TAMPEREEN YLIOPISTO
Johtamiskorkeakoulu

RISKIENHALLINTAPROSESSI PIENISSÄ JA KESKISUURISSA YRITYKSISSÄ JA VALVONTAYMPÄRISTÖN MERKITYS RISKIENHALLINNAN TOTEUTTAMISESSA

Tilintarkastuksen ja arvioinnin

maisteriohjelma

Pro gradu -tutkielma

Tammikuu 2014

Ohjaaja: Lasse Oulasvirta

Annika Suokas

Tiivistelmä

Tampereen yliopisto: Johtamiskorkeakoulu, finanssihallinto ja julkisyhteisöjen laskentatoimi

Tekijä: SUOKAS, ANNIKA

Tutkielman nimi: Riskienhallintaprosessi pienissä ja keskisuurissa yrityksissä ja valvontaympäristön merkitys riskienhallinnan toteuttamisessa

Pro gradu -tutkielma: 79 sivua, 2 liitesivua

Aika: tammikuu 2014

Avainsanat: Sisäinen valvonta ja tarkastus, riskienhallinta, valvontaympäristö, pieni ja keskisuuri yritys, COSO-viitekehikko

---

Tässä tutkielmassa selvitetään pienten ja keskisuurten yritysten riskienhallintaa, riskienhallintaprosessia, valvontaympäristöä ja valvontaympäristön merkitystä riskienhallinnan toteuttamisen kannalta. Työn tarkoitus on selvittää, millaista riskienhallintaa pk-yrityksissä kannattaa toteuttaa ja soveltuvatko COSO-viitekehikot pk-yritysten riskienhallinnan toteuttamiseen. Tutkielmassa pyritään saavuttamaan kokonaiskuva riskienhallinnasta ja valvontaympäristöstä erilaisten riskienhallintaprosessien lähestymisen avulla. Tutkimus on kvalitatiivinen ja pohjautuu pääasiassa aiheesta löytyvään kirjallisuuteen ja tutkimuksiin. Kvalitatiivista tutkimusta täydentää pienimuotoinen haastattelututkimus valitsemilleni kahdeksalle pk-yritykselle.

Riskienhallinta on tärkeä osa yrityksen liiketoimintaa ja sisäistä valvontaa. Riskienhallinnan tarkoitus on auttaa yritystä sen tavoitteiden saavuttamisessa, tunnistamalla, arvioimalla ja hallitsemalla yritystä uhkaavia riskejä ja muita epävarmuuksia. Valvontaympäristö muodostuu ennen kaikkea yrityksen johtamistavasta ja valvontakulttuurista ja on siten koko riskienhallintaprosessin lähtökohta. Riskienhallinnan arviointiperusteena on käytetty muun muassa sisäisen valvonnan perusmääritelmää ja mallia COSO-IC-viitekehikkoa sekä perusteellisemmin riskienhallintaan pohjautuvaa COSO-ERM-viitekehikkoa.

Tutkielmassa todetaan, että pienissä ja keskisuurissa yrityksissä riskienhallintaa ei kannata irrottaa omaksi kokonaisuudekseen, vaan riskienhallintaa tulisi toteuttaa osana yrityksen päivittäistä johtamista. Riskienhallinta tulisi integroida osaksi pk-yrityksen strategiaa, filosofiaa ja johtamista. COSO-ERM-viitekehikon soveltaminen on pk-yrityksissä mahdollista, mutta ei välttämättä kannattavaa.

Haastateltavissa yrityksissä riskienhallintaa toteutetaan ensisijaisesti vakuuttamisen avulla. Haastateltavat yritykset eivät tunnistaneet COSO-viitekehikkoja, mutta pitivät COSO-mallien osa-alueita käytännönläheisinä ja sovellettavissa olevina. Yrityksen valvontaympäristö koostuu riskienhallintafilosofiasta, riskinottohalukkuudesta, johdon asenteista, rehellisyydestä, eettisistä arvoista, pätevyyteen sitoutumisesta, organisaatiorakenteesta, vastuiden ja velvollisuuksien jakamisesta ja

henkilöstöhallinnon menettelytavoista. Valvontaympäristön asenteet ja johtamiskulttuuri vaikuttavat riskienhallintaprosessin laajuuteen, riskienhallinnan toteuttamiseen sekä siihen miten yritys suhtautuu riskienhallintaan.

SISÄLLYS

Kuviot:

1 JOHDANTO

1.1 Aihealueen esittely ja merkitys

Sisäisen valvonnan ja riskienhallinnan merkitys on kasvanut yritystoiminnassa, koska talouden epävarmuus, toiminnan muutokset ja kansainvälistyminen luovat paineita nykyajan yrityksille. Teknologisen kehityksen myötä liiketoiminta kohtaa nykyään sellaisia uusia riskejä, joita ei edes aikaisemmin tunnettu. Alati jatkuva tietotekniikan kehitys, lain vaatimusten muutokset, ympäristön epävarmuus ja katastrofit ovat tuoneet nämä riskit osaksi liiketoimintaa. (Vaughn 1997, 6; Crouhy, Galai & Mark 2001) Yritysten kohtaamat riskit ovat siis muuttuneet etenkin kansainvälistymisen ja atk-teknologian kehityksen myötä.

Kaikkeen yritystoimintaan liittyy siis huomattavan paljon mahdollisia uhkia ja tulevaisuuteen kohdistuvaa epävarmuutta. Arkisessa yritystoiminnassa on paljon riskejä, joiden kanssa on vain opeteltava elämään. Yritykset eivät voi olla huomioimatta niitä uhkaavia vaaratekijöitä, jotka asettavat yrityksen toiminnan vaakalaudalle. Suomessakin on paljon yrityksiä, jotka hyvästä liikeideasta huolimatta eivät ole pystyneet jatkamaan toimintaansa, vaan ovat sen sijaan ajautuneet konkurssiin tai saneerausratkaisuun. Yrityksessä tai sen ympäristössä on sattunut jotain sellaista, minkä olemassaolosta yrityksen johdolla on saattanut olla vain vähän tietoa. (Suominen 2003, 7)

Riskienhallintaa voidaan pitää ensinnäkin johtamisen perustehtävänä ja osana tehokasta sisäistä valvontaa. Riskienhallinta on itse asiassa jatkuva prosessi, johon osallistuu koko organisaation henkilöstö. Riskienhallinnan tarkoitus on vähentää epävarmuuksia, mutta myös auttaa organisaatiota sen tavoitteiden saavuttamisessa tehokkaasti ja organisaation ensisijaista tehtävää kunnioittaen. (Holopainen ym. 2006, 34; Williams, Smith & Young 1998, 53)

Koska yritykset kohtaavat nykyään lukuisia riskejä ja tarvitsevat apua tehdäkseen järkeviä päätöksiä, tarvitaan tehokas riskienhallintaprosessi. Moni yritys vain tunnistaa riskit ja luokittelee ne joko korkeiksi, keskitasoisiksi tai mataliksi, kun taas toiset yritykset käyttävät apunaan monimutkaisia kvalitatiivisia tai kvantitatiivisia analyyseja

ymmärtääkseen ja arvioidakseen riskejä. (Moeller 2007, 21–22) Tehokkaasti ja tarkoituksenmukaisesti järjestetty riskienhallinta voi olla yritysten välisessä kilpailutilanteessa jopa kilpailuvaltti.

