehdytykseen kiinnittää huomiota. Mikäli palaute koskee esim. hinnoittelua tai tuotteita ylipäätään, tulee näitä seikkoja tarkentaa. Jatkuvuutta kyetään varmistamaan sillä, että asiakkaita ylipäätään kehotetaan antamaan palautetta toiminnasta. Kun negatiivista asiakaspalautetta saadaan, tulee asiakkaaseen ottaa yhteyttä ja korjata tilanne mahdollisuuksien mukaan toiveita vastaavaksi.

13 Sähköiset informaatiokanavat (kotisivut, uutiskirje) eivät toimi.

Kotisivuille tai julkaistavaan uutiskirjeeseen voi päätyä virheellistä informaatiota. Kotisivujen päivitystahti voidaan myös kokea liian hitaaksi tai suppeaksi. Syynä tähän on

huolimattomuus tietojen tarkistamisessa tai arviointivirhe päivitysten tarpeellisuuden osalta. Nämä voivat vaikuttaa yrityksen maineeseen tai mielikuvaan siitä. Vakavimmillaan ne voivat johtaa myös rahallisiin menetyksiin. Ennaltaehkäisynä on julkaistavien tietojen lähdekriittinen tarkastelu sekä tarkistaminen. Päivityksiä ajatellen tulee luoda tarkistuslista päivitettävistä asioista sekä vastuutettava kotisivujen päivitys. Jatkuvuuden varmistamiseksi virheet tulee korjata asianmukaisesti sekä prosessia tarkistaa tarvittavilta osin.

Taloushallinto

14 Kirjanpitovirhe.

Kirjanpitovirhe voi ilmetä esimerkiksi virheellisenä tiliöinnin kirjauksena, mikä aiheutuu huolimattomuudesta. Seurauksena voi olla virheellinen raportti tai tilinpäätös. Kuten muutkin huolimattomuusvirheet, myös tämä on ennaltaehkäistävissä tarkkaavaisuudella ja asiaan paneutumisella. Toiminnan jatkuvuus varmistetaan korjaamalla virhe.

15 Likviditeettiongelmat.

Ongelmat maksuvalmiudessa johtavat tyypillisimmillään siihen, että käteinen raha ei riitä ostolaskun maksuun. Syynä tähän on rahan riittävyyteen liittyvä arviointivirhe. Seurauksena tästä on joko tilinylityksestä seuraavat lisäkulut tai maksujen myöhästymisestä aiheutuneet viivästyskulut. Riskiä ennaltaehkäistäkseen tulee rahavirtoja ja maksuvalmiustilannetta seurata aktiivisesti. Lisäksi yrityksellä on periaate, jonka mukaisesti käteistä tai nopeasti käteistettävää varallisuutta on runsaasti. Toiminnan jatkuvuuden kannalta on oleellista korjata tilanne mahdollisimman pian sen huomaamisesta.

16 Häiriö laskujen maksussa.

Laskujen maksuhäiriö tarkoittaa ostolaskujen maksamista eräpäivän jälkeen. Syynä tähän on se, että erääntyvien laskujen maksusta ei pidetä riittävästi huolta tai että vastuuhenkilö puuttuu tai hän ei ole tehtäviensä tasalla. Seurauksena tästä yrityksen maksuhäiriömerkinnän riski kasvaa. Ennaltaehkäisyksi tulee määritellä ostolaskujen maksuprosessi tarkasti. Jatkuvuus tässä tilanteessa varmistetaan erääntyneiden laskujen välittömällä maksamisella.

Seuranta ja raportointi

17 Kaikkia tarpeellisia asioita ei seurata.

Tämä riski toteutuu siinä vaiheessa kun havaitaan, että jotain oleellista tietoa on jäänyt saamatta sen vuoksi, että jatkuvaa seurantaa ei ole olemassa. Syynä on, että prosesseja ei ole mietitty loppuun saakka. Seurauksena on, että tietoa ei ole riittävästi päätöksenteon tueksi. Ennaltaehkäisynä toimii prosessien säännöllinen kartoitus. Jatkuvuus varmistetaan prosessikaavioiden päivityksellä kartoitusten tulosten mukaan.

18 Ei raportoida riittävästi.

Edellisen kaltainen tilanne on se, että havaitaan raportoinnin olevan puutteellista esimerkiksi siten, että viranomaiselta tulee kehotus lähettää raportti tietystä asiasta. Syynä tälle on se, että informaatiota velvoitteista ei ole riittävästi ja seurauksena se, että informaatio ei liiku yrityksestä eteenpäin. Ennaltaehkäisynä tulee velvoitteista varmistua etupainotteisesti siten, että kokonaistilanteen seuranta on yhden tahon (toimitusjohtaja) vastuulla. Riskin toteutuessa prosessia tulee tarkentaa ja päivittää vastaamaan vaatimuksia.

19 Raportointivirhe.

Raporteissa voi ilmetä useita virheitä, jotka voivat johtua huolimattomuudesta tai virheellisestä alkuperäisen tiedon lähteestä. Mikäli virhettä ei ajoissa huomata, seurauksena on se, että eteenpäinkin mahdollisesti päätöksenteon tueksi toimitettava data on virheellistä. Näin alun perin pienikin virhe voi lähteä kertautumaan. Ennaltaehkäisyksi tiedon lähteistä ja prosessin sujuvuudesta tulee varmistua. Myös raporttien laadintaan tulee paneutua siten, että ne kootaan tarkkaavaisuutta noudattaen. Jatkuvuus varmistetaan sillä, että havaittu virhe korjataan ja prosessia tarkistetaan tarvittavilta osin.

20 Raportteja ei lähetetä ajallaan.

Raportoinnissa tyypillinen riski on raporttien lähettäminen myöhässä. Se voi johtua inhimillisestä unohduksesta tai resurssien vähyydestä. Seurauksena on, että informaatio ei liiku osapuolilta toisille. Ennaltaehkäistäkseen tätä tulee laadittuja työlistoja seurata päivittäin ja työmääriä kontrolloida siten, että jokaisella on riittävästi aikaa ja osaamista selviytyä tarvittavista asioista. Jatkuvuuden varmistamiseksi myöhästyneet

raportit tulee lähettää välittömästi ja tarvittaessa tehdä muutoksia vastuualueisiin tai prosesseihin.

Prosesseihin liittyvistä riskeistä olennaisimmiksi luokiteltiin numerot 1, 7, 8, 9, 11, 19 ja 20. Niihin tulee siis kiinnittää erityishuomiota kun prosessien riskienhallinnan toimenpiteitä laaditaan.

6.3.2 Oikeudelliset riskit

Oikeudelliset riskit voivat aiheutua ulkoisten tekijöiden sekä yrityksen oman toiminnan vaikutuksesta. Ne voivat liittyä kaikkeen liiketoimintaan. Yrityksen toimintaan sovellettavien säädösten ja määräysten tulkintaan, soveltamisalaan sekä voimassaoloon liittyy epävarmuustekijöitä, joista voi aiheutua huomattavia tappioita ja joilla voi olla merkitystä oikeudellisen vastuun ja mahdollisen korvausvelvollisuuden kannalta. Sopimusten voimassaoloon ja sisältöön liittyvät riitaisuudet voivat vaikuttaa haitallisesti yrityksen toimintaan. Epäedullisista sopimuksista irtautumiseen ja korvaavan sopimuksen solmimiseen voi liittyä tappion vaara. Tämä koskee erityisesti vakioehtoisten sopimusten käyttöä. Myös julkaistaviin dokumentteihin, kuten esitteisiin ja mainontaan, voi liittyä vahingonkorvauksen mahdollisuus tai maineen ja arvostuksen heikkenemisen riski. (Finanssivalvonnan standardi 4.4.b 2004, 19.)

Vaikka oikeudellisten riskien huomioiminen on yrityksen toiminnan kannalta oleellista, on niiden esiintymistodennäköisyys käytännössä hyvin pieni. Oikeudelliset riskit eivät näyttäydy yrityksen päivittäisessä toiminnassa niin selkeästi, että niiden havaitseminen olisi ilmeistä. Tämän vuoksi yrityksellä on käytössään ulkopuolisia konsultteja, jotka oman alansa asiantuntijoina voivat auttaa eteen tulevissa tilanteissa.

Rahastojen arvonlaskenta sekä asiakas- ja osuusrekisteri

21 & 22 Säädöksiä tai määräyksiä tulkitaan väärin.

Oikeudellinen riski toteutuu jos esimerkiksi sijoitusrahastolakia tai rahaston sääntöjä tulkitaan virheellisesti. Käytännössä tämä voi tarkoittaa esimerkiksi sitä, että rahaston varat eivät ole hajautettuna tarpeeksi moneen sijoituskohteeseen tai osuustodistus, joka voidaan antaa vain nimetylle osuusrekisteriin merkitylle osuudenomistajalle tai

hänen valtuuttamalleen, luovutetaan väärälle henkilölle. Syynä voi olla tiedon puute tai toiminnan huolimattomuus. Seurauksena voi olla valvovan viranomaisen langettama hallinnollinen seuraamus tai korvausvelvollisuus vahinkoa kärsineelle osapuolelle. Ennaltaehkäisynä on lakeihin, asetuksiin ja määräyksiin perehtyminen huolellisesti sekä tarvittaessa ulkopuolisen konsultin käyttäminen. Jatkuvuuden varmistamiseksi virhe tulee välittömästi korjata. Numerot 21 ja 22 myös luokiteltiin oleellisiksi riskeiksi.

Asiakaspalvelu

23 Erimielisyydet sopimusten voimassaolosta tai sisällöstä.

Asiakkaiden kanssa voi ilmetä erimielisyyksiä esimerkiksi lunastusilmoituksen jättämisajankohdasta, joka vaikuttaa lunastustoimeksiannon toteuttamisajankohtaan. Syynä tälle on yleensä se, että toinen tai molemmat osapuolet eivät ole perehtyneet sopimusehtoihin tarpeeksi tai ymmärrys niistä ei ole yhteneväistä. Seurauksena tästä voi olla epämieluisa asiakaskokemus ja mainehaitta. Ennaltaehkäisynä on sopimusehtojen selkeyttäminen sekä perusteellinen läpikäynti asiakkaan kanssa ennen sopimuksen allekirjoitusta. Jatkuvuus varmistetaan sillä, että pyritään molempia osapuolia tyydyttävään sovintoon sekä selkeytetään prosessia ja sopimuksia.

