# RISKIENHALLINTA
# Riskiraportoinnin ja riskienhallinnan kehittyminen - Case Kemira Oyj, Neste Oil Oyj, Aspo Oyj ja Finnlines Oyj

Organisaatiot ja johtaminen
Maisterin tutkinnon tutkielma
Mia-Stiina Heikkala
2009

**Markkinoinnin ja johtamisen laitos**
HELSINGIN KAUPPAKORKEAKOULU
HELSINKI SCHOOL OF ECONOMICS

*Parhaalle ystävälleni ja miehelleni Janille*

*”We don´t do things because they´re easy. We do them because they are hard.”*

*John F. Kennedy*

**Sisällysluettelo**

## Kuvaluettelo



## Taulukkoluettelo

# 1 Johdanto

Tutkielman tausta ja motivaatio

Tutkielman aihe on neljän listatun yrityksen riskiraportoinnin ja riskienhallinnan kehittyminen julkisen aineiston eli vuosikertomus- ja tilinpäätösinformaation avulla. Tutkimuksen kohdeyrityksinä ovat Kemira, Neste Oil, Aspo ja Finnlines. Tutkielman aihepiiri liittyy valveutuneempien ja aktiivisempien omistajien lisääntyneisiin vaatimuksiin saada tietoa omistamiensa yritysten hallintotavasta, riskienhallinnasta sekä monen suuntaisesta vuoropuhelusta. Tällä tavalla pyritään tuomaan läpinäkyvyyttä yritysten toimintaan. Omistajien etuja palvelemaan on luotu yhä tiukentuneempia suosituksia, jotka määrittelevät muun muassa, miten listattujen yritysten tulee raportoida riskienhallinnastaan. Yritysten riskienhallinnan raportointi muodostaa keskeisen kanavan, jonka avulla omistajat voivat nähdä, miten yritykset hallitsevat riskejään sekä millainen on niiden suhtautuminen riskeihin. Tätä muutosta kuvaa myös se, kuinka sanan riski esiintyminen on lisääntynyt tutkielman kohdeyritysten vuosikertomus- ja tilinpäätösinformaatiossa. Esiintymiskerrat ovat lisääntyneet seuraavasti: Kemira vuonna 2005: 88 ja vuonna 2007: 214; Neste Oil vuonna 2005: 182 ja vuonna 2007: 219; Aspo vuonna 2005: 46 ja vuonna 2007: 81; Finnlines vuonna 2005: 31 ja vuonna 2007: 55. Sanan riski esiintyminen on siis kaksinkertaistunut kahdessa vuodessa. Myös pääoman painopiste on siirtynyt perinteisestä aineellisesta pääomasta aineettomaan, inhimilliseen pääomaan, joten sijoittajien on saatava tietää, millä tavalla yrityksiä johdetaan. Sijoittajien näkökulmasta on siis tärkeää ottaa huomioon yritysten toteuttama hallinnointitapa, jonka avulla voidaan pyrkiä tehokkaampaan riskienhallintaan, kestävämpään toimintaan sekä parempaan pääoman tuottoasteeseen.

## Tutkielman tavoitteet ja rajaukset

Tutkielmani päätavoitteena on verrata tutkielman kohdeyritysten Kemiran, Neste Oilin, Aspon ja Finnlinesin riskiraportoinnin ja riskienhallinnan kehittyneisyyttä COSO ERM-viitekehyksen vaatimuksiin ja selvittää, täyttävätkö kohdeyritysten riskiraportointi ja riskienhallinta nämä vaatimukset. Samalla arvioin, kuinka kohdeyritysten riskienhallinta on kehittynyt vuodesta 2005 vuoteen 2007. Havainnoin myös, miten hyvin tutkielman kohdeyritysten riskienhallinta vastaa sidosryhmien, lainsäädännön ja suositusten vaatimuksia. Teen tutkimuksen perustuen julkiseen vuosikertomus- ja tilinpäätösaineistoon sisältyvään riskienhallintaa koskevan tietoon.

Tutkielmani viitekehikoksi olen valinnut kansainvälisen riskienhallinnan viitekehikon COSO ERM -mallin, jota vasten analysoin kohdeyritysten riskiraportoinnin ja riskienhallinnan tasoa. COSO ERM -mallista ei ole saatavilla kovin paljon tutkimusaineistoa, koska sen tutkiminen on vielä lapsenkengissä. Yleisenä suuntauksena näyttäisi kuitenkin olevan, että sen puitteissa tullaan tekemään myös akateemista tutkimusta. Esimerkiksi kansainvälinen sisäisen tarkastuksen ammattijärjestö IIA (Institute of Internal Auditors) Research Foundation keskittyy riskienhallinnan tutkimukseen (IIA). COSO ERM -mallin soveltamisesta ei siis löydy paljon tutkimustietoa, mutta käytännössä mallia sovelletaan yleisesti sekä Suomessa että kansainvälisesti. Vuosikertomusten ja tilinpäätösten sisältö riskienhallinnan osalta on vaihtelevaa ja monitulkintaista. Ne toimivat usein ainoana kanavana, jonka avulla sijoittajat voivat hahmottaa, kannattaako johonkin yritykseen sijoittaa: kykeneekö yritys hallitsemaan riskejään vai onko se liian halukas ottamaan niitä. Tutkielman empiirinen aineisto pohjautuu kohdeyritysten antamaan julkiseen vuosikertomus- ja tilinpäätösinformaatioon. Samaa informaatiota käyttävät analyytikot, sijoittajat ja omistajat analysoidessaan yritysten riskienhallinnan tasoa. Oman haasteensa tähän tuo se, miten tutkielman kirjoittaja tulkitsee vuosikertomusten ja tilinpäätösten tekstiä. Tutkijan rooli siis vaikuttaa tulkinnan lopulliseen tulokseen. Sama koskee analyytikoiden tekemiä tilinpäätösanalyyseja, joissa ei ole olemassa yhtä ainoaa totuutta vaan tulkintoja on yhtä monta kuin tulkitsijoita. Pyrin kuitenkin viemään tutkimusaineistoa viitekehikon pohjalta mahdollisimman objektiivisesti eteen-

päin. On myös tärkeää muistaa, että julkinen, kirjallisessa muodossa oleva materiaali voi rajata tulkinnan mahdollisuuksia, koska analysoin riskienhallinnan kehittymistä tutkimusaineiston alkuperäisen muodon perusteella.

## Tutkimusmenetelmä

Tutkielmani aineisto koostuu neljän suomalaisen pörssiyrityksen vuosikertomus- ja tilinpäätösinformaatiosta vuosilta 2005 ja 2007. Riskienhallintaa koskevan tiedon lisäksi olen poiminut asioita vuosikertomus- ja tilinpäätösmateriaalin muista osioista, jotka tukevat tutkielman empiiristä analyysia, esimerkiksi sisäisen toimintaympäristön ja tavoitteenasettelun osioissa. Olen myös lainannut vuosikertomus- ja tilinpäätösmateriaalien tekstiä muuntelemattomana, jotta lukija pystyisi yhdistämään tekstin alkuperäisen kontekstin tutkielman analyysiin.

Keskityn tutkielmassani neljän listatun yrityksen riskienhallinnan kehittymisen analysointiin. Pyrin muodostamaan jokaisen kohdeyrityksen riskienhallinnan kehittymisestä mahdollisimman todenmukaisen kuvan. Tutkielmassa käytetyn COSO ERM-viitekehyksen tehtävänä on toimia ainoastaan suosituksena, miten riskienhallinnasta tulisi raportoida, eikä yksityiskohtaisena ohjeistuksena. Olen poiminut tutkielmaan tutkimusaineiston tekstiä sen alkuperäisessä muodossa, koska tarkoituksena on muodostaa mahdollisimman objektiivinen kuva riskienhallinnan kehittymisestä. Täten ei synny mahdollisuutta, että tutkielman kirjoittaja olisi muokannut tekstiä omien tarpeidensa mukaisesti. Tutkielman tuloksia ei myöskään tule yleistää, koska tutkimusotos sisältää vain neljä pörssiyritystä, joiden riskiraportoinnin kehittymistä analysoidaan yhden tutkijan näkökulmasta käsin. Tarkoitus ei myöskään ole muodostaa kokonaiskuvaa listattujen yritysten riskienhallinnan kehittymisen tasosta, vaan hahmottaa, miten yritykset ovat raportoineet riskienhallinnastaan, miten riskeistä raportoiminen on kehittynyt vuodesta 2005 vuoteen 2007 ja täyttääkö näiden kohdeyritysten riskiraportointi COSO ERM -viitekehikon sekä lainsäädännön ja suositusten vaatimukset sekä sijoittajien tavoitteet.

## Keskeiset käsitteet

Klassisen riskienhallinnan terminologia on pysynyt hämmästyttävän samansisältöisenä vuosikymmenestä toiseen (Kuusela & Ollikainen 2005, 155). Seuraavaksi käyn läpi keskeisimmät riskienhallinnan avainkäsitteet, jotka auttavat selventämään riskienhallinnan abstrakteja merkityksiä ja hahmottamaan, mitä riskit, riskienhallinta, sisäinen valvonta ja riskinottohalukkuus merkitsevät yritysten liiketoiminnassa.

Empiirisessä analyysissa käyttämäni COSO ERM -mallin (2004, 16) mukaan *riski* on mahdollisuus, joka voi vaikuttaa positiivisesti tai negatiivisesti tavoitteiden saavuttamiseen. Tapahtumat, joilla on negatiivinen vaikutus, edustavat riskiä ja tapahtumat, joilla on positiivinen vaikutus, voivat vähentää negatiivisia vaikutuksia tai luoda uusia mahdollisuuksia. Peter L. Bernsteinin, Wall Streetillä toimivan ekonomistin, mukaan sana *”riski”* on peräisin varhaisesta Italian sanasta risicare, joka tarkoittaa uskaltaa. Riskiä määriteltäessä tulisi tarkastella epätoivotun seuraamuksen haitallisuutta ja todennäköisyyttä. Riski toteutuu yleensä vaaralle altistumisen seurauksena ja sen hyväksyttävyys riippuu monista tekijöistä (Kuusela & Ollikainen 2005, 16). Riskille voidaan myös antaa matemaattinen määrittely. Suominen (2003, 10) määrittelee riskin matemaattisesti seuraavalla tavalla: riski = todennäköisyys x riskin laajuus tai vakavuus. Kuusela & Ollikainen lisäävät (2005, 150), että riskien luonteeseen liittyy usein myös uusien ja ennen kokemattomien ilmiöiden kohtaaminen, yllätyksellisyys. Vaughan (1996, 8) puolestaan määrittelee riskin olosuhteeksi, jossa on mahdollista, että tapahtuman lopputulos poikkeaa toivotusta tai odotetusta lopputuloksesta. Riskiin liittyy sekä tappion mahdollisuus että menettämisen uhka. Kun sanomme, että riski on mahdollinen, sen toteutumisen todennäköisyys vaihtelee nollan ja yhden välillä. Olennainen riskiin liittyvä piirre on myös epävarmuus (Kuusela & Ollikainen 2005, 28). Riskijatkumon toinen pääty muodostaa mahdollisuuden. Ottamalla riski voidaan saavuttaa haluttu tavoite. Riskin merkittävyyden voisi sanoa olevan sen todennäköisyyden ja vaikuttavuuden tulo. Yritystoiminta ja johtaminen ovat jatkuvaa tasapainoilua mahdollisuuksien saavuttamisen ja riskinoton välillä.

*Riskienhallinta* on COSO ERM -mallin (2004, 16) mukaan organisaation hallituksen, johdon ja muun henkilökunnan toteuttama prosessi, jota sovelletaan strategian laadinnassa ja koko organisaatiossa. Riskienhallinnan tarkoituksena on tunnistaa organisaatioon vaikuttavia potentiaalisia tapahtumia ja pitää riskit riskinottohalukkuuden rajoissa, jotta voidaan olla kohtuullisen varmoja organisaation tavoitteiden toteutumisesta. Suomisen (2003, 27) mukaan riskienhallinta on käsitteenä monisuuntainen ja toistuva prosessi, jossa toiminnan kaikki osa-alueet vaikuttavat tai voivat vaikuttaa toisiinsa Riskienhallinta on abstraktia toimintaa, jossa määritellään etukäteen mahdolliset liiketoimintaan vaikuttavat uhat ja mahdollisuudet. Samanaikaisesti se on myös konkreettista toimintaa, jossa käydään perusteellisesti läpi eri liiketoimintojen osa-alueet. Riskienhallinnalla on perinteisesti tarkoitettu prosessia, jonka avulla yritystä uhkaavia vaaroja voidaan torjua ja niistä aiheutuvia menetyksiä minimoida. Blummen ym. (2005, 78) mukaan riskienhallinta on prosessi, jonka avulla yritys pyrkii hallitsemaan ja torjumaan tavoitteidensa saavuttamista vaarantavia uhkia. Riskienhallinnan määritelmään liittyy olennaisesti sisäisen valvonnan määritelmä, jonka esittelen seuraavaksi.

*Sisäisen valvonnan* määritelmä sisältää sisäisen tarkastuksen kansainvälisen ammatillisen ohjeistuksen (2007, 19) mukaan johdon, hallituksen ja muiden osapuolten toimenpiteet, joiden avulla parannetaan riskienhallintaa ja lisätään päämäärien ja tavoitteiden saavuttamisen todennäköisyyttä. Johto suunnittelee, organisoi ja ohjaa toimintaa niin, että päämäärien ja tavoitteiden saavuttamisesta saadaan kohtuullinen varmuus. Sisäisen valvonnan määritelmä auttaa ymmärtämään tutkielmassa käytetyn viitekehikon kontekstia. Hirvosen ym. (2003, 232) mukaan sisäisen valvonnan, riskienhallinnan toimenpiteiden ja periaatteiden tulisi olla luonnollinen osa yrityksen jokapäiväistä toimintaa. Blumme ym. määrittelevät sisäisen valvonnan corporate governancen perustavaa laatua olevaksi osatekijäksi. Sisäisen valvonnan avulla johdolla on mahdollista saada yritys toimimaan haluamallaan tavalla (mt. 33.)

*Riskinottohalukkuus* (risk appetite) on se riskin taso, jonka yritys on valmis ottamaan pyrkiessään visionsa mukaisiin tavoitteisiinsa (COSO ERM, 2004, 124). Riskinottohalukkuus heijastelee yrityksen riskienhallintafilosofiaa ja vaikuttaa tällä tavalla yrityksen kulttuuriin ja tapoihin toimia. Riskinottohalukkuus käydään läpi strategiaa laadittaessa,

jolloin strategiasta johdetun toivotun lopputuloksen tulee olla yhdensuuntainen yrityksen riskinottohalukkuuden kanssa. Riskinottohalukkuuden määrittelyssä on huomioitava yrityksen tosiasiallinen riskinottokyky. Erilaiset strategiat asettavat yrityksen alttiiksi erilaisille riskeille ja strategian laadinnassa käyttöön otettu riskienhallinta auttaa yrityksen johtoa valitsemaan yrityksen riskienottohalukkuuteen sopivan strategian (mt. 28.) Yrityksen johto tähtää organisaation, ihmisten, prosessien ja infrastruktuurin yhdenmukaistamiseen hyödyntääkseen menestyksekkäästi strategian toteuttamistaan ja varmistaakseen, että yritys pitäytyy riskinottohalukkuutensa rajoissa (mt. 40). Moellerin (2007, 51) mukaan riskinottohalukkuuden perusajatus on siinä, että jokaisen yrityksen riskinottohalukkuuden taso määrittää, hyväksyykö vai hylkääkö se kulloinkin kyseessä olevat riskit. Riskinottohalukkuus on keskeinen tekijä yritysten riskiraportoinnissa ja sen kehittymisessä, koska yrityksen omistajien tulisi saada mahdollisimman todenmukainen kuva yrityksen riskinottohalukkuuden tasosta. Tulen palaamaan näihin käsitteisiin ja sovellan niitä myöhemmin tutkielmassa.

Tutkielman rakenne

Tässä ensimmäisessä luvussa on esitetty tutkielman motivaatio, tavoitteet ja rajaukset. Olemme käyneet myös lyhyesti läpi tutkimusmenetelmän ja tutkielman sisällön kannalta keskeisimmät käsitteet. Toisessa luvussa määritellään riskienhallinnan raportoinnin kannalta merkittävät taustatekijät eli hyvän hallinnointitavan mukaiset suositukset sekä lainsäädännön sisältämät säännökset. Luvussa käsitellään myös sidosryhmien odotuksia riskiraportoinnin suhteen sekä riskiraportointi sidosryhmille. Kolmannessa luvussa esitellään tutkielman riskienhallinnan viitekehikko COSO ERM -malli ja käydään riskienhallintaprosessi läpi. Neljännessä luvussa avataan tutkimusmenetelmä auki ja tarkastellaan sen toimivuutta tutkielman kontekstissa. Samassa luvussa esitellään myös lyhyesti tutkielman kohdeyritykset, niiden toimialat ja keskeisimmät tunnusluvut. Viidennessä eli empiiristä analyysia käsittelevässä luvussa analysoidaan vuosikertomus- ja tilinpäätösmateriaalin sisältämää riskienhallintaa koskevaa informaatiota. Kuudennessa eli viimeisessä luvussa esitellään tutkielman johtopäätökset.

# 2 Riskiraportoinnin konteksti

Corporate governancen rooli on keskeinen puhuttaessa pörssiyritysten riskienhallinnan kehittymisestä ja mahdollisimman hyvästä ja laadukkaasta raportoinnista yrityksen omistajille. Tässä luvussa käydään läpi, mikä on tämän hyvän hallinnointitavan merkitys pörssiyritysten riskienhallinnalle ja mitä se merkitsee yritysten omistajien näkökulmasta katsottuna. Luvussa käydään ensin läpi corporate governancen rakenne ja sen tärkeimmät toimielimet, jonka jälkeen tarkastellaan lyhyesti sen kehitystä tähän päivään. Lopuksi käydään läpi keskeisimmät seikat lainsäädännöstä ja suosituksista riskienhallinnan osalta ja esitellään uusin, vuoden 2009 alussa voimaan tullut koodi.

## *2.1 Corporate governance*

Hirvosen ym. (2003, 26) mukaan pörssiyritysten ulkomainen omistus on Suomessa maailman korkeinta. Tämä johtuu osaltaan Suomen osakemarkkinoiden vapautumisesta vuonna 1993, jolloin amerikkalaiset sijoittajat levittäytyivät Euroopan pääomamarkkinoille. Samanaikaisesti suomalaiset yritykset halusivat vähentää omistustaan ja valtio yksityistää. Yritysten omistuksen institutionalisoitumisen ja kansainvälistymisen takia omistajien asema on korostunut. Tämän takia corporate governancea kehitetään jatkuvasti. Listayhtiöiden hallinnointi– ja ohjausjärjestelmien vuoden 2003 suosituksen mukaan corporate governance pyrkii lisäämään listattujen yritysten läpinäkyvyyttä ja korkeatasoista hallinnointia. Selkeästi määritellyt ja kansainvälisen käytännön mukaisesti suunnitellut menettelytavat helpottavat sijoituspäätösten tekemistä Tämä auttaa yritysten omistajia muodostamaan selkeämmän käsityksen pörssiyritysten toiminnasta ja seuraamaan niiden liiketoiminnan kehittymistä. Modernin corporate governance–ajattelun peruselementti onkin se, miten yritysjohto saataisiin toimimaan omistajien edun mukaisesti (Hirvonen ym. 2003, 29). Sijoituspäätöksiä tehtäessä asianmukaisella corporate governance-järjestelmällä on useiden tutkimusten mukaan tärkeä rooli. Sijoituspäätöksiä tehdessään sijoittajat arvioivat taloudellisia merkkejä samalla tasolla kuin yrityksen hallinto- ja johtamisjärjestelmiä ja ovat valmiita maksamaan lisämaksua

(premium) yrityksistä, jotka omaavat korkeatasoiset johtamisjärjestelmästandardit (Alftan ym. (2008, 33–34.)

Corporate governance voidaan ilmiönä jakaa ulkoiseen ja sisäiseen osaan. Ulkoinen corporate governance kuvaa osakemarkkinoiden käyttäytymistä yritykseen päin, kun taas sisäinen corporate governance tarkoittaa ”yrityksen toimintaa yhtiökokousten välillä ja omistajien vaikutusta yrityksen johtamistapaan niin, että omistajien tavoitteet toteutuvat yrityksen strategiassa ja operatiivisen toiminnan ohjaamisessa” (Hirvonen ym. 2003, 28.) Tästä samasta asiasta on kyse myös COSO ERM -mallissa, jossa yrityksen riskienhallinta on kytketty sen strategisiin, taloudellisiin ja toiminnallisiin tavoitteisiin (Alftan ym. 2008, 85). OECD eli Taloudellisen yhteistyön ja kehityksen järjestö (Organisation for Economic Co-operation and Development) määrittelee vuonna 2004 uudistetuissa hyvän hallintotavan periaatteissaan corporate governancen olevan hallituksen tai sitä vastaavan elimen, omistajien, johdon ja muiden intressiryhmien välisten suhteiden verkosto. Corporate governance on hallinto- ja johtamistapa, joka antaa kehikon, jonka avulla asetetaan ne keinot ja tavoitteet, joiden avulla organisaatioiden toimintaa voidaan seurata ja saavuttaa niiden tavoitteet. OECD sisällyttää corporate governancen käsitteeseen myös yritysten ylimmän ja toimivan johdon, niiden omistajien sekä muiden sidosryhmien väliset suhteet (OECD.) Alftanin ym. (2008, 11) mukaan corporate covernance tarkoittaa järjestelmää, jolla yhtiöitä ja muita organisaatioita johdetaan ja valvotaan ja sitä, miten ja millaista tietoa eri sidosryhmille annetaan. Hyvä hallintotapa on myös yrityksen strategian keskeinen osa (mt.33.)

Tutkielman kohdeyritykset ovat (Kemiraa lukuun ottamatta) tekemisissä merenkulun kanssa ja koska tutkielman kirjoittaja on itsekin merenkulun ammattilainen, on corporate governance -sanalla erityinen merkitys tutkielman kontekstissa. Hirvonen ym. (2003, 23) kirjoittavat, että englanninkielisen governance-sanan latinankielinen kantasana on gubernare = pitää perää, ohjata eli corporate governancen avulla yritystä ohjataan omistajien näkökulmasta käsin. Myös laivan kippari ”styyraa” laivaa ja katsoo, että se saapuu perille mahdollisimman turvallisesti ja taloudellisesti. Corporate governancen voisi siis kuvailla olevan pörssiyritysten riskienhallinnan äiti, koska sen avulla yritysten omistajat pystyvät helpommin ohjaamaan yrityksen johtoa, joiden velvollisuus on huo-

lehtia yrityksen toimivasta riskienhallinnasta ja tätä kautta myös selkeästä riskiraportoinnista. Tätä tarkoittaa omistajaohjaus, joka voidaan ymmärtää ilman sen tarkempaa määrittelyä. Hirvonen ym. (2003, 23) kirjoittavat omistajaohjauksen ketjusta, jossa omistajat valitsevat yrityksen hallituksen, joka puolestaan valitsee yritykselle toimivan johdon. Omistajien valitsemat riippumattomat tilintarkastajat valvovat, että omistajaohjauksen ketju toimii sille tarkoitetulla tavalla. Seuraavaksi käydään lyhyesti läpi corporate governancen toimielinten keskeisimmät roolit ja tehtävät, jotta pörssiyritysten riskiraportoinnin kehittymistä olisi helpompi hahmottaa niiden toiminnan läpinäkyvyyden, informatiivisuuden sekä sujuvan viestinnän valossa.

*Yhtiökokous* on paikka, jossa omistajat kykenevät käyttämään päätösvaltaansa. Osakeyhtiölain mukaan yhtiökokouksilla on aina ylin päätösvalta, koska se voi valita tai erottaa hallituksen. Kaikille toimielimille, jotka tässä käydään läpi, on määritelty omat tehtävänsä ja yhtiökokous voi päättää ainoastaan osakeyhtiölain sille säätämistä tai sallimista asioista. Hirvosen ym. (2008, 89-90) mukaan yhtiökokouksessa voidaan antaa hallitukselle lainmukaisia ohjeita, mutta on tärkeää ymmärtää, että yhtiökokouksen ja hallituksen suhde on ennen kaikkea yhteistyösuhde, ei alistussuhde.

Osakeyhtiön *hallituksen* keskeiset tehtävät ovat yrityksen sisäinen hallinto ja yrityksen edustaminen (Hirvonen ym.2008, 102-103). Hallituksen tehtäviä ovat sisäisen valvonnan toteuttaminen itse tai toimitusjohtajan tai muiden avustajien kautta. Johdon raportointi on keskeisessä asemassa, jonka avulla hallitus voi toteuttaa mahdollisimman hyvää sisäistä valvontaa. Hallituksen tulee ohjeistaa toimitusjohtajaa siitä, millaista raportointia se edellyttää. Riskienhallinnan osalta hallitus valvoo, että strategisia tavoitteita uhkaavat riskit ovat hallinnassa. Hallituksen tulee myös vuosittain käydä läpi yrityksen toimintaan vaikuttavat keskeiset riskit ja niiden hallinta sekä antaa niihin liittyviä ohjeita toimitusjohtajalle tarpeen vaatiessa (Hallitustyöskentelyn opas 2004, 27–29, 77.) Hirvosen ym. (2003, 231) mukaan riskiarvioinnin läpikäyminen vähintään kerran vuodessa mahdollistaa hallituksen muodostamaan kokonaisvaltaisen kuvan yrityksen riskienhallinnan tilasta sekä riskiasemasta. Hallituksen rooli on erityisen keskeinen yritysten riskienhallinnan toimivuuden suhteen, koska se vastaa viime kädes-

sä riskienhallinnasta. Tehokas riskienhallinta edellyttää selkeää ja toimivaa riskiraportointia, joka kuvastaa suoraan yrityksen sisäisen valvonnan ja riskienhallinnan kuvaa.

Osan hallituksen valvontatehtävistä suorittaa erityinen *tarkastusvaliokunta*. Tarkastusvaliokunta pitää perustaa yrityksissä, joiden liiketoiminta on niin laajaa, että se edellyttää mahdollisimman tehokasta taloudellista raportointia koskevien asioiden valmistelua. Riskienhallinnan osalta tarkastusvaliokunta voi arvioida sen riittävyyttä sekä asianmukaisuutta Tarkastusvaliokunta raportoi kaikista toimistaan hallitukselle (Hallitustyöskentelyn opas 2004, 37.) Hirvonen ym. (2003, 231-232) kirjoittavat myös, että hallituksen tarkastusvaliokunnan tai vastaavan tulisi säännöllisesti keskustella toimitusjohtajan kanssa yrityksen merkittävimmistä riskeistä sekä mahdollisesta muuttuneesta riskiasemasta.

Suurissa osakeyhtiöissä on lain mukaan oltava *toimitusjohtaja*, joka vastaa hallituksen alaisuudessa yrityksen juoksevasta toiminnasta (Hirvonen ym.2008, 112). Käytännössä toimitusjohtaja edustaa yritystä enemmän kuin hallitus. Toimitusjohtajan kelpoisuus ei kuitenkaan kata yrityksen laajakantoisia tai epätavallisia toimia. Hallitus valitsee toimitusjohtajan ja toimitusjohtaja on yrityksen tärkein toimielin, vaikka oikeudellisesti se on hallitus (mt.102-103.) Rahoitustarkastus (RATA) määrittelee toimivan johdon tehtäviksi sisäisen valvonnan ja riskienhallinnan näkökulmasta seuraavaa: “toiminnan ja avainhenkilöiden valvonta, sisäisen tarkastuksen, tilintarkastajien ja muiden valvontaa suorittavien elinten toiminnan tukeminen sekä niiden antamien havaintojen ja suositusten hyväksikäyttö, riskien ja riskienhallinnan toimivuuden seuranta sekä riskinottoon nähden riittävän pääomatason valvonta, viranomaisraportoinnin oikeellisuuden valvonta sekä sääntelyn noudattamisen valvonta” (RATA.) Yritysjohto nähdään merkittävänä sidosryhmänä yrityksissä, joissa omistus ja johto ovat eriytyneet, koska heidän odotetaan toimivan omistajien intressien mukaisesti (Hirvonen ym. 2003, 70).

*Johtoryhmä* koostuu yrityksen toimivasta johdosta ja on hallituksen alainen elin. Johtoryhmän perustehtäviin kuuluu toimitusjohtajan avustaminen yrityksen strategian muovaamisessa, suunnitelmien laatimisessa sekä niiden toteuttamisen ohjaamisessa. Johtoryhmän toiminnan määrittelemiseen ei ole olemassa erillisiä säännöksiä, vaan johto-

ryhmä voidaan nähdä toimitusjohtajan työkaluna yrityksen asioiden hoitamisessa. Lainsäädännöllisesti epävirallinen johtoryhmä on kuitenkin merkityksellinen osa yritystä, koska parhaimmillaan se omalta osaltaan tukee jäseniään heidän vastuualueidensa johtamisessa sekä päätöksenteossa (Hirvonen ym.2003, 115.)

Hirvonen ym. (2003, 28) kirjoittavat *tilintarkastajien* riippumattomuuden merkityksen korostuminen olevan näkyvä muutos puhuttaessa tämän ajan pörssiyritysten toiminnasta. Tilintarkastajien ja johdon suhteen säilyminen edellyttää johdon luottamusta. Enronin ja muiden vastaavien tilinpäätösskandaalien takia yhteiskunnan sekä omistajien olisi viisasta vahvistaa tilintarkastajien riippumattomuutta. Omistajien tulisi siis olla aktiivisia tilintarkastajien valinnassa, vaikka käytännössä hallituksen mielipide on tässä asiassa ratkaiseva (mt. 92.) Tilintarkastajan tehtävä on varmistaa ja vahvistaa, että johdon antama tieto on luotettavaa. Tällä tavalla suojataan omistajia mahdolliselta johdon aseman väärinkäyttämiseltä ja varmistetaan, että omistajat voivat käyttää heille kuuluvaa lainmukaista päätöksentekovaltaa ja tehdä oikeita päätöksiä. Tilintarkastaja voidaan nähdä omistajien edun valvojana sekä luottohenkilönä (mt.116.)

Riippumattomalla *sisäisen tarkastuksen* roolilla on keskeinen merkitys yritysten riskienhallinnan toimivuuden onnistumisen suhteen. Riippumaton sisäinen tarkastus tarjoaa tehokkaimmillaan hedelmällisen, objektiivisen sekä arviointikykyisen yhteistyösuhteen yrityksen riskienhallintatoiminnon kanssa. Hyvä sisäisen tarkastus arvioi niitä kontrolleja, joiden avulla pyritään hallitsemaan liiketoiminnan riskejä sekä tuo varmuutta kyseisten kontrollien toimivuudesta ja olemassaolosta (Hirvonen ym. 2003, 232.)

Tutkielmassa käytetty COSO ERM -malli toimii täydentävänä työkaluna myös corporate governancen suhteen. Moellerin (2007, 345) mukaan sisäisen valvonnan parantaminen näyttäisi olevan selkeä trendi; COSO ERM -malli ei kosketa ainoastaan hallitusta tai ylintä johtoa, vaan se koskee yrityksen jokaista työntekijää, kuten myös sisäinen valvonta koskee kaikkia. COSO ERM -malli ei ole vielä tehnyt maailman valloitusta yrityksen hallituksille, mutta tämän ajan yritysten tulisi kiinnittää enemmän huomiota ja varata aikaa riskien arviointiin ja hallintaan. Moeller ennustaa myös erillisten riskivaliokuntien perustamisen lisääntymistä sijoittajien pyynnöstä. Seuraavassa kappaleessa

tarkastellaan lyhyesti corporate governancen kehitystä Suomessa ja kansainvälisellä tasolla sekä sen nykysuosituksia.

## 2.2 Corporate governancen kehitys ja nykysuositukset

Vuonna 1997 annettiin Suomen ensimmäinen corporate governance -suositus Keskuskauppakamarin ja Teollisuuden ja Työnantajain Keskusliiton (nykyinen Elinkeinoelämän keskusliitto EK) toimesta. Hex Oyj (nykyinen NASDAQ OMX Helsinki Oy), Keskuskauppakamari ja Teollisuuden ja Työnantajain Keskusliitto (nykyinen Elinkeinoelämän keskusliitto EK) totesivat vuonna 2003 listayhtiöiden ohjaus- ja valvontajärjestelmien toiminnan kasvaneen merkityksen ja kansainvälisen kehityksen ja asettivat työryhmän uudistamaan suosituksia. Joulukuussa 2003 annettiin tämän työn pohjalta suositus listayhtiöiden hallinnointi- ja ohjausjärjestelmistä (Corporate Governance Finland). Vuoden 2003 suositusta listayhtiöiden hallinnointi- ja ohjausjärjestelmistä on pidetty toimivana sekä kansainvälisesti korkeatasoisena. Suositus on selvästi parantanut suomalaisten yhtiöiden hallinnointitapaa. Kansainvälisen kehittymisen sekä uusien sääntelyiden myötä on päivittämistarpeita kuitenkin ilmennyt. Arvopaperimarkkinayhdistys asetti corporate governance -työryhmän päivittämään ja kehittämään suositusta. Tämän työn tuloksena Arvopaperimarkkinayhdistys ry:n hallitus hyväksyi lokakuussa 2008 Suomen listayhtiöiden hallinnointikoodin, joka korvaa vuonna 2003 annetun suosituksen listayhtiöiden hallinnointi- ja ohjausjärjestelmistä (Corporate Governance Finland.) Alftanin ym. (2008, 23) näkemyksen mukaan Suomen corporate governancen kehitys noudattaa samansuuntaisia linjoja kuin Euroopassa ja muissa maissa. Seuraavassa kappaleessa luodaan hetkeksi silmäys corporate governancen kansainväliseen kehitykseen.