Suomessa pienillä ja keskisuurilla yrityksillä on taloudessa merkittävä rooli. Suurin osa yrityksistämme on pk-yrityksiä, vaikka muutamat suuryritykset saavatkin usein näkyvyyttä tiedotusvälineissä ja mediassa. Pk-yritykset muodostavat väistämättä talouselämämme perustan. (Elinkeinoelämän keskusliitto EK, 2013) Koska pk-yrityksillä on vahva asema niin Suomessa kuin myös koko Euroopassa, on mielestäni mielekkäämpää tutkia riskienhallintaa ja riskienhallintaprosesseja nimenomaan pienissä ja keskisuurissa yrityksissä.

Yrityksen sisäinen valvonta ja riskienhallinta osana yrityksen sisäistä valvontaa ovat yleensä myös erilaista pörssiyhtiöissä kuin taas esimerkiksi pk-yrityksissä ja perheyrityksissä. Perheyrityksessä tai muussa pienessä organisaatiossa omistajan roolin, toiminnan ja päätöksenteon suhteen on huomattavia eroavaisuuksia verraten suurempiin organisaatioihin. Pienissä yrityksissä omistaja on yleensä liikkeellepaneva voima ja omistaja toimii yrityksen johtotehtävissä. (Holopainen ym. 2010)

Monilla pienillä yrityksillä ei välttämättä ole monipuolisia ja täydellisiä riskienhallintaprosesseja, koska yrityksellä ei ole yksinkertaisesti aikaa, eikä sillä ole myöskään tarpeellista tietoa riskienhallinnan toteuttamiseksi. Riskienhallinta voi olla lähes olematonta ja yksinkertaista, esimerkiksi mikroyrityksissä. Vaikka pk-yritykset olisivatkin tietoisia riskienhallinnasta ja sen teorioista, voi näiden yritysten johtoa mietityttää riskienhallinnasta ja sisäisestä valvonnasta aiheutuvat kustannukset. Monet pk-yritykset eivät varmasti ole myöskään edes kuulleet sisäisen valvonnan ja riskienhallinnan teorioista, mutta saattavat kuitenkin soveltaa niitä tiedostamattaan. Yritysten johto voikin toiminnassaan tunnistaa ja arvioida riskejä päivittäin.

Pk-yrityksissä tulisi kuitenkin kiinnittää huomiota sisäiseen valvontaan ja riskienhallintaan, koska väärinkäytöksiä esiintyy paljon niissä organisaatioissa, joissa sisäinen valvonta ja sen toiminnot on tehottomasti järjestetty. Tehokas sisäinen valvontajärjestelmä sen sijaan auttaa eettisten toimintatapojen järjestämisessä ja pienentää siten myös virheiden sattumisen mahdollisuutta. (Ahokas 2012, 22–23)

Riskienhallinnan ja valvonnan arviointiperusteena on usein käytetty ja tullaan mitä luultavimmin käyttämään myös jatkossa organisaatioiden kokonaisvaltaisen valvonnan ja riskienhallintajärjestelmän COSO-ERM-viitekehikkoa. Kehikko on julkaistu vuonna 2004, ja Suomessa se on otettu käyttöön muun muassa valtionhallinnossa. On kuitenkin muistettava, että riskienhallinta ja sen toteuttaminen ovat aina organisaatiokohtaisia ratkaisuja. (Holopainen ym. 2006, 35) Yrityksen riskienhallintaan ja sen prosesseihin vaikuttavat ennen kaikkea johdon asenteet, johtamistapa ja valvontakulttuuri, eettiset arvot ja johdon periaatteet ja toimintatavat. Pohjimmiltaan onkin kyse siitä, millainen suhtautuminen yrityksellä ja sen johdolla on riskienhallintaan ja riskienhallintaprosessiin.

1.2 Tutkimusongelma, keskeiset rajaukset ja tavoitteet

Tutkimuksen tarkoitus on kuvata pienen ja keskisuuren yrityksen riskienhallintaa ja valvontaympäristön merkitystä riskienhallinnan toteuttamisessa. Tutkimus syventää kandidaatin tutkielmaani ja paneutuu aiheeseen entistä laajemmin ja syvällisemmin. Elinkeinoelämän keskusliiton www-sivujen mukaan (15.7.2013) pieniä ja keskisuuria yrityksiä ovat ne, joiden palveluksessa on enintään 250 työntekijää. Määritelmän mukaan mittarina käytetään taseen loppusummaa tai liikevaihdon määrää yhdessä henkilömäärän kanssa. Liikevaihdon on oltava alle 50 miljoonaa tai taseen loppusumman alle 43 miljoonaa euroa. Suomessa käytössä on ollut myös 50 työntekijän raja, koska valtaosassa maamme yrityksistä työskentelee alle 50 työntekijää. Yllä mainittujen ehtojen lisäksi yrityksen on oltava riippumaton. Kaikkien kolmen kriteerin eli henkilömäärän, liikevaihdon määrän tai taseen loppusumman sekä riippumattomuuden on oltava voimassa yhtä aikaa. Tämän lisäksi pk-yritykset voidaan luokitella mikroyrityksiin, pieniin yrityksiin tai keskisuuriin yrityksiin. (Elinkeinoelämän keskusliitto EK, 2013)

Tutkimusongelma rajautuu seuraaviin kysymyksiin.

Tutkimuskysymykset:

Millaista riskienhallintaa pk-yrityksissä kannattaa toteuttaa?

Onko COSO-ERM-viitekehikon tai COSO-IC-viitekehikon soveltaminen pk-yrityksissä mahdollista?

Millaista riskienhallintaa haastateltavissa pk-yrityksissä toteutetaan?

Tunnistavatko haastateltavat yritykset COSO-viitekehikot ja soveltavatko ne malleja tietämättään?

Mikä merkitys valvontaympäristöllä on yrityksen riskienhallinnassa ja sen toteuttamisessa?

Tarkastelen tutkimusongelmia muun muassa COSO-IC-viitekehikon, COSO-ERM-viitekehikon, kirjallisuuden, osakeyhtiölain ja muun lainsäädännön avulla. Valvontaympäristö sisältää hallituksen ja muun johdon asenteet ja toimenpiteet koskien valvonnan tärkeyttä organisaatiossa. Valvontaympäristö luo myös puitteen sisäisen valvontajärjestelmän ensisijaisten tavoitteiden saavuttamiselle. (Holopainen ym. 2006, 41) Lyhyesti voisikin sanoa, että valvontaympäristössä on kyse johtamistavasta ja valvontakulttuurista. Valvontaympäristö on tiiviisti yhteydessä hyvään johtamis- ja hallintotapaan. Tarkastelenkin tutkimuksessa myös osakeyhtiölain ja muiden ohjeiden asettamia vaatimuksia yrityksen toiminnalle, koska ne antavat ne puitteen, joiden mukaan valvontaympäristössä tulisi toimi.

Tarkoitukseni ei ole kuvailla laajasti COSO-malleja, vaan rajaan tutkimuksen pienten ja keskisuurten riskienhallintaan ja valvontaympäristöön. Tutkielman tarkoitus on saavuttaa kokonaiskuva yrityksen riskienhallinnasta ja valvontaympäristöstä. Tutkielmassa pääpaino on *riskienhallinnassa*. Tutkielma alkaa johdannolla, jota seuraa teoreettinen viitekehys. Tutkielma integroituu laajasti teoriaan, joten teorian osuus on tutkimuksessa laaja. Kolmannessa luvussa selvitän yleisesti riskienhallintaa ja pk-yritysten riskienhallintaa. Kolmannessa luvussa esittelen myös riskienhallinnan erilaisia prosesseja, joiden tarkoitus on selventää erilaisia riskienhallinnan käytettyjä malleja ja niiden soveltuvuutta myös pk-yrityksiin.