24 Dokumentit virheellisiä tai epäeettisiä.

Käytännössä dokumenttien virheellisyys voi tarkoittaa esimerkiksi sitä, että rahastosta perittävät kulut on ilmoitettu väärin rahastoesitteessä. Tämä on seurausta siitä, että dokumenttien laadintaan ei ole perehdytty tarpeeksi ja niitä ei ole riittävästi tarkistettu. Seurauksena voi olla rahallinen korvausvelvollisuus sekä yrityksen maineen heikentyminen. Ennaltaehkäisy liittyy dokumenttien huolelliseen laatimiseen sekä tarvittaessa ulkopuoliseen konsultaatioon. Lisäksi uuden sijoitusrahastodirektiivin mukainen määrämuotoinen KIID-dokumentti vähentää esitteissä olevien virheiden todennäköisyyttä. Jatkuvuus varmistetaan virheen korjaamisella.

Taloushallinto

25 Lainsäädännöllisten velvoitteiden laiminlyönti.

Taloushallintoa ajatellen oikeudellisista riskeistä tyypillisin on lainsäädännöllinen laiminlyönti eli esimerkiksi kirjanpitolain muutos, jota ei huomioida. Syynä tähän on huolimat-

tomuus tai vastuiden epäselvyys. Seurauksena voi olla taloudellisia menetyksiä esimerkiksi lisäverojen tai veronkorotusten muodossa. Tilannetta voidaan ennaltaehkäistä alan käytäntöjen ja lakimuutosten aktiivisella seuraamisella sekä ulkopuolisella konsultaatiolla. Jatkuvuus varmistetaan prosessin tarkentamisella ja mahdollisen virheen korjaamisella.

Henkilöstö

Yrityksen palveluksessa työskentelevien ja siihen rekrytoitavien henkilöiden ammattitaidon on oltava riittävä suhteutettuna työtehtäviin yrityksen koko, toiminnan laajuus ja luonne huomioiden. Ammattitaidolla tarkoitetaan henkilön kelpoisuutta, riittävää koulutusta ja kokemusta sekä kykyä suoriutua tehtävistään. Uuden työntekijän hyvämaineisuuteen ja taustoihin on kiinnitettävä huomiota. (Finanssivalvonnan standardi 4.4.b 2004, 21.)

Tehtävien hoitamiseen tulee varata riittävästi henkilöstöä. Liiketoiminnan jatkuvuuden turvaamiseksi on avaintehtäviä hoitavilla henkilöillä oltava varahenkilöt sairastumisen, tapaturman tai yllättävän palvelusuhteen päättymisen varalta. (Finanssivalvonnan standardi 4.4.b 2004, 21.)

Salassapitoa koskevat periaatteet on vahvistettava. Niillä pyritään varmistamaan, ettei yrityksen toimihenkilö ilmaise asiakkaan tai muun valvottavan toimintaan liittyvän henkilön taloudellista asemaa tai henkilökohtaisia oloja koskevaa seikkaa tai liike- tai ammattisalaisuutta, jollei se, jonka hyväksi vaitiolovelvollisuus on annettu, anna suostumustaan sen ilmaisemiseen. (Finanssivalvonnan standardi 4.4.b 2004, 21.)

Lisäksi tulee vahvistaa palkitsemisjärjestelmiä koskevat periaatteet. Niissä on varmistettava, etteivät palkitsemisjärjestelmät houkuttele ei-toivottuihin menettelytapoihin tai hallitsemattomaan riskinottoon. (Finanssivalvonnan standardi 4.4.b 2004, 21.)

Henkilöstön ollessa yrityksen tärkein voimavara se on myös suurin riskien aiheuttaja. Valtaosa tässä yhteydessä tunnistetuista riskeistä liittyy yrityksen sisäiseen toimintaan ja kulminoituu siinä nimenomaan henkilöstön suorittamiin toimiin. Riskienhallintamielessä henkilöstönäkökulma siis on keskeisin. Tässä jaottelussa henkilöstöön liittyvät

riskit on yhdistetty kaikkiin osa-alueisiin kuuluviksi siten, että ne on jaoteltu henkilöstöstä johtuviin sekä henkilöstöön kohdistuviin riskeihin.

Henkilöstöstä johtuvat

26 Salassapitovelvollisuuden laiminlyönti.

27 Tiedonantovelvollisuuden laiminlyönti asiakkaille.

28 Kavallus, petos, lahjuksen ottaminen.

29 Arvopaperimarkkinarikos tai -rikkomus.

30 Vahingonteko.

31 Valtuuksien puuttuminen/ylittäminen.

32 Asiakastietojen väärinkäyttö.

33 Liikesalaisuuden rikkominen.

34 Lain ja hyvän tavan vastainen tai harhaanjohtava markkinointi ja palveluntarjonta.

35 Selonottovelvollisuuden laiminlyönti.

36 Toimeksiantojen säännösten vastainen toteuttaminen.

37 Asiakasvarojen säännösten vastainen käsittely.

Kaikkien näiden syynä on joko tahallisuus, huolimattomuus tai tietämättömyys. Koska kyseessä ovat yrityksen toiminnan kannalta merkittävät riskit, seurauksena on todennäköisesti vahingon aiheutuminen yritykselle. Mikäli vahingot ovat merkittäviä, voi kyseeseen tulla viranomaisen langettama hallinnollinen seuraamus. Ennaltaehkäisynä on tahallisuudesta johtuvien virheiden suhteen ennalta määrätyt sanktiot (työsopimuslain mukaiset suullinen huomautus, kirjallinen varoitus ja työsopimuksen päättäminen), inhimillisten virheiden osalta huolellisuuteen kannustaminen ja työtehtävien moitteettoman suorittamisen mahdollistaminen sekä tavoista, säännöistä ja käytännöistä tiedottaminen siten, että koko henkilöstöllä on yhtenäinen kuva toiminnan periaatteista ja ohjeista. Merkittävistä toimihenkilöistä täytetään myös Fit&Proper -ilmoitus, joka on henkilön luotettavuutta, sopivuutta ja ammattitaitoa koskeva selvitys. Jatkuvuus varmistetaan siten, että vahingot pyritään korjaamaan mahdollisimman pian niiden huomaamisesta ja haitalliset vaikutukset pyritään minimoimaan.

38 Ammattitaidottomuus.

Tilanne, jossa todetaan henkilön olevan taitoihinsa ja osaamiseensa nähden liian vaativissa tehtävissä, johtuu väärästä rekrytoinnista tai koulutuksen ja perehdytyksen puutteista. Seuraus ammattitaidottomuudesta ovat virheet, jotka aiheuttavat yritykselle

vahinkoa. Tätä ennaltaehkäistäkseen yrityksen tulee suorittaa uusien henkilöiden rekrytointi riittävää huolellisuutta ja perehtyneisyyttä noudattaen siten, että henkilön osaamisen tasosta varmistutaan. Lisäksi perehdyttämiseen tulee varata riittävästi aikaa ja resursseja. Jatkuvuutta ajatellen oleellista on tehdyn virheen korjaaminen sekä henkilön lisäohjeistaminen tai -koulutus.

39 Irtisanoutuminen tai työsuhteen päättäminen.

Henkilön työsuhteen päättymiseen liittyvä riski on yritykselle tärkeän osaamisen ja tiedon menettäminen lähtevän henkilön mukana. Syynä voivat olla sekä henkilökohtaiset että yritykseen liittyvät seikat. Seurauksena on henkilön työpanoksen menettäminen sekä edellä mainittu tietojen mahdollinen katoaminen, jollei sitä ehditä riittävästi irtisanomisaikana siirtää seuraajalle. Tällaisia tilanteita ennaltaehkäistäkseen henkilökunnan hyvinvoinnista ja jaksamisesta tulee pitää huolta. Jatkuvuus voidaan varmistaa sillä, että uuden henkilön rekrytointi aloitetaan välittömästi kun tieto työsuhteen päättymisestä saadaan ja samalla sitoutetaan jäljelle jäävä henkilöstö työskentelemään yrityksessä vähintään ylimenoajan. Lisäksi sovelletaan yrityksen sisäistä avainhenkilöiden paikkausjärjestelmää.

Henkilöstöön kohdistuvat

40 Työnantajan työsopimuslain rikkomukset.

Tähän ryhmään on yhdistetty kaikenlaiset työnantajan rikkomukset kuten syrjintä-, palkka-, korvaus-, irtisanomis- ja työmarkkinariidat. Syitä voi etsiä samoista lähteistä kuin henkilöstöstä johtuvissakin riskeissä: tahallisuudesta, huolimattomuudesta tai tietämättömyydestä. Mikäli työntekijäpuoli lähtee ajamaan asiaa viranomaisteitse, voi seurauksena olla oikeudenkäynnistä, vahingonkorvauksista ja sakoista aiheutuvia kuluja sekä mainehaitta, mikäli tapaus nousee julkiseksi. Tilanteita voi ennaltaehkäistä sillä, että työnantajan edustaja varmistuu velvoitteistaan ja noudattaa niitä asianmukaisesti. Jatkuvuutta ajatellen harkittavia vaihtoehtoja ovat sovintoratkaisuun pyrkiminen tai langetetun seuraamuksen suorittaminen.

Henkilöstöön liittyvistä riskeistä olennaisimmiksi luokiteltiin numerot 26, 28, 29 ja 32. Niihin tulee siis kiinnittää erityishuomiota kun riskienhallinnan toimenpiteitä laaditaan.

6.3.3 Jatkuvuussuunnittelu

Jatkuvuussuunnittelulla tarkoitetaan varautumista liiketoiminnan keskeytyksiin siten, että yrityksen toimintaa pystytään jatkamaan ja tappioita rajoittamaan erilaisissa liiketoimintaa kohtaavissa häiriötilanteissa. Jatkuvuussuunnittelussa laaditaan tärkeimmille liiketoiminta-alueille jatkuvuussuunnitelmat, joiden pohjalta toimintaa jatketaan mahdollisessa häiriötilanteessa. (Finanssivalvonnan standardi 4.4.b 2004, 22.)

41 - 45 Liiketoimintaa häiritsevä tilanne.

Liiketoimintaa häiritseväksi tilanteeksi luokitellaan tässä yhteydessä yrityksen henkilöstöä, toimitiloja, tietojärjestelmiä tai tietoliikennettä kohdanneet vahingot tai tahalliset teot, vesivahingot, tulipalot sekä teknisen infrastruktuurin häiriöt. Syynä näihin kaikkiin on yrityksen ulkopuolella oleva pääosin kontrolloimattomissa oleva tekijä. Tyypillistä on lisäksi, että riski toteutuu ilman ennakkovaroitusta. Seurauksia voi olla useita: arvonlaskentaa ei saada suoritettua, asiakas- ja osuusrekisteriä ei saada päivitettyä, asiakaspalvelu eikä seuranta tai raportointi toimi. Ne voivat siis kohdistua yhteen, useaan tai kaikkiin tarkasteltaviin osa-alueisiin. Sen vuoksi tässä yhteydessä riski on eritelty kaikkien osa-alueiden osalta. Tämänkaltaisten tilanteiden ennaltaehkäisy tilanteiden luonteen vuoksi on yrityksen oman vaikutusvallan ulkopuolella. Jatkuvuuden varmistaminen toteutetaan erillisessä sisäisessä muistiossa esitellyn toipumissuunnitelman esittelemällä tavalla. Nämä on myös luokiteltu oleellisiksi riskeiksi.