Yhdysvaltojen Sarbanes-Oxley-laki, joka säädettiin kirjanpitoskandaalien jälkeen, on kansainvälisistä corporate governance-suosituksista kaikkein merkittävin (Hallitustyöskentelyn opas 2004, 12). Alftan ym. (2008, 22) kirjoittavat, että Euroopassa eri maiden välillä on ollut eriäväisyyksiä corporate governance-säännöstöissä sekä ohjeistuksissa, joten yhtenäistämistarpeita on ollut olemassa jo pitkään. EU julkaisi vuonna 2002 niin sanotun Winterin raportin, joka on sittemmin ollut pohjana muun muassa corporate

governance -kysymyksissä. Winterin raporttia ei kuitenkaan sellaisenaan ole hyväksytty, mutta Euroopan komissio julkaisi sille vastineen, joka on tällä hetkellä käynnissä oleva etenemissuunnitelma Euroopan Unionin yhtiöoikeuden uudistamiseksi ja omistajaohjauksen parantamiseksi (Action Plan on Modernising Company Law and Enhancing Corporate Governance in the EU). Myös Suomen osakeyhtiölaissa on yhteneväisyyksiä Winterin raportin kanssa. Euroopan komissio on myös antanut erilaisia suosituksia ja direktiivejä, jotka koskevat corporate governancen osa-alueita, jotka on jo osittain huomioitu kansallisissa säännösmuutoksissa. Uudet EU-direktiivit korostavat kokonaisvaltaisen riskienhallinnan roolia. Sisäisen valvonnan vaatimus sisältyy ensimmäisen kerran myös lakitekstiin. On myös tärkeää huomata, että direktiivien sisäisen valvonnan vaatimukset eivät rajoitu pelkästään taloudelliseen raportointiin (mt. 23.) Seuraavaksi tarkastellaan corporate governancen taustalla vaikuttavia lainsäädännöllisiä tekijöitä sekä nykysuosituksia riskienhallinnan osalta.

Corporate governance-suositusten (2003, 4) mukaan suomalaisten pörssiyhtiöiden hallinnointi- ja ohjausjärjestelmiä sekä tiedottamista koskevat perussäännökset sisältyvät yhtiö-, kirjanpito- ja arvopaperimarkkinalainsäädäntöön sekä Helsingin Pörssin sääntöihin. *Osakeyhtiölaissa*, joka uudistettiin vuonna 2006, säädellään hyvän johtamis- ja hallintojärjestelmän perusasioita. Osakeyhtiölaki korostaa myös yritysten toimintamahdollisuuksien monipuolistumista. Tämä seikka kuvastaa myös riskienhallinnan kasvavaa merkitystä: toiminnan laajentuessa ja monistuessa lisääntyvät myös riskit. Alftanin ym. (2008, 16) mukaan corporate governancen kannalta on tärkeää, että hallituksen yleistoimivalta yhtiön toiminnan ohjaajana perustuu osakeyhtiölakiin. Johdon vastuuta arvioitaessa kiinnitetään huomio siihen, kuinka yhtiön toiminta ja hallinto on organisoitu. Hallituksen on jatkuvasti seurattava, tuottavatko yrityksen raportointijärjestelmät riittävästi sellaista tietoa, jonka avulla muodostetaan kuva yrityksen nykyisestä tilasta. Osakeyhtiölaki sisältää myös vaatimuksen osakkeenomistajien yhdenvertaisesta kohtelusta.

*Arvopaperimarkkinalaki* on alun perin säädetty aikana, jolloin ulkomaalaisten sijoittajien osakeomistusta rajoitettiin ja arvopaperikauppa Suomessa koostui ainoastaan suomalaisista arvopapereista ja toimijoista. Arvopaperimarkkinalakia on muutettu useaan

otteeseen ja vuonna 2008 valtiovarainministeriö aloitti sen kokonaisuudistuksen valmistelun. Arvopaperimarkkinalaki koskee muun muassa osakkaiden ja yritysten velvollisuuksia sellaisissa tilanteissa, joissa osakkeita tai muita arvopapereita lasketaan liikkeelle. Yritysten, joilla on julkisen kaupankäynnin kohteena olevia arvopapereita, tulee julkistaa viipymättä ne päätökset sekä toimintaa koskevat asiat, joilla on olennainen vaikutus liikkeelle laskettujen arvopapereiden arvoon. Corporate governancen osalta arvopaperimarkkinalakia on uudistettu siten, että vuoden 2009 alusta julkisen kaupankäynnin kohteena olevien arvopaperien liikkeellelaskijoiden tulee antaa osana säännöllistä tiedonantovelvollisuuttaan selvitys hallinto- ja ohjausjärjestelmästään (corporate governance statement). Riskienhallinnan osalta selvityksen on sisällettävä ”kuvaus liikkeeseenlaskijan taloudelliseen raportointiin liittyvien sisäisen valvonnan ja riskienhallinnan pääpiirteistä.” Lisäksi tilanteissa, joissa tilintarkastajat toteavat tilintarkastuskertomuksessa, että selvitys hallinto- ja ohjausjärjestelmästä on ristiriidassa tilinpäätöksen kanssa tai sitä ei ole annettu, liikkeellelaskijoiden on välittömästi julkistettava tilinpäätös, toimintakertomus sekä tilintarkastuskertomus (Alftan ym. 2008, 16-17.)

*Kansallinen corporate governance -suositus* on joulukuussa 2003 voimaan tullut suositus listayhtiöiden hallinnointi- ja ohjausjärjestelmistä, jonka mukaan listattujen yhtiöiden on selostettava periaatteet, joiden mukaan riskienhallinta on järjestetty (corporate governance–työryhmä 2003, suositus 50). Riskienhallintaa koskeva suositus numero 50 on kokonaisuudessaan seuraava: ”Riskienhallinnan järjestäminen: Yhtiön on selostettava periaatteet, joiden mukaan riskienhallinta on järjestetty. Riskienhallinta on osa yhtiön valvontajärjestelmää. Riskienhallinnan avulla pyritään varmistamaan, että yhtiön liiketoimintaan vaikuttavat riskit tunnistetaan ja niitä seurataan. Toimiva riskienhallinta edellyttää riskienhallinnan periaatteiden määrittämistä. Yhtiön toiminnan arvioimiseksi on tärkeää, että osakkeenomistajille annetaan riskienhallinnasta riittävästi tietoa. Myös hallituksen tietoon tulleiden merkittävien riskien selostaminen on suositeltavaa”. Suosituksen ensisijaisina tavoitteina ovat listayhtiöiden tiedonkulun tehostaminen, sijoittajille ja osakkeenomistajille annettavan tiedon yhtenäistäminen, toiminnan läpinäkyvyyden parantaminen sekä toimintatapojen yhtenäistäminen. Noudata tai selitä –periaate (comply or explain) on suosituksen keskeisin periaate (Alftan ym. 2008, 29). Corporate covernance -suosituksen (2003, 4) mukaan tämä tarkoittaa sitä, että yrityksen tulee noudattaa

kyseistä suositusta kokonaisuudessaan. Jos yritys kuitenkin poikkeaa suosituksesta, sen on ilmoitettava kyseinen poikkeaminen ja sen syy. Yritysten on lisäksi annettava www-sivuillaan ja vuosikertomuksessaan tieto suosituksen noudattamisesta. Suositus on laadittu täydentämään lakisääteisiä menettelytapoja, koska suomalainen hallinnointi- ja ohjausjärjestelmä perustuu pakottavaan lainsäädäntöön.

*Kansallinen asialuettelo listaamattomille yrityksille* on luettelo, joka mahdollistaa listaamattomien yritysten hallinnon kehittämisen. Keskuskauppakamarin vuonna 2006 julkaisema asialuettelo mahdollistaa sellaisia listaamattomia yrityksiä kehittämään hallinnointi- ja ohjausjärjestelmiään, joille listayhtiöiden corporate governance -suositus on liian vaativa. Listaamattomien yritysten asialuettelo on vapaaehtoinen. Yritys voi toimia ja menetellä ilman tiedonantovelvollisuutta omien lähtökohtiensa ja tarpeidensa mukaan. Tavoitteet riskienhallinnasta ja sisäisestä valvonnasta ovat samat kuin listatuilla yrityksillä. Eroja kansallisen ja listaamattomien suosituksilla löytyy ainoastaan suositusten perussisällöstä, esimerkiksi sisäisen valvonnan toimintaperiaatteet voidaan määritellä vapaaehtoisesti. Riskienhallintaa lähestytään laajemmin, esimerkiksi asialuettelossa käydään läpi toiminnan eri osa-alueita ja niihin liittyviä riskejä. Myös kokonaisvaltaisen riskienhallinnan hyötyjä arvioidaan (Alftan ym. 2008, 21-22.)

*Suomen listayhtiöiden hallinnointikoodi* on aikaisemmin mainitun corporate governance-suosituksen päivitetty versio, joka on tullut voimaan 1.1.2009. Corporate governance -koodin tarkoituksena on parantaa kansainvälisten sijoittajien tiedonsaantia Suomen corporate governance -järjestelmästä ja erityisesti osakkeenomistajien oikeuksista. Koodi korvaa aikaisemman, vuoden 2003 suosituksen ja se täydentää lakisääteisiä menettelytapoja. Koodin tavoitteena on, että listautuneet yritykset noudattaisivat kansainvälistä ja korkeatasoista hallinnointitapaa. Koodin toivotaan myös yhtenäistävän pörssiyhtiöiden toimintatapoja sekä osakkeenomistajille ja muille sijoittajille annettavaa tietoa. Koodin mukaan riskienhallinnan, sisäisen valvonnan ja sisäisen tarkastuksen tavoitteena on varmistaa, että yhtiön toiminta on tehokasta, tuloksellista, informaatio luotettavaa ja että säännöksiä ja toimintaperiaatteita noudatetaan. Myös liiketoimintaan liittyvät riskit tulisi tunnistaa, arvioida ja seurata. Koodissa on täsmennetty noudata tai selitä -periaatetta, joka antaa joustovaraa uuden koodin soveltamisessa sekä antaa selke-

ämmän ja varmemman kuvan yrityksen johdon tekemistä perusteluista omistajille ja sijoittajille. Koodin suositus numero 46:een on lisätty velvollisuus selostaa hallituksen tietoon tulleet merkittävimmät riskit ja epävarmuustekijät sekä ne periaatteet, joiden mukaan riskienhallinta on järjestetty. Toimiva riskienhallinta edellyttää riskienhallinnan periaatteiden määrittämistä ja yrityksen toiminnan arvioimiseksi riskienhallinnasta tulee antaa riittävästi tietoa. Koodin suositus numero 51:n mukaan yrityksen on annettava erillinen kertomus hallinto- ja ohjausjärjestelmästään tilinpäätöksen ja toimintakertomuksen yhteydessä. Riskienhallinnan osalta selvitykseen on sisällytettävä kuvaus taloudelliseen raportointiprosessiin liittyvien sisäisen valvonnan ja riskienhallinnan järjestelmien pääpiirteistä, joissa tulee pääpiirteittäin kuvata, miten yrityksen riskienhallinta ja sisäinen valvonta omalta osaltaan varmistavat luotettavan taloudellisen raportoinnin (Corporate Governance Finland.) Corporate governance -koodin merkitystä pörssiyritysten riskienhallinnan kehittymiselle ei voi jättää huomioimatta; koodin suosituksista ei voi poiketa siltä osin kuin ne kuvaavat pakottavaan sääntelyyn sisältyvää velvoitetta. Tästä näkökulmasta on edelleen todettava, että corporate governance -koodin kehittymisen myötä riskienhallinnan tärkeyden korostuminen tulee mitä luultavammin näkymään johtavien ja suurempien pörssiyhtiöiden riskienhallinnan raportoinnissa; yritysten on pidettävä niiden hallitus selkeästi, ajankohtaisesti ja entistä tehokkaammin informoituna merkittävimmistä riskeistään.

## 2.3 Sidosryhmien odotukset riskiraportoinnin suhteen

Yritysten tärkeimpiä sidosryhmiä ovat muun muassa asiakkaat, omistajat, henkilöstö, ympäristö, rahoittajat, tavarantoimittajat sekä yhteiskunta. Tutkielmassa käsitellään sijoittajien odotuksia riskiraportoinnin suhteen, koska sijoittajat omistavat yrityksen ja heille tulee antaa oikeaa ja riittävää tietoa, kannattaako heidän sijoittaa kyseiseen yritykseen vai ei (Alftan ym. 2008, 33). Hirvonen ym. (2003, 70) mainitsevat englanninkielisen termin ”stakeholders”, joka kuvaa hyvin sidosryhmien suhdetta yritykseen panoksen haltijana, jotka odottavat saavansa panoksiaan vastaavan korvauksen yritykseltä.

Hirvonen ym. (2003, 26) nimeävät yritysten omistusten pirstoutumisen, kansainvälistymisen ja arvomaailman amerikkalaistumisen tekijöiksi, jotka ovat kasvattaneet liiketoiminnan läpinäkyvyyden ja oikeellisuuden sekä sijoittajaviestinnän merkitystä. Riskiraportointi ja sen kehittymisen merkitys tulee kasvamaan samanaikaisesti sijoittajien pitkäjänteisyyden kanssa, koska sijoituksia arvioidaan yhä useammin tulevaisuuden odotuksiin perustuen. Alftanin ym. (2008, 32) mukaan vakavat virheet kirjanpidossa ja raportoinnissa ovat nousseet valokeilaan koskien käytössä olevia menettelytapoja. Kansainvälisen ja suomalaisen kehityksen myötä sidosryhmäraportointia, erityisesti riskienhallinnan ja sisäisen valvonnan osalta, tullaan kehittämään entistä avoimemmaksi ja tarkemmaksi.

Kuuluvaisen (ks. Holopainen ym. 2006, 26) mukaan pörssiyhtiöiden suhde rahoitusmarkkinoihin asettaa vaatimuksia sijoittajien tiedonsaannin suhteen. Pörssiyritys voi hakea rahoitusta suoraan markkinoilta, jossa toimivat sijoittajat luonnollisesti asettavat omat vaatimuksensa niiden toiminnalle ja tätä kautta riskien merkitys ja niistä tiedottaminen korostuvat. Sijoittajien tulee olla varmoja siitä, että he eivät ole sijoittamassa liian riskialttiiseen yritykseen tai sellaiseen yritykseen, jolla on liian voimakas riskinottohalukkuus. Hyväuskoiset sijoittajat ovat aikaisemmin investoineet suuria määriä yrityksiin, mutta nykyään sijoittajat ovat varuillaan ja vaativat oikea-aikaista ja kontrolloitua tietoa yritysten tilasta. Omistajien ja sijoittajien tulee siis olla selvillä yritysten riskienhallinnan toimivuudesta sekä liiketoimintaa uhkaavista riskeistä (mt. 26.) Hirvonen ym. (2003, 30) tarkastelevat omistajien intressien turvaamista agenttiteorian valossa, jonka mukaan omistaja on päämies ja yritysjohto omistajien agentti, jonka tehtävänä on toimia omistajien intressien mukaisesti. He näkevät agenttiteorian ratkaisevan samaa ristiriitaa, jossa yritys hakee ulkopuolista rahoitusta etsiessään liiketoiminnalleen parasta mahdollista tuottoa. Alftanin ym. (2008, 33) mukaan potentiaaliset sijoittajat ja osakkeenomistajat haluavat vertailukelpoista ja ajanmukaista tietoa ja vaativat, että yritykset toimivat corporate governance -ohjeistusten ja –säännösten mukaisesti. Omistajille annetun tiedon tulee olla luotettavaa, ajankohtaista ja vertailukelpoista, mutta se ei saa vahingoittaa yritystä tai paljastaa liikesalaisuuksia.

## 2.4 Riskiraportointi sidosryhmille

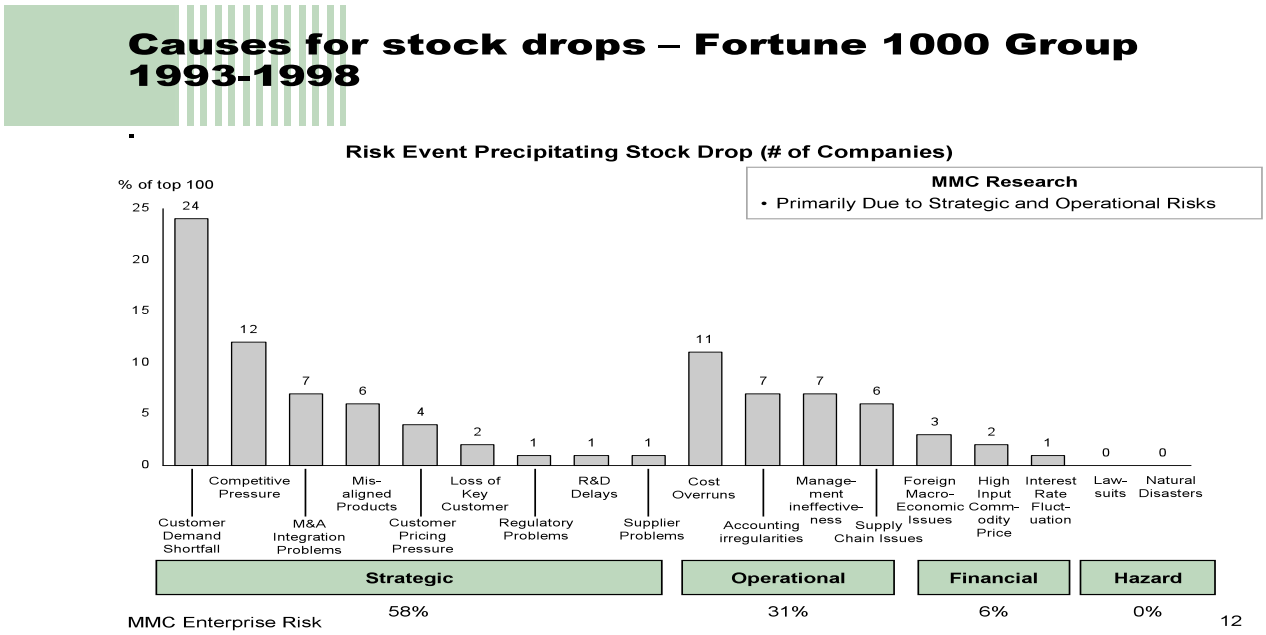
Raportoinnin luotettavuus ja lakien ja määräysten noudattamista koskevien tavoitteiden saavuttaminen on organisaation päätösvallassa, joten on kohtuullista olettaa, että riskienhallinta omalta osaltaan varmistaa niiden toteutumisen. Moellerin (2007, 101-102) mukaan täsmällinen raportointi on yrityksen menestyksen kannalta kriittinen tekijä monessa suhteessa. Toimialasta huolimatta jokainen yritys kohtaa riskejä, jotka johtuvat yksiköiden raportoinnin virheistä. Olisi hyvä, jos jokainen yksikkö huolehtisi, että heidän antamansa tiedot ovat oikein. Hyvin toimivilla sisäisillä valvontatoimenpiteillä on tässä kohtaa suuri merkitys. Huomio tulisi keskittää puutteellisiin raportteihin ja niiden aiheuttamiin riskeihin, jotka olisi hyvä ottaa huomioon kaikilla tasoilla. Moeller myös tähdentää, että yrityksellä on eri keinoja viestiä riskienhallinnastaan sen omistajille. Yritysten kotisivut, vuosikertomukset sekä tilinpäätökset ovat riskiraportoinnin parhaita välineitä (mt. 58.) Pörssiyritysten ulkomaisten sijoittajien ja osakkeenomistajien ainoana tiedonlähteenä toimivatkin julkiset raportit, tiedotteet, tilinpäätökset sekä vuosikertomukset. Tilinpäätös, jonka sisältöä säätelevät kirjanpitolaki, osakeyhtiölaki sekä listayhtiöitä koskeva arvopaperimarkkinalaki, kiinnostaa omistajia ja sijoittajia osingonmaksu- ja arvonluontikyvyn, mutta myös riskienhallinnan osalta. Tilinpäätöksen yhteydessä esitetyt kuvaukset johtamisjärjestelmästä, tutkimus- ja kehittämistoiminnasta, riskeistä, strategiasta, markkinaosuuskehityksestä ja aineettomista kilpailutekijöistä, joiden merkitys sisäisenä arvonkehittämiskeinona kasvaa kaiken aikaa, luovat pohjaa yrityksen arvonluontikyvyn ja osakkeiden arvonkehityksen arvioinnille. Toimintakertomuksen perusteella sidosryhmät arvioivat listattujen yritysten hallinto- ja ohjausjärjestelmien luotettavuutta.

Riskiraportoinnin merkityksestä sijoittajien suhteen on tehty monia tutkimuksia. Ernst & Youngin (EY) tutkimus Guiding investors through rocky waters (2006) perustuu siihen, miten suomalaiset listatut yritykset raportoivat riskienhallinnan tasostaan. Vakuuttavan riskiraportoinnin avulla sijoittajat kykenevät muodostamaan havaintoja yrityksen riskisyydestä ja soveltamaan sitä yhteen oman riskiprofiilinsa kanssa. Riskien paljastaminen auttaa sijoittajia päättämään, ovatko he valmiita suojautumaan jäännösriskeiltä, jotka ovat jääneet yritykseltä hoitamatta. Selkeän riskiraportoinnin avulla

yrityksen johto todistaa, että se on tietoinen yrityksen riskeistä ja sillä on keinot suojautua riskeiltä. Yritysten, jotka keskittyvät taloudellisten riskien raportoimiseen, tulisi laajentaa riskiraportointiaan myös operatiivisiin ja strategisiin riskeihin, koska niillä on suurin vaikutus strategisten tavoitteiden saavuttamiseen. Yritysten tarjoaman riskitiedon tulee olla todenmukaista, oivaltavaa sekä heijastaa yrityksen sen hetkistä riskienhallinnan tilaa. Merkittäväksi haasteeksi jää sopivan ja riittävän riskien paljastamisen tason valitseminen sekä riittävän riskien ja riskienhallinnan kuvauksen antaminen. Tuoreen Ernst & Young:in The 2009 Ernst & Young business risk report- tutkimuksen mukaan riskienhallintaa tullaan kehittämään ja toteuttamaan entistä enemmän, mutta tällä hetkellä yritykset tekevät aivan liian vähän tällä saralla. Strategiset riskit ovat yhä suuremmassa roolissa, kun taas yritykset keskittyvät liian usein helpommin hallittaviin operatiivisiin riskeihin. Kyseisen tutkimuksen keskeinen sanoma on, että yrityksen johdon tulee ottaa strateginen näkökulma kohtaamiensa riskien hallintaan ja olla koko ajan hereillä, nopealiikkeinen ja valmiina määrittelemään riskinottohalukkuutensa ja –kykynsä, jota sen on tarkkailtava koko ajan (Ernst & Young.)

Strategisten riskien merkityksestä kertoo myös Compustat Mercer Management Consulting:in teettämä tutkimus ajanjaksolta 1993–1998, jossa analysoitiin 100 Fortune 1000:een, joka sisältää 1000 Yhdysvaltojen suurinta yritystä, kuuluvaa yritystä. Kyseisten yritysten arvo laski yhden kuukauden aikana 25 %. Tämä johtui ensisijaisesti strategisista ja operatiivisista riskeistä, jotka ovat usein vakuutuskelvottomia (uninsurable) ja edellyttävät johdolta kykyä parantaa, muuttaa ja/tai sopeuttaa organisaatiossa työskentelevien ihmisten rooleja, prosesseja sekä teknologiaa. Tutkimus osoittaa, että perinteisillä riskeillä, esimerkiksi rahoitusriskeillä, ei olekaan suurin vaikutus. Seuraavan kaaviokuvan avulla voidaan tarkastella, kuinka merkittävä vaikutus strategisilla riskeillä on yritysten arvoon verrattuna operatiivisiin ja taloudellisiin riskeihin.

**Kuva 1. Strategisten riskien vaikutus suhteessa operatiivisiin ja taloudellisiin riskeihin**




Lähde: Marsh

KPMG:n tutkimuksessa corporate governance -suositusten soveltamisesta analysoitiin 122 (93 % OMX Helsingin Pörssin yhtiöistä) huhtikuun 2008 alkuun mennessä julkaistua vuoden 2007 vuosikertomusta ja tilinpäätösinformaation corporate governance-osiota. Tutkimuksen sanoma riskienhallinnan osalta oli, että riskienhallinta oli selostettu ”vähintään kohtuullisesti”. Riskiselvitys saattoi kuitenkin jäädä puutteelliseksi eli yritysten pitäisi kiinnittää enemmän huomiota yhtiökohtaisten riskien kuvaamiseen (Alftan ym.2008,151.

# 3 Kokonaisvaltaisen riskienhallinnan viitekehys COSO ERM

Moeller (2007, 111) listaa niitä ajatuksia, jotka puhuvat sen asian puolesta, miksi COSO ERM -malli on valittu tutkielman viitekehikoksi: COSO ERM -malli sopii kaiken kokoisille ja eri toimialoilla toimiville yrityksille. COSO ERM -malli ei ainoastaan pyri vähentämään riskejä, vaan pyrkii myös johtamaan niitä. Malli erottuu muista riskienhallinnan viitekehikoista edukseen siinä, että se pyrkii tunnistamaan yrityksen riskinottohalukkuuden ja soveltamaan riskienhallinnan osaksi strategian asetantaa. COSO ERM-malli tarjoaa kiehtovan mahdollisuuden tarkastella tutkielman kohdeyritysten riskienhallinnan ja riskiraportoinnin kehitystä, koska tutkija voi asettautua samanlaiseen asemaan kuin sijoittajat.

Committee of Sponsoring Organisations of the Treadway Commission (COSO) julkaisi COSO-raportin vuonna 1992, jonka tarkoitus oli määrittää vilpilliseen taloudelliseen raportointiin johtavat tekijät ja suositusten antaminen kyseisten raportointien vähentämiseksi. Moellerin (2007, 49) mukaan COSO:n sisäisen valvonnan mallia (Internal Control Integrated Framework, COSO IC) on alun perin lähdetty kehittämään siitä ideasta käsin, että riskienhallinnan viestintä ei ole toiminut hallituksen ja johdon välillä. Blummen ym. (2005, 34) mukaan COSO-malli on kuin ”virstanpylväs sisäisen valvonnan teoriassa”, koska se on alallaan ensimmäinen esitellessään sisäisen valvonnan määritelmän ja sen osatekijöiden kuvaukset.

Vuonna 2004 julkaistiin COSO IC -viitekehyksen pohjalta luotu Enterprise Risk Management - Integrated Framework–viitekehys eli COSO ERM -malli. COSO ERM -mallin rikkaus on siinä, että se yhdistää alkuperäiseen sisäisen valvonnan malliin laajaalaisemman riskienhallinnan näkökulman. COSO ERM -mallin tarkoitus ei suinkaan ole syrjäyttää sisäisen valvonnan mallia, vaan liittää se luonnolliseksi osaksi mukaan. Moellerin (2007, 92) mukaan COSO ERM -malli tarjoaa järkeenkäyvän mallin, jonka avulla yrityksen on mahdollista saavuttaa sen tavoitteet, joihin luonnollisesti liittyy aina riskejä

ja mahdollisuuksia. Holopainen ym. (2006, 35) kirjoittavat, että on hyödyllistä tiedostaa, että riskienhallinnan toteuttaminen on aina kunkin yrityksen sisäisesti tekemä ratkaisu ja sitä ei voida kaavamaistaa vain yhteen, tiettyyn malliin. COSO ERM -mallin soveltamisen arvioinnissa on siis tärkeää muistaa, että sen tarkoitus on suositusten antaminen, joita kukin organisaatio voi halutessaan hyödyntää omassa liiketoimintaympäristössään. Moellerin (2007) mukaan COSO ERM -malli ei vielä ole kovin tunnettu sisäisen valvonnan ja riskienhallinnan viitekehys, mutta hän ennustaa, että sen merkitys tulee tulevaisuudessa kasvamaan.

Blumme ym. (2005, 85) kiteyttävät ytimekkäästi COSO ERM -mallin perusajatuksen: se pyrkii luomaan yhteyden organisaation tavoitteiden, toiminnallisen rakenteen ja riskienhallinnan välille. COSO ERM -mallin mukainen kokonaisvaltainen riskienhallinta kytketään yrityksen strategisiin, toiminnallisiin ja taloudellisiin tavoitteisiin. Riskejä tarkastellaan koko yrityksen tasolla eikä pelkästään yksittäisistä toiminnoista ja niihin liittyvistä riskeistä käsin. Yrityksen taloudellinen ja toiminnallinen kokonaishyöty pyritään maksimoimaan nimenomaan riskienhallinnan keinoin. COSO ERM -mallin mukaan riskienhallinnan pyrkimyksenä Blummen ym. mukaan on:

- riskinottohalun ja strategian yhdistäminen, jossa johto ottaa huomioon organisaation riskinottohalun ja –kyvyn arvioidessaan strategisia vaihtoehtoja, asettaessaan tavoitteita ja kehittäessään riskienhallintamenettelyjä
- riskien hallintaan liittyvien päätösten parantaminen, jossa riskienhallinta luo mahdollisuuden tunnistaa mahdollisia riskejä sekä valita oikea riskienhallintakeino
- toiminnallisten yllätysten ja tappioiden vähentäminen, jossa organisaatiot kykenevät havaitsemaan liiketoimintaa uhkaavat riskit nopeammin ja ryhtymään hallintatoimiin, tällöin yllätykset ja niihin liittyvät menetykset ja kustannukset vähenevät
- koko organisaatiota kattavien ja kertautuvien riskien havaitseminen ja hallitseminen. Organisaatiota uhkaavat riskit koskettavat useampia organisaatioyksiköitä ja kokonaisvaltainen riskienhallinta auttaa johtoa ymmärtämään riskien keskinäiset vaikutukset

- mahdollisuuksien hyödyntäminen, jossa johdolla on mahdollisuus havaita ja hyödyntää uusia mahdollisuuksia kattavien riskiarviointien avulla
- pääoman käytön parantaminen, jossa johto voi kattavan ja luotettavan riski-informaation avulla tehokkaasti arvioida kokonaispääoman tarvetta ja pääoman allokointia sisäisesti

## 3.1 Organisaation tavoitteiden jaottelu COSO ERM -mallin mukaan

COSO ERM -mallissa (2004, 5) organisaation tavoitteet laaditaan ensin strategisella tasolla, jonka avulla luodaan perusta toiminnallisille, raportoinnin ja vaatimuksenmukaisuutta koskeville tavoitteille. Strategiset, korkean tason tavoitteet ovat organisaation toiminta-ajatuksen mukaisia ja sitä tukevia. Toiminnalliset tavoitteet liittyvät yrityksen toimintojen suorituskykyyn ja tehokkuuteen, joiden avulla yritys voi saavuttaa lopulliset tavoitteensa. Johdon tulee varmistaa, että nämä toiminnalliset tavoitteet vastaavat todellista toimintaympäristöä. Raportoinnin tavoitteet koskevat raportoinnin luotettavuutta. Luotettava raportointi tarjoaa yrityksen johdolle tarkoituksenmukaista ja huolellisesti laadittua tietoa, joka tukee johdon päätöksentekoa ja yrityksen toimintojen ja suorituskyvyn valvontaa. Vaatimuksenmukaisuutta koskevat tavoitteet liittyvät siihen, että yritys toimii lainsäädännön ja tarvittavien ohjeiden mukaisesti. Tämä asettaa omat vaatimuksensa yrityksen toiminnalle.

Tavoitteiden ryhmittely mahdollistaa huomion keskittämisen sisäisen valvonnan eri puoliin. Myös erottelu sen suhteen, mitä sisäiseltä valvonnalta voidaan odottaa kunkin tavoiteryhmän suhteen, sallitaan. Strategisten tai toiminnallisten tavoitteiden saavuttaminen ei aina ole yrityksen vaikutusvallan alla, koska niiden suhteen on olemassa virheellisten päätösten, arvioiden tai ulkoisten tapahtumien aiheuttamat riskit. Raportointia tai vaatimustenmukaisuutta koskevat tavoitteet puolestaan ovat yrityksen vaikutusvallan alla, koska ne perustuvat pitkälti ulkopuolisten määräämille standardeille. Suurin riski on, että näitä vaatimuksia ei noudateta. Näissä vaatimuksissa asetetaan myös velvoitteita riski-informaatiolle, jossa sidosryhmille kerrotaan riskienhallinnan järjestämisestä sekä merkittävimmistä riskeistä (COSO ERM 2004, 35-40.) Esimerkiksi IFRS 7 (International Financial Reporting Standards) vaatii yrityksiä kertomaan rahoitusinstrument-

teihinsa liittyvistä riskeistään ja siitä, kuinka yritys hallitsee kyseiset riskit (Poole & Spooner 2007, 467). Riskienhallinta varmistaa näiden tavoitteiden toteutumisen. Toimivan riskienhallinnan avulla voidaan saada kohtuullinen varmuus siitä, että johto ja hallitus saavat ajoissa tiedon näiden tavoitteiden toteutumisvauhdista ja näkevät, mihin suuntaan yritys on todellisuudessa menossa. Osana toimivaa riskienhallintaa johto pystyy huolehtimaan siitä, että yrityksen päämäärä, strategiset ja osatavoitteet ovat yhteneväisiä yrityksen riskinottohalun kanssa (COSO 2004, 35 – 40.) Moeller (2007, 60-61) korostaa virallisen päämäärän julistamisen tärkeyttä, jonka avulla voidaan myös muodostaa käsitys, millainen on yrityksen asenne riskejä kohtaan. Tämä auttaa yritystä valitsemaan, kehittämään ja toteuttamaan edellä mainitut tavoitteet, joiden toteutuminen pyritään varmistamaan kokonaisvaltaisen riskienhallinnan avulla. Näitä tavoitteita tarkastellaan lähemmin COSO ERM -mallin osa-alueiden tavoitteiden asettamisen osiossa.

Edellä mainitun tavoiteluokittelun avulla organisaatio voi keskittyä riskienhallintansa osa-alueisiin, jotka ovat kiinteä osa johtamisprosessia ja perustuvat siihen, kuinka organisaatiota johdetaan. Edellä esitellyt tavoitteet luokitteluineen (se, mihin organisaatio pyrkii) ja organisaation riskienhallinnan osa-alueet (se, mitä tarvitaan tavoitteiden toteuttamiseksi) ovat suorassa suhteessa toisiinsa. COSO ERM -viitekehyksen mukaisen kokonaisvaltaisen riskienhallinnan tavoitteiden ja osa-alueiden suoraa suhdetta toisiinsa kuvaa seuraava kuva eli COSO-kuutio.

**Kuva 2. Riskienhallinnan osa-alueet ja tavoitejaottelu COSO ERM -mallin mukaan**


Lähde: COSO ERM 2004, 41

## 3.2 Riskienhallinnan osa-alueet

COSO ERM -mallin mukaan organisaation riskienhallinta on monisuuntainen ja toistuva prosessi, jossa lähes kaikki osa-alueet vaikuttavat tai ainakin voivat vaikuttaa toisiinsa. Moellerin (2007, 102) mukaan COSO-kuution jokainen riskienhallinnan osa-alue ja osio liittyvät vahvasti toisiinsa. Esimerkiksi sisäisen toimintaympäristön osa-alueen tulee tarjota riittävät puitteet riskien mahdollisimman huolelliselle raportoinnille, jota puolestaan tukevat tapahtumien tunnistamisen ja riskien arvioimisen osa-alueet. Jokaista osa-aluetta tulisi tarkastella ja johtaa edellä tarkasteltujen strategisten, toiminnallisten, raportointia sekä vaatimusten mukaisuutta koskevien tavoitteiden sisältämien riskien näkökulmasta. Seuraavaksi tarkastellaan kutakin osa-aluetta COSO ERM -mallin viitekehyksen mukaan.