Neljännessä pääluvussa tarkastelen valvontaympäristöä, johtamistapaa ja valvontakulttuuria sekä lainsäädännön asettamia rajoituksia ja velvoitteita yritysten johdolle. Viidennessä kappaleessa esittelen yritykset, joita olen haastattelut ja saadut tutkimustulokset. Viimeinen kappale käsittelee tutkimuksen keskeisiä johtopäätöksiä ja yhdistää haastatteluiden tulokset ja muut johtopäätökseni yhtenäisiksi keskeisiksi päätelmiksi.

1.3 Tutkimusmenetelmät

Teen teoreettisen ja kvalitatiivisen, eli laadullisen tutkimuksen, jossa lähteinä käytän pääasiassa aiheesta löytyvää kirjallisuutta. Muita lähteitä ovat muun muassa artikkelit, erilaiset sähköiset julkaisut ja ajantasainen lainsäädäntö. Tutkimus on laadullista ja kuvailevaa. Määrittelen myös keskeisimmät käsitteet, joten tutkielma sisältää myös käsiteanalyysia. Pyrin tutkimuksen aikana tekemään päätelmiä ja johtopäätöksiä aikaisemman kirjallisuuden ja tutkimusten pohjalta. Teen laadullisen ja kirjallisuuteen pohjautuvan tutkimuksen, koska mielestäni kirjallisuusaineisto soveltuu tutkimusmateriaaliksi tässä tutkielmassa. Metsämuurosen (2006) mukaan tutkimusaineiston keruussa ja analysoinnissa on otettava ensisijaisesti huomioon tutkimusmateriaalin soveltuminen tutkimukseen.

Aion tehdä myös *teemahaastatteluja* valitsemilleni noin 5-10 pienyritykselle. Olen yhdessä työantajani kanssa sopinut, että valitsemme yhdessä sopivat ja mielenkiintoiset yritykset haastatteluita varten. Työskentelen tilitoimistossa, joten valitsen haastateltavat yritykset asiakkaistamme. Haastatteluiden tarkoituksena on selvittää, millaista riskienhallintaa näissä yrityksissä toteutetaan ja soveltavatko ne COSO-viitekehikkoja riskienhallinnan prosessissaan tai niiden osatekijöitä ja missä määrin. Haastatteluiden kysymykset tulevat liittymään myös valvontaympäristöön ja sen merkitykseen yritysten riskienhallinnan toteutumisessa. Haastatteluiden tarkoitus on tukea muuta aineistoa ja siitä tehtyjä päätelmiä. Kyseessä on siis pienimuotoinen haastattelututkimus. Haastateltavat yritykset valitaan eri toimialoilta, koska tutkielman tarkoitus ei ole tutkia riskienhallintaa toimialakohtaisesti. Haastateltavat yritykset koostuvat mikro- ja pienyrityksistä.

Kvalitatiivisessa tutkimuksessa lähtökohtana on todellisen elämän kuvaaminen, ja tutkimuksessa pyritään tutkimaan kohdetta mahdollisimman kokonaisvaltaisesti. Nykyisin termi laadullinen sisältää useita merkityksiä, ja myös kvalitatiivisen tutkimuksen lajeja on lukuisia. Kvalitatiiviselle tutkimukselle on ominaista muun muassa induktiivinen analyysi, jonka tarkoitus on paljastaa odottamattomia seikkoja. Lähtökohtana onkin aineiston monitahoinen ja yksityiskohtainen tarkastelu. Tutkimuksen perusperiaate on myös tutkijan kriittinen suhtautuminen kirjallisuuteen ja muuhun lähdeaineistoon. (Metsämuuronen 2006)

Tutkimuksessa käytetään myös laadullisia metodeja aineiston hankinnassa. Lisäksi laadullisessa tutkimuksessa tutkimussuunnitelma muotoutuu usein vasta tutkimuksen edetessä. Tutkimus toteutetaan joustavasti ja suunnitelmia voidaan muuttaa työn edetessä. (Hirsjärvi, Remes & Sajavaara 2009, 161–164)

Kvalitatiivista eli laadullista tutkimustyötä voidaan pitää siis pitkäkestoisena tutkimuksena ja jatkumona. Tutkielmani onkin pitkäkestoinen tutkimusprosessi ja tutkimusongelma saattaa tarkentua ja täsmentyä prosessin edetessä ja vaiheittain. (Alasuutari, 1995) Ensisijainen tarkoitukseni on kuitenkin saada kokonaisvaltainen ymmärrys tutkimusongelmasta ja hahmottaa näiden ongelmien välisiä suhteita. Tarkoitukseni ei siis ole vain selittää tai kuvailla tutkimustuloksia ja ongelmia. (Eskola & Suoranta 1998)

1.4 Käsitys tuloksista

Työssä tullaan selvittämään, mitä riskienhallinta on, millaisia riskienhallintaprosesseja on ja millaista riskienhallintaa pk-yrityksissä kannattaa toteuttaa. Arvioni on, että pienissä ja keskisuurissa yrityksissä riskienhallinta voi olla joustavampaa ja käytännönläheisempää kuin suuryrityksissä. Pienissä ja keskisuurissa yrityksissä on kuitenkin mahdollista soveltaa riskienhallinnan teorioita, kuten ERM-viitekehikkoa. Moni pieni tai keskisuuri yritys saattaakin soveltaa riskien arvioimisessa tietämättään jompaakumpaa näistä riskienhallinnan viitekehikoista. Työssä selviää myös se, millaisista osa-alueista yrityksen valvontaympäristö muodostuu ja mikä valvontaympäristön merkitys on toimivan riskienhallintaprosessin kannalta, ja miten tärkeäksi yritykset kokevat valvontaympäristön.

Arvioni on, että haastattelemissani yrityksissä ei sovelleta sisäisen valvonnan ja riskienhallinnan teorioita. Riskienhallinta on varmasti näissä yrityksissä minimaalista ja olematonta. Uskon, että yritykset ovat kuitenkin kiinnostuneita riskienhallinnasta ja sen tuottamista hyödyistä, mutta eivät kuitenkaan ole kehittäneet itselleen toimivaa ja käytettävää riskienhallinnan mallia. Arvioin, että näiden yritysten riskienhallinta, sen suunnittelu ja toteuttaminen on alkutekijöissään.

2 TEOREETTINEN VIITEKEHYS

2.1 Sisäinen valvonta ja riskienhallinta

Sisäinen valvonta voidaan määritellä prosessiksi, jonka ensisijaisesti saavat aikaan organisaation ihmiset eli yleensä esimerkiksi hallitus, toimiva johto ja muu henkilöstö. Sisäisen valvonnan tarkoitus on auttaa organisaatiota sen tavoitteiden saavuttamisessa, mutta myös sen varmistamisessa, että organisaatiossa tiedetään mahdollisista uhista, menestykseen liittyvistä puutteista mutta myös menestymisestä. (Holopainen ym. 2010, 51–52)

Sisäisen valvonnan tavoitteet on määritelty COSO-raportissa ja ne voidaan luokitella toiminnan tarkoituksenmukaisuuteen, tehokkuuteen, taloudellisen raportoinnin luotettavuuteen ja lakien, sääntöjen mukaiseen toimintaan. Tämä COSO-raportin mukainen luokittelu koostuu siis kolmesta keskeisestä tavoitteesta. (Moeller 2007, 4-5) Sisäisen valvonnan tehtävä on siis auttaa organisaatiota toimimaan sääntöjen, lakien ja muiden ohjeiden mukaisesti. Samalla se auttaa yritystä toimimaan kuitenkin myös tehokkaasti, kannattavasti ja sen etua edistävällä tavalla. Valvonnan tehtävänä ei siis ole vain lakisääteisten arvojen noudattamisen edistäminen vaan myös koko yrityksen edun ja toiminnan parantaminen.