6.3.4 Varautuminen poikkeusoloihin

Poikkeusoloihin varautumisella tarkoitetaan suuronnettomuuden tai muun vakavan yrityksen toimintakykyyn oleellisesti vaikuttavan seikan ilmenemisen varalta tehtävää suunnitelmaa. Sitä voidaan soveltaa myös muihin vakaviin häiriöihin ja kriiseihin kuten pandemiaan tai muuhun yrityksen henkilöstön toimintakykyä vakavasti vaarantavaan uhkaan. Huomioitava on myös yrityksen toimitilojen tai tietojenkäsittely-ympäristön tuhoutuminen. (Finanssivalvonnan standardi 4.4.b 2004, 25, 36 - 37.)

46 Liiketoiminnan kokonaan keskeyttävä tilanne.

Tämä on edellisessä kohdassa esiteltyä liiketoiminnan häiriötä vakavampi tilanne, jossa on kyseessä suuronnettomuus tai muu vakava yrityksen toimintakykyyn oleellisesti vaikuttava seikka, muut vakavat häiriöt ja kriisit, toimitilojen tai tietojenkäsittely-

ympäristön tuhoutuminen. Seurauksena on yrityksen koko toiminnan keskeytyminen. Ennaltaehkäisy ja jatkuvuuden varmistaminen kuten edellä liiketoiminnan häiriötilanteessa. Tämä on luokiteltu oleelliseksi riskiksi.

6.3.5 Tietojärjestelmät

Tietojärjestelmien tulee olla riittävät ja asianmukaisesti järjestetty (Finanssivalvonnan standardi 4.4.b 2004, 27). Rahastoyhtiöllä tietojärjestelmäosaamista ostetaan ulkopuoliselta palveluntarjoajalta, mutta tietokannat ja ohjelmat sijaitsevat yrityksen omalla palvelimella. Käytettävästä järjestelmästä huolimatta mahdolliset riskit näyttäytyvät samantyyppisinä.

47/54/57/61 Järjestelmästä ei saa tietoa.
Riski sille, että tietojärjestelmästä ei saa tietoa ulos kulminoituu henkilöstön koulutuksen tai perehdytyksen puutteeseen. Sen vuoksi ennaltaehkäisyksi järjestelmiin tutustuminen ja niiden käyttökoulutus on suoritettava perusteellisesti sekä on huolehdittava, että ohjeet ja tietojärjestelmätuki ovat saatavilla. Jatkuvuus kyetään varmistamaan riittävällä järjestelmäkoulutuksella sekä osaamisen seurannalla.

48/55/58/62 Järjestelmä toimii väärin.
Syynä tähän on järjestelmä- tai ohjelmistovirhe, joka aiheuttaa virheitä arvonlaskentaan, asiakas- ja osuusrekisteriin tai seurantaan ja raportointiin. Ennaltaehkäisyksi tälle tulee käytettävistä ohjelmistotoimittajista varmistua huolella etukäteen esim. suositusten kautta, sillä yrityksellä ei lähtökohtaisesti itseltä löydy kompetenssia arvioida järjestelmien testaus- ja toimivuustasoa riittävässä laajuudessa. Jatkuvuuden varmistaminen hoidetaan korjaamalla tapahtunut virhe ja järjestelmävirheen korjauksella tai järjestelmän vaihdolla. Nämä on luokiteltu oleellisiksi riskeiksi.

49/52/59 Tekijän tekemä tallennusvirhe tietojärjestelmään.
Tyypillisimmillään tämä tarkoittaa epähuomiossa järjestelmään tallennettua näppäilyvirhettä, jonka syynä on huolimattomuus. Seurauksena on, että arvonlaskenta tai asiakas- ja osuusrekisteri on virheellinen. Ennaltaehkäisynä on tallennusten tekeminen huolellisuutta ja riittävästi aikaa käyttäen sekä tarkkojen noudatettavien prosessikuva-

usten laatiminen. Jatkuvuus varmistetaan sillä, että tallennusvirheet korjataan heti kun ne havaitaan. Nämä on luokiteltu oleellisiksi riskeiksi.

50/53/60 Datasta johtuva tallennusvirhe tietojärjestelmään.

Datasta johtuva tallennusvirhe tarkoittaa käytännössä sitä, että käytetty alkuperäinen data on virheellistä, minkä vuoksi riskin hallinta on haastavampaa kuin esimerkiksi edellisen kohdan tapauksessa. Riskin ehkäisemiseksi tulee varmistua datan lähteiden luotettavuudesta, oikeellisuudesta ja asianmukaisuudesta. Jatkuvuus varmistetaan sillä, että virheelliset tiedot korjataan heti kun ne havaitaan. Nämä on myös luokiteltu oleellisiksi riskeiksi.

51/56 Tarvittavaa dataa ei saa käyttöön tai toimitettua asiakkaalle.

Tämä voi tarkoittaa esim. katkosta internet-yhteydessä tai tietoliikennehäiriötä. Tätä voi ennaltaehkäistä hankkimalla varayhteyden toiselta operaattorilta kuin miltä kiinteä yhteys on hankittu. Jatkuvuus varmistetaan sillä, että operaattoria informoidaan katkoksesta ja odotetaan yhteyden korjaantumista.

Kaikkia tietojärjestelmiä koskevia riskejä ovat seuraavat:

63 Laiterikko.

Tyypillisimmillään tämä tarkoittaa tietokoneen rikkoutumista, mikä johtuu laitteen vanhentumisesta, viallisuudesta tai väärästä käytöstä. Seurauksena on työnteon häiriö tai vakavammassa tapauksessa keskeytyminen. Ennaltaehkäisy liittyy laitteiston säännölliseen päivittämiseen ja uusimiseen, käyttöohjeistukseen perehtymiseen sekä tietojen säännölliseen varmuuskopiointiin. Jatkuvuus kyetään varmistamaan varalaitteistolla eli esimerkiksi kannettavilla tietokoneilla, joissa on sama käyttövalmius kuin pöytäkoneissa.

64 Sähkökatko.

Jos sähkönjakeluun tulee häiriö, työnteko todennäköisimmin keskeytyy. Koska tilannetta ei voi käytettävissä olevin resurssein ennaltaehkäistä, tulee työn alla oleva aineisto tallentaa määräajoin. Toiminnan jatkuvuus on varmistettu siten, että yrityksen palvelimeen on liitetty vara-akku, joka ajaa järjestelmän hallitusti alas, ettei palvelimella olevia tietoja menetetä.

65 Ulkoistetun tai automatisoidun palvelun häiriö.
Muutamia toimintoja on yrityksessä ulkoistettu. Tästä käytännön esimerkki on maksuliikenneohjelma. Jos sen toimintaan ilmaantuu häiriö, tiliotteiden automaattinen päivittäinen nouto ei toimi. Syynä on yleensä yrityksestä riippumaton seikka, joka kuitenkin aiheuttaa työnteon häiriintymisen tai keskeytymisen. Ennaltaehkäisynä tässä on palveluntarjoajan prosessien toimivuudesta varmistuminen. Jatkuvuutta ajatellen häiriöstä informointi ja ongelman ratkeamisen odottaminen ovat lyhyellä tähtäimellä ainoat keinot. Jos häiriöiden esiintyminen on jatkuvaa, tulee harkita palveluntarjoajan vaihtoa.

6.3.6 Tietoturvallisuus

Tietoturvallisuus tarkoittaa sitä, että yrityksen tiedot, palvelut, järjestelmät ja tietoliikenne tulee olla suojattu ja varmistettu sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Yleisiä tietoturvallisuuteen liittyviä vaatimuksia ovat säilytettävän, siirrettävän ja käsiteltävän tiedon luottamuksellisuus siten, että tieto ei paljastu sivullisille, muuttumattomuus siten, että tieto säilyy eheänä sekä käytettävyys siten, että tieto on saatavissa oikeaan aikaan siihen oikeutetulle. Nämä koskevat kaikkia tarkasteltavia osa-alueita. (Finanssivalvonnan standardi 4.4.b 2004, 28.)

Tietojärjestelmiin pääsyä tulee valvoa. Myös tietojärjestelmissä käsiteltävien tapahtumien kiistämättömyys sekä keskenään kommunikoivien osapuolten tunnistaminen ja todentaminen on hoidettava asianmukaisesti. Lisäksi tietojärjestelmissä käsiteltävät tapahtumat pitää voida aukottomasti jäljittää. (Finanssivalvonnan standardi 4.4.b 2004, 29.)

Tietoturvallisuudesta huolehtiminen on yrityksen riskienhallinnallisista tavoitteista tärkeimpiä. Kaikki siihen liittyvät riskit on luokiteltu oleellisiksi.
66 Tieto ei säily luottamuksellisena.
Tiedon luottamuksellisuuden menetyksestä käytännön esimerkki on asiakastietojen vuotaminen julkisuuteen. Tämä voi johtua tahallisuudesta, huolimattomuudesta tai tietämättömyydestä. Koska finanssialalla tietojen luottamuksellisuuteen tulee kiinnittää erityishuomiota, voi seurauksena olla viranomaisen langettama hallinnollinen seuraamus tai vähintään korvausvelvollisuus ja mainehaitta. Ennaltaehkäisynä tässä tapauksessa on järjestelmien ja prosessien varmistaminen henkilökohtaisilla käyttäjätunnuksil-

la ja salasanoilla. Lisäksi sähköpostiviesteissä tulee välttää arkaluonteisen tiedon (kuten henkilötunnuksien) julkaisua. Jatkuvuus tulee varmistaa tilanteen välittömällä ja asianmukaisella korjaamisella.

67 Tieto ei säily muuttumattomana.

Tiedon eheyden rikkoutuminen tarkoittaa viestitetyn tai tallennetun tiedon muuttumista sen jälkeen, kun tiedon todennettu luoja on sitä viimeksi käsitellyt. Käytännössä tiedon eheys voi kärsiä hakkerointitapauksissa, jossa tietoja tarkoituksella vääristetään. Tämä voi johtua tahallisuudesta, huolimattomuudesta tai tietämättömyydestä. Seuraukset ovat vastaavat kuin edellisessä kohdassa. Ennaltaehkäisyksi tiedot tulee varmuuskopioida päivittäin siten, että tilanne on joka hetkellä palautettavissa vähintään edellisen päivän tasolle. Jatkuvuus tulee varmistaa tilanteen välittömällä ja asianmukaisella korjaamisella.