### 3.2.1 Sisäinen toimintaympäristö

Blummen ym. (2005, 36) mukaan sisäinen toimintaympäristö peilaa suoraan yrityksen valvontakulttuuria. Sisäinen toimintaympäristö toimii riskienhallinnan kaikkien muiden osa-alueiden perustana ja vaikuttaa siihen, miten strategiat ja tavoitteet määritellään, liiketoiminnot järjestetään ja riskit tunnistetaan, arvioidaan ja hoidetaan. Moeller (2007, 102) korostaa, että sisäisen toimintaympäristön sisältämä riskinhallintafilosofian määrittäminen ja ymmärtäminen sekä riskinottohalukkuuden tunnistaminen ovat keskeisimmät tekijät, joilla on vaikutus COSO ERM -mallin muihin osiin. Sisäinen toimintaympäristö voidaan jakaa kolmeen osaan: toimintakulttuuriin, organisaatioon ja resursseihin, joita käsitellään seuraavissa kappaleissa.

COSO ERM -mallin (2004, 27 – 34) sisältämään toimintakulttuuriin sisältyy riskienhallintafilosofia, joka viestitään ja huolehditaan sen merkityksen ymmärtämisestä kaikkialla organisaatiossa sekä sanoin että todellisten toimien avulla. Johdon toimintatapa ja filosofia vaikuttavat siihen, miten organisaatiota johdetaan. Riskinottohalukkuus kuvastaa yrityksen riskienhallintafilosofiaa ja vaikuttaa yrityksen kulttuuriin ja toimintatyyliin. Yritys voi menestyä huomattavasta riskienottohalukkuudesta huolimatta. Hallitus toimii suunnannäyttäjänä, jolla on merkittävä vaikutus johtamistapaan ja valvontakulttuuriin, koska hallituksen toiminta heijastuu suoraan yrityksen ylimpään johtoon. Hallituksen aseman tulisi säilyä itsenäisenä ja sen tulisi suurimmaksi osaksi muodostua ulkopuolisista ja riippumattomista jäsenistä, jotka kykenevät tasapuolisemmin arvioimaan, että johto toteuttaa tehokasta riskienhallintaa. Hallituksen tulisi käsitellä myös vaikeita ja ongelmallisia asioita. Hallituksen tulee myös olla tietoinen merkittävimmistä yritystä kohtaavista riskeistä ja siitä, että johto reagoi niihin asiaankuuluvalla tavalla. Hallituksen tulee myös tiedostaa yrityksen riskinottohalukkuuden taso. Rehellisyys ja eettiset arvot ovat yrityksen toimintakulttuurin tuotteita, jotka määrittelevät, miten organisaatiossa todellisuudessa toimitaan ja miten ylin johto haluaa yrityksen toimivan. Yrityksen työntekijöiden eettisten arvojen ja rehellisyyden taso määrittävät sisäisen valvonnan tehokkuuden tason. Yrityksen johdon antama esimerkki vaikuttaa siihen, miten yrityksessä käyttäydytään. Käyttäytymisnormeilla on olennainen vaikutus myös yrityksen maineeseen. Moeller (2007, 57) korostaa yrityksen menettelytapojen (code of

conduct) sisäistämisen tärkeyden merkitystä kaikkialla yrityksessä. Henkilövoimavaroja koskeva politiikat ja käytännöt viestivät henkilöstölle, mitä heiltä odotetaan. Sääntöjen rikkominen aiheuttaa toimenpiteitä, joka viestii organisaation suhtautumisesta sääntöjen rikkomiseen. Moellerin mukaan yrityksessä ei saisi olla niin sanottuja harmaan alueen toimintoja, vaan selkeitä käytäntöjä, jotka viestitään ja toteutetaan myös sidosryhmien suuntaan.

Sisäisen toimintaympäristön organisaatio-komponentti sisältää organisaation rakenteen, jota kehitetään vastaamaan yrityksen tarpeita ja mahdollistamaan yrityksen tavoitteiden saavuttamisen, niiden suunnittelun, toteutumisen ja valvonnan. Moeller (2007, 57) painottaa, että organisaation rakenteen tulisi tehokkaammin mukailla COSO ERM-mallia, koska huonosti organisoitu rakenne vaikeuttaa myös riskienhallinnan toimintojen suunnittelua, toteuttamista, valvontaa sekä seurantaa. COSO ERM -mallin mukaan liiketoiminnan luonne ja yrityksen koko vaikuttavat organisaatiorakenteen tarkoituksenmukaisuuteen. Valtuudet ja velvollisuudet jaetaan organisaatiossa usein monelle eri taholle, myös alaspäin, jolloin osa sisäisestä valvonnasta on yksilöillä, jotka ovat lähempänä ydinliiketoimintaa. Raportointisuhteiden ja valtuutusten dokumentointi on toimiva tapa, jossa määritellään työntekijöiden ongelmanratkaisukyky ja valtuuksien rajat. Blummen ym. (2005, 39) mukaan asianmukainen vastuiden ja valtuuksien jakaminen huomioi myös hyväksyttävän riskinottotason.

Kolmas sisäisen toimintaympäristön osa-alue on resurssit. Pätevyyteen sitoutuminen edellyttää johdon määrittämiä pätevyystasoja tietyille tehtäville ja niiden muuttamisen tiedoiksi ja taidoiksi. Johto ratkaisee myös sen, kuinka hyvin tehtävät tulee suorittaa. Henkilöstön pätevyyden mittaaminen tulee sopeuttaa yrityksen strategiaan ja tavoitteisiin. Vaaditun pätevyyden ja kustannusten välillä tulee myös vallita tasapaino. Blumme ym. (2005, 65) mainitsevat, että yrityksellä tulee lisäksi olla tarkoituksenmukaiset tietojärjestelmät sekä palvelut, laitteet ja tilat, joita tehtävien tuloksellinen hoito edellyttää.

COSO ERM -mallin keskeinen ajatus on, että jokainen organisaation työntekijä osallistuu jollakin tavalla organisaationsa riskienhallinnan prosessiin. Seuraavassa kappaleessa luodaan silmäys COSO ERM -mallin sisäiseen toimintaympäristöön liittyviin riskienhallinnan rooleihin ja vastuisiin, joilla on olennainen merkitys tehokkaan ja toimivan riskienhallinnan kannalta. Rooleja ja vastuita voidaan tarkastella COSO ERM -mallin avulla tekemällä jako sisäisiin ja ulkoisiin osapuoliin.

Riskienhallinnan roolit ja vastuut

Sisäiset osapuolet eli yrityksen henkilökunta käsittää hallituksen, jonka rooli riskienhallinnan suhteen on jo edellä tuotu esille. Riskin omistajuus on viime kädessä toimitusjohtajalla, jonka velvollisuutena on yhdessä ylemmän johdon kanssa huolehtia siitä, että jokainen riskienhallinnan toiminto on paikallaan. Toimitusjohtajalla on välitön raportointivelvollisuus hallituksen suuntaan, jos odottamattomat tapahtumat ovat ristiriidassa yrityksen riskinottohalukkuuden kanssa. Ylin johto on vastuussa omien vastuualueidensa riskienhallinnan osalta ja sen tulee ohjata riskienhallinnan komponentteja omien vastuualueidensa mukaisesti. Ylin johto ohjaa riskienhallinnan vastuuta muille johtajille, joilla on käytännönläheisempi rooli, esimerkiksi neuvojen jakaminen tapahtumien tunnistamistekniikoiden sekä riskien arvioinnin suhteen. Jokaisen yksikön johtajan tulee olla vastuussa ylemmälle johdolle omasta riskienhallinnan vastuualueestaan. Riskienhallintajohtaja toimii keskeisenä riskienhallinnan toimintojen yhdistäjänä, joka avustaa muuta johtoa asianmukaisessa riskiraportoinnissa sekä tukee ja mahdollistaa linjajohtajien roolia heidän vastuualueidensa riskienhallinnan osalta. Riskienhallintajohtajan tehtäviin voi kuulua myös riskienhallinnan menettelytapojen perustaminen, auktoriteettien ja vastuuvelvollisuuksien rajaaminen, riskienhallinnan edistäminen ja yhdistäminen liiketoiminnan muihin osa-alueisiin, yhteisen riskienhallinnan kielen perustaminen sekä viestiminen toimitusjohtajalle. Toimitusjohtajalla, talousjohtajalla tai muulla ylimmän johdon edustajalla voivat myös toimia riskienhallintajohtajan roolissa. Talousjohtajan rooli on riskienhallinnan osalta merkityksellinen, koska hänen työnkuvaansa kuuluu raportoinnin väärinkäytösten estäminen ja niiltä suojeleminen, ilmapiirin luominen eettisen toimintatavan suhteen sekä yrityksen raportointijärjestelmien suunnitteleminen,

toteutus ja seuranta. Talousjohtajan tulisi olla tasavertainen jäsen riskienhallinnan päätöksiä tehtäessä. Sisäinen tarkastus puolestaan avustaa johtoa ja hallitusta tutkimalla, arvioimalla, raportoimalla ja suosittelemalla parannuksia riskienhallinnan toimivuuden ja tehokkuuden suhteen. Jokainen organisaation työntekijä voi myös tuottaa sellaista tietoa, jota käytetään riskien tunnistamisessa tai arvioimisessa. He ovat velvollisia tukemaan riskienhallintaan liittyvän tiedon eteenpäin viemistä ja tarvittaessa raportoimaan ylemmälle taholle esimerkiksi mahdollisista väärinkäytöksistä. Organisaation riskienhallinta on siis jokaisen työntekijän velvollisuus ja nämä roolit ja velvollisuudet tulisi määritellä hyvin sekä viestiä tehokkaasti jokaiselle (COSO ERM 2004, 84–89.)

Ulkoisia osapuolia riskienhallinnan vastuiden ja roolien suhteen ovat esimerkiksi ulkopuoliset tarkastajat, jotka taloudellisen raportoinnin lisäksi konsultoivat johtoa esimerkiksi tuomalla esiin havaitsemiaan puutteita riskienhallinnassa tai sen valvonnassa sekä antavat suosituksia niiden parannusten osalta. Lainsäätäjät ja viranomaiset luovat sääntöjä, jotka auttavat johtoa asettamaan lakisääteiset ja säännönmukaiset vähittäisvaatimukset riskienhallinnalle ja tarjoavat asianmukaista tietoa, suosituksia ja ohjeistuksia riskienhallinnan soveltamisessa sekä tarvittavissa parannuksissa. Asiakkaat, liiketoimintakumppanit, myyjät ja velkojat tarjoavat riskienhallinnan osalta tärkeää tietoa, joka voi vaikuttaa riskienhallinnan tavoitteiden toteutumiseen, esimerkiksi yllättävä kysynnän kasvu, eroavaisuudet laskutuksissa, henkilöstön epärehellinen tai epäeettinen toiminta tai mahdolliset maksuvaikeudet. Yrityksellä tulee olla resursseja tällaisen tiedon vastaanottamiseen sekä siihen reagoimiseen. Ulkoistetut palveluntarjoajat toimivat yrityksen puolesta monien päivittäisten liiketoimintojen osalta. Analyytikot ja tiedotusvälineet voivat tarjota näkemyksiä, miten muut tahot hahmottavat yrityksen suorituskyvyn, yritystä kohtaavat taloudelliset ja toimialariskit, toimialan trendit ja voimassa olevien strategioiden vaikutuksen yrityksen suorituskykyyn (COSO ERM 2004, 89-91.)

Sisäisellä toimintaympäristöllä on siis olennainen merkitys riskienhallinnan toimivuudelle ja onnistumiselle ja se luo riskienhallinnan perustan. Ilman sen osatekijöiden toimivuutta ja samaan suuntaan katsomista ei yrityksen riskienhallinta voi onnistua. Seuraavaksi tarkastellaan tavoitteiden asettamista COSO ERM -mallin mukaisesti.

### 3.2.2 Tavoitteiden asettaminen

COSO ERM -mallin mukaan tavoitteiden asettamisessa tavoitteet laaditaan ensin strategisella tasolla, jonka avulla luodaan perusta toiminnallisille, raportoinnin ja vaatimuksenmukaisuutta koskeville tavoitteille. Näiden osatavoitteiden avulla voidaan tunnistaa kriittiset menestystekijät ja ymmärtää sekä viestiä ne tehokkaammin läpi koko organisaation. Ilman onnistuneita osatavoitteita yritys ei voi saavuttaa suurempia strategisia tavoitteitaan. Nämä neljä erillistä, mutta osittain päällekkäistä (tavoite voi sisältyä useaan luokkaan) tavoiteluokkaa soveltuvat organisaatioiden erityyppisiin tarpeisiin ja voivat olla eri johtajien vastuulla. Luokittelun avulla voidaan myös tehdä ero yksittäisiin luokkiin kohdistuvien odotusten välillä. Toimintojen johdonmukainen suunnittelu, seuranta ja ohjaus sekä niihin liittyvä tavoitteiden määrittely ovat edellytyksiä tavoitteita uhkaavien riskien tunnistamiselle. Riskienhallinnalla varmistetaan, että johdolla on käytössään toimiva prosessi tavoitteiden asettamiseen, valitut tavoitteet ovat organisaation toiminta-ajatusta tukevia ja ne ovat sopusoinnussa organisaation riskinottohalukkuuden kanssa. Tavoitteiden tulee linkittyä organisaation eri tasoille ja olla sisäisesti yhdenmukaisia. Alempien tason tavoitteiden tulee palvella ylemmän tason tavoitteita, jotka puolestaan palvelevat yrityksen kokonaistavoitteita (COSO ERM 2004, 35 - 40.) Blumme ym. (2005, 65) mainitsevat, että organisaation perustehtävän tulisi olla kaikkien organisaation jäsenten tiedossa. Moeller (2007, 62) korostaa tavoitteiden asettamisen suhteen jälleen kerran virallisen päämäärän merkitystä, koska se määrittää yrityksen tavoitteet ja kuvastaa sen asenteen riskejä kohtaan. Huolellisesti julistettu päämäärä auttaa yrityksiä suunnittelemaan ensin strategiset ylätason tavoitteet, jonka jälkeen ne voivat laatia niiden osa-tavoitteet.

Tavoitteen asettaminen on edellytys COSO ERM -mallin seuraaville osa-alueille eli tapahtumien tunnistamiselle, riskien arvioinnille ja riskeihin vastaamiselle, jotka muodostavat riskienhallintaprosessin ytimen. Loput osatekijät muodostavat riskienhallintaprosessin kontekstin ja taustan, jossa riskienhallintaprosessi toimii.

### 3.2.3 Tapahtumien tunnistaminen

Tapahtumien tunnistamisessa tunnistetaan organisaation tavoitteiden toteutumiseen vaikuttavat sisäiset ja ulkoiset tapahtumat ja samalla tehdään ero mahdollisuuksien ja riskien välillä. Riskien tunnistaminen on jatkuva kertautuva prosessi, joka on tehokkaan sisäisen valvonnan kriittinen osatekijä. Mahdollisuudet kanavoidaan takaisin johdon strategian- ja tavoitteenasetteluun. Negatiiviset tapahtumat edustavat riskiä, joka vaatii johdon arviointia ja reagoimista. Riskienhallintaprosessin kannalta tämä vaihe tarkoittaa riskien tunnistamista ja kirjaamista. Tapahtumia tunnistettaessa johto käy säännöllisesti läpi koko organisaation laajuisesti erilaisia sisäisiä ja ulkoisia tekijöitä, jotka voivat aikaansaada mahdollisuuksia tai riskejä. Ulkoisia tekijöitä voivat olla taloudelliset, ympäristö, poliittiset, sosiaaliset tai teknologiset tekijät. Sisäisiä tekijöitä voivat olla rakenteellisiin, henkilöstöön, prosessiin ja teknologiaan liittyvät tekijät. Tapahtumia pitäisi myös tunnistaa toimintojen tasolla. Tämä auttaa COSO ERM -mallin seuraavan osatekijän eli riskien arvioinnin toimintayksiköissä tai osastoilla. Organisaatiotason riskien aiheuttamia seikkoja voivat olla esimerkiksi taloudelliset muutokset, kilpailuun tai lainsäädäntöön liittyvät asiat, asiakkaiden vaihtuvat odotukset ja tarpeet sekä teknologian kehitys. Toimintokohtaisia riskejä voivat olla johtamisvelvollisuuksien muutokset, tiedonkulun katkeaminen, muutokset toiminnassa, tehoton hallitus sekä henkilöstön laatu (COSO ERM 2004, 41-47.)

Tapahtumien tunnistamistekniikoita voivat olla tapahtumien inventointi, sisäiset analyysit, tapahtumien nopeuttaminen tai kiihdyttäminen, työpajat ja haastattelut, prosessin etenemisen analyysit, tapahtumaan johtavien tekijöiden seuranta sekä yksittäisten tapahtumien syyn tunnistaminen (COSO 2004, 41 - 47). Blummen ym. (2005, 65) mukaan riskien tunnistaminen on kattavaa ja systemaattista ja sen tulee kattaa keskeiset hankkeet ja projektit koko yrityksen osalta. Suomisen (2003, 40) mukaan riskikohteiden tunnistaminen on toimivan riskianalyysin edellytys. Monipuolisen ja toimivan tunnistamisvälineistön avulla saadaan päivänvaloon myös piileviä riskejä, joiden olemassaolosta yritys ei ole ollut lainkaan tietoinen. Riskianalyysi tulee toteuttaa huolellisesti ja järkevästi. Seuraavassa osiossa tarkastellaan COSO ERM -mallin riskien arvioinnin osa-aluetta.

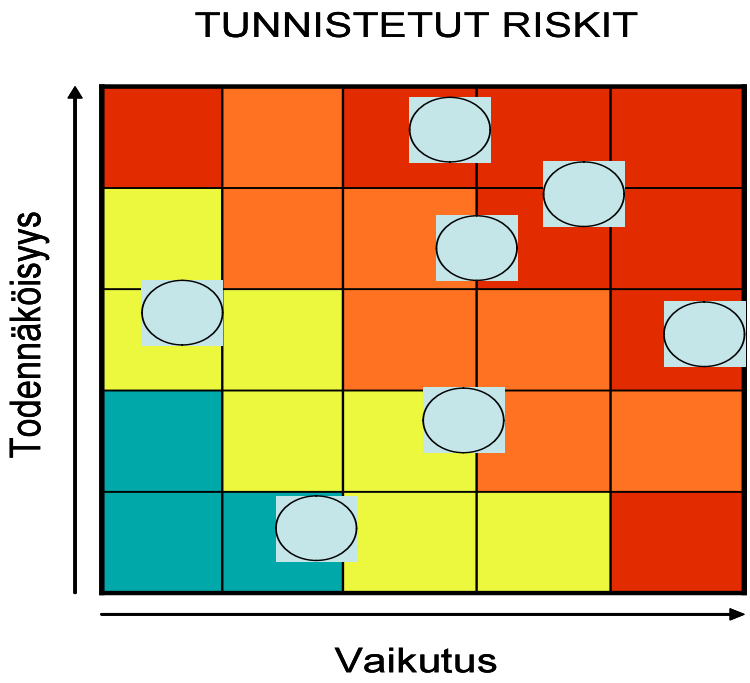
### 3.2.4 Riskien arviointi

Riskien arvioinnissa otetaan huomioon niiden todennäköisyys ja vaikutukset, minkä pohjalta päätetään, kuinka ne on hallittava. Jokaisen yrityksen toimintaan kohdistuu ulkoisista tai sisäisistä lähteistä peräisin olevia riskejä, jotka pitää arvioida. Riskien arviointi on yrityksen tavoitteiden saavutettavuutta uhkaavien tekijöiden analysointia ja määrittämistä. Riskit voidaan arvioida bruttoriskeinä ja jäännösriskeinä. Riskien arviointi on riskienhallintaprosessin toinen vaihe, jossa riskit priorisoidaan ja valmistaudutaan toimenpiteisiin niiden saattamiseksi halutulle tasolle. Riskien arvioinnissa tulee tunnistaa muuttuneet olosuhteet ja ryhtyä tarvittaviin toimenpiteisiin niiden suhteen. Tunnistaessaan riskejä riskin arvioinnin yhteydessä johdon tulee kohdistaa niihin tarvittavat valvontatoimenpiteet, joita käsitellään tutkielman COSO ERM -mallin valvontatoimenpiteiden osiossa. Riskien arviointi muodostaa pohjan päätöksille, jotka määrittävät, miten riskejä tullaan hallitsemaan (COSO ERM 2004, 49 – 54.) Moellerin (2007, 73) mukaan riskien arviointi on COSO ERM -mallin ydin, koska se saa yrityksen pohtimaan, kuinka paljon mahdolliset riskit mahdollisesti vaikuttavat sen tavoitteiden saavuttamiseen. Blumme ym. (2005, 66) tähdentävät, että riskejä tulee arvioida objektiivisesti ja säännöllisesti ja olennaiset riskit on arvioitava riittävän kattavasti.

Riskejä arvioidaan ja tunnistetaan systemaattisissa riskikartoituksissa, joiden tavoitteina on löytää ja yksilöidä uhkia. Yleisin kartoitusmenetelmä on riskien itsearviointi. Riskiä mitataan yleisimmin tapahtuman todennäköisyyden ja vaikutuksen suuruuden avulla, jota arvioitaessa määritellään ensin ns. bruttoriski eli riskin todennäköisyys ja vaikutus ilman hallintakeinoja. Tästä edetään riskin hallintakeinon tunnistamisen ja vaikutuksen arvioinnin kautta netto- eli jäännösriskin määrittämiseen. Yrityksen riskinottohalusta ja riskinottokyvystä riippuen jäännösriski on joko hyväksyttävissä tai sitten hallintakeinoa pitää tehostaa. Tunnistetut ja arvioidut riskit voidaan esittää riskimatriisissa, joka visualisoi yrityksen riskiavaruuden (Blumme ym. 2005, 81.) Seuraava kuva on esimerkki riskimatriisista. Matriisin värit kertovat suhtautumisesta riskiin. Punaisiin matriisin osiin osuvat riskit on välittömästi saatava parempaan hallintaan ja vihreille alueille osuvat riskit voidaan puolestaan hyväksyä sellaisinaan. Näin matriisilla voidaan esittää organi-

saation riskinottohalukkuus yhdellä havainnollisella tavalla. Riskien asemoituminen matriisiin perustuu yleensä ainakin osin subjektiivisiin näkemyksiin, mikä vähentää tällaisen esityksen luotettavuutta todellisesta riskiavaruudesta.

**Kuva 3. Riskimatriisi: tunnistettujen riskien asemoituminen matriisiin riskin todennäköisyyden ja vaikutuksen perusteella**




Lähde: Blumme ym. (2005, 81)

Riskien arviointimetodologia koostuu COSO ERM -mallin (2004, 52-53) mukaan kvalitatiivisista sekä kvantitatiivisista menetelmistä. Johto turvautuu usein laadullisiin arviointimenetelmiin kun riskit eivät ole laskettavissa, tietoa ei ole riittävästi saatavilla laskennallisiin analyyseihin tai niiden analysointi ei ole kustannustehokasta. Kvantitatiiviset menetelmät täydentävät laadullisia arviointimenetelmiä, tuovat riskien arviointiin enemmän tarkkuutta ja niitä sovelletaan monimutkaisissa ja pitkälle viedyissä toiminnoissa. Kvantitatiiviset menetelmät soveltuvat parhaiten tilanteisiin, joissa aikaisemmat tapahtumat ovat tiedossa, säännöllisiä ja sallivat luotettavan ennustamisen. Kvantitatiivisia arviointimenetelmiä ovat vertaaminen muihin tekijöihin, todennäköisyysmallit ja ei-todennäköisyysmallit, jotka tukeutuvat subjektiivisiin arviointeihin

arvioidessaan tapahtumien vaikutusta ilman todennäköisyyksien laskemista. Ei-todennäköisyysmenetelmistä esimerkkinä on herkkyysanalyysi, jota tutkielman kohdeyritykset ovat myös käyttäneet. Herkkyysanalyysia käytetään arvioitaessa tavanomaisten tapahtumien vaikutusta tai muutoksia mahdollisissa tapahtumissa. Riskien luonne ja miten ne liittyvät tilanteeseen, vaikuttavat arviointimenetelmien valinnan. Yrityksen johdon vastuulla on tarkastella riskien keskinäisiä suhteita ja vaikutuksia.

Tilinpäätökseen liittyvässä toimintakertomuksessa tulee arvioida merkittävimpiä riskejä ja epävarmuustekijöitä. Riskit voidaan toimintakertomuksessa jakaa esimerkiksi strategisiin, operatiivisiin, rahoitus- sekä vahinkoriskeihin. Omia luokitteluryhmiä voi myös käyttää, mutta tällöin tulee määritellä, mitä kullakin riskiluokalla tarkoitetaan. Samalla voidaan kuvata keinot ja välineet, joita hyödynnetään riskien ja epävarmuustekijöiden hallinnassa sekä se, jos näitä ei ole käytössä. Yrityksen strategiset riskit voidaan kirjanpitolautakunnan yleisohjeen (toimintakertomuksen laatiminen) mukaan jakaa kilpailutilanteeseen markkinoilla ja valintoihin maantieteellisistä alueista, joilla yritys toimii sekä yrityksen asemaan tuotantoketjussa. Strategiset riskit voidaan lisäksi jakaa riippuvuuteen rajoitetusta määrästä asiakkaita, muutoksiin asiakaspreferensseissä sekä teknologiseen kehitykseen. Operatiiviset riskit voivat koskea esimerkiksi riippuvuutta henkilöstön osaamisesta, epätavallisia suhdannevaihteluita kysynnässä, häiriöitä toimitusketjussa , raaka-aineiden ja muiden tuotannontekijöiden hintavaihteluita ja patenttien ja muiden teollisoikeuksien pitävyyttä. Rahoitusriskit taas voidaan ryhmitellä korko-, valuutta-, likviditeetti- ja luottoriskiin (Kirjanpitolautakunta.)

Riskien erilaiset luokittelut helpottavat riskien tunnistamista ja hallintaa. Riskejä jaotellaan paitsi luonteen, myös sen mukaan, mihin yrityksen toimintoihin ne voivat vaikuttaa. Riskit jaetaan niin sanottuihin riskilajeihin ja moni riski voi kuulua useampaankin riskilajiin. Esimerkiksi tuoteriskit ovat yleensä myös liikeriskejä (Pk-yrityksen riskienhallinta.) Kyseisellä sivustolla riskit luokitellaan liikeriskeihin, tuoteriskeihin, henkilöriskeihin, sopimus- ja vastuuriskeihin, ympäristöriskeihin, tietoriskeihin, projektiriskeihin, keskeytysriskeihin, rikosriskeihin sekä paloriskeihin. Liikeriskit puolestaan voidaan luokitella seuraavan kuvan osoittamalla tavalla.

**Kuva 4. Liikeriskit**


Lähde: Pk-yrityksen riskienhallinta

Dynaamiset riskit muuttuvat suhdanteiden ja olosuhteiden mukaan. Tekniset, taloudelliset ja poliittiset riskit kuuluvat useimmiten liikeriskeihin, koska niistä voi seurata yhtä hyvin voittoa kuin tappiota. Dynaamisia riskejä kutsutaan myös spekulatiivisiksi riskeiksi, koska toimija voi itse vaikuttaa niihin eikä niitä yleensä voi siirtää muiden kannettaviksi. Staattisista eli vakuutusriskeistä ei taas voi seurata voittoa, ainoastaan menetyksiä. Ne ovat yrityksen tai yksilön tahdosta riippumattomia. Tietty määrä vahingollisia tapahtumia sattuu, vaikka riskien olemassaolo tiedostettaisiin kuinka hyvin. Staattisten riskien toteutumisen todennäköisyys on helpommin arvioitavissa kuin dynaamisten riskien todennäköisyys. Staattisia riskejä voidaan kutsua myös puhtaiksi riskeiksi. Puhdas riski liittyy tilanteeseen, jossa vaihtoehtona on joko tilanteen säilyminen ennallaan tai menettämisen mahdollisuus. Puhtaat riskit voidaan jakaa henkilöihin tai omaisuuteen kohdistuviin sekä vastuu- ja riippuvuusriskeihin (Kuusela & Ollikainen 2005, 33 -34.)

Riskejä voidaan siis luokitella usealla eri tavalla. Tutkielman empiirisen analyysin osassa käytetään yksinkertaista perusluokittelua, joka mahdollistaa riskitietojen vertailun kohdeyritysten vuosikertomus- ja tilinpäätöstiedoissa. Luokittelu jaottelee riskit strategisiin, operatiivisiin ja taloudellisiin/rahoitukseen liittyviin riskeihin.

### 3.2.5 Riskeihin vastaaminen

Riskien vastaamisen suhteen organisaation johto päättää, millaisiin riskeihin vastataan ja millä tavalla. Organisaation riskinottohalukkuus tai riskinottokyky määrittää sen strategian, jonka organisaatio valitsee hallitakseen ja hoitaakseen vastaan tulevat riskit (Matyjewicz & D´ Arcangelo 2004, 67.) COSO ERM -mallin (2004, 55) mukaan yrityksen johdon tulee ottaa koko yrityksen laajuinen tai portfolio-näkökulma riskeihin ja arvioida, että jäännösriski on riskinottohalukkuuden rajoissa. Riskien vastaamisen vaiheessa päätetään kunkin riskin riskienhallintastrategiasta eli siitä, millaisiin toimenpiteisiin ryhdytään riskien pienentämiseksi. Riskienhallintamenettelyt perustuvat kustannus- ja/tai hyötyarviointiin. Moellerin (2007, 81-82) mukaan riskienhallintamenettelyjä tulee arvioida liiketoiminnan, osastojen ja toimintojen näkökulmasta, jotta saataisiin todellinen kokonaiskuva yrityksen riskien vaikutusten tai todennäköisyyden laajuudesta koko organisaation tasolla. Moellerin mukaan riskien vastaamisen vaihe on kenties kaikkein vaikein COSO ERM -mallin vaihe, koska läheskään kaikkia riskejä ei nähdä konkreettisesti (mt. 79). Blumme ym. (2005, 82) esittävät, että yrityksen johdon tulee valita keinot tunnistettujen sekä merkittävien riskien hallitsemiseksi yrityksen riskienhallintastrategian mukaan. Tavoitteena on riskien toteutumisen todennäköisyyden optimointi, koska kaikkia riskejä ei pystytä eliminoimaan ja toteutuvat riskit yrityksen on oltava valmis kantamaan. Toimivien riskienhallintakeinojen avulla riskit saadaan siirrettyä hyväksyttävälle tasolle, joka vastaa yrityksen riskienhallintastrategiaa ja riskinottokykyä.

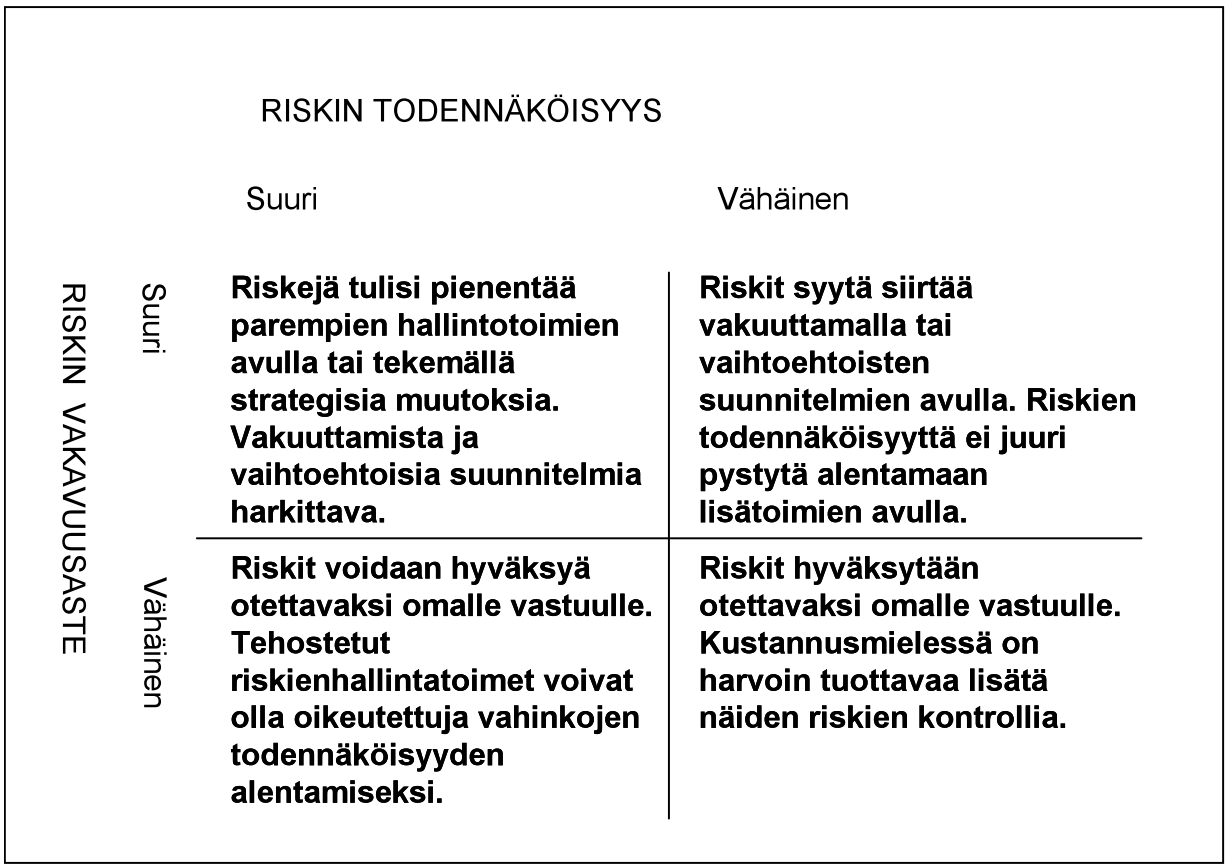
Tavallisimpia riskienhallinnan keinoja COSO ERM -mallin (2004, 55) mukaan on riskin välttäminen, jossa pois suljetaan riskiä lisäävät tekijät, esimerkiksi tuotantolinjan sulkeminen, tietyn osan myyminen tai uuden markkina-alueen rajaaminen. Riskiä vähentämällä pyritään vähentämään riskin todennäköisyyttä ja/tai vaikutusta. Tämä koskee esimerkiksi lukematonta määrää päivittäisiä liiketoiminnan päätöksiä. Riskin jakamisessa siirretään tai jaetaan jotakin riskin osaa, esimerkiksi vakuuttamalla, ulkoistamalla tai sijoittamalla. Riskejä hyväksymällä ei ryhdytä minkäänlaisiin toimenpiteisiin riskin todennäköisyyden tai vaikutuksen suhteen. Suomisen (2003, 101 -102) mukaan

riskienhallintakeinojen ”äitinä” ja peruskeinona voidaan pitää riskin välttämistä, jota soveltamalla yritys pidättyy riskialttiiseen omaisuuteen, henkilöön tai toimintaan kohdistuvista toimista. Riskin vähentäminen puolestaan tähtää vahinkotapahtuman todennäköisyyden tai seurausten pienentämiseen. Riskin jakaminen on keskeinen liikeriskien hallinnan menetelmä, jonka avulla tähdätään yksipuolisuudesta aiheutuvien riskien torjumiseen (mt. 104). Riskienhallintakirjallisuudessa suojaustoimenpiteet ovat perinteisesti painottuneet vahinkoriskien hallintaan johtuen paljolti siitä, ettei liikeriskien suojaukseen ole ollut saatavilla vakuutuksellisia ratkaisuja (Kuusela & Ollikainen, 2005, 158). Kokonaisvaltainen riskienhallinta ja sen integrointi johtamisjärjestelmäkokonaisuuteen alkaa vihdoin antaa organisaatioille todellisia välineitä myös liikeriskeiltä suojautumiseksi. Suomisen (2003, 159-162) mukaan vakuuttaminen riskienhallintamenetelmänä painottuu päätöksenteossa erityisesti silloin, kun sekä riskien todennäköisyyttä että riskien vakavuusastetta pidetään riittävän suurina. Päätöksentekomielessä tämä vaihtoehto on mielenkiintoisin: pyritäänkö suureksi koetulle riskille löytämään vakuutuksen asemasta jokin muu riskienhallinnallinen ratkaisu. Riskit voidaan myös hyväksyä otettavaksi omalle vastuulle. Tehostetut riskienhallintatoimet voivat olla oikeutettuja vahinkojen todennäköisyyden alentamiseksi.