(Holopaisen ym. 2010, 52) mukaan sisäisessä valvonnassa ei ole myöskään vain kyse ohjeiden noudattamisesta vaan koko organisaation valvonnan tilasta ja siitä miten ihmiset siihen suhtautuvat. Holopaisen 2010, 52–53 mukaan sisäinen valvonta syntyy kokonaisuudessaan siitä, miten organisaatio toimii ja ajattelee. Tämä johtuu siitä, että organisaatiossa vallitsee organisaation itsensä synnyttämä kulttuuri, eettinen toiminta ja ajattelutavat. Yrityksen sisäisessä valvonnassa keskeistä onkin siis se, millainen valvontakulttuuri ja ajattelutapa yhteisöön on muodostunut.

(Ahokaan 2012, 11–12) mukaan sisäiselle valvonnalle ei ole yksiselitteistä määritelmää, vaan kyse on organisaation sisällä rakennetuista toimenpiteistä ja tavoista, joiden avulla pyritään varmistamaan toiminnan tavoitteellisuus ja toimintaohjeiden mukainen toiminta, toiminnan tuloksellisuus ja laillisuus. Ahokkaan mukaan organisaation

sisäinen valvonta onkin aina erilainen riippuen muun muassa yrityksen koosta, omistussuhteista, toimialasta ja siitä miten yritys toimii.

Committee of Sponsoring Organizations of The Tradaway Comissionin julkaiseman COSO-raportin (1992, 3-5) mukaan sisäinen valvonta merkitsee tilanteesta riippuen eri asioita, mutta keskeistä siinä valvonnan onnistumisen kannalta on yhteisen päämäärän löytäminen. Organisaatiolla on tavoitteita, jotka se pyrkii saavuttamaan ja niiden avulla organisaatio pystyy tyydyttämään myös tarpeensa. COSO-raportti esittää sisäisen valvonnan keskeisiksi tavoitteiksi lainmukaisuuden, tiedon luotettavuuden ja toiminnan tehokkuuden. Raportin mukaan sisäinen valvonta luo yhteisöön standardin, jonka mukaan toimitaan. Tämän avulla yritys voi arvioida omaa toimintaansa ja valvontaprosessejaan.

Riskienhallinta voidaan nähdä tärkeänä osana yrityksen toimintaa ja laatujohtamista. Riskienhallintaprosessin avulla on mahdollista saavuttaa uusia mahdollisuuksia, mutta välttää myös epämiellyttäviä yllätyksiä. Riskienhallinta parantaa myös suunnittelua, yrityksen toimintaa ja tehokkuutta. Riskienhallinnalla on myös tärkeä rooli yrityksen taloudellisen tilanteen parantamisessa ja kustannustehokkuudessa. Monipuolisen riskienhallinnan avulla yritys ylläpitää monipuolisia suhteita sijoittajiin, työntekijöihin ja johtoportaaseen. Riskienhallinta auttaa myös oikea-aikaisessa ja riittävässä tiedonkulussa eri yksikköjen, toimielinten ja osastojen kesken. Kaiken lisäksi riskienhallinta parantaa yrityksen läpinäkyvyyttä, luotettavuutta ja edesauttaa henkilöstön hyvinvointia. (Standards Australia / Standards New Zealand 2004,7-9)

Nykyään yritykset kohtaavat monilla yrityksen toiminnan osa-alueilla riskejä, jotka liittyvät informaatiotekniikan kehitykseen, liiketoimintaan ja kaupankäyntiin. Ilman toimivaa riskienhallintaa, yritys kohtaa monet näistä riskeistä. Riskienhallinta voidaan nähdä prosessina, joka kattaa koko organisaation ja jokaisen sen toiminnon. Riskienhallinta tulisikin liittää yrityksen operatiivisiin ja strategisiin toimintoihin. Yrityksiä koskevat säännökset, kuten corporate governce suosittelevat, että riskienhallinta olisi osa yrityksen kulttuuria ja visiota. Yrityksellä saattaa olla oma sisäisen tarkastuksen yksikkönsä, joka huolehtii riskienhallinnan järjestämisestä, mutta on olemassa myös muita tapoja järjestää riskienhallintaprosessi. Riskienhallinta on tärkeää, koska nykyään yrityksien tulee olla moderneja, dynaamisia, valmiita

muutokseen ja koko ajan tietoisia mahdollisista muutoksista. (CIPFA 2001, 2-3; Crouhy, Galai & Mark, 2001)

Tehokas ja toimiva sisäinen valvonta ja riskienhallinta kuuluvat väistämättä riskienhallinnasta tietoisten yritysten toimintaprosesseihin. Sisäiselle valvonnalle ja riskienhallinnalle on kuitenkin esitetty myös kritiikkiä ja rajoitteita. Raudanojan & Johanssonin (2009) mukaan sisäisen valvonnan ja riskienhallinnan tulee ensisijaisesti kohdistua tarkoituksenmukaisiin tarkastuskohteisiin. Heidän mukaansa liikavalvonta yhteisössä ei tuota yhteisölle hyötyjä ja lisäarvoa. Tämän lisäksi Maijoor (2000) on kritisoinut riskienhallinnan ja sisäisen valvonnan tavoitteita. Hänen mukaansa sisäinen valvonnan tavoitteet ovat sovellettavissa koko organisaation toimintaan kaikilla osa-alueilla, mikä tekee sisäisen valvonnan määrittelystä turhaa. Sisäisen valvonnan tavoitteet liittyvät järjestelmään, jonka ensisijaisina tavoitteina on auttaa organisaatiota sen tavoitteiden saavuttamisessa. Maijoorin (2000) mukaan nämä tavoitteet voidaan liittää kaikkiin organisaatioin toimintoihin. Tällöin sisäinen valvonta olisi osa koko organisaation toimintaa, eikä sitä voisi mitenkään erotella. Maijoorin (2000) kritiikki sisäistä valvontaa kohtaan perustuu siis sisäisen valvonnan määrittelyyn. Mielestäni COSO-mallien ja sisäisen valvonnan pohjimmainen ajatus on kuitenkin liittää sisäinen valvonta osaksi organisaation kaikkia toimintoja.