68 Tieto ei ole käytettävissä.

Se, että tieto ei ole käytettävissä voi tarkoittaa esimerkiksi sitä, että tietokantayhteys ei toimi. Syynä tähän on tietoteknisen ratkaisun toimintahäiriö ja seurauksena se, että prosessit eivät etene. Ennaltaehkäisynä on riittävä koulutus sekä perehdytys ja tietoteknisistä ratkaisuista varmistuminen. Jatkuvuus varmistetaan sillä, että järjestelmää korjataan ja parannetaan tarvittavilta osin.

6.3.7 Rikosriskit

Tässä yhteydessä rikosriskeihin luokitellaan yritykseen ulkopuolelta kohdistuva rikosten mahdollisuus, mistä aiheutuu aineellista tai aineetonta vahinkoa. Tähän liittyen kaikki riskit luokiteltiin oleellisiksi.

69 Rahanpesu.

Rahanpesu voi rahastoyhtiön tapauksessa tarkoittaa rikoksella hankitun rahan kierrättämistä sijoitusrahaston kautta. Tilanteita voi ennaltaehkäistä noudattamalla asiakkaan tuntemisen ja tunnistamisen periaatteita sekä asiakassuhteen riskiperusteista arviointia ja säännöllistä seurantaa. Jatkuvuus varmistetaan viranomaisilmoituksella, mikäli ilmenee aihetta epäillä rahanpesua.

70 Varkaus, ryöstö.

Koska rahastoyhtiössä ei käsitellä käteistä rahaa, kohdistuu varkaus todennäköisimmin yrityksen aineelliseen omaisuuteen kuten tietokoneisiin. Ennaltaehkäisy liittyy varastettavan laitteiston säilyttämiseen lukituissa tiloissa ja hälytysjärjestelmän säännölliseen ylläpitoon. Jatkuvuus varmistetaan rikosilmoituksella ja mahdollisuuksien mukaan menetetyn omaisuuden takaisin hankkimiseen viranomaisten avustuksella.

71 Väärennös.

Väärennös voi liittyä esimerkiksi perusteettomaan lunastusilmoitukseen. Ennaltaehkäisyksi dokumenttien ja toimeksiantojen aitoudesta tulee varmistua niiden vaatimisella kirjallisessa muodossa allekirjoituksin varustettuna tai asiakas muulla tavoin tunnistamalla. Jatkuvuus varmistetaan tilanteen korjaamisella heti kun väärennös on todettu ja tekemällä rikosilmoitus.

72 Uhkailu, kiristys.

Uhkailulla tai kiristyksellä pyritään saamaan perusteetonta etua tai hyötyä. Sen ennaltaehkäisy on haasteellista. Toiminnan jatkuvuudesta varmistutaan tekemällä asiasta viranomaisilmoitus.

73 Murtautuminen tietojärjestelmään.

74 Haittaohjelman levittäminen.

75 Tietojärjestelmään kohdistuva palvelunestohyökkäys.

Nämä kolme riskiä liittyvät läheisesti myös tietojärjestelmäriskeihin. Käytännössä kyse voi olla osuusrekisterijärjestelmään hakkeroitumisesta, yrityksen sisäverkkoon päässeestä tuhoisasta viruksesta tai palvelimeen kohdistuvasta haitallisesta hyökkäyksestä. Kaikkien tapausten ennaltaehkäisyyn kuuluu tietoturvasta huolehtiminen ja jatkuvuus varmistetaan tietoturva-aukkojen paikkaamisella.

6.3.8 Muut

Edellä läpi käydyssä riskikartoituksessa on useassa kohdin viitattu riskien seurauksissa mainehaittaan. Sitä voidaan analysoida myös itsenäisenä riskinään (numero 76). Maineriski tarkoittaa sitä, että yrityksen maine vahingoittuu sisäisten tai ulkoisten väärinkäytösten tai virheiden vuoksi. Syitä voi olla lukuisia kuten huolimattomuus toiminnassa, prosessien epätarkkuus, puutteellinen ohjeistus tai vastuiden epäselvyys. Yhtäkaikki

seurauksena on asiakkaiden ja yleisön luottamuksen heikentyminen tai vakavammassa tapauksessa menettäminen. Tilanteita kyetään ennaltaehkäisemään maineeseen liittyvien seikkojen huomioinnilla prosessien suunnittelussa. Jatkuvuus puolestaan varmistetaan mahdollisten virheiden välittömällä ja tarkoituksenmukaisella korjaamisella, rehellisellä julkisella pahoittelulla sekä prosessien tarkentamisella. Maineriski luokitellaan oleelliseksi riskiksi.

6.3.9 Jaottelu riskien kriteerien mukaan

Jokainen tunnistettu riski jaoteltiin kolmella eri kriteerillä: riskin muodostumislokaation, sen tietoisuusasteen sekä vaikutustavan perusteella. Näitä ulottuvuuksia tarkastelemalla riskejä analysoitiin yhteensä 77 kappaletta, sillä yhdessä riskissä oli näkökulmasta riippuen eri luokittelukriteerejä käytössä.

Analysoidut riskit jakaantuivat muodostumislokaation perusteella siten, että 27 kpl (35 %) riskeistä arvioitiin tapahtuvaksi yrityksen ulkopuolella ja 50 kpl (65 %) luettiin sisäiseen toimintaympäristöön kuuluviksi. Tämä vahvistaa sitä, että tarkasteltujen riskien valossa yrityksellä on hyvä edellytykset hallita kattavasti riskikenttäänsä, sillä sisäisen toimintaympäristön tekijöitä on huomattavasti helpompi havaita, analysoida ja valvoa kuin ulkoisen.

Riskien tietoisuusastetta tarkasteltiin siitä näkökulmasta, että tiedostetuissa riskeissä, joita havaittiin kaksi kappaletta (3 %), katsottiin olevan mukana hyötymismotiivi ja riskinoton olevan silloin tietoista. Tiedostamattomiin riskeihin (75 kpl/97 %) laskettiin luettavaksi sellaiset riskit, joita ei tarkoituksellisesti pyritä ottamaan, mutta jotka toiminnan luonteen vuoksi ovat olemassa. Kyseessä ei ole siis tiedostamatta jättäminen siinä mielessä, että kyseisiä riskejä ei olisi lainkaan analysoitu tai pohdittu.

Riskit näyttäytyivät vaikutustavoiltaan hyvin tasaisina. Välillisiä vaikutuksia oli 36 kappaleella (47 %) ja välittömiä 41 kappaleella (53 %). Toiminnan kannalta oleellista on kiinnittää huomiota ensin mainittuun ryhmään sillä niiden vaikutukset ovat vakavampia välillisen vaikutustavan luonteen vuoksi eli siksi, että ne voivat vääristää toimintaa pitkään ennen kuin ne havaitaan.

6.4 Riskien arviointi

Riskien arvioinnissa on kaksi perusulottuvuutta: riskin toteutumistodennäköisyys sekä sen potentiaalinen vaikutus. Todennäköisyys riskin toteutumiselle on määritelty asteikolla A = korkea (tapahtuu keskimäärin kerran kuukaudessa), B = keskimääräinen (tapahtuu keskimäärin kerran vuodessa), C = matala (tapahtuu keskimäärin kerran 10 vuodessa) ja potentiaalista vaikutusta kuvataan kolmiportaisella asteikolla, jossa 1 tarkoittaa vakavinta vaikutusta, 2 haitallista vaikutusta ja 3 vähäistä vaikutusta. Näin yhdistämällä Triage sekä riskimatriisi, saadaan riskit luokiteltua taulukkoon, jossa tunnistettujen riskien todennäköisyys kuvataan pystyakselilla ja vaikutus vaaka-akselilla. Taulukosta kyetään yhdellä silmäyksellä hahmottamaan todennäköisimmät sekä vaikutuksiltaan vakavimmat riskit sekä jokaisen vakavuus/vaikutus -kombinaation riskien määrä. Se on esitetty ohessa (Taulukko 1). Riskien arvioinnin perusteena on käytetty riskin ja sen potentiaalisten vaikutusten peilaamista subjektiivisesti toiminnan kokonaiskuvaan sekä aiemmin toteutuneisiin riskeihin. Oleellisiksi luokiteltujen riskien numerot on lihavoitu.

Taulukko 1. Operatiivisten riskien luokittelu taulukkomuodossa.

Toteutumistodennäköisyys:			
A (korkea)			2
B (keskimääräinen)	24	**1**, 3, 4, 5, 6, 10, 12, 13, 14, 15, 16, 17, 18, **19, 20,** 38, **49**, **50**, **52, 53**, **59**, 60, 65	
C (matala)	**21, 22,** 25**, 26, 28, 29** 30**, 32**, 33, 34, 36, 37 **41, 42, 43, 44, 45, 46** 63, 64, **66, 67, 68, 69** **70, 71, 72, 73, 74, 75, 76**	**7, 8, 9, 11**, 23, 27 31, 35, **39**, 40, 47, **48** 51, 54, **55**, 56, 57, **58** 61, **62**	
Vakavuus:	**1** (vakavin)	**2** (haitallinen)	**3** (vähäinen)

Taulukon perusteella suurin osa riskeistä (31 kpl/41 %) kuuluu luokkaan C1 eli ne ovat erittäin epätodennäköisiä, mutta vaikutuksiltaan vakavimpia. Tässä lokerossa on myös eniten oleelliseksi luokiteltuja riskejä. Seuraavaksi eniten on haitallisia riskejä, jotka ovat erittäin epätodennäköisiä (20 kpl/26 %) kuuluen luokkaan C2 tai todennäköisiä (23 kpl/30 %) kuuluen luokkaan B2. Jäljelle jäävään prosenttiin kuuluu yksi B1 luokkaan kuuluva sekä yksi A3 luokkaan kuuluva riski.

Jatkuvan riskienhallinnan kannalta eniten huomiota tulee kiinnittää luokkiin A1, A2, B1 ja B2, joiden sisältämiä riskejä voi olettaa tapahtuvan siten, että ne uhkaavat toimintaa. Vaikka 1-luokan riskejä on lukumäärältään paljon, on niiden esiintymistodennäköisyys niin minimaalinen, että niiden varalta on katsottu riittäväksi kertaluonteinen varautumissuunnitelma. Niihin käytetty aika voi olla pois sinänsä vaikutuksiltaan vaatimattomammilta, mutta todennäköisyydeltään suuremmilta riskeiltä.

6.5 Riskeihin vastaaminen

Laaditun riskienhallintasuunnitelman mukaan Rahastoyhtiössä operatiivisiin riskeihin pyritään vastaamaan kolmella tavalla: pienentämällä, jakamalla ja pitämällä. Lähtökohtaisesti kaikki analysoidut riskit ovat sen luontoisia, ettei niiden mahdollisuutta voi täysin poissulkea tai käytettävissä olevien resurssien puitteissa ja toiminnan jatkuvuuden

kannalta niiden täydellistä poissulkemista ei ole mielekästä toteuttaa. Niiden uhka on siis koko ajan läsnä.