Kuuselan & Ollikaisen (2005, 158) mukaan hyvältä riskienhallinnalta voidaan edellyttää kaikkien tunnettujen riskienhallintakeinojen tehokasta soveltamista. Päätöksenteon perimmäiseksi hyvyys-kriteeriksi muodostuu tällöin yrityksen riskinkantokyvyn oikea mitoitus. Systemaattisesti hoidettu riskienhallinta turvaa yrityksen toiminnan jatkumisen ja toimivan riskienhallinnan turvin yrityksellä on enemmän potentiaalia kohdata paitsi tavanomaisia myös uusia ja tuntemattomia riskejä. Seuraava kuva kertoo, millaisia vaihtoehtoja yrityksellä on arvioidessaan riskien todennäköisyyden ja vaikutusten mahdollisuutta omaan riskinottokykyynsä. Peruskysymyksenä kuvaa tarkastellessa on, kuinka paljon yritys analysoi omia mahdollisuuksiaan sekä riskinottokykyään pyrkiessään löytämään sille soveltuvat riskienhallinnan välineet ja keinot. Esimerkiksi vakuutuspainotteinen riskienhallintakeino on helppo ja turvallinen silloin, kun riskin todennäköisyys on alhainen, mutta riittävien vakuutusten avulla voidaan suojautua riskin vakavammilta vaikutuksilta. Riskin vakavuusasteen ja riskin todennäköisyysasteen ollessa korkea, yritys voi soveltaa strategiaansa tehdessään riskienhallintaratkaisuja riskinotto-

kykynsä mukaan. Tällainen toimintatapa integroi yrityksen riskienhallinnan yrityksen päätöksentekoon mukaan, jossa riskienhallinta on luontainen osa johtamisjärjestelmää, eikä erillinen toiminto. Samanlainen ajattelutapa liittyy myös kokonaisvaltaisen riskienhallinnan COSO ERM -malliin, jonka yhtenä perusajatuksista on yrityksen strategian, riskinottokyvyn ja –halun yhdenmukaistaminen.

**Kuva 5. Riskienhallintapäätöksiä koskevat vaihtoehdot**




Lähde: Kuusela & Ollikainen 2005, 159

### 3.2.6 Valvontatoimenpiteet

Valvontatoimenpiteiden avulla laaditaan ja toteutetaan ne toimintalinjat ja menettelytavat, joiden avulla pystytään tehokkaasti vastaamaan riskeihin. Blumme ym. (2005, 66-67) korostavat valvontatoimenpiteiden suunnittelussa keskeisten toimintaprosessien ja niihin liittyvien riskien ja valvontatoimenpiteiden kuvaamista sekä ajan tasalla olevaa jatkuvuussuunnitelmaa. Valvontatoimenpiteiden tulee lisäksi kattaa toiminnan ja talouden laillisuuden, hallinnassa olevien omaisuuden ja varojen turvaamisen, toiminnan tuloksellisuuden sekä johtamisen ja ulkoisen ohjauksen edellyttämät todenmukaiset ja riittävät talouteen ja toimintaan liittyvät tiedot. Johdon tulee päättää käytettävistä valvontatoimenpiteistä. COSO ERM -mallin (2004, 64) mukaan valvontatoimenpiteisiin liittyy kaksi keskeistä tekijää: politiikka eli toimintaperiaate, joka määrittää, mitä pitäisi tehdä sekä toimenpiteet, joilla politiikka toteutetaan. Politiikat viestitään usein suullisesti ja niitä tulee toteuttaa tunnollisesti, johdonmukaisesti ja syvällisesti, koska ilman tarkkaa keskittymistä yksittäinen toimenpide on hyödytön. Valvontatoimenpiteiden avulla varmistetaan, että yrityksessä toimitaan johdon antamien toimintaohjeiden mukaisesti. Valvontatoimenpiteitä toteutetaan läpi koko organisaation kaikilla tasoilla ja kaikissa toiminnoissa ja niiden tehtävänä on kohtuullisen varmuuden tuottaminen yrityksen tavoitteiden saavuttamisen suhteen.

Valvontatoimenpiteet voidaan jaotella COSO ERM -mallin (2004, 61-66) mukaan esimerkiksi ennalta estäviin, paljastaviin, manuaalisiin, tietoteknisiin ja johtamiskontrolleihin. Valvontatoimenpiteet jaetaan sen mukaan, millä tavalla eri tasoilla toimiva henkilöstö on niistä vastuussa. Ylimmän tason katsauksissa toimintojen suorittamista verrataan budjettiin, ennusteisiin, aikaisempiin ajanjaksoihin ja kilpailijoihin. On tärkeää saada selville, missä laajuudessa tavoitteet on saavutettu. Operatiivinen johto tarkastelee yksikkönsä suoritusraportteja. Informaation tuottamisessa luodaan kontrollit, joiden avulla tarkistetaan liiketoimien paikkansapitävyyttä, loppuunsaattamista ja toimintavaltuuksia. Fyysisissä kontrolleissa laitteet, tavaraluettelot, arvopaperit, kassa ja muut varat turvataan fyysisesti ja lasketaan säännöllisesti sekä verrataan niitä kontrolliluetteloihin. Suoritusmittareissa yhdistetään toiminnallista tai taloudellista tietoa toisiin-

sa yhdessä suhteiden analysoimisen, tutkivien ja korjaavien toimien kanssa. Tehtävien eriyttämisessä työtehtävät jaetaan tai erotellaan eri ihmisten kesken, jotta vältytään virheriskiltä tai sopimattoman käyttäytymisen aiheuttamalta riskiltä. Ratliff ym. (1996, 101) jakavat valvontatoimenpiteet ehkäiseviin kontrolleihin, jotka estävät virheiden ja epäonnistumisten syntymistä, etsiviin kontrolleihin, jotka on suunniteltu löytämään tapahtuneita virheitä, korjaaviin kontrolleihin, jotka korjaavat löytyneitä virheitä sekä ohjaaviin kontrolleihin, jotka on suunniteltu edistämään positiivisia tuloksia. Lisäksi voidaan määritellä kompensoivat kontrollit, joita voidaan hyödyntää ensisijaisen kontrollin ollessa puutteellinen.

### 3.2.7 Informaatio ja tiedonkulku

Informaation ja tiedonkulun osa-alue ylläpitää organisaation vuorovaikutus- ja raportointikanavia, joiden avulla yrityksen johto, henkilöstö ja sidosryhmät saavat käyttökelpoista, olennaista ja ajan tasalla olevaa tietoa toimintaan vaikuttavista tekijöistä (Blumme ym. 2005, 67). Tietojärjestelmät tuottavat raportteja, jotka sisältävät toiminnallista, taloudellista ja lainsäädäntöön liittyvää tietoa. Sisäisesti luodun tiedon lisäksi käsitellään tietoa ulkoisista tapahtumista, toiminnasta ja olosuhteista. Tämä on tarpeellista asioista perillä oleville päätöksentekijöille sekä ulkoiselle raportoinnille. Tehokkaan viestinnän tulee kulkea organisaatiossa ylhäältä alas, poikittain sekä alhaalta ylös. Ylin johto viestii koko henkilöstölle selvästi sen, että valvontavelvollisuuksiin tulee suhtautua vakavasti. Organisaation henkilöstön olisi hyvä ymmärtää oma roolinsa valvontajärjestelmässä sekä yksilökohtaisten tehtävien suhde toisten tekemään työhön. Henkilöstöllä tulisi olla käytössään välineet viestittää merkittävää tietoa yrityksessä ylöspäin. Tehokasta viestintää tarvitaan myös ulkoisten osa-puolien suuntaan, kuten asiakkaisiin, tavaran toimittajiin, osakkeenomistajiin ja muihin sidosryhmin. Tämä on tärkeää palautteen vastaanottamisen sekä yrityksen omien toimintaperiaatteiden julkistamisen kannalta (COSO ERM 2004, 67-74.)

Myös osakkeenomistajien, lainsäätäjien ja analyytikoiden olisi hyvä saada yrityksiltä tietoa, joka palvelee heidän tarpeitaan ja jotta he kykenevät ymmärtämään, millaisia riskejä ja millaisissa olosuhteissa yritys toimii. Tämän viestinnän tulisi olla asiaankuu-

luvaa ja ajanmukaista ja sen tulee olla yhdenmukainen lakien ja muiden säännösten kanssa (COSO ERM 2004, 67 - 74.) Moellerin (2007, 87-88) mukaan yrityksillä on tarve kehittää sellainen riskien valvonta- ja viestintäjärjestelmä, joka yhdistää sen tärkeimmät sidosryhmät yhteen ja joiden avulla tärkeimmät sidosryhmät saisivat tietoa yrityksen kiinnostuksesta hallita riskejään. Moeller painottaa, että jos yritykset eivät viesti riskienhallinnastaan kokonaisvaltaisesti sen tärkeimmille sidosryhmille, ei niiden riskienhallinnan hankkeilla ole suurta arvoa. Omistajia voi esimerkiksi informoida ja varoittaa osallistumasta liian riskisiin hankkeisiin. Toisaalta väärin tai liian heppoisin perustein tulkitut viestit saattavat johtaa virheellisiin ja riskisiin päätöksiin. Kantavana ajatuksena jälleen kerran on viestiä yrityksen kokonaisvaltaisen riskienhallinnan tärkeyden merkitys läpi koko organisaation ja yrityksen tärkeimmille sidosryhmille. Riskienhallinnan raportointi muodostuu COSO ERM -mallin tavoitteiden kautta, mutta tiedon ja viestinnän osasta löytyy myös raportointia koskevia yhtäläisyyksiä. Tutkielman aihepiiriä tarkastellessa onkin hyvä pitää mielessä, kuinka paljon COSO ERM -viitekehikon tiedon ja viestinnän osio pitää sisällään ulkopuolisille sidosryhmille suuntautuvaa raportointia.

### 3.2.8 Seuranta

Seurannan avulla toteutetaan sisäisen valvonnan ja riskienhallinnan tehokkuuden kehittämistä ja arviointia. Moeller (2007, 86, 89) kirjoittaa, että vaikka kyseinen osa-alue on COSO ERM -mallin kuutiossa yksin alhaalla, on sillä kuitenkin kokonaisvastuu mallin kaikkien muiden osa-alueiden tarkastelussa. Seuranta määrittää jokaisen muun osion toiminnan, koska sen perustavin tarkoitus on seurata, kuinka hyvin COSO ERM-viitekehys toimii yrityksessä. Toimiva seuranta antaa myös vinkkejä, missä kohtaa voidaan parantaa toimintaa (mt. 92.) Seuranta tarvitsee prosessia, jonka avulla valvontajärjestelmän toimintaa voidaan arvioida jatkuvasti. Yrityksen riskienhallinnan puutteet raportoidaan ylemmälle johdolle ja vakavimmat puutokset raportoidaan välittömästi johtoryhmälle. Sisäisen valvonnan järjestelmiä ovat COSO ERM -mallin (2004, 75-82) mukaan esimerkiksi jatkuva seuranta, joka liittyy tavanomaiseen, päivittäiseen toimintaan. Jatkuva seuranta tulisi liittää yrityksen toistuviin ja normaaleihin toimintarutiineihin, koska siellä se toimii ajantasaisesti, reagoi muuttuviin olosuhteisiin ja on syvään

juurtuneena yrityksen toimintaan. Jatkuvaan seurantaan kuuluu säännönmukaiset johtamis- ja ohjaustoimet, vertailut, täsmäytykset ja muut rutiinitehtävät. Valvontaa suorittavien ihmisten kokemus ja pätevyys tulee myös ottaa huomioon. Erillisten arviointien suhteen on arvioitava tapahtuvien muutosten luonne ja aste, niihin liittyvät riskit sekä valvontaa suorittavien ihmisten pätevyys ja kokemus. Erilliset arvioinnit voivat kohdistua koko valvontajärjestelmään tai yksittäisiin hallintamenettelyihin. Syitä, miksi johto voi päättää erillisen arvioinnin tarpeellisuudesta, voivat olla esimerkiksi suuret hankinnat tai käyttöönotot, merkittävä strategia- tai johtamismuutos tai muutokset toiminnassa tai taloudellisen informaation tuottamisessa.

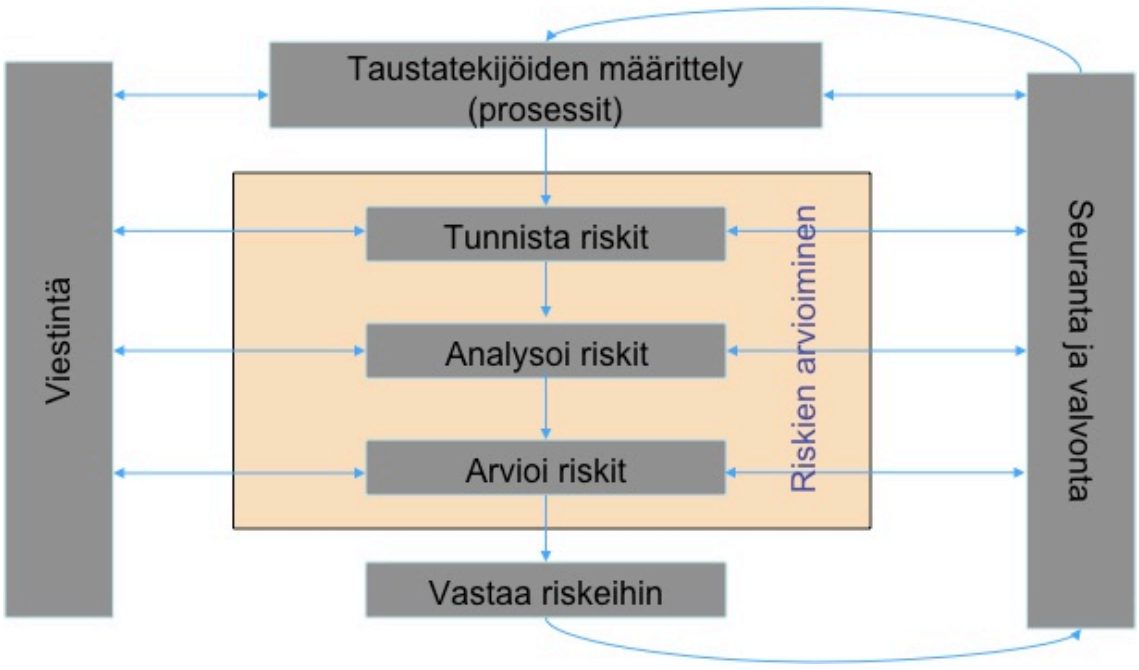
Puutteet yrityksen riskienhallinnan toimivuuden suhteen voidaan havaita monesta suunnasta, kuten jatkuvan seurannan, erillisten arviointien ja ulkoisten osapuolten avulla. Ulkoisten osapuolten antamaa palautetta ja tietoa yrityksen riskienhallinnan tasosta ei kannata aliarvioida, vaan tarvittaviin korjaaviin toimenpiteisiin tulisi ryhtyä välittömästi. Havaittaviin puutteisiin riskienhallinnan tasosta tulee suhtautua vakavasti, koska niillä voi olla merkittävä vaikutus yrityksen tavoitteiden saavuttamiseen. Sisäiset valvontajärjestelmät myös muuttuvat jatkuvasti, koska tavat, ympäristö, yritykset ja ihmiset kehittyvät kaiken aikaa. Johdon on seurattava seurantajärjestelmien toimintaa ja tarvittaessa päätettävä uusista toimenpiteistä (COSO ERM 2004, 75–82.) Seuraavassa kappaleessa käydään läpi vielä erikseen riskienhallintaprosessi, joka sisältää myös COSO ERM -mallin edellä mainitut keskeiset elementit.

## 3.3 Riskienhallintaprosessi

Kuusela ja Ollikainen (2005, 126) määrittelevät kokonaisvaltaisen riskienhallinnan prosessiksi, johon vaikuttavat yhtiön hallitus, johto ja työntekijät. Prosessia toteutetaan organisaation strategia- ja suunnitteluprosessissa jatkuvasti. Kokonaisvaltainen riskienhallintaprosessi on kehitetty tunnistamaan seikkoja, jotka voivat vaikuttaa yritykseen sekä hallitsemaan riskejä määritellyn riskinottohalukkuuden piirissä, jotta yrityksen tavoitteiden saavuttaminen olisi riittävän luotettavalla pohjalla. Hirvosen ym. (2003, 230-231) mukaan toimivan riskienhallinnan edellytys on systemaattisen riskienhallintaprosessin noudattaminen. He jakavat riskienhallintaprosessin neljään vaiheeseen, joista

ensimmäinen ja perustava vaihe on liiketoiminnan tavoitteiden läpikäyminen ja avaintavoitteiden tunnistaminen. Riskienhallintaprosessin toinen vaihe on sellaisten riskien kartoitus- ja analyysivaihe, jossa yrityksen tavoitteita uhkaavien riskien vakavuus ja todennäköisyys arvioidaan, priorisoidaan ja niille määritellään hyväksyttävä taso. Tämän vaiheen jälkeen näille riskeille arvotetaan ja tarvittaessa määritellään tarvittavat kontrollit, joiden avulla niitä hallitaan. Yrityksellä pitää olla toimivat ja riskien hallintaan sopivat menetelmät käytettävissään. Tässä vaiheessa päätetään myös riskien raportoinnista. Neljännessä vaiheessa koko riskienhallintaprosessi sisällytetään osaksi toiminnan johtamista. Riskienhallinta voidaan käsittää jatkuvana prosessina, jossa toiminta ensin organisoidaan ja sen jälkeen sitä seurataan ja kehitetään jatkuvasti. Tehokas kommunikoiminen yrityksen eri tasojen ja koko henkilöstön kesken on erityisen tärkeää. Alla oleva kuva selvittää edellä käsitellyn riskienhallintaprosessin yksinkertaistettuna.

**Kuva 6. Riskienhallintaprosessi**




Lähde: AS/NZS 4360, Riskienhallintastandardi

Palautteen kerääminen organisaation eri tasoilta, prosesseista ja työntekijöiltä on ensiarvoisen tärkeää riskienhallintaprosessissa. Palautejärjestelmä on ikään kuin jatkuva prosessi, jossa kerätään tietoa sekä tunnetuista että ennen näkemättömistä tapahtumista (Merna & AL-Thani 2005, 226-227). Myös COSO ERM -mallin kokonaisvaltaisen riskienhallinnan viitekehys perustuu koko organisaation läpi leikkaavaan riskitiedon tuottamiseen ja keräämiseen.

Moeller (2007, 74) tähdentää, että COSO ERM -mallin tarkoitus ei ole tarkkojen riskilaskelmien kehittäminen, vaan kokonaisvaltaisen kuvan muodostaminen tehokkaan riskienhallinnan kannalta. COSO ERM on kattava viitekehys, mutta on tärkeää pitää mielessä, että se on kuitenkin vain viitekehys. COSO ERM ei siis sellaisenaan tuo valmista ratkaisua kehitettäessä organisaatioiden riskienhallintaa, vaan tarjoaa yrityksen johdolle ja hallitukselle kohtuullisen varmuuden yrityksen tavoitteiden saavuttamiseksi. Riskienhallinnan rajoitukset voivat COSO ERM -mallin (2004, 93) mukaan johtua johtamisprosessien luontaisista rajoituksista, inhimillisistä virheellisistä päätöksistä tai erehdyksistä. Johto voi sivuuttaa riskienhallintaprosessin ja siinä olevat riskeihin vastaamiseen ja valvontatoimenpiteisiin liittyvät päätökset. Riskienhallinnan kontrolleja voidaan myös kaihtaa salassa eri ihmisten kesken. Kustannukset ja riskeihin vastaamisen hyödyt voivat myös olla rajoittavia tekijöitä. Lisäksi riskit liittyvät tulevaan toimintaan, joka on luonnostaan epävarmaa. Monahan (2008, 119) ilmaisee henkilökohtaisen tyytymättömyytensä COSO ERM -viitekehystä kohtaan, koska hänen mielestään se tarjoaa liian vähän ohjeistusta tehokkaan riskienhallinnan viitekehyksen suunnitteluun ja toteutukseen. COSO ERM -viitekehys ei hänen mukaansa myöskään määrittele kunnollista metodologiaa riskin määrittämiselle.

# 4 *Tutkimuksen suorittaminen*

## *4.1 Tutkimusmenetelmä*

Tutkielmani tavoitteena on selvittää, miten kohdeyritysten riskiraportointi ja riskienhallinta on kehittynyt vuodesta 2005 vuoteen 2007. Lisäksi tutkin, täyttääkö kohdeyritysten riskiraportointi lainsäädännön ja suositusten vaatimukset sekä sidosryhmien tavoitteet.

Tutkielmani viitekehikoksi olen valinnut kokonaisvaltaisen riskienhallinnan viitekehyksen COSO ERM -mallin, jonka valintakriteerit olen perustellut kokonaisvaltaisen riskienhallinnan viitekehyksen kappaleen alussa. Koskisen ym. (2005, 233) mukaan tutkimuksen tavoitteet ja näkökulman tärkeimmät rakenneosat määrittelevät analyysissa noudatetun menetelmän. Silverman (2006, 194) tähdentää, että tekstiä analysoitaessa on tärkeää pitää näkökulma koko ajan mielessä, koska se mahdollistaa kulloinkin tarvittavat metodit ja konseptit.

Valitsemani tutkimusmenetelmä on laadullinen, joka perustuu aineistolähtöiseen analyysiin. Tutkielmani aineisto muodostuu neljän suomalaisen pörssiyrityksen vuosikertomus- ja tilinpäätösinformaatiosta. Olen myös poiminut empiiriseen analyysiini tekstiä tutkielmani kohdeyritysten vuosikertomus- ja tilinpäätösmateriaalin muista osista, joka jämäköittää analyysiani. Lähestyn tutkielmani aineistoa omalla tavallani ja kerron oman pohdintani kautta, miten luen ja tuotan jäsennyksiä aineistosta. Alasuutarin (2001, 88) mukaan laadullinen aineisto on kuin ”pala tutkittavaa maailmaa” sekä näyte tutkimuksen kohteena olevasta kulttuurista ja kielestä. Laadullisen aineiston tärkeimpiä ominaisuuksia ovat monipuolisuus, ilmaisullisuus, rikkaus sekä kompleksisuus (mt.84). Eriksson & Kovalainen (2008, 16) kirjoittavat, että metodologiat eivät ole tiiviissä yhteydessä tai rajoittuneita suhteessa toisiinsa. Laadullisen tutkimuksen analysointiin on olemassa useita keinoja, mutta näiden keinojen yksityiskohtaiseen toteuttamiseen on tarjolla vain vähän neuvoja. Koskisen ym. (2005, 241) mukaan laadulliset tutkijat rakentavat usein menetelmiä tutkimustensa tarpeiden mukaisesti, eivätkä läheskään aina noudata orjallisesti jonkin tietyn menetelmän periaatteita. Huolellisesti tehty aineistolähtöinen tutkimusote voi parhaimmillaan tuottaa selkeän ja helposti viestittävän tulkinnan, joka myös kuvaa aineiston kattavasti (mt.231).

Aineistoni kohdeyritysten riskienhallinnan raportoinnin taso vaihtelee suuresti, joten poikkeamien esiin nostaminen nostaa yksittäiset tapaukset erityishuomion kohteeksi. Olen rakentanut oman tutkimusmenetelmäni muun muassa analyyttisen induktion sekä retorisen diskurssianalyysin avulla. On tärkeää huomata, että analysointimenetelmä perustuu suurimmaksi osaksi tutkijan omaan ja yksilökohtaiseen tapaan. Analyyttinen induktio on menetelmä, joka korostaa päättelyssä havaittavien poikkeavien tapausten,

jotka rajaavat sekä osoittavat päättelyä, tärkeyttä ja antaa käteviä työvälineitä päättelyn järjestämiseen (Koskinen ym. 2005, 233). Myös pelkkä aineiston systemaattinen ja analyyttinen lukeminen tuottaa perusteltuja ja mielenkiintoisia tulkintoja (Koskinen ym. 2005, 241). Retorisen diskurssianalyysin avulla pohdin, millaisia keinoja kohdeyritykset käyttävät pyrkiessään vakuuttamaan sijoittajat riskien ja riskienhallinnan asianmukaisesta hoidosta.

## 4.2 Tutkimuksen luotettavuus

Olen liittänyt tutkielmani analyysiin suoria lainauksia tekstistä, jotka auttavat lukijaa arvioimaan, miten olen tulkinnut esiin nostamiani havaintoja. Koskisen ym. (2005, 229) mukaan tutkimuksen tunnusmerkkinä pidetään sitä, että se johtaa selkeään tulkintaan, jolla on mahdollisuus keskustella aikaisemman tutkimuksen kanssa. Tulkinnan tavoitteena on kuvata ja selittää kaikki ne aineiston kuvaukset, jotka sen pitäisikin selittää (mt.249). Mäkelän (ks. Mäkelä; 1990, 33) mukaan metodin jäljiteltävyys on ”avain tulkinnan luotettavuuteen”, jonka avulla voidaan tarkistaa, miten tutkimus on tehty. Hakalan (2008, 178) mukaan analyysissa on tärkeintä löytää aineiston taakse piilotettu tieto, omalla ajattelulla höystettynä. Päätelmien teko ja analyysi ovat päämääriä, joihin tutkijan tulee sitoutua jo tutkimuksen alkuvaiheessa (mt.181). Silvermanin (2008, 153–154) mukaan tekstin analysoiminen koetaan vaikeampana kuin esimerkiksi sosiaalisten tilanteiden havainnoiminen. Hänen mukaansa tutkijat eivät myöskään hyödynnä tekstien potentiaalia rikkautta. Toisaalta tekstin sanotaan olevan luotettavampaa kuin havainnointi, koska se on jo valmiina olemassa ja ei ole vielä suodattunut tutkijan mielen läpi (mt.285). Luotettavuus syntyy tekstiä analysoitaessa siitä, että sitä analysoidaan erilaisten kategorioiden, peruskäsitteiden, kautta. Tekstin tulisi olla kategorisoitu standardoidulla tavalla, jotta kuka tahansa tutkija voi toimia samalla tavalla kyseisen tekstin suhteen (mt.286).

Julkinen vuosikertomus- ja tilinpäätösmateriaali ovat ainoita julkisia dokumentteja, joiden avulla yritysten sidosryhmät voivat muodostaa oman arvionsa siitä, miten yritykset raportoivat riskeistään. Se, mitä raportoidaan ulospäin ”kauniisti ja retorisesti”, ei välttämättä kuvaa todellista totuutta. Tutkielmani aineistossa on kyse samasta asiasta.

Asettaudun analyyttisen ja rehellistä tietoa etsivän tutkijan rooliin, joka pyrkii saamaan mahdollisimman todenmukaisen ja laajan käsityksen kohdeyritysten riskiraportoinnin kehittymisen tasosta. Etsin aineistosta myös ristiriitaisuuksia, enkä ainoastaan sopusointuisia tulkintoja, jotka tukevat suositusten mukaista raportointia. Hiljaisten, rivien välistä luettavien asioiden lisäksi pyrin myös tuomaan esiin ”vilkkaita” tapahtumia. Koskinen ym. (2005, 245) esittävät muutamia keinoja siihen, miten aineistoa pitäisi tulkita mahdollisimman avoimesti, kunnes ollaan varmoja aineiston uskottavuudesta. Aineistoon liittyvien epätäydellisten typologioiden eli luokittelujen avulla voidaan etsiä ”hiljaisuuksia” eli asioita, jotka jäävät aineistossa piiloon. Alasuutari (2001, 77–78) kirjoittaa, että tieteellinen tutkimus on merkkien tulkitsemista ja uusien johtolankojen aktiivista tuottamista. Vihjeiden ja johtolankojen avulla voidaan yrittää päätellä jotain, mikä ei ole paljaalla silmällä havaittavissa. Asioita ei saa ottaa sellaisena, kuin ne näyttävät. Alasuutarin (2001, 78) mukaan aineistosta tehtävät havainnot ja tutkimustulos ovat eri asioita: kiinnostavasta aineistosta voidaan tehdä huonoa tutkimusta ja arkielämän kannalta irrelevantit seikat voivat johtaa tärkeisiin ja tieteellisesti kiinnostaviin tutkimustuloksiin. Ehrnroothin (ks. Mäkelä; 1990, 36) mukaan tieteellisen menetelmän päämäärä on perusteltavuus, ei uskottavuus.

Rajauksena haluan mainita, että analyysini koskee pientä aineistoa, jonka avulla en voi tehdä yleistyksiä. Analyysin tulokset koskevat ainoastaan kohdeyritysten riskiraportoinnin ja riskienhallinnan kehittymistä. Tutkielmani aineistolähtöisestä analyysista tekee haastavan se seikka, että ei ole olemassa erillisiä tai tarkkoja ohjeita siitä, miten COSO ERM -näkökulman toteutuminen näkyy yritysten riskienhallinnan raportoinnissa tai sen kehittymisessä. Aineiston kohdalla on tärkeää ymmärtää, että kyseessä eivät ole ainoastaan satunnaisesti poimitut seikat, vaikka aineisto on varsin suppea eli tietoa ei ole paljon koskien kohdeyritysten riskienhallintaa. Pyrin kuitenkin perustamaan analyysini aineistosta löytyviin luotettaviin päättelyihin, jotka olen kategorisoinut luotettaviksi. Mäkelän (ks. Mäkelä; 1990, 53) mukaan analyysin kattavuus on sitä, että tutkija ei perusta tulkintojaan satunnaisiin poimintoihin. Alasuutarin (2001, 214) mukaan paikallinen selittäminen perustuu siihen, että mahdollisimman moni aineiston johtolanka puhuu sen puolesta. Mäkelä (ks. Mäkelä; 1990, 53) tähdentää, että epävarmuus ja epäily ovat kuitenkin aina mukana tiedettä harjoittaessa.

## 4.3 Tutkimuksen toteuttaminen

Tutkielman kohdeyrityksistä kolmella on liiketoimintaa merenkulun alalla. Laivaston hallinnointi tuo erityisen näkökulman kohdeyritysten liiketoimintaan ja sitä kautta niiden riskienhallintaan ja sen kehittymiseen. Lisäksi tutkielman kohdeyritykset edustavat kukin hyvin erilaista vaihetta riskienhallinnassaan. Tutkielman aineistona on vuosikertomus– ja tilinpäätösmateriaali vuosilta 2005 ja 2007. Aineisto on ulkoiselta olemukseltaan samankaltaista, koska kyseessä on vuosikertomus- ja tilinpäätösmateriaali, joka noudattaa samanlaista kaavaa jokaisen pörssiyrityksen kohdalla. Silvermanin (2006, 194) mukaan analysoitavan tekstin pitäisi olla samankaltaista ja sitä tulee olla rajattu määrä. Mäkelän (ks. Mäkelä; 1990, 53) mukaan on tärkeää miettiä etukäteen, miten laadullisen tutkimuksen aineisto saadaan prosessoitavaan ja hallittavaan muotoon. Aineiston määrä on myös pidettävä sopivana. Brymanin & Burgessin (1994, 217) mukaan laadullisen tutkimuksen ydin on aineiston keräämisen ja analysoinnin jatkuva vuorovaikutus.

Tutkielman aineisto on valmiina analysoitavaksi sellaisenaan, koska tutkimukseni tarkoitus on nimenomaan tutkia, miten kohdeyritykset raportoivat riskienhallinnastaan julkisen aineiston perusteella. Olen jakanut aineiston keskeisimpien riskienhallinnan teemojen mukaan molempien vuosien 2005 ja 2007 osalta. Nämä teemat olen jaotellut sen mukaan, mitkä asiat olen kokenut keskeisimmiksi ja tärkeimmiksi asioiksi analyysin kannalta. Aineistolähtöisestä analyysista tekee haastavaksi se seikka, että ei ole olemassa erillisiä tai tarkkoja ohjeita siitä, miten kyseisen näkökulman toteutuminen näkyy yritysten riskienhallinnan raportoinnissa. Ehrnroothin (ks. Mäkelä; 1990, 37–38) mukaan aineisto kaipaa aina käsittelyä ennen analyysia kaikessa empiirisessä tutkimuksessa. Käsittelyssä aineistosta karsitaan kaikki turha pois. Lisäksi se saatetaan sellaiseen muotoon, jossa se on valmis eriteltäväksi ja valmiina vastaamaan niihin kysymyksiin, joiden vastaamista varten se on koottu. Koskinen ym. (2005, 231) painottavat, että aineiston analyysia pitäisi edeltää aineiston huolellinen lukeminen ja silmäileminen, usein jopa monta kertaa. Muistiinpanojen tekeminen ja yleiskuvan hahmottaminen antavat tutkimukselle ikään kuin alustavan hahmon. Koskinen ym. (2005, 231) jakavat

analyysin valmistelevat vaiheet kahteen osaan: tutkimusvaiheeseen ja analyyttisempaan vaiheeseen. Aineiston yksityiskohtaista analyysia ei saisi aloittaa ennen tutkimusvaihetta, jonka aikana aineisto teemoitetaan alustavasti.