2.2 COSO-viitekehikon historia

Sisäistä valvontaa on yritetty määritellä Yhdysvalloissa jo 1940- luvulta lähtien, mutta viranomaiset ryhtyivät vaatimaan yritysten sisäiseltä valvonnalta todellisia tuloksia vasta 1970-luvulla. Vuonna 1985 perustettiin The Treadway Commission, jonka tehtävänä oli selvittää mikä organisaatioissa johtaa vilpilliseen talouden raportointiin, ja antaa suositukset niistä toimenpiteistä, joilla vilpillistä toimintaa vähennetään. Taustalla olivat myös lisääntyneet tilivelvollisuuden, sisäisen valvonnan ja avoimuuden vaatimukset koskien yhtiöiden raportointia ja toimintaa. Komitea teki yhteistyötä tarkastus- ja valvontajärjestöjen kanssa (IIA, FEI, AICPA), ja yhteistyön siivittämänä lopulta syntyi Committee of Sponsoring Organizations of The Treadway Commission(COSO), joka julkaisi COSO- raportin ensimmäisen kerran vuonna 1992. (Holopainen ym. 2006, 43) COSO Internal Control – Integrated Framework on sisäisen valvonnan perusmääritelmä ja malli (Moeller 2007, 4). COSO-raportti esittää yleispätevän sisäisen valvonnan mallin ja se on sovellettavissa kaikkiin niihin organisaatiotyyppeihin, joilla on tavoitteellista toimintaa. Mallin avulla on mahdollista myös kehittää organisaatioiden sisäistä valvontaa. (Holopainen ym. 2010, 49)

Vuonna 2004 julkaistiin kuitenkin sisäistä valvontaa ja riskienhallintaa koskeva kokonaisvaltainen arviointikehikko ja ajatusmalli COSO Enterprise Risk Management-Integrated Framework, joka täydentää aiemmin julkaistua COSO-IC-kehikkoa (Holopainen ym. 2006, 37). ERM-mallin taustalla on USA:n kiristynyt lainsäädäntö sekä yritysten johtamis- ja hallintojärjestelmien tiukemmat vaatimukset. Näistä mainittakoon Sarbanes Oxley-laki ja Corporate Governance. (Alftan ym. 2008, 86)

Kolmiulotteisena mallina COSO-ERM näyttää hyvin samanlaiselta verrattuna COSO-IC-malliin (Moeller 2007, 47). Vaikka COSO-ERM perustuu keskeisiltä osiltaan aikaisempaan sisäisen valvonnan malliin, COSO-ERM on kuitenkin COSO-IC-kehikkoa laajempi ja käsittelee riskienhallintaa entistä syvällisemmin. Mallin rikkaus piileekin siinä, että se tuo riskienhallinnan laajaksi osaksi sisäistä valvontaa. Molemmilla sisäisen valvonnan ja riskienhallinnan teorioilla on ollut kuitenkin suuri merkitys sisäisen valvonnan kehittämisessä. Malleja on sovellettu niin yritysmaailmassa kuin myös julkisella sektorilla.

2.3 COSO-IC

COSO-IC, joka on julkaistu ensimmäisen kerran vuonna 1992, on alkuperäinen sisäisen valvonnan yleispätevä malli. Se on ensimmäinen sisäisen valvonnan malli, joka esittää tarkan määritelmän sisäisestä valvonnasta ja sen osatekijöistä. Ennen mallin julkaisua, yritysmaailmassa oli ollut puhetta jo vuosia sisäisestä valvonnasta, yrityksien sisäisistä käytännöistä ja prosesseista, mutta silti tarkka yrityksen sisäisen valvonnan määritelmä puuttui. COSO-ICI:n tavoitteet ovat sisäisen valvonnan yleiset lähtökohdat, eli toiminnan tehokkuus, taloudellisen raportoinnin luotettavuus ja oikeellisuus sekä lakien ja säännösten noudattaminen. COSO-IC voidaan nähdä sekä viisiulotteisena mallina, eli horisontaalisena mallina, että myös kolmiulotteisena eli vertikaalisena mallina. (Moeller 2007, 4-5)

COSO:n mukaan sisäisen valvonnan tavoite on saavuttaa kohtuullinen varmuus liittyen sen kolmeen päätavoitteeseen, eli toimintojen tarkoituksenmukaisuuteen ja tehokkuuteen, taloudellisen raportoinnin luotettavuuteen ja lakien sekä sääntöjen mukaiseen toimintaan. Ensimmäinen tavoite liittyy oleellisesti yrityksen liiketoimintaan ja yrityksen tehokkuus- ja tuottavuustavoitteisiin. Taloudellinen raportointi liittyy taas muun muassa tilinpäätöksen luotettavuuteen ja siihen antaako tilinpäätös ja muut yrityksen taloudelliset raportit oikeat ja riittävät tiedot yrityksen taloudesta ja toiminnasta. Kolmas tavoite viittaa taas siihen, kuinka yhteisössä noudatetaan lakeja ja yhteisössä vallitsevia sääntöjä. (Ahokas 2012, 24–26, ks. myös. COSO 2013)

Kolmiulotteisena mallina COSO-IC perustuu yksiköiden toimintoihin, valvontatoimenpiteiden, tavoitteiden ja yksiköiden välisiin suhteisiin sekä taloudelliseen raportointiin, operaatioihin ja lainmukaisuuteen. COSO-ICI:N varsinaiset horisontaaliset osa-alueet ovat seuranta, tieto ja viestintä, valvontatoimenpiteet, riskien arviointi ja valvontaympäristö. (Moeller 2007,5) Näistä viidestä osa-alueesta yhteisön sisäinen valvonta koostuu.

(Moellerin 2007, 4-5) mukaan kaikki osa-alueet ovat COSO-IC mallissa yhteydessä toisiinsa, eikä niitä voi erottaa toisistaan. On myös huomattava, että COSO-ICI:n komponentit sisältävät myös muita yksilöllisiä osa-alueita riippuen organisaation luonteesta. Yksi mielenkiintoinen piirre mallissa on myös se, että kaikki komponentit tarvitsevat toisiansa, eikä se ole kokonainen jonkun puuttuessa. Jokainen mallin osa-

alue auttaa myös sisäisen valvonnan mallin ymmärtämisessä. Mallin ehkä tärkein osa-alue, eli valvontaympäristö luo vahvan perustan mallille ja sen muille osatekijöille. Valvontaympäristö organisaatiossa määritteleekin sen, miten organisaatiossa toimitaan, ja millainen ilmapiiri ja asenne yrityksen työntekijöillä ja erityisesti sen johdolla, eli yleisimmin toimitusjohtajalla ja hallituksella on. Yrityksen johdon asenteet välittyvät nopeasti myös alemmille tahoille ja sen työntekijöihin, mikä vaikuttaa koko organisaation asenteisiin, mielipiteisiin ja mielialaan. Valvontaympäristö voi siis tuoda toimintaan kurinalaisuutta ja lainmukaisuutta.

Riskienarviointi tarkoittaa olennaisten riskien tunnistamista yhteisössä. Riskienarviointi luo myös perustan yrityksen riskienhallinnalle. Valvontatoimenpiteillä tarkoitetaan toimenpiteitä, joiden avulla pyritään ehkäisemään uhkia ja varmistamaan myös tavoitteiden saavuttaminen. Tieto ja viestintä sisältävät kaiken tiedonkulun yhteisössä. Informaatiolla ja kommunikaatiolla yrityksen joka tasolla onkin merkitystä. On tärkeää, että keskeinen informaatio välittyy johtoportaalta alaspäin ja myös toisin päin. Seuranta on taas johdon tai siihen tarkoitetun erillisen yksikön, kuten sisäisen tarkastuksen tekemää arviointia sisäisen valvonnan onnistumisesta ja tehokkuudesta. (Ahokas 2012, 26–27)

Vuoden 2013 toukokuussa COSO julkaisi päivitetyn version tästä sisäisen valvonnan perusmääritelmästä ja mallista. Uusi versio huomioi talouden ja teknologian muutokset. Päivitetty versio sisältää samat tavoitteet ja pääosa-alueet. Uudessa versiossa on kuitenkin 17 uutta pääsääntöä, jotka koskevat mallin viittä pääperiaatetta. Näiden sääntöjen ja ohjeiden tarkoitus on auttaa mallin käyttäjiä sen soveltamisessa. (Journal of accountancy, 2013)