65 kappaleeseen (86 %) analysoiduista riskeistä valittiin vastaamistavaksi riskin pienentäminen. Tämä johtuu pääosin siitä, että valtaosaan riskeistä liittyy mahdollisuus inhimillisiin virheisiin (huolimattomuus, erehdys, unohdus), joita on mahdollista rajoittaa muun muassa tarkistuslistoilla, tuplatarkistuksilla, koulutuksella, kertaamisella ja varaamalla aikaa prosessin läpivientiin.

Riskeistä valittiin pidettäväksi tai hyväksyttäväksi kolme kappaletta (4 %): numerot 64 sähkökatko, 72 uhkailun tai kiristyksen mahdollisuus sekä 76 maineriski. Nämä olivat sellaisia riskejä, jotka pääosin uhkaavat yritystä sen ulkopuolelta ja joiden estämiseksi on hankala tehdä mitään. Maineriskin kohdalla olisi voitu soveltaa myös edellä esitettyä pienentämisen periaatetta. Yrityksen maine perustuu sen tuotteisiin, johtoon, taloudelliseen suorituskykyyn ja markkina-asemaan. Maine rakentuu mielikuvista, näkemyksistä sekä mielipiteistä, joiden perusteella yrityksen sidosryhmät muodostavat yleisarvion yrityksestä. Maineeseen on haastavaa tietoisesti vaikuttaa, etenkin maineen parantamiseen. Tämän vuoksi sen kohdalla on katsottu sopivaksi vastaamiskeinoksi maineriskin eli negatiivisen maineen mahdollisuuden hyväksyminen. Luonnollisesti yrityksessä ei pyritä tietoisesti ottamaan riskejä, jotka uhkaisivat sen mainetta.

Kahdeksaa kappaletta (11 %) analysoiduista riskeistä päädyttiin jakamaan eli hankkimaan vakuutus niiden varalta. Valtaosa näistä liittyy liiketoiminnan erilaisiin häiriötilanteisiin kuten tulipaloihin, vesivahinkoihin ja varkauksiin. Yksi merkittävä vakuuttamisen piirissä oleva riski on rahastojen arvonlaskennan virhe, jonka varalta yrityksellä on toimitusjohtajan ja hallituksen vastuuvakuutus. Sen tarkoituksena on korvata ne varallisuusvahingot, jotka vakuutetut ovat aiheuttaneet toimiessaan vakuutuksenottajan edustajina ja joista vakuutetut ovat voimassa olevan oikeuden mukaan korvausvastuussa.

Riskien tunnistamiskappaleessa oli jo eritelty millä tavoin analysoituja riskejä pyritään ennaltaehkäisemään sekä miten yrityksen toiminnan jatkuvuus varmistetaan, mikäli riski toteutuu. Nämä ovat perustana varasuunnitelmalle kunkin riskin kohdalla.

6.6 Valvontatoimenpiteet

Riskienhallinnan valvonta on suunnitelman laatimisen jälkeen yksi merkittävimmistä vaiheista. Siinä on oleellista, että merkittävät riskit on huolellisesti kartoitettu ja valvontatoimenpiteistä näiden riskien havainnointiin tai korjaamiseen on päätetty. Tähän edellä esitellyn riskienhallintaprosessin on ollut tarkoitus vastata. Prosessissa kartoitetuille operatiivisille riskeille kehitettiin jokaiselle oma mittarinsa. Nämä mittarit on tarkoitus käydä läpi todentavan valvonnan hengessä kerran vuodessa siten, että tarkastellaan niiden toimintaa ja käyttökelpoisuutta. Merkittävää on myös, että valvontatoimenpiteiden toimintaa kontrolloidaan, testataan ja parannetaan tarvittaessa. Käytännössä mikäli jokin edellä mainituista mittareista osoittautuu epäkelvoksi tai sen ei todeta mittaavan tarkoituksenmukaista asiaa, tulee sitä muuttaa.

Jokaiselle hallinnon piiriin kuuluvalle osa-alueelle (arvonlaskenta, asiakas- ja osuusrekisteri, asiakaspalvelu, taloushallinto sekä raportointi ja seuranta) laadittiin tarkistuslistat, jotka käydään läpi säännöllisesti ehkäisevää valvontaa ajatellen. Oleellista on, että tehtävien erillään pito toteutuu mahdollisuuksien mukaan tässä eli tarkastuslistan käy läpi joku muu kuin joka suorittaa kyseistä toimintaa. Yrityksen henkilöstömäärän rajallisuuden vuoksi tähän ei kaikkina aikoina käytännössä kuitenkaan päästä. Oleellista kuitenkin on, että kriittisinä hetkinä (rahastojen merkintäpäivät, tilinpäätöshetki) tarkistuslistat käy läpi joku muu kuin päivittäin kyseisiä tehtäviä suorittava henkilö.

Ohjaavaa valvontaa suoritetaan siten, että saadaan aikaan tai edistetään toivottuja tapahtumia eli saadaan henkilöstö toimimaan halutulla tavalla. Käytännössä tämä tarkoittaa sisäistä valvontaa, jota johtaa hallitus. Päivittäisestä valvonnasta vastaa toimitusjohtaja, joka raportoi hallitukselle. Sisäiseen valvontaan kuuluvat riskien arviointi ja säännösten noudattaminen. Näistä toiminnoista vastaa toimitusjohtaja. Tarkemmin näihin liittyvät periaatteet on määritelty yrityksen sisäisessä muistiossa.

6.7 Informaatio ja tiedonkulku

Sisäisen tiedottamisen periaatteiden rungoksi ja vastuiden selventämiseksi yrityksessä on laadittu dokumentti, jossa on listattu kaikki säännöllisesti raportoitavat ja tiedotettavat asiat vastuuhenkilöineen, kohderyhmineen ja määräaikoineen. Kertaluontoisista

tiedotettavista asioista henkilöstölle vastaa muutoin toimitusjohtaja. Hän on vastuussa myös raportoinnista hallitukselle ja omistajille.
Tiedonkulun varmistamiseksi laadittu riskienhallintamateriaali sijoitetaan yrityksen verkkolevylle siten, että jokaisella työntekijällä on pääsy ja muokkausoikeus siihen. Jokainen työntekijä velvoitetaan myös seuraamaan tilannetta niin, että kun epäkohtia toiminnassa ilmenee, asia otetaan esille välittömästi ja tarkastetaan pitääkö prosesseja tai toimintaohjeita päivittää.

6.8 Seuranta

Riskienhallintasuunnitelmaa seurataan pääasiassa sisäisen valvonnan periaatteita noudattamalla. Yrityksen hallinnosta vastaava henkilö on tässä avainroolissa. Käytännön tason valvontaa suorittavat työntekijät oman toimensa ohessa, sillä heillä on kattavin käytännön tuntemus ja he ovat lähimpänä riskien todellista toteutumista.

Yrityksen ulkopuolista riskienhallinnan seurantaa toteutetaan valvovan viranomaisen sekä säilytysyhteisön toimesta, jotka molemmat tekevät tarkastuksen rahastoyhtiöön noin kerran vuodessa. Tuolloin käydään suullisesti läpi riskienhallinnan nykytila ja varautumisen taso. Heidän ohella myös tilintarkastajat tekevät hallinnon tarkastuksen vuosittain, jossa he käyvät läpi myös riskienhallinnan tasoa. Mikäli tarkastuksissa ilmenee oleellisia puutteita tai kehityskohteita, päivitetään riskienhallintamateriaalia palautteen mukaisesti.

Oleellisin merkitys riskienhallinnan seurannassa on yrityksen sisäisillä toimenpiteillä. Seurantaa voidaan toteuttaa puolivuosittain tarkastettavilla ja tarpeiden mukaan päivitettävillä prosessikuvauksilla, jotka antavat kokonaiskuvan yrityksen sisäisistä prosesseista. Lisäksi merkittävää on riski- ja kontrollimateriaalin säännöllinen tarkastelu ja ajan tasalla pitäminen. Erityisesti huomioon tulee ottaa valvovan viranomaisen antamat määräykset, ohjeistukset ja suositukset. Tarkastelu toteutetaan puolivuosittain siten, että jokainen operatiiviseen työhön osallistuva käy huolellisesti läpi olemassa olevan riskienhallintamateriaalin ja vertaa sitä käytännön työssä eteen tulleisiin riskeihin. Säännöllisten määrämuotoisten tarkastuksien ohella prosessien jatkuva seuraaminen ja parantaminen ovat oleellisia huomioitavia asioita.

Rahastojen arvonlaskennan virheet sekä muut mahdolliset taloudellisiin tappioihin vaikuttaneet tapahtumat dokumentoidaan ja raportoidaan asianmukaisesti yrityksen hallitukselle sekä toimintaa valvoville tahoille. Tarkemmin eritellen kirjataan kuvaus tapahtumasta ja siihen johtaneet syyt, aiheutuneet kustannukset sekä ennaltaehkäisevään ohjeistukseen tehdyt tarkennukset.

7 KEHITTÄMISTEHTÄVÄN TULOKSET

7.1 Tehdyt toimenpiteet

Kehittämistehtävän aikana toteutettiin useita konkreettisia toimenpiteitä, jotka dokumentoitiin. Merkittävin näistä on riskijaottelutaulukko, joka on työn liitteenä 1. Se sisältää yhteenvedon kartoitetuista ja analysoiduista Rahastoyhtiön operatiivisista riskeistä, jotka on jaoteltu ensin osa-alueittain (prosessit, oikeudelliset riskit, henkilöstö, jatkuvuussuunnittelu, varautuminen poikkeusoloihin, tietojärjestelmät, tietoturvallisuus, rikosriskit sekä muut mainittavat asiat toisin sanoen mainekysymys) ja sen jälkeen toiminnoittain (rahastojen arvonlaskenta, asiakas- ja osuusrekisteri, asiakaspalvelu, taloushallinto sekä seuranta ja raportointi). Riskit yksilöitiin juoksevin numeroin. Niistä eriteltiin konkreettinen riskitekijä, käytännön esimerkki kyseisestä riskistä, syyt riskin toteutumiselle, riskin toteutumisen seuraukset, toimenpiteet toteutumisen ennaltaehkäisyksi sekä toiminnan jatkuvuuden varmistaminen riskin toteutuessa. Tämän jälkeen riskit luokiteltiin muodostumislokaation, tietoisuusasteen, vaikutustavan, vakuutettavuuden sekä riskiin vastaamistavan perusteella. Riskit myös arvioitiin toteutumistodennäköisyytensä sekä vaikutuksensa perusteella. Lisäksi jokaiselle riskille laadittiin konkreettinen mittari, selostettiin mittarin käyttöperiaate ja määriteltiin tavoitearvo. Riskeistä myös tunnistettiin toiminnan kannalta olennaiset ja keskeiset riskit. Mittaustulokset esitettiin siten, että tarkasteluperiodin ajalta laskettiin toteutuneiden riskien lukumäärät, kirjattiin huomioita toteutuneista riskeistä. Viimeiseksi laskettiin kuinka moni analysoiduista riskeistä pysyi tavoitearvonsa sisällä.