Olen jakanut tutkielman empiirisen analyysin COSO ERM -viitekehyksen osa-alueiden mukaisesti kahdeksaan osaan: sisäinen toimintaympäristö, tavoitteiden asettaminen, tapahtumien tunnistaminen, riskien arviointi, riskeihin vastaaminen, valvontatoimenpiteet, informaatio ja tiedonkulku. Tapahtumien tunnistamisen ja riskien arvioinnin käsittelen yhdessä. Ne ja riskeihin vastaaminen muodostavat riskienhallintaprosessin ytimen. Valvontatoimenpiteet sekä tiedon ja viestinnän osa-alueet rajaan tutkimukseni ulkopuolelle, koska niiden tutkiminen julkisen informaation perusteella on hankalaa. Valvontatoimenpiteet määrittelen kuulumaan enemmänkin sisäisen valvonnan suurempaan kokonaisuuteen kuin riskienhallintaprosessiin. Informaatio ja tiedonkulku on myös vaikeasti eristettävissä julkisesta informaatiosta ja sisältyy elimellisesti viitekehyksen muihin osioihin.

Kunkin tutkimukseen sisältyvän riskienhallinnan osa-alueen alle olen poiminut keskeisimmät riskienhallintaan liittyvät asiat, jotka olen jakanut alakohdiksi. Tällä tavalla pystyn käsittelemään näin laajaa aineistoa. Kunkin osa-alueen alakohdan alussa esittelen, miten tutkin kyseistä asiaa aineistosta. Tämän jälkeen etenen alakohtien yksityiskohtaisempaan käsittelyyn. Kunkin alueen keskeisimmät havainnot olen kirjoittanut jokaisen osa-alueen kohdan alkuun.

## 4.4 Kohdeyritykset

Olen valinnut tutkielman kohdeyrityksiksi Kemira Oyj:n, Neste Oil Oyj:n, Aspo Oyj:n sekä Finnlines Oyj:n. Yhteistä näille kaikille yrityksille Kemiraa lukuun ottamatta on se, että niillä on omistuksessaan laivastoa. Kemiran mukaan ottamista merenkulun toimialan yritysten joukkoon puoltaa se seikka, että sillä on aikoinaan ollut omistuksessaan yksi laiva, m/s Kemira, joka on sittemmin myyty ulkomaille. Laivaston omistaminen ja hallinta antaa oman erityispiirteensä kohdeyritysten liiketoiminnalle, koska laivastoon on sitoutunut paljon pääomaa ja merikuljetukset ovat alttiita monille erilaisille riskeille.

Yrityksen toimialalla ja sen valitsemalla strategialla on vaikutusta siihen, minkälaisia strategisia, operatiivisia tai taloudellisia riskejä yritys kohtaa. Kukin yritys tuo esille niitä riskejä, joita se haluaa tuoda. Seuraavassa kappaleessa esittelen kohdeyritysten toimialat lyhyesti.

*Kemiran* toimiala on kemikaaliteollisuus ja yritys toimii yli 10 maassa. *Neste Oil* on korkealaatuisiin puhtaamman liikenteen polttoaineisiin keskittyvä jalostus- ja markkinointiyhtiö. *Neste Oilin* toimialoja ovat öljynjalostus, erikoistuotteet, shipping, biodiesel ja öljyn vähittäismyynti. *Neste Oililla* on toimintaa 11 maassa. *Aspon* toimialaluokitus on teollisuustuotteet ja –palvelut eli se tarjoaa teollisuuden logistiikkapalveluja energia-alan ja prosessiteollisuuden yrityksille. *Aspon* toimialoja ovat Aspo Chemicals, Aspo Shipping ja Aspo Systems. *Aspon* toiminta on keskittynyt Itämeren alueelle. *Finnlines* on yksi Euroopan suurimmista aikataulutettuun linjaliikenteeseen erikoistuneista varustamoista, jonka merikuljetukset ovat keskittyneet Itämerelle ja Pohjanmerelle. *Finnlines* tarjoaa satamapalveluja lähinnä Helsingissä, Turussa ja Kotkassa. *Finnlinesin* toimialat ovat varustamotoiminta, merikuljetukset sekä satamatoiminnot. Yhtiö toimii kahdeksassa maassa. Kaikki tutkielman kohdeyritykset on listattu OMX Pohjoismaiseen Pörssiin.

Seuraavalla sivulla olevaan taulukkoon olen koonnut tärkeimmät tunnusluvut vuodelta 2007. Kohdeyritysten keskeisten tunnuslukujen ymmärtäminen ja vertailu auttaa ymmärtämään myös riskienhallinnan ja riskienhallintaraportoinnin eroja yhtiöiden välillä. Liikevaihdon osalta on suluissa luku vuodelta 2005.

**Taulukko 1. Kohdeyritysten tärkeimmät tunnusluvut 2007**

| Tunnusluvut (milj. euroa) | Kemira | Neste Oil | Aspo | Finnlines |
|---|---|---|---|---|
| Liikevaihto (suluissa 2005) | 2810 (1 994,4) | 12103 (8150) | 267 (204,9) | 685,5 (747) |
| Liikevoitto | 143 | 801 | 24 | 68,8 |
| ROE | 6 | 25,6 | 25,4 | 8,0 |
| ROIC | 8 | 26,2 | 25,7 | 6,9 |
| Omavaraisuusaste | 39 | 49,9 | 45,1 | 31,1 |
| Velkaantumisaste | 92 | 23,7 | 32,4 | 167,4 |
| Tulos/osake | 0,53 | 2,25 | 0,59 | 0,83 |
| Henkilöstö | 10007 | 4810 | 699 | 481 |

*Neste Oil* on kohdeyrityksistä selvästi suurin. Sen kannattavuus on myös omalla tasollaan. *Aspo*, joka on kohdeyrityksistä liikevaihdolla mitaten selkeästi pienin, yltää kannattavuusluvuissa lähelle *Neste Oilin* tasoa. Riskienhallinnan kehittyneisyyden ja sen raportoinnin suhteen oletan, että yrityksen koko on suurin selittävä tekijä: suurella organisaatiolla on riittävästi resursseja myös riskienhallinnan ja raportoinnin kehittämiseen. Vaikka *Kemira* on liikevaihdoltaan selvästi *Neste Oilia* pienempi, sen henkilökuntamäärä on yli kaksinkertainen *Neste Oiliin* nähden. *Finnlinesin* liikevaihto on yli kaksi kertaa suurempi kuin *Aspon*, mutta sen henkilökuntamäärä on kuitenkin selvästi pienempi kuin *Aspon*. Riskienhallinnan kehittyneisyyden suhteen *Kemira* ja *Neste Oil* kilpailevat samassa sarjassa ja vastaavasti Aspo ja Finnlines samassa sarjassa keskenään.

# 5 Riskienhallinnan raportointi vuosikertomuksessa ja tilinpäätöksessä

Tutkielman empiirisessä osassa perehdyn kohdeyritysten riskiraportointiin ja riskienhallintaan, joiden kehittymistä arvioin COSO ERM -mallin pohjalta. Aineistona käytän kohdeyritysten vuosikertomus- ja tilinpäätöstietoja kahdelta eri vuosilta eli vuosilta 2005 ja 2007. Käyn läpi COSO ERM -mallin jokaisen osa-alueen samassa järjestyksessä kuin se on kirjoitettu teoria-osaan. Olen nostanut jokaisen osa-alueen alle olennaisemmat asiat, joiden avulla havainnoin, miten kohdeyritysten riskienhallinnasta antama riskienhallintainformaatio vastaa COSO ERM -mallin suosituksia. Nämä olennaisimmat asiat vastaavat COSO ERM -mallin teorian mukaisia kuvauksia. Peilaamalla COSO ERM -mallin osa-alueiden sisältämiä olennaisempia piirteitä kohdeyritysten aineistosta poimittuihin vastaaviin asioihin pyrin muodostamaan mahdollisimman todenmukaisen käsityksen siitä, vastaako kohdeyritysten riskiraportointi käyttämäni viitekehikon suosituksia. COSO ERM -mallin osa-alueiden systemaattinen läpikäynti mahdollistaa asioiden tarkastelun perustavanlaatuisista, yleisistä asioista yksityiskohtaisempaan suuntaan etenevän dialogin.

Aloitan empiirisen analyysin tarkastelemalla COSO ERM -mallin perustana olevaa sisäistä toimintaympäristöä ja sen keskeisimpiä elementtejä toimintakulttuuria, organisaatiota ja resursseja, jonka jälkeen etenen tavoitteiden asettamiseen ja riskien tunnistamiseen, arviointiin ja vastaamiseen. COSO ERM -mallin seuraavien osa-alueiden eli valvontatoimenpiteiden ja informaation ja tiedonkulun jätän analyysini ulkopuolelle, koska näitä alueita on vaikea analysoida pelkän julkisen informaation perusteella. Viimeisenä analysoin seurannan osa-aluetta.

## 5.1 Sisäinen toimintaympäristö

Sisäinen toimintaympäristö luo perustan sille, millä tavalla yrityksen henkilöstö suhtautuu riskeihin ja valvontatoimenpiteisiin. Sisäistä toimintaympäristöä voidaan COSO ERM -mallin mukaan analysoida toimintakulttuurin, organisaation ja resurssien kautta.

Kohdeyrityksistä *Kemira* hyödyntää käyttämääni viitekehikkoa COSO:a. Kertoessaan sisäisestä valvonnastaan *Kemira* summeeraa oman sisäisen toimintaympäristönsä vuosikertomuksessaan seuraavasti:

> ”Kemiran arvot ja liiketapaperiaatteet (Kemira Code of Conduct) luovat perustan yhtiön hallinnoinnille ja keskeisten sidosryhmien kanssa toimimiselle. Liiketapaperiaatteet on saatettu tiedoksi konsernin koko henkilöstölle. Kemiran jokaisella työntekijällä on oikeus ja velvollisuus tehdä ilmoitus lain ja liiketapaperiaatteiden vastaisesta toiminnasta. Vuosittain tehtävällä henkilöstökyselyllä sekä sisäisen valvonnan kyselyllä kartoitetaan henkilöstön näkemyksiä työilmapiiristä ja sisäisen valvonnan tilasta”.

Tämä *Kemiran* antama esimerkki antaa hyvän käsityksen siitä, millainen sisäisen toimintaympäristön tulisi olla COSO ERM -mallin mukaisesti. Seuraavissa kappaleissa käyn kohdeyritysten toimintaympäristöä läpi toimintakulttuurin, organisaation ja resurssien kautta. Kunkin osion loppuun olen koonnut keskeisimmät johtopäätökset.

### 5.1.1 Toimintakulttuuri

Sisäisen toimintakulttuurin osalta tutkin aineistosta asioita liittyen johdon sitoutumiseen ja vastuun kantamiseen, riskinottohalukkuuteen ja –kykyyn, eettisiin periaatteisiin (tai arvoihin), sääntöihin ja niiden noudattamiseen, ilmapiiriin ja kannustinjärjestelmiin, jotka ovat riskienhallinnan kannalta COSO ERM -mallin toimintakulttuurin keskeisimmät tekijät. Nämä asiat olen poiminut COSO ERM -mallin sisäisen toimintaympäristöön kuuluvan toimintakulttuurin alakohdan alta. Pyrin näiden asioiden avulla todentamaan, vastaako kohdeyritysten riskienhallinnan kehittyminen COSO ERM -mallin suosituksia. Olen valinnut kyseiset asiat siten, että ne ilmentäisivät kohdeyritysten toimintakulttuuria mahdollisimman todenmukaisesti.

Sisäiseen toimintaympäristöön kuuluvan toimintakulttuurin arvioinnin kohteena COSO ERM -mallin mukaan on, että yrityksen johto on sitoutunut toimintaan ja kantaa sille kuuluvan vastuun toimintojen kokonaisuudesta ja niiden kehittämisestä sekä tuloksellisuudesta. Pelkän julkisen aineiston perusteella en pysty analysoimaan johdon sitoutu-

mista toimintaan, mutta analysoin johdon toimintaan sitoutumista esiintuotujen politiikkojen ja menettelytapojen kautta. Jos johto on esimerkiksi kirjoittanut riskienhallintapolitiikan ja siihen on viittaus aineistossa, oletan että johto olisi sitoutunut myös riskienhallintaan ja sen kehittämiseen.

*Kemira* kertoo kumpanakin vuonna johdon tavoitteiden, vastuunjaon ja riskirajojen tarkemman määrittelyn löytyvän eri konserniohjeista. *Neste Oililla* on hallituksen hyväksymät yleiset riskienhallintaperiaatteet, joissa esitetään riskienhallinnan tavoitteet, periaatteet, prosessit ja vastuut. Tämä tuodaan esille molempina vuosina. *Kemira* ja *Neste Oil* tuovat esille myös muita politiikkoja ja periaatteita, joilla johto osoittaa tahtotilansa eri asioiden hoitamisesta. *Aspo* kuvaa kumpanakin vuonna johdon vastuita ja sitoutumista seuraavasti: ”Johto vastaa riittävien toimenpiteiden määrittämisestä, toteuttamisesta sekä toimenpiteiden toteutumisen seurannasta osana normaalia toiminnan ohjausta.” *Aspo* tuo lisäksi esille johdon vastuun osana normaalia toiminnan ohjausta. Tiettyjen riskien osalta *Aspon* riskienhallinnan periaatteet ja keskeisin sisältö määritellään konsernitason politiikoissa ja ohjeissa. *Finnlines* ei kumpanakaan vuonna tuo esille johdon vastuita tai sitoutumista riskienhallintaan tai toimintaan yleensä, eikä kerro mahdollisista politiikoistaan tai menettelytavoistaan asiaan liittyen. Päätelmäni tästä on, että *Kemira, Neste Oil* ja *Aspo* tuovat esille konserniohjeet tai –periaatteet, joiden mukaan riskienhallintaa toteutetaan, kun taas *Finnlines* ei tuo esille tietoja, jotka osoittaisivat johdon sitoutumista toimintaan.

COSO ERM -mallin mukaan toimintakulttuurista kertoo myös se, että *johto on määritellyt ja viestinyt yrityksen riskinottohalukkuuden ja –kyvyn*. Analysoin kohdeyritysten riskinottohalukkuutta ja –kantokykyä etsimällä viittauksia mahdollisista riskienhallintapolitiikkaa koskevista linjauksista sekä strategiaan sisältyvistä riskienhallintaperiaatteista. Riskinottohalukkuus ja –kantokyky on olennainen seikka analysoitaessa yritysten riskienhallinnan tasoa ja niiden suhtautumista riskeihin, joten etsin tutkimusaineistosta erityisesti suoria riskinottohalukkuuteen ja –kantokykyyn liittyviä viittauksia.

*Kemiran* riskienhallintainformaatiossa ei ole mainintaa riskinottohalukkuudesta, mutta se määrittelee riskinkantokyvyn, johon se peilaa kokonaisriskitasoaan. *Kemiran* kohdal-

la riskinkantokyvystä kertova osio on mainittu samanlaisena kumpanakin vuonna. *Neste Oil* ei määrittele riskinottokykyään tai -halukkuuttaan vuonna 2005, mutta vuonna 2007 se kertoo määritelleensä hyväksytyt riskinottorajat, joiden sisällä se jopa pyrkii lisäämään riskinottohalukkuuttaan. *Aspolla* ja *Finnlinesilla* ei ole kumpanakaan vuonna mainintaa riskinottohalukkuudesta tai –kyvystä. Kohdeyrityksistä ainoastaan *Neste Oil* kertoo riskinottohalukkuudestaan ja sekin vasta vuonna 2007. *Kemira* puolestaan tuo esille riskinkantokyvyn, johon se kertoo peilaavansa kokonaisriskitasoaan. Siihen nähden että riskinottokyvyn ja –halukkuuden määrittely ovat COSO ERM -mallin suosittelemia toimivan riskienhallinnan perusedellytyksiä, on yllättävää, että kohdeyritykset kertovat asiasta niin vähän.

COSO ERM -mallin mukaista toimintakulttuuria kuvastaa myös se, että yrityksellä on yhteisesti hyväksytyt eettiset periaatteet, jotka sen jäsenet tuntevat ja toimivat ylimmästä johdosta alkaen niiden mukaisesti. COSO ERM -mallin sisäisen toimintaympäristön toimintakulttuuri muodostaa hedelmällisen maaperän toimivalle riskienhallinnalle silloin, kun odotusten mukainen toimintatapa viestitetään kaikille ja kytketään kaikkeen päätöksentekoon ja suunnitteluun. Myös hyvän hallinnon periaatteiden vastaiseen toimintaan puututaan nopeasti. Arvioin kohdeyritysten eettisyyttä eettisten sääntöjen tai periaatteiden avulla. Jos aineistossa ei ole mainintaa eettisistä periaatteista, arvioin kohdeyritysten eettisyyttä mahdollisesti esiintuotujen arvojen perusteella.

*Kemiralla* riskienhallinnan perusmääritelmään on lisätty tavoitteiden saavuttaminen kestävällä ja eettisellä tavalla. *Kemira* ilmaisee eettiset periaatteensa molempina vuosina näin: ”Kemiran arvot ja eettiset periaatteet luovat perustan yhtiön hallinnoinnille ja keskeisten sidosryhmien kanssa toimimiselle.” *Neste Oililla* ei ole mainintaa eettisistä periaatteista. Syksyn 2005 aikana *Neste Oililla* käynnistettiin arvoprosessi, jonka osana koko henkilöstö mietti nykyistä toimintakulttuuria ja tulevia arvoja. Arvoprosessin tavoitteena oli löytää yhteinen arvopohja, joka auttaa yhtiötä kohtaamaan strategiset haasteet. *Neste Oilin* arvot julkistettiin keväällä 2006 ja arvokeskusteluja jatkettiin vuonna 2007 tiimeissä ja osastoilla. *Aspo* ei mainitse eettisiä periaatteita tai arvoja kumpanakaan vuonna. *Finnlines* ei mainitse eettisiä periaatteitaan, mutta kumpanakin vuonna aineistossa on listattu arvot, jotka ovat asiakaskeskeisyys, tuloksellisuus, henki-

löstötyytyväisyys sekä vastuullisuus, jonka mukaan kestävän kehityksen periaatteita noudatetaan. Ympäristövastuullisuus on osa päivittäistä toimintaa ja turvallisuusnäkökohdat otetaan kaikessa toiminnassa huomioon.

Ainoastaan *Kemira* mainitsee eettiset periaatteensa. *Neste Oil* kertoo arvoprosessistaan ja *Finnlines* listaa arvonsa. *Aspo* ei tuo esille mitään eettisyyteen viittaavaa. Eettisten arvojen kirjaaminen ei vielä Suomessa ole kovin yleistä. Uskoisin, että syy tähän löytyy suomalaisesta kulttuurista ja liiketoimintamme kansainvälisestä suhteellisen korkeasta etiikasta. Suomalainen ei myöskään koe eettisen toimintansa paranevan eettisten ohjeiden kautta. Kansainvälisesti tilanne on kuitenkin toinen ja uskon *Kemiran* olevan yksi suomalaisista edelläkävijöistä eettisten periaatteidensa kehittäjänä ja hyödyntäjänä. Eettiset periaatteet voidaan myös nähdä riskienhallintakeinona.

Se, että *organisaation jäsenet tuntevat toimintaa ohjaavat keskeiset säännöt ja noudattavat niitä,* vahvistaa COSO ERM -mallin suosittelemaa yhtenäistä toimintakulttuuria. COSO ERM -mallin suositusten mukaan organisaatiossa olisi hyvä olla systemaattinen tapa, jonka avulla henkilöstölle kerrotaan olennaisista toimintaa ohjaavista säännöistä. Lisäksi poikkeamiin olisi hyvä reagoida johdonmukaisesti ja oikeudenmukaisesti. Sisäisen valvonnan yksi tavoite on lakien ja ohjeiden noudattaminen. Koska ohjeiden noudattamisesta on aineistossa vain vähän mainintoja, etsin aineistosta viitteitä sisäisen valvonnan järjestämisestä.

Vuonna 2005 *Kemira* kirjoittaa sisäisen valvonnan järjestelmästään, jota tukevat ”vahvistetut politiikat ja toimintaohjeet, joita noudatetaan kaikissa konserniyhtiöissä.” Vuonna 2007 *Kemira* mainitsee sisäisen valvonnan ja yhtiön toiminnan olevan järjestetty ”lakien, määräysten ja yhtiön hallituksen vahvistamien hyväksyttyjen liiketapaperiaatteiden (Kemira code of conduct) mukaisesti.” *Kemiraa* koskee esimerkiksi uusi kemikaalilainsäädäntö (REACH), joka on hyvä esimerkki uusista lainsäädännön tuomista riskeistä. *Neste Oililla* tarkastusvaliokunta avustaa hallitusta sisäisen valvonnan arvioinnissa vuonna 2005. Vuonna 2007 *Neste Oilin* ympäristöperiaatteisiin (HSE= Health, Safety, Environment) kuuluu muun muassa lainsäädännön ja yritykselle myönnettyjen lupien noudattaminen. Ympäristöperiaatteiden julistaminen kumpanakin vuon-

na kuvastaa hyvinvointiin, turvallisuuteen ja ympäristöön liittyvien lakien noudattamiseen ja tällä alueella riskien välttämiseen liittyvää asennetta. *Aspo* mainitsee säännösten noudattamisen valvonnasta seuraavanlaisesti: ”Konserniyhtiöiden controllerit ovat vastuussa lainsäädännön ja konsernin ohjeiden noudattamisesta.” Substanssilakien kohdalla on maininta: ”Ympäristöpolitiikan lähtökohtana on lainsäädäntö.” *Aspo* haluaa kuitenkin hoitaa kriittiset ympäristöasiat ”yli lain ja määräysten edellyttämien minimirajojen.” *Finnlinesin* aineistossa mainitaan kumpanakin vuonna, että hallituksen tehtävänä on huolehtia sisäisen valvonnan toimivuuden seurannasta. *Finnlinesilla* sisäisen valvonta on määritelty seuraavasti: ”Konsernin sisäinen valvonta on järjestetty controllertoimintona.”

*Kemira* ja *Neste Oil* tuovat esille sisäisen valvonnan siten, että siitä voidaan päätellä niiden noudattavan tiettyä systematiikkaa ohjeiden ja säännösten noudattamisessa. Myös *Finnlines* kertoo sisäisestä valvonnastaan, mutta on aineiston perusteella ymmärtänyt sen väärin, koska sisäinen valvonta ei voi olla järjestetty controllertoimintona; sisäinen valvonta on laajempi kokonaisuus, johon controllertoiminnon työ toki kiinteästi liittyy. *Aspossa* controllerit ovat vastuussa lainsäädännön ja konsernin ohjeiden noudattamisesta, joten tämä ilmaus poikkeaa teoriasta, koska lainsäädännön ja ohjeiden noudattamisen vastuu on ylempänä organisaatiossa, käytännössä toimitusjohtajalla ja viime kädessä hallituksella.

COSO ERM -mallin mukaan *organisaation ilmapiirin tulee kannustaa keskusteluun ja myös epäkohtien esilletuomiseen*. Ilmapiirin kannustavuus tekee toimintakulttuurista myös riskienhallinnan kehittämisen kannalta suotuisan, koska uudet ehdotukset ja kritiikki käsitellään rakentavalla tavalla ja myös epäonnistumisia hyväksytään. Työtyytyväisyyskyselyt toimivat usein tällaista myönteistä kehitystä ilmentävänä mittarina, joten analysoin kohdeyritysten ilmapiirin kannustavuutta työtyytyväisyystutkimusten tulosten avulla.

Vuonna 2005 *Kemiran* teettämät työtyytyväisyyskyselyiden tulokset ovat ”globaalia vertailuaineistoa selvästi korkeammalla.” *Kemiran* hyvästä erinomaiseksi -ohjelman yhtenä tavoitteena on ”yrittäjyyttä ja osallistumismahdollisuuksia korostava, keskuste-

leva ja iloinen yrityskulttuuri.” Vuoden 2007 aineistossa *Kemiralla* korostetaan osallistumista ja jokaisen työntekijän mahdollisuutta vaikuttaa omaan työhönsä sekä työympäristönsä kehittämiseen. Työhyvinvoinnin jatkuva kehittäminen on tärkeä osa *Kemiran* henkilöstöstrategiaa. Vuonna 2005 *Neste Oilissa* vuosittain tehtävän henkilöstötyytyväisyyskyselyn tulokset kertovat henkilöstön ”korkeasta motivaatiosta ja innostuneisuudesta uuden yhtiön rakentamisessa.” *Neste Oililla* pyritään käsittelemään ajankohtaisia asioita sekä vaihtamaan ajatuksia ja kokemuksia henkilöstön ja johdon välillä. Kehityskeskustelut tukevat päivittäisjohtamista ja antavat tilaisuuden molemminpuoliseen palautteen antoon. Vuonna 2007 henkilöstön tyytyväisyys on ”huippuluokkaa”. Esimiesten tuki alaisten kehittymispyrkimyksissä korostuu ja ilmapiiri on kannustava. Johdon ja alaisten väliseen kommunikaatioon panostetaan ja tämä helpottaa uusien ajatusten ja palautteen antamista. *Aspolla* ei ole mainintaa työtyytyväisyyskyselyistä kumpanakaan vuonna. Vuonna 2005 kannustavaa työilmapiiriä pyritään luomaan henkilökunnan aloitemahdollisuuden avulla. Vuonna 2005 *Aspo* ilmaisee pyrkivänsä johtamisen avulla tukemaan sitoutumista ja kannustamaan entistä parempiin suorituksiin. *Finnlines* mainitsee kumpanakin vuonna yhdeksi arvokseen henkilöstötyytyväisyyden, jonka mukaan *Finnlines* on ”luotettava ja innostava työnantaja, joka kohtelee henkilöstöään tasa-arvoisesti ja oikeudenmukaisesti.”

*Kemiran* ja *Neste Oilin* työtyytyväisyystutkimusten tulokset antavat ymmärtää, että yhtiöt panostavat työilmapiirin kehittämiseen ja avoimeen, keskustelevaan organisaatiokulttuuriin, millä on varmasti positiivinen vaikutus myös COSO ERM -mallin mukaisille riskienhallinnan edellytyksille. Toimiva riskienhallinta edellyttää kulttuuria, jossa riskejä ja epäkohtia voidaan tuoda avoimesti esille pelkäämättä oman aseman heikkenemistä. *Aspon* ja *Finnlinesin* antamassa informaatiossa ei ole tietoja työtyytyväisyystutkimuksista.

*Kannustinjärjestelmien oikeudenmukaisuus ja järkevyys ovat edellytys COSO ERM-mallin mukaiselle hyvälle toimintakulttuurille.* Kannustimien tulisi olla avoimia, johdonmukaisia ja yleisesti hyväksyttyjä sekä vaikuttaa myönteisesti organisaation tuloksellisuuteen ja ilmapiiriin. Kohdeyritykset kertovat aineistossa palkitsemisjärjestelmis-

tään ja kehityskeskustelukäytänteistä, joiden perusteella analysoin niiden kannustinjärjestelmien järkevyyttä ja oikeudenmukaisuutta COSO ERM -mallin osoittamalla tavalla.

Vuonna 2005 *Kemiran* palkitsemisen kannustavuutta on parannettu kehittämällä bonusjärjestelmiä paremmin tavoitteita tukevaksi. Vuonna 2007 palkitseminen perustuu ”sisäiseen oikeudenmukaisuuteen, ulkoiseen kilpailukykyyn ja suoritukseen.” Kehitystyökalut eli henkilöstökysely, kehityskeskustelut ja 360-palaute muodostavat toimenpiteiden suunnittelun perustan ja erityinen huomio kiinnitetään palkitsemisen kilpailukykyyn ja kannustavuuteen. *Neste Oililla* perustetaan henkilöstörahasto vuonna 2005. Vuoden 2007 tasa-arvosuunnitelmassa painotetaan palkkakehityksen tasa-arvoisuutta ja palkkaluokitusten ajantasaisuutta. *Neste Oilin* tavoitteena on ”tasa-arvoinen työyhteisö”, jota kehitetään rekrytoinnissa, palkitsemisessa, kehittämisessä ja uralla etenemisessä. *Neste Oilin* johdonmukaisista kannustimista kertoo vuosittaiset kehityskeskustelut, joiden avulla varmistetaan, että tavoitteet todella ymmärretään oikein. Tasa-arvoisen työyhteisön kehittäminen on myös askel oikeudenmukaiseen kannustamiseen. Kannustinjärjestelmistä *Aspo* mainitsee vuosikertomuksessaan kumpanakin vuonna johdon palkitsemis- ja kannustinjärjestelmät. Vuonna 2005 perustetaan henkilöstörahasto. *Finnlinesilla* hallitus päättää erillisistä johdon tulospalkkausjärjestelmistä. Palkkausjärjestelmistä tai tulos- tai kehittämiskeskusteluista ei löydy muuta mainintaa kumpanakaan vuonna.

*Kemira* on kehittänyt laaja-alaisesti palkitsemisjärjestelmäänsä selkeämpään ja informatiivisempaan suuntaan vuodesta 2005 vuoteen 2007. *Kemira* toimii tässä kohtaa hyvänä esimerkkinä siinä, että se nimeää palkitsemisen ja oikeudenmukaisuuden yrityskulttuurinsa osatekijöiksi ja kiinnittää ”erityistä huomiota” kannustavuuteen. Myös *Neste Oil* korostaa oikeudenmukaisen kannustamisen merkitystä. *Kemira* ja *Neste Oil* pyrkivät annetun informaation mukaan kannustinjärjestelmien avoimuuteen, johdonmukaisuuteen ja yleiseen hyväksyttävyyteen COSO ERM -mallin mukaisesti. *Aspo* ja *Finnlines* keskittyvät johdon palkitsemisjärjestelmän esilletuomiseen. Viime aikainen kehitys on herättänyt paljon keskustelua johdon palkitsemisjärjestelmien toimivuudesta. Näkisin, että palkitsemisjärjestelmät ovat kannustaneet lähinnä ylisuureen riskinottoon, joka on yhtenä osatekijänä syksyllä 2008 alkaneessa maailmanlaajuisessa talouskriisissä.

Kohdeyrityksistä *Kemira*, *Neste Oil* ja *Aspo* tuovat esille konserniohjeet tai –periaatteet, joiden mukaan riskienhallintaa toteutetaan. *Kemira* ja *Neste Oil* tuovat esille myös muita politiikkoja ja periaatteita, joilla johto osoittaa tahtotilansa eri asioiden hoitamisesta. *Aspo* tuo lisäksi esille johdon vastuun osana normaalia toiminnan ohjausta. *Finnlines* ei tuo esille tietoja, joiden voisin tulkita osoittavan johdon sitoutumista toimintaan. COSO ERM -mallin mukaan johdon tulee tehdä selkeät linjaukset ja näyttää omalla toiminnallaan esimerkkiä. Jos ylin johto ei toimi viitoittamansa tien mukaisesti, ei voida olettaa, että muukaan henkilöstö sitä tekisi. COSO ERM -mallin mukaisesta johdon tahtotilan osoittamisesta kertovat *Kemira* ja *Neste Oil* selkeästi. *Kemiran* ja *Neste Oilin* lisäksi *Aspo* tuo esille politiikkoja ja menettelytapoja, mikä kuvastaa COSO ERM-mallin mukaista sisäisen toimintaympäristön perustan luomista riskienhallinnalle sekä sisäiselle valvonnalle.

Siihen nähden että riskinottokyvyn ja –halukkuuden määrittely ovat toimivan riskienhallinnan perusedellytyksiä, on yllättävää, että kohdeyritykset kertovat asiasta niin vähän. *Neste Oil* on ainoa, joka ilmaisee puhtaasti riskinottohalukkuutensa COSO ERM -mallin suosittelemalla tavalla. Oletan, että syy tähän on asian vaikeus ja riskienhallinnan kehittyminen liiaksi erillään strategisesta johtamisesta, jonka yhteydessä riskejä käytännössä otetaan strategiaa määriteltäessä. Toivoa sopii, että kohdeyrityksissä, joissa riskinottokyky ja –halukkuus on tuotu esille riskienhallintainformaation yhteydessä, ymmärretään riskinottokyky strategiaa laadittaessa ja syntyvät riskit strategisia valintoja tehtäessä.

Ainoastaan *Kemira* mainitsee eettiset periaatteensa ja viestii näin tehokkaasti siitä, mikä on oikein ja mikä väärin. Tällä tavalla organisaatiolla on mahdollisuus tehokkaasti puuttua yrityksen periaatteiden vastaiseen toimintaan. Uskon, että eettisten periaatteiden määrittely ja niistä viestiminen lisääntyy Suomessa ainakin suurimpien ja kansainvälisten yritysten joukossa voimakkaasti lähivuosien aikana. Eettiset periaatteet ja niiden mukaiset toimintatavat luovat COSO ERM -mallin mukaan perustan riskienhallinnan toimivuudelle, koska niiden mukaan toimiminen mahdollistaa oikean ja totuudenmukaisen suhtautumisen ja asennoitumisen riskienhallintaan ja mahdollisten väärinkäytösten estämisen. COSO ERM -malli suosittelee johdon ja henkilöstön itseohjautuvuuden

lisäämistä, jolloin jokainen organisaation jäsen toimisi itse annettujen ja oikeiden periaatteiden mukaisesti. Tämän johdosta ylhäältä saneltu autoritäärinen malli ei ole COSO ERM -mallin mukainen tapa toimia.

COSO ERM -mallin mukaan organisaatiossa tulee olla systemaattinen tapa, jolla henkilöstölle kerrotaan olennaisista toimintaa ohjaavista säännöistä. Poikkeamiin tulisi myös reagoida johdonmukaisesti ja oikeudenmukaisesti. Kohdeyrityksissä tämän asian toimivuudesta antoi viitteitä sisäisen valvonnan toimivuudesta kertovat osiot. *Kemira* ja *Neste Oil* kertovat sisäisestä valvonnastaan kattavasti. Controllerfunktio nousi esille erillisenä ohjeistuksen toimivuutta varmistavana tekijänä *Aspolla* ja *Finnlinesilla*. Tämän näkökulman perusteella voin todeta, että sisäinen valvonta on yleisellä tasolla monissa organisaatioissa varsin kehittymätöntä, mitä kuvaa *Finnlinesin* väärinymmärrys sisäisen valvonnan suhteen.