2.4 COSO Enterprise Risk Management – Integrated Framework

Kokonaisvaltaisessa riskienhallinnassa on kyse riskienhallinnan kytkemisestä organisaation toiminnallisiin, taloudellisiin ja strategisiin tavoitteisiin. Riskienhallintaa myös tarkastellaan koko organisaation tasolla. COSO-ERM-mallissa riskienhallinnan tavoitteita ovat riskinottohalun ja strategian yhdenmukaistaminen, toiminnallisten yllätysten ja tappioiden vähentäminen, kertautuvien ja organisaationlaajuisten riskien havaitseminen ja hallinta, mahdollisuuksien hyödyntäminen ja pääoman käytön tehostaminen. (Alftan ym. 2008, 85–87)

ERM-mallista julkaistussa tiivistelmässä (2004, 4) todetaan, että riskienhallinnan luontaisten ominaisuuksien avulla, organisaatio pystyy saavuttamaan liiketaloudelliset tavoitteensa eli tulos- ja kannattavuustavoitteet. Riskienhallinta mahdollistaa myös paremman ja tehokkaamman raportoinnin sekä lakien ja muiden säännösten ja määräysten noudattamisen. (COSO-ERM 2004, 4)

Moellerin (2007, 50–52) mukaan COSO-ERM on ensinnäkin prosessi, jonka organisaation ihmiset saavat aikaan. Mallia tulisi noudattaa koko organisaatiossa aina pienimmästä yksiköstä suurimpaan, ja se on huomioitava myös strategisia tavoitteita asetettaessa. Yksi avaintekijä on, että organisaation täytyy luokitella sen riskinottohalukkuus. Yrityksessä on huomioitava se riskien määrä, jonka yritys on valmis hyväksymään. ERM-kehikon tarkoitus on ennen kaikkea auttaa organisaatiota sen tavoitteiden ja päämäärien saavuttamisessa. (Moeller 2007, 50–52)

Moellerin (2007, 53) mukaan ERM-mallia ei kuitenkaan tulisi pitää vain paranneltuna ja uutena versiona COSO-IC-mallista, koska sillä on muun muassa erilaisia tavoitteita ja käyttötapoja. ERM käsitteleekin sisäistä valvontaa entistä kattavammin ja keskittyy aikaisempaa selkeämmin ja perusteellisemmin organisaatioiden riskienhallintaan. Tarkoituksena ei siis ole syrjäyttää aiempaa sisäisen valvonnan mallia, vaan liittää se osaksi riskienhallintaa. (Moeller, 2007) Tästä voikin päätellä, että ERM perustuu aikaisempaan sisäisen valvonnan malliin ja on työstetympi versio edeltäjästään.

ERM on siis kolmiulotteinen malli, jonka jokainen taso on yhteydessä toisiinsa. Se sisältää vertikaalisen tason, joka edustaa yrityksen toiminnallisia tavoitteita. Horisontaalinen taso edustaa taas riskikomponentteja, joita on mallissa kahdeksan.

Viimeinen taso ottaa huomioon koko organisaation, esimerkiksi toimialayksiköt, liiketoimintayksiköt ja tytäryhtiöt. (Moeller 2007, 53) ERM-mallissa organisaation riskienhallintaprosessi koostuu kahdeksasta toisiinsa liittyvästä osa-alueesta. Osa-alueet ovat valvontaympäristö, tavoitteenasettelu, tapahtumien tunnistaminen, riskienarviointi, riskeihin vastaaminen valvontatoimenpiteet, tieto ja viestintä sekä seuranta. (Moeller, 2007)

Ilman valvontaympäristöä koko mallia ei edes käytettäisi, koska valvontaympäristöllä tarkoitetaan johdon asennoitumista riskeihin ja riskienhallintaprosesseihin. Johdon mielenkiinto tehokkaaseen riskienhallintaan ja kattavaan riskienhallintaprosessiin muodostaa koko mallin olemassaolon ja perustan. (Moeller, 2007) Moellerin (2007, 54) mukaan tämä taso eli valvontaympäristö luo perustan kaikille muille osatekijöille organisaation COSO-mallissa, mikä taas vaikuttaa siihen, miten strategiat ja tavoitteet tulisi asettaa. ERM-mallin sisäinen ympäristö käsittelee samoja alueita kuin COSO-IC-malli, mutta ERM tarkastelee alueita syvemmin ja huomio myös tulevaisuuden.

Kuva 1. COSO-ERM – viitekehikko (COSO, 2004)

2.5 Valvontaympäristö

Valvontaympäristöllä on tässä tutkielmassa iso rooli, koska se voidaan mielestäni nähdä tärkeimpänä osatekijänä, niin alkuperäisessä COSO-IC mallissa kuin myös myöhemmin julkaistussa COSO-ERM mallissa. Valvontaympäristössä on kyse siitä, miten organisaatio ja sen johto suhtautuvat riskeihin ja sisäiseen valvontaan kaikessa toiminnassaan. Kuten aiemminkin jo totesin, myös sisäisen valvonta määräytyy yhteisön toimintakulttuurin ja ajattelutavan mukaisesti.

Itse asiassa valvontaympäristö on koko ERM-viitekehyksen perusta ja kivijalka. Sisäinen valvontaympäristö sisältää organisaation ilmapiirin ja se asettaa perustan sille, miten riskit nähdään koko yhteisössä. (Journal of Accountancy, 2008) ERM-mallista julkaistussa tiivistelmässä (2004, 3) todetaan, että valvontaympäristö ja sen ilmapiiri määrittävät myös sen, miten koko henkilöstö suhtautuu riskeihin ja riskienhallintaan organisaatiossa. Henkilöstö käsittelee riskejä ja toimii valvontaympäristön ilmapiirin ja asenteiden pohjalta. Valvontaympäristö vaikuttaa siis koko henkilökunnan toimintaan.

Sisäinen valvontaympäristö on nimenomaan COSO-mallin luoma käsite organisaation riskienhallinnan mallissa ja se on tärkeä osa niin COSO-IC-kehikkoa kuin myös COSO-ERM-kehikkoa. COSO-IC-viitekehikko on asettanut valvontaympäristön alimmalle tasolle, kun taas COSO-ERM-viitekehikossa sisäinen ympäristö on ylimpänä, muiden osatekijöiden päällä. Viitekehikot tarkastelevat organisaation valvontaympäristöä eri nimityksillä. COSO-IC kutsuu sitä sisäiseksi valvontaympäristöksi (Internal control environment), ja COSO-ERM-viitekehikossa sitä käsitellään sisäisenä ympäristönä (Internal environment). Molemmissa viitekehikoissa on kuitenkin sama ajatus siitä että, sisäinen valvontaympäristö luo perustan ja pohjan koko mallille ja muille riskienhallinnan vaiheille. (Moeller, 2007)

Valvontaympäristö koostuu monista toisiinsa linkittyvistä alueista. Näitä ovat riskienhallinta-ajattelu, johdon periaatteet, toimintatavat ja asenteet, rehellisyys ja eettiset arvot, henkilöstön pätevyys, organisaatiorakenne, valtuuksien ja velvollisuuksien jakaminen ja henkilöstöhallinnon menettelytavat (Moeller 2007; ks. myös Holopainen ym. 2006).