Kehittämisen kohteena olleista toiminnoista eli rahastojen arvonlaskennasta, asiakas- ja osuusrekisteristä, asiakaspalvelusta, taloushallinnosta sekä seurannasta ja raportoinnista laadittiin prosessikuvaukset. Niissä eriteltiin suoritettavat toimenpiteet, niiden järjes-

tys ja lopputulos. Lisäksi jokaiselle toiminnolle luotiin työohjeet eli vaiheittaiset ja yksityiskohtaiset ohjeet prosessin suorittamiseksi. Lopuksi laadittiin tarkistuslistat, jotka koostuivat yksityiskohtaisesta listauksesta prosessiin liittyvistä tarkistettavista asioista.

Laadittua riskienhallintasuunnitelmaa seurattiin viikoilla 9-26 (27.2.2012 - 28.6.2012). Riskijaottelutaulukossa eriteltyjen riskien ilmenemismäärä mitattiin kyseisellä ajanjaksolla. Lisäksi toimintokohtaisia tarkistuslistoja täytettiin mittausajanjaksolla alaluvussa 4.1 esitellyn aikataulun mukaisesti.

7.2 Ulkopuolisten tahojen palaute

Tarkasteluajanjakson aikana ulkopuolisista valvontaa suorittavista tahoista säilytysyhteisö sekä tilintarkastaja tekivät tarkastuksia rahastoyhtiön ja rahastojen toiminnasta. Näissä suhteissa ulkopuoliset tahot eivät löytäneet oleellista huomautettavaa yrityksen toiminnasta riskienhallinnan näkökulmasta. Palaute tämän kehittämistehtävän mukaisesta riskienhallintasuunnitelman päivityksestä on tulossa myöhemmin syksyllä.

Tästä kappaleesta on salattu tarkempi ulkopuolisten tahojen palaute.

7.3 Mittaustulokset

Alaluvussa 4.3 on esitelty työn mittarit. Koko kehitystehtävän onnistumista mitattiin neljällä eri mittarilla. Ensimmäinen mittauksen kohde oli suunnitelman käyttöönoton onnistuminen ja sovellettavuus eli millä tasolla sitä pystyttiin yrityksessä soveltamaan. Toisena mittauskohteena oli suunnitelman käyttökelpoisuus ja hyödyllisyys yritykselle. Kolmas mittauskohde oli riskienhallinnan laajuus, jota mitataan tunnistettujen riskien lukumäärällä. Neljäntenä mitattiin riskienhallinnan tason optimaalisuutta. Lisäksi laadittua suunnitelmaa mitattiin siten, että jokaiselle yksittäiselle kartoitetulle riskille määriteltiin erikseen oma mittarinsa ja tavoitearvonsa.

7.3.1 Suunnitelman käyttöönoton onnistuminen ja sovellettavuus

Ensimmäinen mittauksen kohde oli suunnitelman käyttöönoton onnistuminen ja sovellettavuus eli millä tasolla sitä pystyttiin yrityksessä soveltamaan. Tätä varten laadittiin

tarkistuslistat (lista suoritetuista toimenpiteistä, jotka kuitataan tarkastetuksi läpi käymisen jälkeen), joiden avulla käytiin läpi riskiprosessien yksityiskohdat ja dokumentoitiin ne. Tavoitteena oli, että listoista tulee täytetyksi vähintään 90 %.

Tuloksena oli, että 71 kaiken kaikkiaan 84 listasta (85 %) tuli täytettyä. Kaikki raportoinnin ja asiakaspalvelun listat (neljä per osa-alue) täytettiin. Osuusrekisterin osalta täytettyä tuli kolme neljästä. Merkittävin vajaus tuli arvonlaskennassa, jossa oli myös eniten täytettäviä listoja. Tavoitteena olleesta 72 listasta täytetyiksi tuli 60 kappaletta (83 %). Pääosin viimeksi mainittu johti siihen, että kokonaisuutena jäätiin viisi prosenttiyksikköä tavoitteesta.

Täytettyjen listojen lukumäärää oleellisempaa informaatiota saatiin kuitenkin itse listojen sisällöstä eli tehdyistä normaalista poikkeavista huomioista. Asiakaspalvelun yksi tarkastuslista käsitti 14 tarkastuskohtaa eli yhteensä tarkasteluajanjakson aikana käytiin läpi 56 kohtaa. Näistä 43 kappaletta (77 %) sai arvon nolla eli kyseisessä asiassa ei ollut huomautettavaa. Arvonlaskennan tarkastuslistat käsittivät yhteensä 48 kohtaa. Kaiken kaikkiaan arvonlaskennan osalta tarkistettuja yksittäisiä asioita oli siis 1 500 kappaletta. Huomautuksia näistä löytyi vain yhdeksästä kohtaa, joten 99,4 % arvonlaskennan tarkistuskohteista oli asianmukaisia. Osuusrekisterin osalta tarkistuslistojen myötä ei löytynyt merkittävää korjattavaa. Raportoinnin osalta käytiin läpi 79 kohtaa, joista 17 (22 %) osalta löytyi huomautettavaa. Näistä kolme laskettiin merkittäviin huomioihin. Muilla ei ollut käytännön toiminnan kannalta mainittavaa merkitystä.

7.3.2 Suunnitelman käyttökelpoisuus ja hyödyllisyys yritykselle

Toisena mittauskohteena oli suunnitelman käyttökelpoisuus ja hyödyllisyys yritykselle. Tämä toteutettiin nykytila- ja loppuanalyyseillä. Näistä saatuja tuloksia verrattiin keskenään ja sen perusteella subjektiivisella yrityksen sisäisellä arvioinnilla mitattiin kuinka paljon riskienhallintaprosessi parantui. Käytännössä laskettiin kuinka moni viitekehyksen määrittelemä riskienhallinnan osa-alue katsottiin parantuneeksi. Tavoitearvo oli yli 50 %. Koska yrityksen riskienhallintaa ei ollut aiemmin tarkasteltu yhtä kokonaisvaltaisesta lähtökohdasta kuin COSO ERM - mallin esittelemässä laajuudessa, voidaan todeta tämän kehittämistehtävän myötä kaikkien osa-alueiden parantuneen. Perusteluina ovat

tehty taustatyö sekä ensimmäistä kertaa näin laaja-alaisesti toteutettu riskien analysointi ja dokumentaatio.

7.3.3 Riskienhallinnan laajuus

Kolmas mittauskohde oli riskienhallinnan laajuus, jota mitattiin tunnistettujen riskien määrällä. Lukumäärä laskettiin ja sitä verrattiin alkutilanteeseen. Tavoitteena oli, että tunnistettujen riskien määrä on suurempi kuin lähtöarvo.

Tuloksena oli, että kahdeksanvaiheisen COSO ERM -malliin soveltuvan prosessin tuloksena tunnistettiin 76 riskiä. Tavoitteeseen päästiin selkeästi, sillä aiemmin riskienhallinnan periaatteita ei yrityksessä ole kartoitettu vastaavassa laajuudessa selkeään teoriapohjaan nojaten. Täten myöskään selkeästi nimettyjä konkreettisen tason riskejä ei ole systemaattisesti kirjattu.

7.3.4 Riskienhallinnan tason optimaalisuus

Neljäntenä mitattiin riskienhallinnan tason optimaalisuutta, joka määriteltiin siten, että riskienhallinnan katsotaan olevan optimaalinen kun operatiivisessa toiminnassa ei ilmene sellaisia virheitä, joiden vuoksi yritys joutuisi korvausvastuuseen ulkopuolisten tahojen suuntaan. Tätä mitattiin toteutuneen korvausvastuun suuruudella. Mikäli korvausvastuuta olisi realisoitunut, sen euromäärä olisi suhteutettu yrityksen taseeseen. Tavoitteena oli, että missään tapauksessa euromäärä ei ylittäisi 1 % edellisen tilikauden taseen arvosta. Tuloksena oli, että mittausajanjakson aikana riskienhallintaprosessi toimi kuten oli tarkoituskin eli erillistä korvausvastuuta ei yrityksen ulkopuolisille tahoille realisoitunut.

7.3.5 Riskienhallintasuunnitelman mittaus

Kehittämistehtävän yhtenä tarkoituksena oli mitata laadittua suunnitelmaa. Tämä toteutettiin siten, että analysoiduille operatiivisille riskeille määriteltiin jokaiselle oma mittarinsa. Niiden tuottamaa dataa mitattiin koko tarkasteluajanjaksolla eli vuoden 2012 helmikuusta kesäkuun loppuun.

Tuloksena oli, että kartoitetuista 76 riskistä seurattiin 68:aa (89 %). Loput kahdeksan riskiä laskettiin kuuluvaksi taloushallintoon, jonka seuraaminen jätettiin kehittämistehtävän ulkopuolelle resurssisyistä. Jokaiselle kartoitetulle riskille määriteltiin tavoitearvo. Näiden arvojen sisälle mahtui 52 riskiä (76 %). Kaikista riskeistä olennaisiksi luokiteltiin 40 kappaletta. Näistä 31 kappaletta (78 %) oli tavoitearvon sisällä.

7.4 Vastaukset tutkimusongelmaan ja -kysymyksiin

Kehittämistehtävän tavoitteena oli Rahastoyhtiön kokonaisvaltaisen riskienhallintasuunnitelman laatiminen ja dokumentointi. Erityisesti tarkoituksena oli eritellä, miten operatiivisia riskejä kyetään tunnistamaan, määrittelemään sekä mittaamaan. Tässä onnistuttiin hyvin, sillä tunnistettujen riskien lukumäärä oli verrattain suuri ja niiden avulla tarkastellut osa-alueet tuli kartoitettua kattavasti. Suunnitelman dokumentointi tuli toteutettua perusteellisesti. Mittausvaiheessa tulivat vastaan työn suurimmat haasteet, sillä tuolloin yrityksen sisällä käytiin läpi monta suurta muutosta. Näiden vuoksi erityisesti kehittämistehtävästä vastaavan työnkuva muuttui niin radikaalisti, että suurin osa huomiosta tuli kohdistaa yrityksen päivittäisten rutiinien hoitamiseen. Sen vuoksi mittausjaksoon ei kyetty enää panostamaan täysimittaisesti, jonka vuoksi se jäi osittain vajavaiseksi. Suunnitelma itsessään tuli kuitenkin toteutettua ja käytäntöön soveltaminenkin saatiin alkuun. Yrityksellä on siis käytössään hyvät lähtökohdat riskienhallinnan jatkokehitykselle.