COSO ERM -mallin mukaan on tärkeää, että uudet ehdotukset ja kritiikki käsitellään rakentavalla tavalla ja epäonnistumisia hyväksytään. Tutkimusaineiston perusteella päättelen, että *Kemira* ja *Neste Oil* panostavat keskustelun lisäämiseen ja myös negatiivisten asioiden esille tuomiseen, koska niiden työtyytyväisyystutkimusten tulokset ilmentävät myönteistä kehitystä asioiden rakentavan käsittelyn suhteen. Myös kannustimien tulee olla avoimia, johdonmukaisia ja yleisesti hyväksyttyjä COSO ERM -mallin mukaan. Tällä tavalla ne vaikuttavat myönteisesti tulokseen ja ilmapiiriin. *Kemira* ja *Neste Oil* pyrkivät annetun informaation mukaan kannustinjärjestelmien avoimuuteen, johdonmukaisuuteen ja yleiseen hyväksyttävyyteen. *Aspo* ja *Finnlines* puolestaan keskittyvät ainoastaan johdon palkitsemisjärjestelmän esilletuomiseen.

### 5.1.2 Organisaatio

COSO ERM -mallin sisäisen toimintaympäristön toinen osa-alue on organisaatio, jonka osalta tutkin aineistossa mainittuja asioita liittyen organisaation rakenteeseen, vastuisiin sekä tehtävien ja valtuuksien määrittelyyn, jotka ovat COSO ERM -mallin mukaan riskienhallinnan keskeisiä tekijöitä.

COSO ERM -mallin mukaan *organisaation rakenteen tulee olla selkeä ja tuettava tuloksellista toimintaa.* Organisaatiorakenne ja vastuunjako mahdollistavat tehtävien ja vastuiden selkeän jaottelun ja tukee perustehtävän ja strategian toteuttamista. Aineistossa kohdeyritykset kertovat organisaatiorakenteensa pääpiirteet, jonka perusteella arvioin rakenteen selkeyttä ja strategian mukaisuutta.

*Kemira* kertoo jakaneensa konsernin neljään vahvaan liiketoiminta-alueeseen vuonna 2005. Jaon perusteena on markkina-aseman muuttuminen. Vuonna 2007 *Kemira* kertoo konsernirakenteesta enemmän. Neljän liiketoiminta-alueen alla ovat strategiset liiketoimintayksiköt ja konsernikeskus huolehtii konsernin sisäisten synergioiden hyödyntämisestä ja johtaa tiettyjä koko konsernia koskevia toimintoja kuten energian hankinta, henkilöstö, lakiasiat, logistiikka, ostot, rahoitus, riskienhallinta, sisäinen tarkastus, talous, tietohallinto, T&K, ympäristönsuojelu ja viestintä. Vuonna 2005 *Neste Oil* sitoutuu kehittämään organisaationsa rakennettaan vastaamaan strategian toteuttamista sekä luomaan yhtenäisiä toimintamalleja. *Neste Oil* kertoo neljästä toimialastaan, jotka ovat öljynjalostus, komponentit, öljyn vähittäismyynti ja shipping. Lisäksi kerrotaan konsernirakenteessa tapahtuneista muutoksista. Konsernirakenne on kumpanakin vuonna säilynyt samanlaisena. *Aspo* jakaa kumpanakin vuonna operatiivisen organisaationsa kolmeen liiketoimintaryhmään ja konsernin esikuntatoimintoihin. *Aspon* liiketoimintaryhmät ovat Aspo Chemicals, Aspo Shipping ja Aspo Systems. *Finnlinesin* päätoimialat ovat merikuljetukset ja satamapalvelut. Näiden kahden päätoimialan tueksi yhtiö tarjoaa asiakkailleen tehokkaan, kattavan ja joustavan tietohallintopalvelun.

*Kemira* on selkeästi parantanut organisaatiorakenteesta annettua informaatiota vuonna 2007. Organisaatiorakenne tuntuu myös vastaavan strategian haasteisiin yhtiön kertoessa organisaatiorakenteen muuttuneen markkina-aseman muutoksen seurauksena. Organisaatiossa on myös keskitetty tiettyjä toimintoja tuloksekkaan toiminnan varmistamiseksi. *Neste Oil* kertoo rakentavansa organisaatiotaan strategisten tavoitteiden toteutumisen varmistamiseksi. Yhtenäistämällä toimintamallejaan se varmasti hakee tuloksellisuutta. *Aspo* ja *Finnlines* kuvaavat organisaationsa rakenteen ylätasolla ottamatta kantaa sen strategian mukaisuuteen.

*Vastuut, tehtävät ja valtuudet on COSO ERM -mallissa määritelty ja viestitty tarkoituksenmukaisesti.* Vastuut ja velvollisuudet tulee määritellä kaikille keskeisille osa-alueille. Etsin aineistosta vastuiden, tehtävien ja valtuuksien määrittelyitä kehityskeskustelukäytänteistä ja riskienhallintaan liittyvän informaation osalta. Julkisen aineiston perusteella en kuitenkaan voi yksityiskohtaisesti päätellä, miten vastuut ja velvollisuudet toteutuvat kohdeyrityksissä.

*Kemira* kertoo vuosikertomus- ja tilinpäätösaineistossaan yhtiöoikeudellisten toimielinten ja johtoryhmän vastuista ja velvollisuuksista. Lisäksi se kertoo kehityskeskustelujen avulla kehittävänsä suorituksia, osaamisen johtamisen sekä organisaation toimivuuden kehittämistä, minkä yhteydessä oletan käytävän läpi myös vastuita, tehtäviä ja valtuuksia. Tämän alueen sisältö on molempina vuosina pääosin sama. Riskienhallintaan kuuluvista vastuista *Kemira* nimeää sisäisen tarkastuksen vastuulle riskienhallintatoiminnon ja -toimenpiteiden arvioinnin. *Kemiran* yksi riskienhallinnan pääperiaatteista on, että riskin omistajuus on liiketoiminnon tai muun toiminnon omistajalla.

*Neste Oil* kertoo molempina vuosina vuosikertomus- ja tilinpäätösaineistossaan yhtiöoikeudellisten toimielinten ja johtoryhmän vastuista ja velvollisuuksista. Lisäksi *Neste Oil* mainitsee vuosittaiset tavoite- ja kehityskeskustelut, joiden avulla varmistetaan, että tavoitteet ovat haasteellisia ja oikein ymmärrettyjä. Tavoite- ja kehityskeskustelujen osalta oletan, että keskeisimmät valtuudet ja tehtävät käsitellään. *Neste Oilin* riskienhallintaperiaatteissa on määritelty riskienhallinnan vastuut, prosessit, periaatteet sekä tavoitteet. *Neste Oil* kuvaa riskienhallinnan vastuita eri tasoilla seuraavasti vuonna 2007:

> ”Neste Oilin hallituksen tarkastusvaliokunta vastaa yhtiön riskienhallinnan laadun, riittävyyden ja tehokkuuden arvioinnista, konsernin riskienhallintayksikkö ohjaa riskienhallintaprosessia ja kehittää sekä arvioi riskienvalvontaprosesseja, toimialat vastaavat itse toimintoihinsa liittyvien riskien hallinnasta ja tukevat näin osaltaan konsernin liiketoimintaa.”

Vuonna 2005 vastuiden kuvaaminen on yksityiskohtaisempi, mutta ei yhtä selkeä kuin vuonna 2007:

> ”Jokainen toimiala vastaa toimintaansa liittyvien riskien hallinnasta, konsernirahoitus vastaa koko konsernin valuutta-, korko-, likviditeetti- ja jälleenrahoitusriskien hallinnasta, konsernin vakuutusyksikkö vastaa tiettyjä operatiivisia riskejä koskevista vakuutuksista, vakuutusten sekä luotto- ja vastapuoliriskien hallinta on organisoitu konsernin riskienhallinnassa, vastapuolten luottokelpoisuutta koskevista päätöksistä huolehtivat linjaorganisaatiot ja luottovaliokunta, johon kuuluvat edustajat yhtiön toimialoilta sekä konsernirahoituksesta ja riskienhallinnasta, tietotekniikkariskien hallinnasta huolehtii konsernin tietohallinto, konsernin turvallisuusriskeistä yritys-turvallisuusyksikkö, toimialat vastaavat terveys-, turvallisuus- ja ympäristöriskien (HSE) hallinnasta”.

*Aspo* kertoo molempina vuosina aineistossaan yhtiöoikeudellisten toimielinten ja johtoryhmän vastuista ja velvollisuuksista. Riskienhallinnan osalta operatiivinen johto vastaa normaalien liiketoimintariskien hallinnasta vastuualueidensa mukaisesti: ”riittävien toimenpiteiden määrittämisestä, toteuttamisesta sekä toimenpiteiden toteutumisen seurannasta osana normaalia toiminnan ohjausta.” Riskin omistajuutta ei mainita erikseen. Tekstistä käy kuitenkin lisäksi ilmi, että riskienhallintaa koordinoi talousjohtaja, joka raportoi suoraan toimitusjohtajalle. Hallitus käsittelee konsernin riskienhallinta-, vakuutus- ja rahoituspolitiikat.

*Finnlines* kertoo yhtiöoikeudellisten toimielinten ja johtoryhmän vastuista ja velvollisuuksista molempina vuosina. Eri yksiköiden johtajat asettavat johtamalleen yksikölle operatiiviset tavoitteet ja huolehtivat resurssien tehokkaasta käytöstä sekä toiminnan mittaamisesta ja kehittämisestä. Vuonna 2005 *Finnlines* kertoo, että konsernin riskienhallinnan periaatteet hyväksyy hallitus ja niiden toteutuksesta vastaa keskitetysti konsernin rahoitusosasto lukuun ottamatta polttoaineklausuuleja, jotka ovat liiketoimintayksiköiden vastuulla. Vuonna 2007 riskienhallinnan vastuut ilmaistaan seuraavasti: ”Riskienhallinta on osa yhtiön valvontajärjestelmää.” Vastuiden ja valtuuksien määrittelystä kerrotaan niukasti. Yhtiöoikeudellisten toimielinten ja johtoryhmän vastuita kuvataan yleisesti. *Kemira* ja *Neste Oil* tuovat esille kehityskeskustelukäytänteensä, joissa

määritellään vastuita ja tehtäviä yksilötasolle asti. Riskienhallinnan osalta vastuita tuodaan esille kaikissa kohdeyrityksissä. *Kemira* tuo esille riskienhallinnan omistajuuden ja *Neste Oil* kirjaa riskienhallinnan vastuita yksityiskohtaisesti. *Aspo* ja *Finnlines* eivät tuo riskienhallinnan vastuita selkeästi esille.

On tärkeää, että organisaatiorakenne tukee perustehtävän ja strategian toteuttamista. *Kemiran* ja *Neste Oilin* kohdalla tämä näkyy aineistosta, joten ne noudattavat COSO ERM -mallin suositusta selkeästä organisaatiorakenteesta. Organisaation toimivuuden kannalta on tärkeää, että vastuut ja tehtävät on määritelty kaikille keskeisille osa-alueille. Yhtiöoikeudellisten toimielinten ja johtoryhmän sekä riskienhallinnan osalta vastuita tuodaan esille kaikissa kohdeyrityksissä. *Kemira* käyttää riskienhallinnan kohdalla omistajuus-käsitettä, mikä on myös COSO ERM -mallin mukaan hyvä käytänne. *Neste Oil* kirjaa riskienhallinnan vastuut tarkasti, joka myös kuvastaa oikea-oppista COSO ERM -mallin suositusta. Seuraavaksi käyn läpi sisäisen toimintakulttuurin kolmannen osion eli resurssit.

### 5.1.3 Resurssit

COSO ERM -mallin mukaisen toimintakulttuurin kannalta on tärkeää, että henkilöstöllä on tehtävien edellyttämä osaaminen: tehokas rekrytointi, osaamisen arviointi ja kehittäminen sekä riittävä, mutta ei liiallinen henkilöstön määrä. Tässä kohdassa etsin aineistosta henkilöstön rekrytointiin, osaamiseen ja kehittämiseen liittyviä tietoja.

*Kemiralla* otettiin vuonna 2005 käyttöön uusi henkilöstötoimintojen tietojärjestelmä, jonka avulla hoidetaan henkilöstön ja organisaation perustietoja, rekrytointiprosessia sekä koulutustietoja esimiesten, henkilöstötoimen ja johdon tarpeisiin. *Kemiralla* on vuosikertomuksen osana henkilöstöä käsittelevä erillinen kohta, jossa kuvataan muun muassa erinomaisen yrityskulttuurin osatekijöitä, jotka ovat arviointimenetelmät, hyvinvointiohjelmat, turvallisuuden kehittäminen, palkitseminen, aloitejärjestelmät sekä johtamis- ja muu henkilökohtainen koulutus. Vuonna 2007 henkilöresursseja käsitellään saman tyyliin kuin 2005. Erinomaisen kulttuurin osatekijöitä on muutettu seuraavasti verrattuna vuoteen 2005: osaaminen, osallistuminen, suoritus ja palkitseminen, resurs-

sit, turvallisuus, hyvinvointi sekä johtajuus. *Neste Oililla* on molempina vuosina henkilöstöä käsittelevä kohta osana vuosikertomusta. Vuonna 2005 *Neste Oililla* kehitettiin henkilötietojärjestelmää, joka otettiin käyttöön vuoden 2006 alussa. Järjestelmällä hallitaan henkilöstön ja organisaatioiden perustietoja, rekrytointiprosessia, koulutustietoja, raportointia sekä palkantarkistusprosessia. Vuonna 2007 *Neste Oilin* henkilöstösuunnittelun tavoitteena on edistää yhtiön strategian toteutumista kehittämällä johtamista, esimiestyötä, asiantuntijuutta ja osaamista. Pitkän tähtäyksen henkilöstösuunnittelulla pyritään siihen, että kullakin liiketoiminnolla on aina sen strategian edellyttämä osaaminen ja tarvittavat resurssit. Tämä varmistetaan onnistuneella rekrytoinnilla, urasuunnittelulla, esimiesroolien ja vastuiden kehittämisellä sekä esimiesten ja henkilöstön jatkuvalla valmennuksella. *Aspo* käsittelee henkilöstöään lyhyesti vuosikertomuksen kohdassa ”henkilöstö ja ympäristö” vuonna 2005. Tekstissä tuodaan esille muun muassa henkilökunnan aloitemahdollisuus, henkilöstörahasto ja turvallisuusasioita. Vuonna 2007 henkilöstöstä ei enää kerrota ja kohdan ”Ympäristö ja henkilöstö” nimi on muuttunut: ”Ympäristö”. Vuonna 2005 *Finnlinesilla* on osana vuosikertomusta henkilöstöraportti, jonka mukaan ”osaavat ja innostuneet ihmiset ovat yhtiön tärkein voimavara ja kilpailukyvyn perusta.” Vuonna 2007 *Finnlinesilla* on samantyyppinen henkilöstöä koskeva osuus vuosikertomuksessa kuin 2005. Sitä ei kuitenkaan enää otsikoida henkilöstöraportiksi. Henkilöstöä koskevassa osuudessa käsitellään koulutusta, organisaatiomuutoksia, rekrytointia, henkistä ja fyysistä toimintakykyä ja tyytyväisyystutkimuksia. Lisäksi on taulukko, jossa esitetään henkilöstöä koskevat merkittävimmät tunnusluvut.

Henkilöstö on annetun informaation mukaan kaikille kohdeyrityksille tärkeässä asemassa. *Neste Oil* ja *Kemira* kertovat henkilöstön kehittämispanostuksistaan selkeästi. Molemmat yritykset kertovat ottaneensa käyttöön henkilöstötietojärjestelmän tarkasteluajanjakson aikana. Tästä päättelen, että molemmat yritykset ovat dokumentoineet ja päivittäneet osaamistarpeet ja – resurssit. *Neste Oililla* henkilöstösuunnittelun tavoitteena on edistää yhtiön strategian toteutumista, mikä kytkee osaamisen kehittämisen toiminnan tarpeisiin. *Finnlinesilla* on vuonna 2005 henkilöstöraportti niminen osio vuosikertomuksessaan ja *Aspokin* käsittelee henkilöstöään omana kohtanaan vuonna 2005. Jostain syystä *Aspo* ja *Finnlines* näyttävät vähentäneen henkilöstöstä annettua raportointia vuodesta 2005 vuoteen 2007.

Organisaatiolla tulisi COSO ERM -mallin suositusten mukaan olla käytössään sellaiset tietojärjestelmät ja tilat, joita tehtävien tuloksellinen hoitaminen edellyttää. Tietojärjestelmistä ja tiloista ei yleensä kerrota erikseen vuosikertomuksen ja tilinpäätöksen yhteydessä. Niitä koskevia kysymyksiä käsitellään kuitenkin osana muuta informaatiota, esimerkiksi suurten tietojärjestelmähankkeiden tapauksessa. Näin on myös tutkielman kohdeyritysten kohdalla. Käyn aineistosta läpi keskeisimmät tietojärjestelmähankkeet, joiden avulla kohdeyritykset mahdollistavat henkilöstönsä tuloksellisen toiminnan.

*Kemira* mainitsee seuraavista tietojärjestelmähankkeistaan kohdeaineistossa: asiakaskohtaisten kokonaisratkaisujen hallintaan kehitetty reaaliaikainen Fennodose-järjestelmä, joka muun muassa mittaa prosessin tilaa, uusittu henkilöstötoimintojen tietojärjestelmä, tuoteturvallisuuteen liittyvän globaalin IT-järjestelmän kehittämisen jatkaminen ja uuden maailmanlaajuisen toiminnanohjausjärjestelmän käyttöönotto. *Neste Oil* tuo esille kaksi tietojärjestelmähanketta: henkilötietojärjestelmän ja kemikaalien tietokantajärjestelmän. Lisäksi *Neste Oil* kertoo, että tietojärjestelmien ja niissä käsiteltävän tiedon merkitys yrityksen toiminnassa ja sen ohjaamisessa kasvaa vuosi vuodelta. Tässä *Neste Oilin* mukaan keskeisiä alueita ovat dokumenttien luokittelun ja hallinnan kehittäminen, järjestelmien käytettävyyden ja luotettavuuden varmistaminen, tietoturvakriteerien määrittäminen sekä varsinaiset tekniset tietoturvaratkaisut. *Aspo* kertoo ottaneensa uuden toiminnanohjausjärjestelmän käyttöön vuonna 2007. Lisäksi se kertoo, että tietotekniikka on entistä suuremmassa roolissa myös huoltoasemien etähallinnassa, jossa *Aspo* käyttää Internet-pohjaista valvontajärjestelmää. *Finnlines* kertoo uuden, asiakaslähtöisen toimintatavan tuoneen suuria muutoksia tietohallintoon, esimerkiksi prosessi tilanvarauksesta laskutukseen hoidetaan uudella järjestelmällä vuodesta 2007.

Edellä käsitellyt henkilöstö- ja tietojärjestelmäresurssit ovat selkeitä resurssien osa-alueita. Lisäksi eri toimialoilla toimivat yritykset tarvitsevat esimerkiksi tiloja, laitteita ja kalustoa tehtäviensä tuloksekkaan hoitamisen edellytykseksi. Esimerkiksi *Finnlines* ja *Aspo* käsittelevät laivastoaan ja kalustoaan osana liiketoimintansa kuvausta. Annettu informaatio riippuu siis paljon toimialasta, jolla toimitaan sekä strategista. Esimerkiksi

*Finnlinesin* suuret investoinnit ropax-aluksiin vuonna 2006 ovat yhtiölle merkittävä kokonaisuus, joka ei voi olla vaikuttamatta yrityksen riskeihin ja niiden hallintaan. Kaikki kohdeyritykset kertovat tietojärjestelmistään ja niihin liittyvistä kehityshankkeista osana muuta toiminnastaan annettua informaatiota. Merkittäviä eroja annetun informaation välillä on vaikea identifioida.

COSO ERM -mallin mukaan on tärkeää, että henkilöstöresurssit ja niiden osaamisen kehittäminen on kytketty toiminnan tarpeisiin. Jokainen kohdeyritys tuo henkilöstöresurssiin liittyviä asioita esille tutkimusaineistossa. *Aspon* ja *Finnlinesin* henkilöstöön liittyvä raportointi vähenee vuodesta 2005 vuoteen 2007. Tähän en löydä selitystä. *Kemira* ja *Neste Oil* kertovat henkilöstöstään johdonmukaisesti ja pyrkivät kuvaamaan henkilöstön osaamista toimintalähtöisesti. Tämä kuvastaa COSO ERM -mallin mukaista suositusta henkilöstön osaamisen kehittämistä organisaation toiminnan tarpeisiin. On myös tärkeää, että yrityksellä on riittävät ja luotettavat toimintaa tukevat tietojärjestelmät ja muut resurssit. Kohdeyritysten antamassa tietojärjestelmiä koskevassa informaatiossa ei ole merkittäviä eroja. Kohdeyritykset antavat tietoja muista resursseistaan toimialansa erityispiirteiden mukaisesti.

COSO ERM -mallin sisäinen toimintaympäristö luo perustan sisäiselle valvonnalle ja riskienhallinnalle ja sen vaikutukset ulottuvat kaikkeen toimintaan. Päätelmäni on, että sisäinen toimintaympäristö eroaa selvästi *Kemiran* ja *Neste Oilin* suhteessa *Aspoon* ja *Finnlinesiin*. Tähän voisi olla syynä se, että suuremmilla yrityksillä, kuten *Kemiralla* ja *Neste Oililla,* on enemmän resursseja myös riskienhallinnan systemaattiseen kehittämiseen ja niille asetetaan myös kovempia vaatimuksia eri sidosryhmien taholta. *Aspon* ja *Finnlinesin* sisäisestä toimintaympäristöstä saa vain vähän tietoa tutkimusaineistosta ja kahden vuoden välillä ei juuri ole muutoksia. *Kemiran* ja *Neste Oilin* sisäinen toimintaympäristö on kehittynyt vuosien välillä kasvun ja liiketoiminnan muun kehittymisen myötä.

## 5.2 Tavoitteiden asettaminen

COSO ERM -mallin tavoitteiden asettaminen kohdan mukaan selkeät tavoitteet ovat systemaattisen riskien tunnistamisen lähtökohta. Tavoitteiden asettamisen osalta tutkin aineistosta, miten kohdeyrityksissä määritellään niiden perustehtävä, visio ja toiminta-strategia, onko niille asetettu selkeät strategiset tavoitteet ja suunnitellaanko ja seura-taanko niiden liiketoimintaa systemaattisesti.

Ennakkoedellytys COSO ERM -mallin mukaiselle toimivalle riskienhallinnalle on, että *organisaatiolla on selkeä perustehtävä ja johto on määritellyt vision ja toimintastrate-gian.* Etsin kohdeyritysten aineistoista selkeitä vision määrittelyjä, joiden avulla pyrin hahmottamaan kohdeyritysten suunnittelun ja tavoitteiden asettamisen lähtökohtia.

Vuonna 2005 *Kemiran* visio on ilmaistu seuraavasti:

> ”Kemiran tavoitteena on olla globaali ryhmä johtavia kemian alan liiketoimintoja, joilla on ainutlaatuinen kilpailuasema ja suuri keskinäinen synergia. Menestys syntyy ainut-laatuisesta strategiasta, joka yhdistetään maailmanluokan tehoon.”

Vuonna 2007 *Kemiran* visiota tai missiota ei mainita, mutta visiota vastaa seuraava kuvaus:

> ”Kemiran tavoitteena on olla toimialoillaan johtava maailmanlaajuinen kemianyhtiö, jonka liiketoiminnoilla on ainutlaatuinen kilpailuasema valituissa asiakassegmenteissä.”

*Kemiran* visio on säilynyt pääpiirteittäin samanlaisena vuodesta 2005 vuoteen 2007. Vuoden 2007 visio korostaa kuitenkin yhtenäisempää *Kemiraa*, kun vuonna 2005 pu-huttiin ryhmästä johtavia kemian alan toimintoja.

Vuonna 2005 *Neste Oilin* visiota tai missiota ei mainita, mutta visiota kuvaa seuraava ilmaus:

> ”Neste Oilin tavoitteena on olla johtava pohjois-eurooppalainen öljynjalostus- ja markkinointiyhtiö, joka on keskittynyt korkealaatuisiin puhtaamman liikenteen öljytuotteisiin ja sitoutunut maailmanluokan toiminnallisiin ja taloudellisiin tuloksiin.”

Vuonna 2007 *Neste Oil* mainitsee visiokseen olla johtava puhtaamman liikenteen polttoaineiden toimittaja. *Aspon* visio molempina vuosina on seuraavanlainen: ”Yrityksen arvon ja osaamisen pitkäjänteinen kasvattaminen yli sukupolvien.” *Finnlinesin* toiminta-*ajatuksena* on kumpanakin vuonna:

> ”Kansainvälisen kaupan edistäminen tarjoamalla tehokkaita ja laadukkaita merikuljetus- ja satamapalveluja lähinnä eurooppalaisen teollisuuden, kaupan ja kuljetusalan tarpeisiin.”

Kaikki kohdeyritykset tuovat visionsa esille aineistossa molempina vuosina. Perustehtävän ja vision olisi hyvä olla lähtökohtana kaikessa suunnittelussa ja näin näyttää kaikissa kohdeyrityksissä olevan. *Aspon* ja *Finnlinesin* visio on pysynyt vuodesta 2005 vuoteen 2007 täysin samana, kun taas *Kemiran* ja *Neste Oilin* visioissa tai niiden ilmaisussa on pieniä muutoksia.

COSO ERM -mallin mukaan organisaation visioon perustuvat *selkeät strategiset tavoitteet ovat riskienhallinnan lähtökohta.* Organisaatioilla tulee olla selkeät strategiset pitkäntähtäimen tavoitteet, jotka tukevat niiden tahtotilan toteutumista. Tutkimusaineistosta ei löydy tietoja alemman tason tavoitteista siten, että voisi päätellä ovatko ne johdettu ylemmän tason tavoitteista. Samoin tavoitteiden priorisoinnista, aikataulutuksesta ja niihin liittyvistä toimenpiteistä, resursseista ja tavoitteiden viestinnästä mittareineen löytyy niukasti, jos ollenkaan tietoja aineistosta. En siis pysty analysoimaan näitä COSO ERM -mallin mukaisen riskienhallinnan kannalta sinänsä olennaisia osatekijöitä, joten tutkin kohdeyritysten aineistossa esille tuomia strategisia toimintaan ja talouteen liittyviä tavoitteita.

Vuonna 2005 *Kemiran* tavoitteena on olla ”globaali yhtiö, jonka liiketoiminnoilla on suuri keskinäinen synergia ja ainutlaatuinen kilpailuasema.” *Kemira* nimeää tavoitteikseen ”lisäarvotuotteiden ja palveluiden osuuden nostamisen, uusien tuotteiden markkinoille tuomisen, tuotevalikoiman ja myynnin laajentamisen, vahvan markkina-aseman rakentamisen yritysostojen- ja järjestelyjen kautta, sisäisen tehokkuuden parantamisen ja pääoman tehokkaamman käytön.” Vuonna 2007 *Kemiran* päämääränä on olla ”maailmanlaajuinen ryhmä johtavia kemian alan liiketoimintoja, joilla on ainutlaatuinen asiakassegmenttilähtöinen kilpailuasema ja suuri keskinäinen synergia.” *Kemiran* strategisissa tavoitteissa korostuu liiketoimintamallin muutosprosessi tuotelähtöisyydestä asiakassegmenttikohtaisten ratkaisujen tarjoajaksi. *Kemiran* strategisia tavoitteita vuonna 2007 ovat kilpailuaseman vahvistaminen olemalla läsnä kaikilla päämarkkinoilla maailmanlaajuisesti, merkittävän aseman saavuttaminen kehittyvillä markkinoilla, kyky palvella maailmanlaajuisia asiakkaita yhdenmukaisesti, ykkösasema maailmanlaajuisesti valituilla markkinoilla ja asiakassegmenteissä sekä ylivoimaisen asiakashyödyn tarjoaminen. *Kemiran* taloudellisia tavoitteita vuonna 2007 ovat orgaaninen kasvu, joka on suurempi kuin 5 % vuodessa, EBIT:in (earnings before interests and taxes) osuuden kasvattaminen suuremmaksi kuin 10 % liikevaihdosta, positiivinen rahavirta investointien ja osinkojen jälkeen, ROCE:n (return of capital employed ) jatkuva parantaminen sekä 40–80 %:n velkaantuneisuuden tavoitealue.

Vuonna 2005 *Neste Oilin* tavoitteena (visiona) on olla:

> ”Pohjois-Euroopan johtava itsenäinen öljynjalostus- ja markkinointiyhtiö, joka keskittyy korkealaatuisiin puhtaamman liikenteen öljytuotteisiin ja on sitoutunut maailmanluokan toiminnallisiin ja taloudellisiin tuloksiin.”

Taloudelliset tavoitteet ovat sijoitetun pääoman tuotto keskimäärin verojen jälkeen vähintään 13% ja velan osuus kokonaispääomasta 25–50 %. Vuonna 2007 *Neste Oilin* tavoitteena on omistaja-arvon kasvattaminen käyttämällä hyväksi yhtiössä olevaa korkealaatuisten polttoaineiden valmistamisen ja myynnin osaamista. *Neste Oil* ei nimeä erikseen strategisia tavoitteita, mutta listaa erikseen kunkin toimialansa tavoitteet. Taloudellisista tavoitteista ei ole mainintaa vuonna 2007. *Aspon* tavoitteena on molempina vuosina ”rakentaa kestäviä, vahvaan partneruuteen ja kumuloituneeseen erikoisosaami-

seen perustuvia asiakassuhteita.” *Aspon* nimeää taloudelliset tavoitteensa seuraavalla tavalla: ”liikevoittoprosentti on keskimäärin lähempänä kymmentä kuin viittä, liikevaihto kasvaa keskimäärin 10–15 prosenttia vuodessa, sijoitetun ja oman pääoman tuotto on keskimäärin yli 20 prosenttia.” Lisäksi *Aspon* tavoitteena on jakaa osinkoa keskimäärin puolet vuoden tuloksesta.

Vuonna 2005 *Finnlines* mainitsee strategisiksi tavoitteikseen markkina-aseman säilyttämisen Suomi-sidonnaisessa rahtiliikenteessä, nykyistä vahvemman aseman Suomi-sidonnaisessa matkustajaliikenteessä, Venäjän tavaraliikenteessä Itämerellä ja Pohjanmerellä ei-Suomi-sidonnaisessa liikenteessä sekä kannattavuuden kasvun. Taloudellisina tavoitteina on molempina vuosina taata laadukkaalla liiketoiminnalla pitkän aikavälin kannattavuus, tuottaa omistajilleen lisäarvoa ja pitää rahoitusrakenne terveenä. Vuonna 2007 strategisiksi tavoitteiksi mainitaan nykyistä vahvempi asema Itämeren ja Pohjanmeren rahtiliikenteessä, Itämeren matkustajaliikenteessä ja Venäjän tavaraliikenteessä sekä kannattavuuden kasvu.

Kaikki kohdeyritykset tuovat aineistossa esille strategisia markkinoihin, asiakkaisiin ja toimintaan liittyviä tavoitteita sekä taloudellisia tavoitteita. Kohdeyrityksillä on siis strategiset pitkäntähtäimen tavoitteet, jotka tukevat niiden tahtotilan toteutumista. *Neste Oil* ei kuitenkaan jostain syystä tuo esille taloudellisia tavoitteitaan vuonna 2007. *Kemiralla* vastaavasti ei ole taloudellisia tavoitteita vuonna 2005. Esille tuotuja riskejä analysoitaessa on mielenkiintoista nähdä, kuinka ne heijastavat strategiaa ja siinä asetettuja tavoitteita. Kohdeyritykset tuovat aineistossa esille lähinnä strategisia tavoitteitaan normaalin käytänteen mukaisesti. Ne eivät tuo aineistossa esille erikseen operatiivisia, raportointiin ja laillisuuteen liittyviä tavoitteitaan. Näkisin, että raportointiin ja laillisuuteen liittyvien tavoitteiden asettaminen on muutenkin harvinaisempaa ja liittyy lähinnä sisäisen valvonnan toimivuuden arviointiin.

COSO ERM -mallin tavoitteiden asettamisen kannalta on tärkeää, että *toimintaa suunnitellaan ja seurataan systemaattisesti kaikilla tasoilla*. Strategian ja siitä johdettujen suunnitelmien tulee perustua ulkoisen ja sisäisen toimintaympäristön analyysiin. Viitteitä systemaattisen toiminnan suunnitteluun on vaikea löytää julkisesta vuosikertomus- ja

tilinpäätösmateriaalista. Näkisin, että kohdeyritysten selkeät tavoitteet antavat kuitenkin ymmärtää, että niiden taustalla on systemaattista suunnittelua. Jotkin kohdeyrityksistä olivat raportoineet tietoja markkinoista ja asiakkaista sekä muusta toimintaympäristöstä. Esimerkiksi tällainen toimintaympäristöanalyysi on yleensä suunnittelun taustalla. Toimintaympäristöanalyysi ja muut suunnitteluun liittyvät raportit ja muistiot jäävät yleensä yrityksen sisäisiksi asiakirjoiksi. Nostan tutkimusaineistosta esiin *Kemiran*, jossa riskit tunnistetaan yhteisesti sovitun itsearviointimallin mukaisesti. Tunnistusprosessissa riskit dokumentoidaan riskikartoiksi ja riskilistoiksi, joiden perusteella laaditut riskienhallintasuunnitelmat liitetään osaksi liiketoimintojen toimintasuunnitelmia. *Kemiran* riskienhallintaprosessi on siis osa normaalia johtamis- ja suunnitteluprosessia.

Perustehtävä ja visio ovat lähtökohtana suunnittelulle kaikissa kohdeyrityksissä. *Kemiran* ja *Neste Oilin* visioissa tai niiden ilmaisussa on pieniä muutoksia vuosien 2005 ja 2007 välillä. Kaikilla kohdeyrityksillä on selkeät perustehtävät ja niille on määritelty selkeät visiot ja toimintastrategiat, joten niiden riskienhallinnan ennakkoedellytykset täyttyvät COSO ERM -mallin mukaisesti. Kohdeyritysten visioon perustuvat selkeät strategiset tavoitteet toimivat parhaan ymmärrykseni mukaan riskienhallinnan hyvänä lähtökohtana. Myöhemmin aineistossa esille tuotuja riskejä analysoitaessa on mielenkiintoista nähdä, kuinka ne heijastavat strategiaa ja siinä asetettuja tavoitteita.