3 PIENTEN JA KESKISUURTEN YRITYSTEN RISKIENHALLINTA

3.1 Pk-yritykset ja niiden määritelmä

Kuva 2. Pk-yritysten luokittelu

Yritys-luokka	Henkilö-kunta	Liike-vaihto tai	Taseen loppusumma
Mikro	<10	2 milj. euroa	2 milj. euroa
Pieni	10- 49	10 milj. euroa	10 milj. euroa
Keskisuuri	50- 249	50 milj. euroa	43 milj. euroa

(Elinkeinoelämän keskusliitto, EK, 2013)

Euroopan komission antaman suosituksen (2003) mukaan mikroyritysten ja pienten sekä keskisuurten yritysten luokka muodostuu yrityksistä, joiden palveluksessa on vähemmän kuin 250 työntekijää, ja joiden vuosiliikevaihto on enintään 50 miljoonaa euroa tai taseen loppusumma on enintään 43 miljoonaa euroa. Yhdessä näitä kutsutaan pieniksi ja keskisuuriksi yrityksiksi. Pk-yritysten luokassa pieni yritys luokitellaan yritykseksi, jonka palveluksessa on vähemmän kuin 50 työntekijää, ja jonka vuosiliikevaihto tai taseen loppusumma on enintään 10 miljoonaa euroa. Pk-yritysten luokassa taas mikroyritys luokitellaan yritykseksi, jonka palveluksessa on vähemmän kuin 10 työntekijää ja jonka vuosiliikevaihto tai taseen loppusumma on enintään 2 miljoonaa euroa. Pk-yritysten on oltava myös riippumattomia. Suosituksen mukaan riippumattomia yrityksiä ovat yritykset, joita ei pidetä suosituksessa tarkoitettuina sidosyrityksinä tai omistusyhteysyrityksinä. (Euroopan komission suositus 2003)

Euroopan komission uuden pk-yrityksiä koskevan uuden määritelmän (2005) mukaan, pk-yrityksen määrittelyssä on lähtökohtana varmistaa, että yritys on todellakin yritys. Tämä toteutuu jos yhteisöllä on taloudellista toimintaa. Ratkaisevaa on siis taloudellinen toiminta eikä niinkään oikeudellinen muoto. Kun yritysmuoto on selvillä, tulee selvittää yrityksen liikevaihto, henkilömäärä ja taseen loppusumma. Pk-yrityksen tulee täyttää henkilöstömäärää koskeva ehto, mutta se voi valita liikevaihdon tai taseen loppusumman välillä. Sen ei siis tarvitse täyttää kumpaakin liikevaihdon ja taseen

loppusumman edellytystä, mutta se voi ylittää näistä toisen. Eli pk-yritysten luokka koostuu yrityksistä, joiden henkilöstömäärä on vähemmän kuin 250 henkilöä, vuosiliikevaihto on enintään 50 miljoonaa euroa tai taseen loppusumma on enintään 43 miljoonaa euroa. (Euroopan Komissio, 2006)

Euroopan unionin komissio antoi vuonna 1996 suorituksen ja tarpeellisen määritelmän pk-yrityksistä ja niiden luonteesta. Määritelmä on hyödyllinen, koska se lisää pk-yritysten välillä vallitsevaa johdonmukaisuutta ja yhtenäisyyttä, varmistaa kilpailua ja estää samalla sen vääristymistä. Määritelmä myös tukee yrityksiä avun tarpeessa. Komissio myöhemmin päivitti määritelmäänsä vuonna 2003 johtuen talouden ja koko Euroopan unionin kehityksestä. Uusi määritelmä tulikin voimaan vuonna 2005. Komission määritelmäsuositus koskee henkilöstömäärää, taseen loppusummaa ja liikevaihtoa. On huomattava, että pk-yritysten tulee täyttää henkilöstömäärää koskeva edellytys, mutta se voi kuitenkin valita joko taseen loppusummaa tai liikevaihtoa koskevien kynnysarvojen välillä. Pk-yritys voi myös ylittää jommankumman näistä kynnysarvoista menettämättä kuitenkaan pk-yrityksen asemaansa. Vaikka määritelmän käyttö onkin vapaaehtoista, sitä pitäisi kuitenkin soveltaa jäsenvaltioissa kaikkiin yrityksiä koskeviin toimenpideohjelmiin, menetelmiin ja toimenpiteisiin. (Euroopan Komissio, 2006)

Pienet ja keskisuuret yritykset koostuvat siis keskisuurista yrityksistä, pienistä yrityksistä ja mikroyrityksistä. Vuonna 2009 Suomessa toimi 320 072 Pientä ja keskisuurta yritystä, joka oli 99,8 % kaikista yrityksistä. Pieniä näistä oli 99,1 % ja keskisuuria 0,7 %.(Tilastokeskus, TK, 2009) Pk-yritykset ovat mielenkiintoinen tutkimuskohde, koska niillä on merkittävä asema niin Suomen kuin koko Euroopan taloudessa. Pk-yrityksiä voidaan pitää Suomessa innovoinnin, yrittäjyyden, suoritteiden kuin myös työpaikkojen lähteinä. On myös huomioitavaa, että lähes kaikki Suomen yritykset kuuluvat pk-yritysten luokkaan.

Pk-yritykset muodostavat siis kattavan kuvan siitä, millaisista yrityksistä Suomen talous- ja elinkeinoelämä oikeasti muodostuu. Pk-yritysten kohdalla on mielenkiintoista nähdä, miten riskienhallinnan ja sisäisen valvonnan yleiset teoriat soveltuvat nimenomaan pk-yrityksiin. Pk-yrityksistä puhuttaessa on myös olennaista huomata, kuinka suuri ero on mikroyritysten ja keskisuurten yritysten välillä. Ero tulee selkeästi esiin kuvassa 1. Pienimpien mikroyritysten ja suurimpien keskisuurten yritysten väliin

mahtuu suuruusluokaltaan vaihtelevia ja riskienhallinnan menettelytavoiltaan erilaisia yrityksiä.

3.2 Osakeyhtiöt ja osakeyhtiölaki

Suomen suosituin yhtiömuoto on selvästi osakeyhtiö. Sen tarkoitus on voiton tuottaminen osakkeenomistajille, jollei yhtiöjärjestyksessä toisin määrätä. Uusi osakeyhtiölaki OYL tuli voimaan 1.9.2006. Osakeyhtiölaki on yleislaki. (Immonen & Nuolimaa 2007) Lakia sovelletaan kaikkiin Suomen lain mukaan rekisteröityihin osakeyhtiöihin, jollei laissa muuta säädetä tai muussa laissa säädetä toisin. Osakeyhtiö voi olla yksityinen tai julkinen. (OYL 1:1) Laki koskee siis kaikkia osakeyhtiöitä, niin pörssiyhtiöitä kuin myös pienyhtiöitä. Vaikka osakeyhtiölaki on osakeyhtiöiden yleislaki, osakeyhtiön toimintaa säätelevät myös monet muut lait, muun muassa kirjanpitolaki- ja asetus, tilintarkastuslaki, arvopaperimarkkinalaki, verolait sekä kilpailua koskeva lainsäädäntö.

Koska suurin osa Suomen yrityksistä on pieniä ja keskisuuria yrityksiä, ja osakeyhtiö on taas suosituin yhtiömuoto, voin todeta että suurin osa Suomen yrityksistä on nimenomaan pieniä ja keskisuuria osakeyhtiöitä. Pienten yritysten kannalta uusi osakeyhtiölaki toi tärkeän muutoksen, kun osakepääoma tippui 8000 eurosta 2500 euroon (Varjo 2006). Muutos onkin lisännyt osakeyhtiöiden määrää.