Ensimmäisen tutkimuskysymyksen tavoitteena oli kartoittaa mitkä ovat rahastoyhtiölle tyypillisiä hallinnon operatiivisia riskejä, joilta halutaan suojautua. Tuloksena oli Excel-taulukon muotoon laadittu riskijaottelulista, jossa käytiin läpi osa-alueittain yrityksen prosessit, oikeudelliset riskit, henkilöstö, jatkuvuussuunnittelu, varautuminen poikkeusoloihin, tietojärjestelmät, tietoturvallisuus, rikosriskit sekä muut mainittavat asiat, tässä tapauksessa mainekysymys. Näin eritellyt riskit on esitelty liitteessä 1.

Toinen tutkimuskysymys käsitteli sitä, miten suojautuminen toteutetaan käytännön tasolla. Tämä ratkaistiin niin, että laadittiin listaus edellä mainitun riskijaottelun perusteella ennaltaehkäisevistä toimenpiteistä riskeittäin. Lisäksi osa-alueittain laadittiin erilliset tarkistuslistat, joiden avulla käydään läpi säännöllisesti erikseen määritellyn aikataulun puitteissa kuhunkin toimintoon liittyvät huomioitavat asiat.

Kolmas tutkimuskysymys etsi vastausta siihen, miten riskienhallintatoimintoa hyödynnetään ja kehitetään edelleen. Tarkoituksena on tehdä riskienhallintasuunnitelman päivitys puolivuosittain. Tähän paneudutaan vielä tarkemmin seuraavassa pääluvussa.

Kaikki tutkimuskysymykset kokonaisuudessaan tähtäsivät tutkimusongelman ratkaisuun eli miten Rahastoyhtiön operatiivisen työn riskienhallintaa saadaan parannettua niin että se palvelee yritystä optimaalisella tavalla. Tutkimusongelma tuli yrityksen toiminnan laajuus ja luonne huomioiden käsiteltyä laajasti ja perusteellisesti. Ongelma siis kyettiin ratkaisemaan.

7.5 Loppuanalyysi

Loppuanalyysissa tarkasteltiin yrityksen operatiivisten riskien hallinnan tilaa suunnitelman laadinnan ja mittausajanjakson jälkeen. Tuloksena oli, että yrityksen riskienhallinta on tällä hetkellä varmemmalla ja vakaammalla pohjalla kuin aiemmin sen vuoksi, että riskilähteitä on käyty läpi systemaattisesti. Niitä on analysoitu laajasti ja prosessi on dokumentoitu kirjalliseen muotoon. Operatiivisten riskien luonteesta johtuen kaikkia mahdollisia riskejä on lähestulkoon mahdoton listata, joten analyysiä on varmasti vielä syytä täydentää tulevaisuudessa. Kaikilla yrityksen työntekijöillä on tällä hetkellä pääsy riskienhallintamateriaaliin, joten riskijaottelua ja toimenpidelistaa on mahdollista päivittää heti kun korjattavaa tai lisättävää ilmenee.

Alussa kappaleessa 2.2 esitellyssä nykytila-analyysissä tuotiin esille yrityksen merkittävimpiä riskien lähteitä. Näihin laskettiin kuuluviksi henkilöstö, tietojärjestelmät ja toimintojen organisointi. Henkilöstön osalta merkittävin riskitekijä olivat ja ovat edelleen inhimilliset virheet, joilta ei missään olosuhteissa voida kokonaan välttyä. Riskipaikkojen tunnistamisella, tuplatarkistuksilla sekä riittävä aika ja työrauha takaamalla voidaan virheitä vähentää ja niiden aiheuttamia vahinkoja pienentää. Konkreettisista toimenpiteistä merkittävin on toiminnoittain laaditut tarkistuslistat, joiden perusteella käydään kuhunkin toimintoon liittyvät keskeiset ja kriittiset toimenpiteet läpi. Listojen tarkoitus on auttaa inhimillisten virheiden tunnistamisessa ja kaikkien oleellisten seikkojen huomioinnissa.

Tietojärjestelmien luotettavuus korostuu erityisesti rahastojen arvonlaskentaprosessissa. Siirtymäaika aiemmasta taulukkolaskentakäytännöstä osuusrekisteripohjaiseen arvonlaskentaan on venynyt alkuperäisestä suunnitelmasta. Tämä on kuitenkin esimerkki siitä, miten sisäisen testauksen kautta halutaan käytettävissä olevan osaamisen puitteissa varmistaa, että prosessin toimivuus on riittävän luotettavalla tasolla ennen kuin uuteen järjestelmään siirrytään täysin.

Toimintojen organisointi riskienhallintanäkökulmasta on järjestetty niin, että yrityksen hallinnossa on yksi vastuuhenkilö, joka jakaa näihin liittyvät tehtävät toimihenkilöille. Toiminnoista on haluttu luoda selkeä kokonaiskuva, josta käy ilmi toimintojen riippuvuussuhteet ja linkittyminen toisiinsa.

Riskienhallintaa itsessään on tuotu aiempaa enemmän mukaan päivittäiseen operatiiviseen toimintaan siten, että tarkastuslistakäytäntö kulkisi luonnollisena osana viikoittaisissa ja kuukausittaisissa rutiineissa mukana. Tällä on pyritty siihen, ettei riskienhallinta jäisi irralliseksi ja kaukaiseksi vaan liittyisi osaksi työkäytänteitä. Yrityksen ollessa muutosvaiheessa henkilöstön vaihtuvuuden vuoksi tämäntyyppisten asioiden tuominen mukaan säännöllisiin työrutiineihin voi olla helpompaa kuin vakiintuneiden käytänteiden muuttaminen. Toisaalta varteenotettavana riskinä voi olla myös näiden seikkojen jääminen muiden uusien asioiden jalkoihin, ellei työkäytäntöjä lähdetä aktiivisesti heti rakentamaan. Yhden vastuuhenkilön nimeämisellä tätä pyritään kuitenkin ehkäisemään.

8 JOHTOPÄÄTÖKSET JA JATKOTOIMENPITEET

8.1 Viitekehyksen soveltuvuus aiheeseen

Valittu teoreettinen viitekehys tuki Rahastoyhtiön operatiivisten riskien hallinnan uudelleenorganisointia, sillä sen avulla pystyttiin vastaamaan asetettuihin tutkimuskysymyksiin ja ratkaisemaan tutkimusongelma. Ensimmäiseen tutkimuskysymykseen vastaus saatiin Gahinin riskimallin sekä Erolan ja Loudon riskikriteerien perusteella. Kuviota täydensi erityisesti alan toimijoille suunnattu Finanssivalvonnan standardi operatiivisten riskien hallinnasta, jossa on esitelty kattava riskijaottelu.

Toiseen tutkimuskysymykseen vastattiin laaditulla riskienhallintasuunnitelmalla, joka rakentui pääosin COSO ERM -mallin kahdeksan osatekijän pohjalle. Niiden perusteella saatiin luotua kattava suunnitelma, jossa käsiteltiin koko riskienhallintaprosessin kaari. Teoriassa vaiheistettiin riskienhallinnan prosessin kulku ja ohjeistettiin periaatteiden vieminen käytännön tasolle. Malli myös tarjosi selkeitä toimintaohjeita. Vaiheita ja niiden käsittelyä tuli tosin yksinkertaistettua, sillä alkuperäinen malli on selkeästi tarkoitettu suurempien yritysten käyttöön, joiden toiminta on laajamittaisempaa. Teoreettisessa mallissa oli siten aineksia laajemmankin suunnitelman laadintaan.

Kolmanteen tutkimuskysymykseen paneudutaan tarkemmin työn viimeisessä alaluvussa. Valittu teoreettinen viitekehys kokonaisuudessaan pystyi ratkaisemaan asetetun tutkimusongelman. Operatiivisen työn riskienhallinta parani oleellisilta osin ja pystyy tätä nykyä tukemaan yrityksen ydinliiketoimintaa ansiokkaasti.

8.2 Päättöreflektointi ja yhteenveto

Kehittämistehtävän tavoitteena oli organisoida ja toteuttaa Rahastoyhtiön operatiivinen riskienhallinta alkutilannetta kokonaisvaltaisemmasta lähtökohdasta. Työn konkreettisena tarkoituksena oli luoda riskienhallintasuunnitelma, jossa on esitelty operatiivisten riskien hallintaan liittyvät toimenpiteet. Tavoitteena oli saada luotua niin yksityiskohtainen, kattava, selkeä ja käyttökelpoinen suunnitelma, että sen liittäminen osaksi yrityksen jokapäiväisiä rutiineja olisi vaivatonta.

Kokonaisuudessaan kehittämistehtävän tavoitteet saavutettiin hyvin. Tavoitteet oli kirjattu niin, että ne painottuivat pääosin lopputuloksiin, mutta itse projektissa myös prosessi asettui merkittävään rooliin. Toimintatutkimuksellista spiraalia (toiminnan suunnittelu > muutoksen toteutus > muutoksen vaikutusten seuranta ja arviointi > toiminnan suunnittelu jne.) ajatellen valtaosa tehdyistä työtunneista painottuivat ensivaiheeseen eli toiminnan suunnitteluun sisältäen toimintaympäristön eli operatiivisen riskikentän kartoituksen. Perusteellisen kartoituksen jälkeen suunnitelman laatiminen ja kirjaaminen luonnistuivat hyvin. Tätä kautta tutkimuskysymyksiin löytyivät vastaukset ja niiden kautta myös alkuperäinen tutkimusongelma saatiin ratkaistua.

Kuten edellä on useasti tuotu esiin, sijoitusalalla tulee myös viranomaismääräykset ottaa aktiivisesti huomioon. Näihin liittyen merkittävä muutos on ollut EU-tason sijoitusrahastodirektiivi (UCITS IV) mikä asettaa lisävelvoitteita rahastoyhtiöiden riskienhallinnalle. Direktiivin keskeinen sisältö on, että riskienhallinta tulee ottaa selkeämmin mukaan rahastoyhtiön päivittäisiin rutiineihin. Tähän kehittämistehtävän aihe ja tutkimusasetelma nojattiin vahvasti. Lopputuloksen on yrityksessä katsottu olevan uuden direktiivin määräysten sekä voimassaolevien Finanssivalvonnan standardien mukainen.

Kehittämistehtävän aihe oli hyvin käytännönläheinen ja oleellinen osa yrityksen toimintaa. Tästä huolimatta on syytä huomioida, että projektissa keskityttiin enemmän taloudellisten tappioiden välttämiseen kuin esimerkiksi yrityksen tuloksen aktiiviseen kasvattamiseen. Tässä suhteessa haasteeksi osoittautui tulosten mittaaminen, sillä vajaan puolen vuoden tarkasteluajanjaksolla ei varmasti pystytä saamaan kaikkia potentiaalisia riskilähteitä esiin.