## 5.3 Riskien tunnistaminen, arviointi sekä niihin vastaaminen

Toiminnan johdonmukainen suunnittelu, seuranta ja ohjaus ja näihin liittyvä tavoitteiden määrittely ovat COSO ERM -mallin mukaisia edellytyksiä tavoitteita uhkaavien riskien tunnistamiselle. Tutkin tavoitteiden saavuttamista uhkaavien riskien tunnistamista ja dokumentointia sekä riskien arviointia kohdeyritysten esille tuomien riskienhallintaprosessin toimintatapojen kautta. Tämän jälkeen nostan esille aineistosta kohdeyritysten esille tuomia strategisia, operatiivisia ja taloudellisia/rahoitukseen liittyviä riskejä. Näitä riskiryhmiä tarkastelen kutakin erikseen. Riskeihin vastaamisen osiossa arvioin, linjaavatko kohdeyritykset, mitä riskejä otetaan ja miten riskejä hallitaan suhteessa niiden riskinottohalukkuuteen ja –kykyyn.

Kohdeyrityksistä haluan jälleen nostaa esiin *Kemiran*, joka hyödyntää käyttämääni viitekehikkoa COSO:a. Kertoessaan sisäisestä valvonnastaan *Kemira* vetää yhteen riskien arviointia koskevat käytänteensä vuosikertomuksessaan seuraavasti:

> ”Kemiran riskienhallinnan perustana on kokonaisvaltaisen riskienhallinnan periaate (Enterprise Risk Management, ERM). Kemirassa kokonaisvaltaisella riskienhallinnalla tarkoitetaan eri riskialueiden, kuten strategisten, vahinko-, operatiivisten sekä rahoitusriskien järjestelmällistä ja ennakoivaa tunnistamista, arviointia ja hallintaa. Tavoitteena on määritellä ja saavuttaa haluttu kokonaisriskitaso suhteessa konsernin riskinkantokykyyn sekä samalla varmistaa toimintojen jatkuvuus”.

### 5.3.1 Riskienhallintaprosessi: tunnistaminen ja arviointi

*Kemiran* riskienhallintaprosessi on aineistossa annetun informaation mukaan molempina vuosina pääpiirteissään samanlainen. Vuonna 2005 *Kemira* lupaa kehittää riskienhallintaansa seuraavasti:

> ”Jatkossa kokonaisvaltainen riskienarviointi ja -hallinta tullaan kiinteämmin liittämään liiketoimintojen omiin suunnitteluprosesseihin, erityisesti strategiseen suunnitteluun. Jatkuvan ja systemaattisen riskienarvioinnin ja hallintatyön lisäksi Kemira-konsernin riskienhallintaa tullaan kehittämään täsmentämällä kokonaisvaltaisen riskienhallinnan organisointia, päivittämällä riskienhallintaan liittyviä politiikkoja ja ohjeistusta sekä lisäämällä konsernin sisäistä riskiraportointia.”

Huolimatta kehityssuunnitelmista vuosien 2005 ja 2007 riskienhallinnan käytänteiden kuvaukset ovat *Kemiralla* pääpiirteissään samanlaiset. Ohessa vuoden 2007 kuvaus:

> ”Riskienhallinnan käytännöt: Kemirassa riskien tunnistus ja arviointi tehdään liiketoiminta-alueittain soveltaen yhteisesti sovittua riskien itsearviointimallia. Liiketoiminta-alueiden riskiraportointia voidaan täydentää tunnistamalla ja arvioimalla riskejä myös esimerkiksi eri tukitoimintojen, suurimpien tehtaiden tai investointiprojektien kannalta. Arviointien tuloksena johdolla ja liiketoiminta-alueilla on käytössään riskikartat sekä riskilistat, joiden perusteella laaditut riskienhallintasuunnitelmat liitetään osaksi liike-

> toimintojen toimintasuunnitelmia. Kustannusedun saavuttamiseksi ja riittävän suojaustason varmistamiseksi tietyt riskienhallintatoimet hoidetaan konsernissa keskitetysti. Tällaisia ovat esimerkiksi tietyt vakuutusohjelmat, kuten konsernin toiminta- ja tuotevastuuvakuutus, kuljetusvakuutus, suurimpien tehtaiden omaisuus- ja keskeytysvakuutukset sekä rahoitusriskien suojaustoimet. Myös teollisuus- ja liiketoimintaympäristön, asiakkaiden ja teknologisen kehityksen seurantaprosessit on järjestetty keskitetysti, jotta pystymme ennakoivasti ja synergisesti vastaamaan muuttuviin olosuhteisiin".

Vuoden 2007 kuvauksessa oli ainoastaan yksi merkittävä ero verrattuna vuoteen 2005: "Liiketoiminta-alueiden riskiraportointia voidaan täydentää tunnistamalla ja arvioimalla riskejä myös esimerkiksi eri tukitoimintojen, suurimpien tehtaiden tai investointiprojektien kannalta." Tätä kohtaa ei siis ollut vuoden 2005 toimintatapakuvauksessa.

Tulkitsen annetun informaation siten, että *Kemiran* vuoden 2005 riskienhallinnan toimintatavan kuvaus on ollut enemmänkin riskienhallinnan tavoitetilan kuvaus, jota kohti on kyllä alettu määrätietoisesti kulkea. Vuoden 2007 kuvaus on uskoakseni jo totuudenmukaisempi ja *Kemiran* riskienhallintaprosessi lähestyy tunnistamisen ja arvioinnin osalta teorian viitekehyksen vaatimuksia. Analyysin tulos on vain suuntaa antava, koska julkinen informaatio ei ole riittävän yksityiskohtaista eikä sen totuudenmukaisuutta pysty todentamaan. Riskienhallinnan kehittäminen on selvästi aikaa vievä prosessi ja siitä raportointi sidosryhmien lisääntyvien vaatimusten pyörteessä vaikeaa.

Vuonna 2005 *Neste Oil* ei varsinaisesti kuvaa riskienhallintaprosessiaan, vaan kertoo lähinnä riskienhallinnan vastuista ja raportoinnista. Vuonna 2005 *Neste Oil* kuvaa riskienhallinnan tulevia haasteita seuraavasti:

> "Neste Oilin riskienhallintaohjelman kehittämisessä keskitytään jatkossa yhtiön kokonaisvaltaisen riskienhallinta- ja -valvontajärjestelmän valmiiksi saamiseen ja käyttöönottoon. Tavoitteena on myös käynnistää tämän järjestelmän osana yhtiön kaikki toimialat ja konsernitoiminnot käsittävä säännöllinen riskienhallintaraportointi".

Vuoden 2007 informaation mukaan riskienhallinta on kehittynyt selvästi ja sen toimintatapoja kuvataan seuraavasti:

> ”Neste Oilin uusi järjestelmä yhdistää riskienhallintakäytäntöjä normaaleihin työrutiineihin koko konsernissa. Prosessin tavoitteena on tunnistaa ja arvioida järjestelmällisesti yhtiön strategia- ja liiketoimintatavoitteita sekä operatiivisia tavoitteita uhkaavat riskit ja raportoida niistä. Työssä hyödynnetään yhtiön eri toimintojen tärkeimpiä riskienhallintakäytäntöjä ja -periaatteita sekä yhdistetään niitä tarpeen mukaan. Kokonaisvaltaisen riskienhallinnan prosessissa riski määritellään yhtiön tavoitteisiin vaikuttavan tapahtuman mahdollisuudeksi. Riskejä mitataan seurausten ja todennäköisyyden perusteella. Riskienhallinnassa pyritään lisäämään tietoista riskinottohalukkuutta hyväksytyissä rajoissa. Tavoitteiden saavuttamista tuetaan seuraamalla markkinoilla, liiketoiminnassa ja muissa asioissa tapahtuvien muutosten vaikutuksia tulokseen. Taloudellisten riskien hallinta kohdistuu tuloksen, taseen ja kassavirran heilahtelun vähentämiseen. Samalla pyritään turvaamaan yhtiön tehokas ja kilpailukykyinen rahoitustoiminta. Strategisessa ja operatiivisessa riskienhallinnassa pyritään jatkuvaan riskien tunnistamiseen, yhtenäiseen määrittelyyn ja priorisointiin sekä ennaltaehkäisyyn”.

Vuonna 2007 *Neste Oil* kertoo riskienhallinnan kehittymistavoitteistaan seuraavasti:

> ”Kokonaisvaltaisen riskienhallinnan kehittämisessä on päästy hyvään alkuun. Jatkossa keskitytään edelleen periaatteiden ja ohjeiden saattamiseen osaksi toimialojen ja konsernitoimintojen päivittäisiä rutiineja. Tämä tukee konsernin strategisten ja liiketoiminnallisten tavoitteiden saavuttamista. Jatkuva seuranta, säännölliset mittaukset, itsearviointi ja riskienhallintatasojen benchmarking-vertailu tähtäävät riskienhallinnan jatkuvaan parantamiseen. Kehittämisalueita ovat investointeihin liittyvä riskienhallinta, maineriskin hallinta, liiketoiminnan jatkuvuussuunnitelmat sekä väärinkäytösten hallintaperiaatteiden määrittely ja käyttöönotto”.

*Neste Oilin* riskienhallintaprosessi vastaa vuonna 2007 annetun informaation mukaan COSO ERM -mallin vaatimuksia riskien tunnistamisen ja arvioinnin osalta. *Neste Oilin* tavoitteena on tunnistaa ja arvioida järjestelmällisesti yhtiön strategia- ja liiketoimintatavoitteita sekä operatiivisia tavoitteita uhkaavat riskit ja raportoida niistä. *Neste Oil*

mittaa riskejä seurausten ja todennäköisyyden perusteella. Se pyrkii jatkuvaan riskien tunnistamiseen, yhtenäiseen määrittelyyn ja priorisointiin sekä ennaltaehkäisyyn. Lisäksi *Neste Oil* huomioi riskinottohalukkuutensa pyrkiessään jopa lisäämään sitä hyväksytyissä rajoissa. *Neste Oil* tuo molempina vuosina hyviä riskienhallinnan kehittämiskohteita esiin. *Neste Oil* kertoo esimerkiksi vuonna 2007 päässeensä kokonaisvaltaisen riskienhallinnan kehittämisessä hyvään alkuun ja keskittyvänsä edelleen periaatteiden ja ohjeiden saattamiseen osaksi toimialojen ja konsernitoimintojen päivittäisiä rutiineja. Tämä kuvaa hyvin riskienhallinnan kehittymisen hidasta muutosprosessia. Vaikka riskienhallinnan toimintatavat ovat jo pitkälle kehittyneitä niiden saattamista laajamittaisesti osaksi päivittäisiä rutiineja jatkuu varmasti vielä pitkään tulematta ehkä koskaan valmiiksi kehityksen viedessä käytänteitä yhä eteenpäin.

*Aspon* riskienhallintaprosessi on aineistossa annetun informaation mukaan molempina vuosina samanlainen. *Aspo* kuvaa sen seuraavasti:

> ”Mahdollisten tapahtumien todennäköisyyden ja vaikutusten perusteella riskit on luokiteltu eri ryhmiin. Luokittelu antaa suuntaa riskienhallintatoimien tärkeysjärjestykselle ja luo yhtenäisen tavan arvioida ja arvottaa riskejä koko konsernissa. Merkittävät, suuret ja kohtalaiset riskit edustavat Aspo-konsernissa normaalia liiketoimintariskiä. Niiden hallinnasta vastaa operatiivinen johto vastuualueidensa mukaisesti. Johto vastaa riittävien toimenpiteiden määrittämisestä, toteuttamisesta sekä toimenpiteiden toteutumisen seurannasta osana normaalia toiminnan ohjausta. Tiettyjen riskien osalta riskienhallinnan periaatteet ja keskeisin sisältö on määritelty konsernitason politiikoissa ja ohjeissa. Vahinkoriskit on katettu asianmukaisin vakuutuksin”.

*Aspon* operatiivinen johto vastaa merkittävistä, suurista ja kohtalaisista riskeistä vastuualueidensa mukaisesti. Riskejä on luokiteltu merkittävyytensä perusteella, mutta varsinaisesta riskienhallintaprosessista ei anneta tietoja, minkä perusteella oletan, että systemaattista riskienhallintaprosessia ei ole. Pienempänä ja suhteellisen vakiintunutta liiketoimintaa harjoittavana organisaationa *Aspo* tuntuu kuitenkin hallitsevan riskejään käytännönläheisesti osana normaalia johtamistaan hyödyntämättä kuitenkaan systemaattisen riskienhallinnan työkaluja. *Aspo* ei tuo esille riskienhallintaan liittyviä kehittämistoimenpiteitä kumpanakaan vuonna.

*Finnlinesin* riskienhallintaprosessista antama informaatio on suppeaa ja merkittäviltä osin samanlaista molempina vuosina. Vuonna 2007 *Finnlines* kertoo riskienhallinnastaan osana valvontajärjestelmän kuvausta ja erillisessä kappaleessa, jossa käsitellään riskienhallintaa ja sisäistä tarkastusta. Alla edellä mainitut kohdat vuosikertomuksesta:

> ”Valvontajärjestelmät: Yhtiön hallitus vastaa hallinnosta ja toiminnan asianmukaisesta järjestämisestä. Käytännössä toimitusjohtajan tehtävänä on huolehtia johtoryhmän tuella sisäisen valvonnan, riskienhallinnan, sisäisen tarkastuksen ja kirjanpidon valvontamekanismien järjestämisestä. Ohjeistus on koko konsernin kattava. Yhtiön taloudellista kehitystä seurataan kuukausittain koko konsernin kattavan raportointijärjestelmän avulla. Riskien hallinta ja sisäinen tarkastus: Hallitus huolehtii siitä, että yhtiössä on määritelty sisäisen valvonnan toimintaperiaatteet ja että yhtiössä seurataan valvonnan toimivuutta. Riskienhallinta on osa yhtiön valvontajärjestelmää. Konserniesikuntaan on keskitetty vastuu konsernin sijoitus- ja käyttöomaisuudesta, investoinneista, rahoituksesta, taloudesta, henkilöstöhallinnosta, viestinnästä ja tietojärjestelmistä. Konsernin talous- ja rahoitusjohtajan (CFO) alaisuudessa toimii taloushallinnon palvelukeskus, jonne on keskitetty koko konsernin maksuliikenne, ulkoinen laskenta ja sisäinen laskenta. Hallitus päättää vuosittain budjetoinnin yhteydessä valuutta- ja korkosuojauksen tasosta ja hyväksyy konsernin ulkopuoliset pitkäaikaiset lainajärjestelyt. Konsernin lakiasiainyksikön vastuulla ovat käyttöomaisuus- ja toiminnan keskeytymisestä aiheutuvat riskit. Lakiasiainyksikköön on keskitetty myös vakuutusten hallinnointi ja koordinointi. Pääosa konsernin sidotusta pääomasta muodostuu laivastosta. Laivasto vakuutetaan aina täyteen arvoon. Haverit ja konevauriot voivat aiheuttaa toiminnan keskeytyksiä, jotka on katettu loss of earnings -vakuutuksilla. Konsernin asiakasluottotappioiden minimoimiseksi asiakkaiden taloudellinen asema ja luottokelpoisuus ovat jatkuvassa seurannassa. Tietojärjestelmien toimivuus varmistetaan laajoin ja kattavin turvallisuusohjelmin sekä varajärjestelmin. Konsernin sisäinen valvonta on järjestetty controllertoimintona. Jokaiselle tulosyksikölle on nimitetty vastuullinen controller, joka raportoi koko konsernin talous- ja rahoitusjohtajalle (CFO). Finnlinesin eri yksiköiden johtajat vastaavat yksiköiden taloudellisesta tuloksesta ja käyttöpääomasta. He asettavat johtamalleen yksikölle operatiiviset tavoitteet ja huolehtivat resurssien tehokkaasta käytöstä sekä toiminnan mittaamisesta ja kehittämisestä”.

*Finnlinesin* rahoitusriskienhallinta on järjestetty keskitetysti ja toiminnan jatkuvuuteen liittyvät ja vakuutettavat riskit on vastuutettu lakiasiainyksikölle. Riskienhallintaprosessista, riskien tunnistamisesta ja arvioinnista tai riskienhallinnan kehittämisestä ei ole mainintoja kumpanakaan vuonna. Aineiston perusteella voin todeta, että *Finnlines* on ymmärtänyt sisäisen valvonnan väärin (vrt. kohta toimintakulttuuri) eikä kerro otsikon sisäinen tarkastus ja riskienhallinta sisäisestä valvonnasta mitään. Annetun informaation mukaan näyttäisi siltä, että Finnlines ei tiedä, mitä sisäinen valvonta ja sisäinen tarkastus ovat.

Kohdeyritysten aineistossa esille tuomat riskit

Kohdeyritykset kertovat merkittävimmistä riskeistään tutkimusaineistossa. Riskejä on lueteltu vuosikertomuksen riskienhallintaa koskevassa osassa, toimintakertomuksessa ja tilinpäätöksen liitetiedoissa. Olen koonnut aineistossa esille tuodut riskit yhtiöittäin ja riskiluokittain (strategiset, operatiiviset ja taloudelliset/rahoitukseen liittyvät riskit) alla oleviin kolmeen taulukkoon. Strategiset, operatiiviset ja taloudelliset/rahoitukseen liittyvät riskit on koottu omiin erillisiin taulukoihin. Taulukoiden hymyilevät hymiöt ilmentävät, mikä kohdeyrityksistä on tuonut kunkin riskin esille. Tällä tavalla voidaan kertasilmäyksellä havaita eri kohdeyritysten esille tuomat riskit sekä tarkastella yksittäisiä riskejä. Jos kohdeyritys ei ole luokitellut riskejään strategisiin, operatiivisiin tai taloudellisiin/rahoitukseen liittyviksi, olen tehnyt tämän luokittelun itse mahdollisimman tarkoituksenmukaisella tavalla. Ainoastaan *Neste Oil* oli tehnyt tämän luokittelun itse. Riskien luokittelu on COSO ERM -mallin kannalta oleellinen, koska COSO ERM-malli lähtee liikkeelle strategisista, operatiivisista taloudellisen raportoinnin ja lainsuustavoitteista. Näihin tavoitteisiin kohdistuvat myös strategiset, operatiiviset ja taloudelliset/rahoitukseen liittyvät riskit, vaikka jaottelu ei olekaan täsmälleen sama. Taulukoiden jälkeen analysoin jokaisen riskiluokan jokaisen kohdeyrityksen kohdalta erikseen.

Taulukko 2. Kohdeyritysten esille tuomat strategiset riskit

| Strategiset riskit | Kemira | | Neste Oil | | Aspo | | Finnlines | |
|---|---|---|---|---|---|---|---|---|
| | 2007 | 2005 | 2007 | 2005 | 2007 | 2005 | 2007 | 2005 |
| Yritysostot | ☺ | | | | | | | |
| Integrointi | ☺ | | | | | | | |
| Muutokset liiketoiminta-alueilla | ☺ | | | | | | | |
| Tuotekehitys | ☺ | | | | | | | |
| Kilpailu | ☺ | | | | | | | |
| Maailman talouskasvun ja öljytuotteiden kysynnän muutokset | | | ☺ | | | | | |
| Strategian mukaisiin uusiin liiketoiminta-alueisiin ja markkinatekijöihin liittyvät riskit | | | ☺ | | | | | |
| Investointien lykkääntymiseen liittyvät riskit | | | ☺ | | | | | |
| Maineriski | | | ☺ | | | | | |
| Jakelukanavien uudelleenjärjestelyt | | | | | ☺ | ☺ | | |
| Muutokset kemianteollisuudessa ja lainsäädännössä | | | | | ☺ | ☺ | | |

Strategiset riskit

*Neste Oil* on kohdeyrityksistä ainoa, joka kertoo erikseen strategisista riskeistään. Myös muut kohdeyritykset tuovat strategisia riskejä esille, mutta eivät mainitse niiden olevan strategisia. Ne puhuvat esimerkiksi merkittävimmistä riskeistään. *Neste Oil* ei tuo esille yhtiötasoisia strategisia tavoitteitaan, mutta kertoo tarkemmin toimialakohtaisista tavoit-

teistaan. Tästä esimerkkinä aineistossa mainittu ”strategian mukaisiin uusiin liiketoiminta-alueisiin ja markkinatekijöihin liittyvät riskit”, joka ei ole tarkasti määritelty, mutta tuo esille tosiasian, että *Neste Oilin* riskejä on linkitetty strategiaan. *Neste Oil* tuo strategisena riskinä esille myös maineriskin, jota yllätykseksi muut kohdeyritykset eivät ole tuoneet esille. *Neste Oil* painii tänä päivänä kipeästi maineeseen liittyvän riskinsä realisoitumisesta Greenpeacen kampanjoidessa *Neste Oilin* palmuöljyprojektia vastaan.

*Aspo* ja *Kemira* tuovat merkittävien riskiensä joukossa esiin riskejä, jotka luokittelen strategisiksi. *Finnlinesin* esiintuomat riskit ovat kaikki taloudellisia tai lähinnä rahoitukseen liittyviä. *Kemira* nimeää vuonna 2005 tavoitteekseen muun muassa vahvan markkina-aseman rakentamisen yritysostojen- ja järjestelyjen kautta. Vaikka tätä nimenomaista tavoitetta ei enää vuonna 2007 mainitakaan, on strategisten riskien listalle noussut kaksi tavoitteeseen vaikuttavaa riskiä ”yritysostot” ja ”integrointi”. *Kemira* linkittää myös riskinsä tavoitteisiin, vaikkakin tässä hieman myöhässä. Uskoakseni vuosien 2005 ja 2006 aikana on tapahtunut jotain, josta on opittu yritysostoihin ja –järjestelyihin liittyvistä riskeistä. *Aspon* esille tuomat strategiset riskit eivät kohdistu yhtiön julkaisemiin strategisiin tavoitteisiin. Tämä johtunee strategisten tavoitteiden suppeasta esittämisestä tutkimusaineistossa, mutta mahdollisesti myös puutteellisesta tavoitteiden asettamisesta

**Taulukko 3. Kohdeyritysten esille tuomat operatiiviset riskit**

| Operatiiviset riskit | Kemira | | Neste Oil | | Aspo | | Finnlines | |
|---|---|---|---|---|---|---|---|---|
| | 2007 | 2005 | 2007 | 2005 | 2007 | 2005 | 2007 | 2005 |
| Tietoturvariskit | | | ☺ | ☺ | | | | |
| Turvallisuusriskit | | | ☺ | ☺ | | | | |
| Vahinkoriskit | | | ☺ | ☺ | | | | |
| Merikuljetusten riskit | | | ☺ | | ☺ | ☺ | | |
| Ympäristöriskit ja vastuut | ☺ | ☺ | | | | | | |
| Henkilöstö | ☺ | | | | ☺ | ☺ | | |
| Hankinnat ja ostot | ☺ | | | | | | | |
| Liiketoimintariskit | | | | | ☺ | ☺ | | |
| Asiakaspysyvyys | | | | | ☺ | ☺ | | |
| Kaluston riittävyys | | | | | ☺ | ☺ | | |
| Katetason säilyttäminen | | | | | ☺ | ☺ | | |
| Raaka-aineiden hintojen vaihtelut | | | | | ☺ | ☺ | | |
| Raaka-aineiden toimittajien välillä tapahtuvat yrityskaupat | | | | | ☺ | ☺ | | |
| Kysynnän ja kilpailuaseman epäsuotuisat muutokset | | | | | ☺ | ☺ | | |
| Luottamusaseman menetys asiakkaan silmissä | | | | | ☺ | ☺ | | |
| Työmarkkinapoliittiset ristiriidat | | | | | ☺ | ☺ | | |
| Kapasiteetin ja kuljetusten optimointi | | | | | ☺ | ☺ | | |
| Kilpailutilanteen tai asiakkaiden ostokäyttäytymisen muutokset | | | | | ☺ | ☺ | | |
| Avainasiakkuuksien menetykset | | | | | ☺ | ☺ | | |

Operatiiviset riskit

*Neste Oil* on kohdeyrityksistä ainoa, joka tuo selkeästi erikseen esille myös operatiiviset riskinsä. Ne ovat kuitenkin melko ylätasolla, eivätkä merikuljetukseen liittyviä riskejä lukuun ottamatta tuo esille *Neste Oilin* erityispiirteitä, vaan voisivat kuulua mille tahansa organisaatiolle. *Neste Oil* ei tuo esimerkiksi ympäristöriskejä esille toimialastaan huolimatta, vaikka tuo muuten ympäristönäkökulmia paljon esille. *Kemira* on kohdeyrityksistä ainut, joka tuo ympäristöriskit ja –vastuut suoraan esille. *Aspo* esittelee operatiiviset riskinsä käytännönläheisimmin ja selkeästi yhtiön omia riskiprofiilin erityispiirteitä esille tuoden, tästä esimerkkeinä kapasiteetin ja kuljetusten optimointi-riski ja luottamusaseman menetys asiakkaan silmissä-riski. Riski luottamusaseman menetyksestä asiakkaan silmissä voitaisiin ehkä luokitella myös strategiseksi sen liittyessä *Aspon* tavoitteeseen ”rakentaa kestäviä, vahvaan partneruuteen ja kumuloituneeseen erikoisosaamiseen perustuvia asiakassuhteita.”

**Taulukko 4. Kohdeyritysten esille tuomat taloudelliset ja rahoitukseen liittyvät riskit**

| Taloudelliset / rahoitusriskit | Kemira | | Neste Oil | | Aspo | | Finnlines | |
|---|---|---|---|---|---|---|---|---|
| | 2007 | 2005 | 2007 | 2005 | 2007 | 2005 | 2007 | 2005 |
| Hintariski (markkinariski) | ☺ | | ☺ | ☺ | | | ☺ | ☺ |
| Valuuttariski (markkinariski) | ☺ | ☺ | ☺ | ☺ | ☺ | ☺ | ☺ | ☺ |
| Korkoriski | ☺ | ☺ | ☺ | ☺ | ☺ | ☺ | ☺ | ☺ |
| Likviditeetti- ja jälleenrahoitusriski / Maksuvalmiusriski | ☺ | ☺ | ☺ | ☺ | ☺ | ☺ | ☺ | ☺ |
| Luotto- ja vastapuoliriski | ☺ | ☺ | ☺ | ☺ | ☺ | ☺ | ☺ | ☺ |
| Pääomarakenteen hallinta | ☺ | | ☺ | | ☺ | | ☺ | |
| Informaatioteknologia | | | | | | ☺ | | |
| Maariski | | | | | | | ☺ | |

Taloudelliset ja rahoitukseen liittyvät riskit

Kaikki kohdeyritykset esittelevät taloudelliset riskinsä melko tasavahvasti. Tähän on todennäköisesti syynä IFRS:n liitetietovaatimuksiin liittyvä lainsäädäntö. Nykyinen taloudellinen tilanne on nostanut taloudellisten ja erityisesti rahoitusriskien merkitystä. Jokainen kohdeyritys on varmasti joutunut tekemään poikkeavia toimenpiteitä rahoituksensa turvaamiseksi. Erityisesti *Finnlines* joutuu painimaan suuren velkataakan kanssa tehtyään mittavia alusinvestointeja viime vuosien aikana.

Riskien tunnistaminen on *Kemiralla* ja *Neste Oililla* systemaattista ja jatkuvaa, riskejä arvioidaan säännöllisesti ja arvioinnin kattavuuteen pyritään. Vaikka *Aspon* riskienhallintaprosessi on annetun informaation mukaan kehittymätön verrattuna *Kemiraan* ja *Neste Oiliin*, se kertoo kuitenkin arvioivansa riskejä niiden todennäköisyyden ja vaiku-

tuksen perusteella. *Aspo* on myös tuonut käytännönläheisesti esille riskejään. *Finnlinesin* kokonaisvaltainen riskienhallinta on aineiston perusteella kehittymätöntä.

Kaikki kohdeyritykset tuovat aineistossa esille taloudellisia tai rahoitukseen liittyviä riskejä. *Neste Oil* on ainut kohdeyrityksistä, joka luokittelee riskit selkeästi strategisiin, operatiivisiin ja taloudellisiin tai rahoitukseen liittyviin riskeihin. Myös *Aspo* ja *Kemira* tuovat esille strategisia tai operatiivisia riskejään, mutta jättävät luokittelun lukijan vastuulle. Aineiston perusteella voin todeta, että riskiraportoinnin taso on eri yrityksillä hyvin vaihtelevaa johtuen hyvin eri tasoisista riskienhallintaprosesseista.

Yksi COSO ERM -mallin riskienhallinnan osa-alue on ulkoisen toimintaympäristön vaikutusten arviointi toimintaan nähden. Uskon, että toimintaympäristöanalyysia on tehty kaikissa kohdeyrityksissä strategiatyön yhteydessä, mutta asian arviointi tutkimusaineiston perusteella on vaikeaa toimintaympäristötiedon hajaantuessa laajalle alueelle aineistossa. Tunnistetuista riskeistä *Aspon* riski ”muutokset kemianteollisuudessa ja lainsäädännössä” ja *Neste Oilin* riski ”maailman talouskasvun ja öljytuotteiden kysynnän muutokset” ovat esimerkkejä toimintaympäristöanalyysin avulla tunnistetuista riskeistä.

Keskeisiin hankkeisiin ja projekteihin liittyy aina merkittäviä riskejä, jotka tulisi tunnistaa. Kohdeyritykset eivät ole kuitenkaan tuoneet tutkimusaineistossa esille yhtään tällaista riskiä. Esimerkiksi *Kemiran* ja *Aspon* toiminnanohjausjärjestelmien uusimishankkeisiin liittyy varmasti merkittäviä riskejä, vaikka niitä ei ole erikseen tuotu esille.

### 5.3.2 Riskienhallintaprosessi: riskeihin vastaaminen

COSO ERM -mallin mukaan arvioidut riskit ja niille valittavat hallintakeinot suhteutetaan organisaation riskinottohalukkuuteen ja –kykyyn sekä hallintamenettelyjen kustannus/hyötyanalyysiin. Analyysin perusteella päätetään, mitä riskejä yritykset suostuvat ottamaan ja miten näitä riskejä hallitaan suhteessa riskinottohalukkuuteen ja –kykyyn. Näitä asioita arvioin riskienhallintakäytänteistä ja tunnistetuista riskeistä tutkimusaineiston perusteella.

*Kemira* kertoo, että arviointien tuloksena johdolla ja liiketoiminta-alueilla on käytössään riskikartat sekä riskilistat, joiden perusteella laaditut riskienhallintasuunnitelmat liitetään osaksi liiketoimintojen toimintasuunnitelmia. Näin *Kemira* ymmärtääkseni liittää riskienhallintasuunnitelmat osaksi johdon tekemää normaalia toiminnansuunnittelua. *Kemira* kertoo myös, että tietyt riskienhallintatoimet hoidetaan konsernissa keskitetysti. Tällaisia ovat esimerkiksi tietyt vakuutusohjelmat, kuten konsernin toiminta- ja tuotevastuuvakuutus, kuljetusvakuutus, suurimpien tehtaiden omaisuus- ja keskeytysvakuutukset sekä rahoitusriskien suojaustoimet. Tästä näkökulmasta voin todeta, että tiettyjen riskienhallintatoimien keskittämisellä *Kemira* pyrkii optimoimaan riskien vähentämisestä saadun hyödyn suhteessa hallintakeinojen kustannusvaikutuksiin.

*Neste Oil* kertoo molempina vuosina pyrkivänsä rajoittamaan riskien vaikutusta erilaisilla riskienhallintastrategioilla. Lisäksi vuonna 2007 *Neste Oil* mainitsee riskienhallintapolitiikan, jossa on esitetty riskienhallintaperiaatteita. Lisäksi *Neste Oil* tuo esille, että riskien hallintaa koskevat toimenpiteet tallennetaan riskirekisteriin. Vuoden 2007 riskienhallintastrategioita kuvaava kohta vuosikertomuksessa on seuraavanlainen:

> ”Strategioita riskienhallintaan: Neste Oil pyrkii rajoittamaan liiketoimintoihinsa kohdistuvien riskien vaikutusta erilaisilla riskienhallintastrategioilla. Yhtiön hallituksen hyväksymässä yleisessä Neste Oilin riskienhallintapolitiikassa on esitetty yhtiön, toimialojen ja toimintojen strategisia sekä operatiivisia tavoitteita uhkaavien riskien hallintaperiaatteet. Konsernin yleiset riskeihin liittyvät tiedot sekä uhkaavien riskien hallintaa koskevat toimenpiteet tallennetaan riskirekisteriin. Politiikassa on määritelty yksityiskohtaiset ohjeet muun muassa konsernia ja toimialoja koskevien strategisten riskien, operatiivisten riskien, markkinariskien, vastapuoliriskien, juridisten riskien sekä turvallisuusnäkökohtiin liittyvien riskien hallintaan. Hallitus hyväksyy myös konsernin rahoitusriskien sekä luotto- ja vastapuoliriskien hallintaperiaatteet. Toimialoilla sekä konserni- ja muilla toiminnoilla on omat riskienhallinnan käytäntönsä, periaatteensa ja menettelynsä. Ne hyväksyy yhtiön toimitusjohtaja”.

*Neste Oil* kertoo siis määrittelevänsä riskienhallintapolitiikassa periaatteet, kuinka organisaation eri tasoilla tulisi hallita strategisia tai operatiivisia tavoitteita uhkaavia

riskejä. Myös rahoitusriskien hallinnasta on olemassa hallituksen hyväksymät periaatteet. Riskienhallintaa koskevat toimenpiteet dokumentoidaan *Neste Oilissa* riskirekisteriin. *Neste Oilin* riskienhallintaa koskevissa periaatteissa uskoisin käsiteltävän seuraavia asioita: riskien priorisointi, hallintamenettelyt (riskin välttäminen, riskin pienentäminen, riskin jakaminen muille, riskin kantaminen), hallintamenettelyiden kustannus/hyöty-arvioinnit, hallintamenettelyistä päättäminen ja riskienhallintamenettelyiden dokumentointi. Näin uskallan olettaa *Neste Oilin* antaman moniulotteisen informaatiokokonaisuuden perusteella. Riskienhallintaa koskevien periaatteiden sisältöä en toki pysty tutkimaan aineistoni perusteella minkään kohdeyrityksen osalta. Hallintakeinoihin liittyvät käytänteet ovat kehittyneet selvästi vuosien 2005 ja 2007 välillä riskienhallintapolitiikan ja hallintatoimenpiteiden kehittymisen myötä.