Työn onnistumisen kannalta ansioksi nousi kehittämistehtävän toteuttajan aktiivinen rooli ja panostus aiheeseen tutkimuksen suorittajana. Vaikka osaltaan tämä oli käytännön sanelema asia henkilöstönvaihdoksista johtuen, antoi se sopivasti haastetta sekä mahdollisuuksia päästä kehittämään yrityksen toimintaa. Suoritettujen mittauksien ja niiden tuottamien tulosten perusteella kohdeyrityksen riskienhallintaan on tuotu ainakin operatiivisen työn näkökulmasta hallittua kokonaisvaltaista lähestymistapaa. Näiden edellytyksien pohjalta yrityksen on mahdollista lähteä jatkokehittämään myös muita toimintoja.

8.3 Jatkotoimenpide-ehdotukset

Kehittämistehtävän kolmas tutkimuskysymys liittyi riskienhallintatoiminnon hyödyntämiseen ja jatkokehittämiseen. Jotta tehdylle työlle ja laaditulle suunnitelmalle saadaan jatkuvuutta, on tarkoituksena päivittää riskienhallintasuunnitelmaa puolivuosittain. Kehittämistehtävän myötä kävi myös ilmi, että toiminnassa on vielä jatkokehittämistarpeita. Yrityksen operatiivinen puoli riskeineen tuli käsiteltyä hyvinkin kattavasti, mutta myös muille toiminnoille tulisi kehittää riskienhallintasuunnitelmat. Tämän tulisi sisältää erityisesti riskien kartoittamisosio, sillä se osoittautui toimivan ja hyödynnettävissä olevan suunnitelman peruskiveksi. Jo laadittua suunnitelmaa voi vielä tarkentaa ja paran-

taa taloushallinnon osatekijöiden suhteen, sillä ne jäivät tämän kehittämisprojektin puitteissa vähemmälle huomiolle käytännön resurssisyistä johtuen. Muilta osin suunnitelma voi toimia perusrunkona myös muiden toimintojen riskikartoituksille.

Konkreettinen työ yrityksessä tämän kehittämistehtävän esittelemissä puitteissa jatkuu edelleen. Tässä suhteessa työllä on kuitenkin hyvät jatkohyödyntämismahdollisuudet kun seurantamittaristo on laadittuna pidempää tarkasteluajanjaksoa varten.

Lähteet

About ISO 2011. International Organization for Standardization. Http://www.iso.org/iso/about.htm. Luettu 8.1.2012.

Ahokas, Niina 2009. Sisäinen valvonta ja SOX. Code of Conduct. Http://www.codeofconduct.fi/sisainen-valvonta-ja-sox2/. Luettu 7.1.2012.

A Risk Management Standard 2003. Federation of European Risk Management Associations. Http://www.ferma.eu/wp-content/uploads/2011/11/a-risk-management-standard-english-version.pdf. Luettu 8.1.2012.

AS/NZS 4360:2004 Risk management 2004. SAI Global InfoStore. Http://infostore.saiglobal.com/store/Details.aspx?productID=381579. Luettu 7.1.2012.

Blumme, Nils ym. 2005. Corporate Governance sisäisen valvonnan ja riskienhallinnan näkökulmasta. Edita, Helsinki.

Coso: About us. The Committee of Sponsoring Organizations of the Treadway Commission. Http://www.coso.org/aboutus.htm. Luettu 15.11.2011.

Erola, Eero & Louto, Pentti 2000. Riskit voimavaraksi - liiketoimintariskien hallinta yrityksessä. Edita, Helsinki.

Finanssivalvonnan standardi 1.3 Luotettava hallinto ja toiminnan järjestäminen 2007. Finanssivalvonta. Annettu 26.10.2007. Http://www.finanssivalvonta.fi/fi/Saantely/Maarayskokoelma/Rahoitussektori/1_Hallinto kulttuuri_ja_liiketoiminta/Documents/1.3.std1.pdf. Luettu 22.12.2011.

Finanssivalvonnan standardi 4.1 Sisäisen valvonnan järjestäminen 2003. Finanssivalvonta. Http://www.finanssivalvonta.fi/fi/Saantely/Maarayskokoelma/Rahoitussektori/4_Vakava raisuus_ja_riskien_hallinta/Documents/4.1.std3.pdf. Päivitetty 16.12.2008.

Finanssivalvonnan standardi 4.4.b Operatiivisten riskien hallinta 2004. Finanssivalvonta. Päivitetty 12.10.2010. Http://www.finanssivalvonta.fi/fi/Saantely/Maarayskokoelma/Rahoitussektori/4_Vakava raisuus_ja_riskien_hallinta/Documents/4.4b.std4.pdf. Luettu 10.11.2011.

Flink, Anna-Liisa & Reiman, Teemu & Hiltunen, Mika 2007. Heikoin lenkki? Riskienhallinnan inhimilliset tekijät. Edita, Helsinki.

Hallinnolliset seuraamukset, 2011. Finanssivalvonta. Päivitetty 11.5.2011. Http://www.finanssivalvonta.fi/fi/Saantely/Hallinnolliset_seuraamukset/Pages/Default.aspx. Luettu 23.8.2012.

Ilmonen, Ilkka & Kallio, Jani & Koskinen, Jani & Rajamäki Markku 2010. Johda riskejä - käytännön opas yrityksen riskienhallintaan. Tammi, Helsinki.

ISO/IEC 31010:2009 2011. International Organization for Standardization. Http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51073. Luettu 8.1.2012.

Juvonen, Marko & Korhonen, Heikki & Ojala, Veli Matti & Salonen, Tero & Vuori, Heli 2005. Yrityksen riskienhallinta. Suomen vakuutusalan koulutus ja kustannus Oy, Helsinki.

Kirppu, Paula 2010. UCITS IV -direktiivin mukana tulevat keskeiset muutokset. Finanssivalvonta. Esitys 2.6.2010.

KvaliMOTV:Reliabiliteetti. Yhteiskuntatieteellinen tietoarkisto, menetelmäopetuksen tietovaranto. Http://www.fsd.uta.fi/menetelmaopetus/kvali/L3_3_2.html. Luettu 18.12.2011.

KvaliMOTV: Validiteetti. Yhteiskuntatieteellinen tietoarkisto, menetelmäopetuksen tietovaranto. Http://www.fsd.uta.fi/menetelmaopetus/kvali/L3_3_1.html. Luettu 18.12.2011.

Menetelmät. VTT. Http://www.vtt.fi/proj/riskianalyysit/riskianalyysit_menetelmat.jsp. Luettu 20.2.2012.

Moeller, Robert R. 2007. COSO enterprise risk management: establishing effective governance, risk, and compliance processes. 2. painos. John Wiley & Sons, Inc., Hoboken, New Jersey.

Potentiaalisten ongelmien analyysi. VTT. Http://www.vtt.fi/proj/riskianalyysit/riskianalyysit_potentiaalisten_ongelmien_analyysi_poa_mk.jsp. Luettu 20.2.2012.

Puttonen, Vesa & Repo, Eljas 2003. Miten sijoitan rahastoihin. WSOY, Helsinki.

Rahastoyhtiöiden markkinaosuudet. Finanssivalvonta. Päivitetty 24.4.2012. Http://www.finanssivalvonta.fi/FI/TILASTOT/ARVOPAPERIMARKKINAT/RAHASTOYHTIOIDEN_MARKKINAOSUUDET/Pages/Default.aspx. Luettu 18.5.2012.

Rahastoyhtiöt 2010. Finanssivalvonta. Päivitetty 24.11.2010. Http://www.finanssivalvonta.fi/fi/Finanssiasiakas/Palveluntarjoajat/Sijoitusala/Rahastoyhtiot/Pages/Default.aspx. Luettu 14.11.2011.

Rahoitussektorin määräyskokoelma. Finanssivalvonta. Päivitetty 7.10.2011. Http://www.finanssivalvonta.fi/FI/SAANTELY/MAARAYSKOKOELMA/RAHOITUSSEKTORI/Pages/Default.aspx. Luettu 15.5.2012.

Riskienhallinnan hyödyt 2009. VTT/Pk-yrityksen riskienhallinta. Http://www.pk-rh.com/startti-riskienhallintaan/riskienhallinnan-hyodyt.html. Luettu 10.11.2011.

Sijoitusrahasto-opas 2009. Suomen pörssisäätiö. Päivitetty 12.3.2009. Http://www.porssisaatio.fi/artikkelit/sijoitusrahasto-opas,12. Luettu 14.11.2011.

Sisäinen valvonta ja riskienhallinta 2012. Elektrobit Oyj. Http://www.elektrobit.com/sijoittajat/hallinto-_ja_ohjausjarjestelma/sisainen_valvonta_ja_riskienhallinta. Luettu 10.11.2011.

Suojanen, Ulla 1992. Toimintatutkimus koulutuksen ja ammatillisen kehittymisen välineenä. Oy Finn Lectura Ab, Helsinki.

Suominen, Arto 2003. Riskienhallinta. 3. painos. WSOY, Helsinki.

Tietoa Finanssivalvonnasta. 2011. Finanssivalvonta. Päivitetty 12.9.2011. Http://www.finanssivalvonta.fi/fi/Fiva/Pages/Default.aspx. Luettu 10.11.2011.

Toimintatutkimus. Ylemmän AMK- tutkinnon metodifoorumi. Http://www.amk.fi/opintojaksot/0709019/1193463890749/1193464158778/1194360111832/1194360447229.html. Luettu 18.5.2012.

Toimintovirheanalyysi. VTT. Http://www.vtt.fi/proj/riskianalyysit/riskianalyysit_toimintovirheanalyysi_tva_mk.jsp. Luettu 20.2.2012.

Toimitusjohtajan ja hallituksen vastuuvakuutus. Pohjola Pankki Oyj. Https://www.pohjola.fi/pohjola/yritys--ja-yhteisoasiakkaat/vakuutukset/vakuutustuotteet/toiminnan-vakuutukset/toimitusjohtajan-ja-hallituksen-vastuuvakuutus?cid=330802624&srcpl=3. Luettu 23.12.2011.

Wesanko, Jyri 2010. Riskienhallintaprosessi ja operatiivisten riskien kvantifiointi. Tutkielma. Turvallisuusjohdon koulutusohjelma. Teknillinen korkeakoulu. Http://lib.tkk.fi/Reports/2010/urn100176.pdf. Luettu 8.1.2012.

What is FERMA? 2011. Federation of European Risk Management Associations. Http://www.ferma.eu/about/mission-and-objectives/what-is-ferma/. Luettu 7.1.2012.

Örndahl, Johanna 2011. UCITS IV -direktiivi: Keskeinen sisältö ja sen vaikutukset. Finanssivalvonta. Esitys 18.10.2011.

Liitteet

Liite 1. *Riskijaottelu (Salainen)*