*Aspon* riskienhallintakeinoja koskevat osuudet ovat samanlaisia molempina vuosina. *Aspo* kertoo, että ”johto vastaa riittävien toimenpiteiden määrittämisestä, toteuttamisesta sekä toimenpiteiden toteutumisen seurannasta osana normaalia toiminnan ohjausta. Tiettyjen riskien osalta riskienhallinnan periaatteet ja keskeisin sisältö on määritelty konsernitason politiikoissa ja ohjeissa.” Esimerkkinä riskienhallintakeinoista *Aspo* mainitsee pitkät asiakassopimukset ja toiminnan jatkuvan seurannan ja kehittämisen. *Aspon* käytännönläheisestä otteesta ja annetun informaation staattisuudesta ja suppeudesta johtuen oletan, että mainituissa konsernitason politiikoissa ja ohjeissa ei käydä läpi kaikkia *Neste Oilin* kohdalla hallintakeinoihin liittyen mainitsemiani asioita. *Finnlines* ei tuo tutkimusaineistossa esille mitään, minkä perusteella voisin arvioida riskeihin vastaamista.

*Kemira, Neste Oil* ja *Aspo* priorisoivat riskinsä, mikä on edellytys COSO ERM -mallin mukaiselle järkevälle riskeihin vastaamiselle. Yritysten on tärkeää kyetä keskittymään merkittävien riskien eliminointiin. Kohdeyritykset eivät suoraan mainitse riskienhallintamenettelyiden valinnasta. *Kemiran* ja *Neste Oilin* riskienhallintaa koskevissa politiikoissa, periaatteissa tai muissa mahdollisissa ohjeissa oletan kuitenkin ohjeistettavan hallintamenettelyjen valintaa (riskin välttäminen, riskin pienentäminen, riskin jakaminen muille, riskin kantaminen). Hallintamenettelyiden kustannus/hyöty-analyysista ei myöskään ole suoria mainintoja. Kaikki yhtiöt *Finnlinesiä* lukuun ottamatta kertovat

riskien hallintamenettelypäätösten olevan osa normaalia johtamista. Ongelmana tässä on kuitenkin systemaattisen riskienhallinnan menetelmien todellinen hyödyntäminen osana johtamista. *Neste Oil* on kohdeyrityksistä ainoa, joka kertoo dokumentoivansa päätetyt riskienhallintatoimenpiteet riskirekisteriinsä.

## 5.4 Valvontatoimenpiteet

COSO ERM -mallin mukaan valvontatoimenpiteet eli kontrollit ovat varmentavia tai tarkistavia menettelyitä tai välineitä, joiden avulla voidaan pienentää riskejä. Valvontatoimenpiteet voivat olla ennakoivia, joilla estetään riskin toteutuminen tai jälkikäteistoimenpiteitä, joilla pienennetään riskin toteutumisen aiheuttamia kielteisiä vaikutuksia. Valvontatoimenpiteiden tehtävänä on tuottaa kohtuullinen varmuus siitä, että organisaation tavoitteet saavutetaan halutulla tavalla. Valvontatoimenpiteet ovat siis jatkoa riskeihin vastaamiselle. Ne ovat niitä pysyviä hallintakeinoja, joiden avulla riskejä pyritään hallitsemaan. Nämä hallintakeinot arvioidaan osana riskienhallintaprosessia mietittäessä tarvittavia uusia hallintakeinoja riskiprofiilin muuttuessa. Valvontatoimenpiteet ovat määritelmällisesti enemmänkin osa sisäistä valvontaa kuin riskien hallintaa, vaikka ovatkin siihen vahvasti kytköksissä edellä mainitulla tavalla. Valvontatoimenpiteistä ei anneta paljoakaan tietoa tutkimusaineistossani eivätkä ne ole edellytys toimivalle riskienhallintaprosessille, joten rajaan niiden käsittelyn pois tutkimuksestani.

## 5.5 Informaatio ja tiedonkulku

COSO ERM -mallin mukainen toimiva tiedonkulku ylläpitää vuorovaikutus- ja raportointikanavia, joiden avulla organisaation johto, henkilöstö ja sidosryhmät saavat oikeaaikaisesti olennaista ja käyttökelpoista tietoa toimintaan vaikuttavista ja tekijöistä. Informaatio ja tiedonkulku ovat riskienhallinnan onnistumisen kannalta olennaisessa osassa. Ne ovat kiinteä osa riskienhallintaviitekehikon kaikkia osa-alueita ja vaikeasti käsiteltävissä vuosikertomus- ja tilinpäätösinformaation perusteella, joten rajaan niiden erillisen käsittelyn tutkimuksen ulkopuolelle.

## 5.6 Seuranta

COSO ERM -mallin mukaisella seurannalla toteutetaan sisäisen valvonnan ja riskienhallinnan tehokkuuden arviointia ja kehittämistä. Seurantaa voidaan toteuttaa jatkuvalla, tavanomaiseen toimintaan liittyvällä seurannalla, erillisillä määräajoin tehtävillä arvioinneilla tai näiden yhdistelmällä. Erilliset määräajoin tehtävät arvioinnit toteutetaan usein sisäisen tarkastuksen toimesta. Kohdeyritysten kohdalla tutkin seurannan osalta, tehdäänkö niissä sisäistä tarkastusta tai arvioidaanko sisäistä valvontaa ja riskienhallintaa.

*Kemira* kertoo vuonna 2005 että sisäinen tarkastus ei ole osa Kemira-konsernin riskienhallintaa, vaan erillinen toiminto, jonka vastuulla on myös konsernin riskienhallintatoiminnon ja -toimenpiteiden tarkastaminen. Vuonna 2007 *Kemira* kertoo sisäisen valvonnan ja riskienhallinnan seurannasta ja tarkastuksesta enemmän:

> ”Seuranta ja tarkastus: Sisäisen valvontajärjestelmän toimivuutta seurataan esimiesten toimesta osana operatiivista johtamista. Kemira-konsernin sisäisen tarkastuksen yksikkö vastaa konsernin riippumattomasta arviointi- ja varmistustoiminnosta, jonka keskeisenä tehtävänä on tukea Kemiran johtoa ja hallitusta niiden valvontatehtävässä. Sisäisen tarkastuksen toiminta-alue on rajoittamaton ja kattaa kaikki konsernin toimialat, yksiköt ja toiminnot. Sisäinen tarkastus raportoi havainnoistaan ja suosituksistaan Kemira Oyj:n tarkastusvaliokunnalle ja hallinnollisesti lakiasiainjohtajalle. Sisäisen tarkastuksen edustaja keskustelee tarkastussuunnitelmastaan ja havainnoistaan vuoden aikana tilintarkastajien kanssa”.

*Neste Oilin* sisäinen tarkastus on järjestetty samalla tavalla molempina vuosina. Se kertoo sisäisestä tarkastuksestaan seuraavasti:

> ”Sisäinen tarkastus: Neste Oilin sisäinen tarkastus on itsenäinen toiminto, jonka tehtävänä on tuoda lisäarvoa yhtiölle ja parantaa sen toimintoja. Sisäinen tarkastus auttaa organisaatiota arvioimaan ja parantamaan riskienhallinnan, taloudellisen valvonnan ja hallinnoinnin prosesseja. Työn perustana ovat kansainväliset sisäisen tarkastuksen ammattistandardit ja eettiset säännöt, jotka on julkaissut The Institute of Internal Auditors. Sisäinen tarkastus raportoi hallituksen tarkastusvaliokunnalle. Hallinnollisesti se rapor-

> toi toimitusjohtajalle. Sisäisellä tarkastuksella ei ole esikuntatoimintona suoraa käskyvaltaa tarkastamiensa toimintojen suhteen. Sisäisen tarkastuksen toimenkuva, valtuudet ja vastuut on virallisesti määritelty toimintaohjeessa. Toimintaohjeen ja vuotuisen toimintasuunnitelman hyväksyy hallituksen tarkastusvaliokunta".

*Aspo* kertoo sisäisestä tarkastuksestaan molempina vuosina täsmälleen samalla tavalla:

> "Sisäinen tarkastus on osa konsernin taloushallintoa. Konserniyhtiöiden controllerit ovat vastuussa lainsäädännön ja konsernin ohjeiden noudattamisesta. He raportoivat konsernin talousjohtajalle. Talousjohtaja raportoi sisäisen tarkastuksen havainnoista toimitusjohtajalle ja hallitukselle. Tarvittaessa sisäistä tarkastusta voidaan vahvistaa ostamalla ulkopuolisia palveluja".

*Finnlinesilla* otsikon "Riskien hallinta ja sisäinen tarkastus" alla kerrotaan molempina vuosina: "Hallitus huolehtii siitä, että yhtiössä on määritelty sisäisen valvonnan toimintaperiaatteet ja että yhtiössä seurataan valvonnan toimivuutta." Sisäisestä tarkastuksesta ei kerrota mitään ja muuten otsikon alla kuvataan lähinnä rahoitusriskien hallintaan liittyviä asioita.

*Kemira* on kehittänyt sisäisen valvonnan ja riskienhallinnan seurannastaan antamaa informaatiota vuodesta 2005 vuoteen 2007, jolloin se kertoo standardin mukaisen sisäisen tarkastuksen lisäksi myös johdon arvioivan sisäistä valvontaa ja riskienhallintaa osana operatiivista johtamista. Myös *Neste Oililla* on standardin mukainen sisäinen tarkastus, joka arvioi sisäistä valvontaa ja sen osana riskienhallintaa. *Aspon* sisäinen tarkastus on organisoitu osaksi taloushallintoa, mikä ei ole standardien mukaista. Sisäistä valvontaa kuitenkin arvioidaan taloushallinnon toimesta sisäistä tarkastusta muistuttavasti. Näkisin tutkimukseni perusteella, että *Finnlines* ei täysin ole ymmärtänyt sisäisen valvonnan ja sisäisen tarkastuksen merkitystä, kuten jo aikaisemmin on tullut ilmi. Se kertoo kuitenkin hallituksen vastaavan sisäisen valvonnan toimivuuden seurannasta.

Kaikilla kohdeyrityksillä on käsitys siitä, että sisäisen valvonnan ja riskienhallinnan toimivuutta tulee seurata. *Kemira* ja *Neste Oil* ovat järjestäneet sisäisen tarkastuksen toteuttaman seurannan moitteettomasti. *Neste Oil* ei kuitenkaan mainitse tavanomaiseen

toimintaan liittyvää johdon tekemää jatkuvaa seurantaa. *Aspo* ei mainitse jatkuvaa seurantaa ja on järjestänyt sisäisen tarkastuksensa standardien vastaisesti osaksi taloushallintoa. Taloushallinto kuitenkin ilmeisesti arvioi sisäisen valvonnan ja riskienhallinnan toimintaa. *Finnlinesilla* ei ole varsinaista sisäistä tarkastusta, mutta se kertoo hallituksen vastaavan sisäisen valvonnan toimivuuden seurannasta. Tehdäänkö *Finnlinesissä* seurantaa, jää arvailujen varaan.

# 6 Yhteenveto ja johtopäätökset

Tutkimuksen päätavoitteena oli verrata neljän merenkulun toimialan (Kemiraa lukuun ottamatta) pörssiyrityksen eli Kemiran, Neste Oilin, Aspon ja Finnlinesin riskiraportoinnin ja riskienhallinnan kehittyneisyyttä COSO ERM -mallin vaatimuksiin ja selvittää, täyttävätkö kohdeyritysten riskiraportointi ja riskienhallinta viitekehyksen vaatimukset. Samalla arvioitiin, kuinka kohdeyritysten riskienhallinta on kehittynyt vuodesta 2005 vuoteen 2007. Tutkimusaineisto koostui julkisesta vuosikertomus- ja tilinpäätösaineiston sisältämästä riskienhallintaa koskevasta tiedosta. Seuraavissa kappaleissa esittelen tutkimuksessa selvinneet asiat.

Yrityksellä, joka on kehittänyt ja panostanut riskienhallintaansa, on paremmat mahdollisuudet kehittyä tulevaisuudessa ja houkutella sijoittajia. Tutkimuksen yleisenä havaintona voidaan todeta, että kohdeyrityksistä kaksi suurinta yritystä eli Kemira ja Neste Oil olivat panostaneet systemaattiseen riskienhallintaansa paljon enemmän kuin pienemmät kohdeyritykset Aspo ja Finnlines. Kemiran ja Neste Oilin riskienhallinta ja siitä raportointi kehittyivät selvästi vuosien 2005 ja 2007 välillä, kun taas Aspon ja Finnlinesin riskiraportoinnissa ja riskienhallinnassa ei tapahtunut kehitystä vertailuvuosien välillä. Kemiran ja Neste Oilin riskienhallinnan voidaan todeta täyttävän COSO ERM -mallin vaatimukset merkittävimmiltä osin, joskin niidenkin riskiraportoinnissa ja riskienhallinnassa oli havaittavissa kehittämistarpeita vielä vuoden 2007 jälkeenkin. Aspon ja Finnlinesin riskienhallinta ei tutkimusaineiston perusteella täytä viitekehikon vaatimuksia. Aspon riskienhallinta tuntuu kuitenkin käytännönläheiseltä ja se on tuonut aineistossa esille eniten tunnistettuja riskejä. Finnlines ei ollut aineiston perusteella panostanut

systemaattisen riskienhallinnan kehittämiseen lainkaan. Sen riskiraportointi tuntuisi perustuvan puhtaasti IFRS:n lähinnä rahoitusriskeihin liittyviin raportointivaatimuksiin. Tutkimuksen pohjalta näkisin, että Finnlines ei ole täysin ymmärtänyt, mitä sisäinen valvonta on.

Kemiralla ja Neste Oililla on enemmän resursseja ja niiden sisäinen toimintaympäristö ja siitä annettu informaatio oli hyvin erilainen verrattuna Aspoon ja Finnlinesiin. Tämä on pääsyy myös riskienhallinnan kokonaisuuden erilaiseen tilaan Kemiralla ja Neste Oililla verrattuna Aspoon ja Finnlinesiin. Kohdeyritykset kertoivat riskinottokyvystään ja –halukkuudestaan yllättävän vähän. Nämä ovat kuitenkin ne tekijät, joiden oletan kiinnostavan sijoittajia. Yhdenkään kohdeyrityksen toimintatapa ei täysin vastannut COSO ERM -mallin vaatimuksia tältä osin. Kemira toi riskinkantokyvyn esille molempina vuosina ja Neste Oil puhui riskinottohalukkuudestaan ja riskirajoista vuonna 2007. Näkisin, että tämä on alue, jossa pörssiyritysten tulisi ja kannattaisi jatkossa kehittää raportointiaan ja osaamistaan.

Kemira oli ainoa, joka mainitsi eettiset periaatteensa. Tällä tavalla se halusi viestiä, miten se haluaa henkilöstönsä käyttäytyvän. Yhtenäiset eettiset periaatteet ovat yhä tärkeämmät toimintaympäristön laajentuessa ja kansainvälistyessä. Toinen asia, jota haluan tutkimuksen perusteella suositella pörssiyhtiöille, on yhteisiin eettisiin periaatteisiin panostaminen Kemiran esimerkkiä noudattaen. Kemira ja Neste Oil kertoivat panostaneensa molempina vuosina myös työtyytyväisyyteensä. Niiden tyytyväisyystutkimusten tulokset ilmensivät myönteistä kehitystä asioiden rakentavan käsittelyn suhteen. Riskienhallinnan kehittymiselle myönteinen ilmapiiri on tärkeä. Kemira ja Neste Oil pyrkivät myös kannustinjärjestelmien avoimuuteen, johdonmukaisuuteen ja yleiseen hyväksyttävyyteen. Aspo ja Finnlines keskittyivät johdon palkitsemisjärjestelmän esilletuomiseen. Kemira oli ainut, joka käytti riskienhallinnan kohdalla omistajuus-käsitettä, mikä on myös COSO ERM -mallin mukainen hyvä käytänne. Jos riskienhallinnan kokonaisuuden omistajuus ja vastuut on selkeästi määritelty, on riskienhallinnan kehittämisellä hyvät onnistumisedellytykset. Samoin on laita yksittäisten riskien ja hallintakeinojen omistajuuden määrittelyn kohdalla. Jokaisella kohdeyrityksillä oli selkeät perustehtävät ja niille oli määritelty selkeät visiot ja toimintastrategiat, joten niiden

riskienhallinnan ennakkoedellytykset täyttyivät tältä osin. Ilman selkeää perustehtävää ja siitä johdettuja tavoitteita ei toimintaa uhkaavia riskejä pystyisi tunnistamaan.

Kemiran ja Neste Oilin riskien tunnistaminen oli systemaattista ja jatkuvaa, riskejä arvioitiin säännöllisesti ja arvioinnin kattavuuteen pyrittiin. Neste Oil oli ainut, joka luokitteli riskit selkeästi strategisiin, operatiivisiin ja taloudellisiin tai rahoitukseen liittyviin riskeihin. Myös Aspo ja Kemira toivat esille strategisia tai operatiivisia riskejään, mutta eivät luokitelleet niitä. Kaikki kohdeyritykset toivat esille taloudellisia tai rahoitukseen liittyviä riskejä. Tutkimukseni perusteella näkisin, että pörssiyritysten olisi hyvä luokitella julkisesti raportoitavat riskit strategisiin, operatiivisiin ja taloudellisiin riskeihin.

Kemira, Neste Oil ja Aspo priorisoivat riskinsä ja pystyivät näin kohdentamaan riskienhallintamenettelyiden kehittämistoimenpiteensä merkittävimpiin riskeihin. Kukaan ei suoraan maininnut kustannus/hyöty-analyysin tekoa uusien hallintamenettelyiden käyttöönottopäätöksiä tehtäessä. Ainoastaan Neste Oil dokumentoi päätetyt riskienhallintatoimenpiteet riskirekisteriinsä. Uusista riskienhallintatoimenpiteistä päättäminen on se kohta riskienhallintaprosessia, jossa vaikutus käytäntöön on suora. On ymmärrettävää, että julkisen aineiston perusteella en päässyt pureutumaan syvälle kohdeyritysten riskienhallintatoimenpiteiden päätöksentekoon. Sain kuitenkin sen käsityksen, että uusien hallintakeinojen kustannus/hyöty-analyysit jäivät usein puutteellisiksi. Näkisin, että kaikkien pörssiyritysten olisi viisasta panostaa tälle alueelle riskinottokyky ja –halukkuus huomioiden.

Kaikilla kohdeyrityksillä oli käsitys siitä, että sisäisen valvonnan ja riskienhallinnan toimivuutta tulee seurata. Kemira ja Neste Oil olivat järjestäneet sisäisen tarkastuksen. Aspo oli järjestänyt sisäisen tarkastuksen standardien vastaisesti osaksi taloushallintoa. Sisäisen tarkastuksen järjestäminen kuvaa yrityksen suhtautumista sisäiseen valvontaan. Toimiva sisäinen tarkastus osaltaan varmistaa riskienhallinta-, valvonta- sekä johtamis- ja hallintoprosessien toimivuutta ja tehokkuutta sekä kehittämistä.

Kemiran ja Neste Oilin riskienhallinnassa oli tapahtunut selkeää kehitystä huolimatta siitä, että vuonna 2005 riskienhallinnasta annettu informaatio näyttäytyi enemmänkin toiveiden tynnyrinä kuin realistisena kuvauksena riskienhallinnan todellisesta tilasta. Vuoden 2007 informaation osalta oletan todellisuuden olevan huomattavasti lähempänä annettua informaatiota ja täyttävän COSO ERM -mallin vaatimukset hyvin. Tekemäni tutkimuksen pohjalta näkisin, että Aspon ja erityisesti Finnlinesin osalta riskienhallinnan kehittyminen on vasta alkamassa. Niiden antama riskienhallintaan liittyvä informaatio ei ollut juurikaan muuttunut vuodesta 2005 vuoteen 2007.

Vaikka Aspon kokonaisvaltainen ja systemaattinen riskienhallinta ei ole vielä kovin pitkälle kehittynyttä, Aspo toi kuitenkin käytännönläheisesti esille tunnistamiaan riskejä tutkimusaineistossa. Aspo on kohdeyrityksistä ainut, joka oli tunnistanut suoraan merenkulun toimialaan liittyviä riskejä. Aspon tunnistamat merenkulkuun liittyvät riskit olivat merikuljetusriski ja kalustoriski. Näitä merenkulkuun liittyviä riskejä pystytään analysoimaan myös pidemmälle COSO ERM -mallia hyödyntäen. Esimerkiksi merikuljetuksiin liittyvät riskit voidaan jakaa yksityiskohtaisempiin riskeihin, joista esimerkkeinä lastin vioittuminen, lastin mereen putoaminen, laivan uppoaminen, karille ajo ja ympäristökatastrofit. COSO ERM -mallin mukaisia riskienhallinnan käytänteitä hyödynnetään laajasti merenkulun toimialan organisaatioissa samalla tavalla kuin muillakin toimialoilla. Samoja käytänteitä voidaan hyödyntää myös hyvin yksityiskohtaisten toimialaan liittyvien riskien analysoinnissa ja hallinnassa. COSO ERM -malli on geneerinen eli sitä voidaan siis hyödyntää kaikissa organisaatioissa niiden toimialasta, koosta, rakenteesta tai kulttuurista riippumatta. COSO ERM -mallin käytänteitä voidaan hyödyntää myös eri riskialueiden tai toimintojen riskienhallintaa kehitettäessä tai arvioitaessa. Esimerkiksi merenkulun turvallisuusriskien hallinta organisaatiotasolla tai vaikka Itämeren tasolla voidaan analysoida COSO ERM -mallin periaatteita hyödyntäen.

Tämän tutkimuksen johtopäätösten rajoituksena on, että ne on tehty perustuen ainoastaan julkiseen informaatioon. Kuten johdannossa olen maininnut, tässä tutkimuksessa olen samanlaisessa asemassa kuin sijoitusanalyytikko, joka myös toimii julkisen informaation varassa. On mahdollista, että esimerkiksi Aspo, joka tuo käytännönläheisesti riskejä esille, mutta ei tuo esille politiikkojaan eikä systemaattisia ja kokonaisvaltaisia

riskienhallintamenettelyitään, on pidemmällä riskienhallintansa kehittämisessä kuin tutkimuksen perusteella nyt ymmärrämme. Tämän tutkimuksen tuloksista huolimatta voi olla, että sekä Aspolla että Finnlinesilla on vahvaa merenkulun riskienhallinnan käytännön osaamista, vaikka ne eivät julistakaan esimerkiksi riskienhallintapolitiikkojaan tai –käytänteitään. Varmuuden saamiseksi tästä sama tutkimus pitäisi toteuttaa perehtymällä käytänteisiin ja johtamiseen, esimerkiksi haastattelujen avulla ja johtamis- ja riskienhallintaprosessien läpikäymisellä paikanpäällä kohdeyrityksissä. Aspo kertookin riskienhallinnan olevan osa johtamisjärjestelmäänsä. Myös ja ehkä erityisesti tällaisessa tutkimuksessa COSO ERM on toimiva viitekehys.

Geneerisenä mallina COSO ERM sopii kokemukseni perusteella erittäin hyvin riskienhallinnan arviointiin ja kehittämiseen erilaisissa toimintaympäristöissä. Malli on kattava ja melko laaja. Sen laajuus ja moniulotteisuus voi kuitenkin aiheuttaa ongelmia kokonaisuuden hahmottamisen kannalta ja eri osa-alueiden erottaminen toisistaan voi olla vaikeaa. Mitä enemmän mallia hyödyntää käytännössä ja oppii ymmärtämään mallin eri osa-alueiden ja ulottuvuuksien keskinäisiä riippuvuuksia, sitä enemmän siitä saa irti. Moniulotteisuus ja laajuus ovat mallin vahvuuksia ja sitä pystyy hyödyntämään hyvin tutkimuksen viitekehikkona. Oikein ymmärrettynä malli auttaa jäsentämään laajaakin tutkimusaineistoa ja helpottaa johtopäätösten tekemistä. COSO ERM -mallin sisältämä riskienhallinnan perusprosessi on käytännönläheinen ja maalaisjärjellä ymmärrettävissä, mikä helpottaa oleellisen esiintuomista tutkimusaineistosta.

Tämän tutkimuksen perusteella erityisesti Kemiran ja Neste Oilin osalta voidaan sanoa, että riskienhallinta kehittyy ja yhtenäistyy nopeasti. Väitän, että COSO ERM -malli vaikuttaa yhtenäistymisen taustalla voimakkaasti. Esimerkkinä tästä Kemira, joka kertoo riskienhallinnasta ja sisäisestä valvonnastaan täysin yhtenäisesti viitekehikon kanssa. Toisena esimerkkinä on valtionhallinnon oma viitekehikko, joka perustuu puhtaasti COSO ERM -malliin. Yritysten ja kaikkien organisaatioiden toimintaympäristön monimutkaistuessa ja muutostahdin yhä kiihtyessä on selvää, että tulevaisuuden ennakointi on päivä päivältä vaikeampaa, mutta myös tärkeämpää. Tässä kehityksessä riskienhallinnan kehittämisen jo nyt korostunut merkitys tulee uskoakseni vain kasvamaan. Riskienhallinta on kehittynyt pitkälle erillisillä keihäänkärkialueilla, kuten rahoitus-, va-

hinko-, turvallisuus- ja tietoturvallisuusriskit. Nyt kehityksen painopiste on enemmän kokonaisvaltaisessa riskienhallinnassa, jota COSO ERM edustaa. Niin sanotut keihäänkärjet muodostuvat osaksi laajempaa kokonaisuutta ja niiden yhteydessä kehitettyjä toimintatapoja opitaan hyödyntämään laajemmin osana kokonaisuutta ja liiketoiminnan johtamista. Corporate governance–kehitys, eli hyvien hallinto- ja johtamiskäytäntöjen kehitys, joka on saanut alkunsa kansainvälisistä yritysskandaaleista, kuten kaikille tutut Enron, Worldcom ja Parmalat, on omiaan vauhdittamaan riskienhallinnan kehitystä. Omistajat ja muut sidosryhmät vaativat yrityksiltä yhä parempaa toiminnan läpinäkyvyyttä sekä väärinkäytösten ja muiden yllätysten torjuntaa. Kokonaisvaltainen ja systemaattinen riskienhallinta on yksi parhaista työkaluista tämän vaatimuksen täyttämiseksi.

Jatkotutkimusten osalta riskiraportoinnin ja sen kehittymisen tiimoilta voisi olla kiinnostavaa tutkia esimerkiksi systemaattisen riskienhallinnan kehittämistä osana operatiivista johtamista ja/tai strategiaprosessia. Monet yritykset antavat ymmärtää, että niiden riskienhallinta on osa johtamisjärjestelmää. Olisi mielenkiintoista tietää, onko se todellisuudessa niin ja miten se on järjestetty eli miten onnistuttaisiin yhdistämään johtamisen ja riskienhallinnan käytänteet onnistuneesti. Toinen mielenkiintoinen aihe tämän teeman osalta olisi riskienhallinta strategian jalkauttamisvälineenä. Riskienhallinnassa joudutaan myös kirkastamaan tavoitteet ja arvioidaan strategisten hankkeiden onnistumismahdollisuuksia.

Toinen mielenkiintoinen jatkotutkimuksen aihe olisi tutkia tunnistettujen riskien julkaisemista osana tilinpäätösinformaatiota ja liikesalaisuuden määrittelyä. Tutkielman kohdeyritykset toivat esille monenlaisia riskejä, mutta nämä esille tuodut riskit eivät kuitenkaan kattaneet yritysten koko riskiprofiilia. Voisiko tähän olla syynä se, että yritykset eivät halua kertoa ja tuoda esiin kilpailijoille omaa ymmärrystä riskeistään eli tuoko yritys silloin oman markkina- ja/tai tuotenäkemyksen liian selvästi esille? Onko riski-informaatiossa siis liikesalaisuuden piiriin kuuluvia asioita, joita ei vain yksinkertaisesti haluta kertoa? Tässä kohtaa ilmenee ristiriita, koska sijoittajan kuuluisi tietää kaikista merkittävistä ja oleellisista riskeistä. Lisäksi vaatimukset riskienhallinnasta lisääntyvät koko ajan.

# 7 LÄHDELUETTELO


Alasuutari, Pertti 2001. Laadullinen tutkimus. Gummerus Kirjapaino Oy, Jyväskylä.

Alftan, Mikko & Blumme, Nils & Heikkala, Jani & Kontula, Lisbet & Miettinen, Olli & Pakarainen, Eija & Sinersalo, Kaarina & Sjölund, Roland & Sundvik, Peter & Tarvainen, Jyri &Tikkanen, Reino & Turakainen, Olli & Urrila, Antti & Vesa, Janne 2008. Corporate Governance sisäisen valvonnan ja riskienhallinnan näkökulmasta. Edita, Helsinki. 2. uudistettu painos.

Blumme, Nils & Karhu, Päivi & Kontula, Lisbet & Laitakari, Jyri & Linna, Mika & Nordin, Jan & Sovasto, Jussi & Tarvainen, Jyri & Tikkanen, Reijo & Turakainen, Olli & Urrila, Antti & Vesa, Janne 2005. Corporate Governance sisäisen valvonnan ja riskienhallinnan näkökulmasta. Edita Prima Oy, Helsinki.

Enterprise Risk Management – Integrated Framework 2004. Committee of Sponsoring Organizations of the Treadway Commission (COSO), Permissions Editor, New Jersey.

Eriksson, Päivi & Kovalainen, Anne 2008. Qualitative Methods in Business Research. TJ International Ltd, Great Britain.

Guiding investors through rocky waters: How well do Finnish companies report on risk? Ernst & Young Transparency Survey. Ernst & Youngin julkaisusarja 4/2006, Helsinki.

Hallitustyöskentelyn opas 2004. Hallitusammattilaiset ry. Datacasa Oy, Helsinki.

Hannula, Antti & Virtanen, V. Olli 2006. Hallituksen puheenjohtajan opas. Datacasa Oy, Helsinki.

Hirvonen, Ahti & Niskakangas, Heikki & Steiner, Maj-Lis 2003. Corporate governance. Hyvä omistajaohjaus ja hallitustyöskentely. WS Bookwell Oy, Juva.

Holopainen, Atte & Koivu, Eila & Kuuluvainen, Antero & Lappalainen, Keijo & Leppiniemi Jarmo & Mikola Matti & Vehmas Keijo 2006. Sisäinen tarkastus. Tietosanoma Oy, Helsinki.

Internal Control- Integrated Framework 1992. Committee of Sponsoring Organisations of the Treadway Commission (COSO). AICPA, New York.

Koskinen, Ilpo, Alasuutari, Pertti & Peltonen, Tuomo 2005. Laadulliset menetelmät kauppatieteissä. Gummerus Kirjapaino Oy, Jyväskylä.

Kuusela, Hannu & Ollikainen, Reijo (toim.) 2005. Riskit ja riskienhallinta. Juvenes Print- Tampereen yliopistopaino Oy.

Matyjewicz, George & D´Arcancelo, James R. 2004. Beyond Sarbanes – Oxley. Internal Auditor 10, 67-72.

McNamee, David 1998. Business risk assessment. The Institute of Internal Auditors, Altamonte Springs, Florida.

Merna, Tony & Faisal, F. AL-Thani 2005. Corporate risk management: An Organizational Perspective. T.J. International Ltd, Padstow, Cornwall.

Moeller, Robert R. 2007. COSO Enterprise Risk Management. Understanding the New Integrated ERM Framework. John Wiley & Sons, Inc., Hoboken, New Jersey.

Monahan, Gregory 2008. Enterprise Risk Management. A Methodology for Achieving Strategic Objectives. John Wiley & Sons, Inc., Hoboken, New Jersey.

Mäkelä, Klaus 1990. Kvalitatiivisen analyysin arviointiperusteet. Teoksessa Kvalitatiivisen aineiston analyysi ja tulkinta, toim. Klaus Mäkelä. Painokaari Oy, Helsinki. 42-61.

Poole, Veronica & Spooner, Andrew 2007. iGaap 2007. Financial instruments: IAS 32, IAS 39 and IFRS 7 explained. Deloitte & Touche LLP & Wolters Kluwer (UK) Limited, London.

Ratliff, Richard L. & Wallace, Wanda A. & Sumners, Glenn E. & McFarland, William G. & Loebbecke, James. K. 1996. Internal Auditing. Principles and Techniques. Second Edition. The Institute of Internal Auditors, Florida.

Risk management AS/NZS 4360 1999. Standards Association of Australia, Strathfield.

Roth, James, Espersen, Donald & Swanson, Daniel 2007. Four Approaches for Enterprise Risk Management. The Institute of Internal Auditors Research Foundation, IIARF, USA.

Silverman, David 2006. Interpreting Qualitative Data. The Aiden Press, Oxford.

Sisäiset tarkastajat ry 2007. Sisäisen tarkastuksen kansainvälinen ammatillinen ohjeistus. Ammattistandardit, eettiset säännöt, käytännön ohjeet. Saarijärven Offset Oy.

Suominen, Arto 2003. Riskienhallinta. 3. uudistettu painos. WSOY - Dark Oy, Vantaa.

Suositus listayhtiöiden hallinnointi – ja ohjausjärjestelmistä 2003. Corporate Governance –työryhmä, Helsinki.

Vaughan, J. Emmett 1997. Risk management. John Wiley & Sons, Inc. United States of America.

**Verkkolähteet:**

Corporate Governance Finland
www.cgfinland.fi, 7.1.2009.

OECD Principles of Corporate Governance 2004
http://www.oecd.org/document/49/0,3343,en_2649_34813_31530865_1_1_1_1,00.html , 12.1.2009.

ECIIA European Confederation of Institutes of Internal Auditing
http://www.eciia.org/publications/eciia-positions/internal-auditing-in-europe.html, 12.1. 2009.

Ernst & Young
http://www.ey.com/global/content.nsf/International/AABS_Strategic_Business_Risk_Report, 18.3.2009.

IIA The Institute of Internal Auditors
http://www.theiia.org/research, 21.4.2009

Kirjanpitolautakunta
http://ktm.elinar.fi/ktm/fin/kirjanpi.nsf/all/F656564842BC1755C22571ED0047A0B1?openDocument, 9.4.2009.

Marsh
www.marsh.ro/download/rm_forum_aw.pdf, 18.3.2009.

PK-yrityksen riskienhallinta. Riskilajit.
http://www.pk-rh.fi/riskilajit, 20.1.2009.

RATA Rahoitustarkastus
http://www.rata.bof.fi/Fin/Saantely/Maarayskokoelma/Voimassa_olevat_standardit_maaraykset_ja_ohjeet/etusivu.htm, 28.1.2009.

Valtiovarainministeriö
Sisäisen valvonnan ja riskienhallinnan arviointikehikko. Ehdotus suositukseksi valtionhallinnon hyväksi käytännöksi.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/08_muut_julkaisut/20051223Valtio/name.jsp, 9.4.2009.

**Tutkimusaineisto:**

Kemira Oyj vuosikertomus ja tilinpäätös 2005 ja 2007

Neste Oil Oyj vuosikertomus ja tilinpäätös 2005 ja 2007

Aspo Oyj vuosikertomus ja tilinpäätös 2005 ja 2007

Finnlines Oyj vuosikertomus ja tilinpäätös 2005 ja 2007