Osakeyhtiöoikeudessa on eräitä keskeisiä periaatteita, jotka liittyvät keskeisesti osakeyhtiön toimintaan. Näitä periaatteita ei välttämättä ole kirjattu itse lakiin, mutta niillä on ollut suuri merkitys ongelmanratkaisu- tai tulkintatilanteissa. Periaatteet ovat oikeushenkilöllisyys ja osakkeenomistajan rajoitettu vastuu, pääoma ja sen pysyvyys, osakkeen luovutettavuus, toiminnan tarkoitus, enemmistöperiaate, yhdenvertaisuus, johdon tehtävä ja tahdonvaltaisuus. (Immonen & Nuolimaa 2007, 19–21)

Tässä tutkimuksessa olen kiinnostunut nimenomaan johdon tehtävästä ja yhtiön johdosta, jotka kuuluvat olennaisesti yhtiön sisäiseen valvontaympäristöön. Tässä tutkielmassa painotetaan osakeyhtiöitä, vaikka riskienhallinnan teoriat soveltuvat myös muihin yhtiömuotoihin. Yhtiön johdolla eli hallituksella, hallintoneuvostolla ja toimitusjohtajalla on suuri merkitys riskienhallinnassa ja valvonnassa. Johdon tulisi toimia yhtiön etua edistävällä tavalla. Valvontaympäristön näkökulmasta on oleellista

se, että noudattaako yhtiön johto lakia, säädöksiä ja eettisiä periaatteita, ja hoitavatko johtoelimet tehtävänsä osakeyhtiölaissa säädetyllä tavalla. Osakeyhtiölaki jakaantuu seitsemään osaan, jotka puolestaan muodostuvat 26 luvusta. Lain toinen osa käsittelee kauttaaltaan yhtiön hallintoa ja tilinpäätöstä. Lain toisen osan kuudes luku taas käsittelee yhtiön johtoa ja edustamista. Käsittelen tätä lain kohtaa perusteellisesti luvussa 4.

3.3 Riskin käsite

Riskiä voidaan luonnehtia niin vaaraksi, uhaksi kuin myös mahdollisuudeksi. Riski on epävarmuus tulevasta, ja se voi muuttua positiiviseksi tai negatiiviseksi. Vaaralla voidaan tarkoittaan terveyteen liittyvää uhkaa, vahinkoa omaisuudelle, ympäristö- tai tuotevahinkoa ja esimerkiksi rahoitukseen liittyviä tappioita. (CIPFA 2001, 19)

Riski on samaan aikaan kuitenkin myös mahdollisuus. Vahinko tai odotettu tapahtuma voikin muuttua positiiviseksi. Toisaalta tapahtunut vahinko voi muodostaa jälkeenpäin myös positiivisia vaikutuksia tai päinvastoin. Joka tapauksessa riskiä voidaan luonnehtia epävarmuudeksi, joka liittyy tulevaisuuteen. (CIPFA 2001, 19) Jokipiin (2006) mukaan riskiä voidaan luonnehtia tapahtumaksi, joka on jollain tasolla ennustettavissa ja sen todennäköisyys ja vahingot arvioitavissa.

Riskienhallinnan standardin AS/NZS 4360:2004 mukaan riski on funktio, jota voidaan kuvata *todennäköisyyden* ja *seurauksen* kombinaationa. Eli riskin käsite voidaan muodostaa, kun seuraus (consequence) kerrottaan todennäköisyydellä (likelihood). Vaikka käytettäisiin kvalitatiivisia tai kvantitatiivisia mittaustapoja, tämä esitystapa on helppo ymmärtää. Kaava edellyttää kuitenkin oikeiden mittareiden ja yksikköjen valintaa, jotta se olisi validi. (Standards Australia / Standards New Zealand 2004, 49–50)

Riskiä voidaan luonnehtia myös mahdolliseksi tappioksi tai häviöksi, joka kohdistuu organisaatioon. Riskin määrittelyn helpottamiseksi on myös matemaattinen kaava, jossa mahdollinen tapahtuma tai mahdollinen riskin esiintyminen kerrotaan tappion mitattavalla arvolla. Tämä kaavan heikkous on kuitenkin sen painottuminen pelkästään riskin negatiiviseen puoleen. Riskiin liittyy joka tapauksessa mahdollisuuksien, riskien ja tappioiden jatkumo. Lopputuloksilla ja tappiolla voi olla niin positiivisia kuin myös

negatiivisakin puolia. Riski voidaankin nähdä siis tapahtumana, johon liittyy mahdollisuus. (Rittenberg & Schwieger 2003, 121)

Yritys voi siis saavuttaa mahdollisella riskin otolla suuria rahallisia hyötyjä, mutta myös suuria rahallisia tappioita. Toisaalta riskin ottamatta jättämiselläkin voi olla negatiivisia seurauksia. Johdon tehtävä onkin arvioida riskin otossa taloudellista tilannetta, markkinatalouden muutoksia, strategisia vaihtoehtoja ja hyötyjä sekä strategisia toimenpiteitä. Johdon tulee myös toimia niin, että se maksimoi riskiin liittyvät hyödyt. (Rittenberg & Schwieger 2003,121)

Riskin voidaan nähdä koostuvan osa-alueista, jotka tulee huomioida arvioinneissa. Ensinnäkin riskillä on sen lähde, jolla tarkoitetaan asiaa, joka aiheuttaa negatiivisen tai vaihtoehtoisesti positiivisen tapahtuman. Riski koostuu myös tapahtumasta, joka aiheuttaa mahdollisen vahingon, tuhon tai hyödyn. Seurauksella taas tarkoitetaan riskin tapahtumasta aiheutunutta lopputulosta, joka voi olla positiivinen tai negatiivinen. Riskistä aiheutunut vaikutus yritykselle voi olla esimerkiksi markkina-aseman huonontuminen, ympäristökatastrofi, omaisuuteen liittyvä vahinko, sijoittajien epäluottamus tai lisääntynyt kilpailukyky. Lopputuloksen jälkeen riskiin liittyy myös syy-komponentti, jonka avulla voidaan miettiä riskin varsinaista aiheuttajaa, ja kysyä miksi näin tapahtui, tai mitä on tapahtunut. Riski liittyy myös toimintoihin, joiden avulla se pyritään hallitsemaan. Yrityksen on myös mietittävä, missä ja milloin riski voi toteutua. (Standards Australia/ Standards New Zealand 2004,38)

Riskeihin liittyy lukemattomia matemaattisia arvioita, kaavoja ja määrittelyä, mutta tarkoitukseni ei ole läpikäydä niitä tässä tutkielmassa.

3.4 Yritystoiminnan riskit ja riskilajit

Kuten jo johdannossa totesin, yritystoiminta sisältää lukemattomia riskejä, jotka tulisi huomioida niin toimintaa suunnitellessa, kuin myös koko yrityksen toiminnan ajan. Sekä Vaughn (1997, 7–9) että Harrington ja Niehaus (2003, 1–3) toteavat, että riskillä voidaan tarkoittaa monenlaisia asioita tieteenalasta riippuen. Heidän mukaansa riski voidaan kuitenkin aina liittää epävarmuuden tunteeseen ja mahdollisiin riskistä aiheutuviin kustannuksiin. Vaughnin (1997, 8) mukaan riskissä on kyse olosuhteesta, jossa mahdollisuus muuttuu epäedulliseksi tapahtumaksi toivottuun nähden.

COSO-ERM-mallin (2004, 2) mukaan tapahtumat, joilla on negatiivisia vaikutuksia edustavat *riskejä*. Tapahtumat, joilla on taas positiivisia vaikutuksia edustavat mahdollisuuksia. Tapahtumat voivat olla joko negatiivisia tai positiivisia, tai jopa molempia yhtä aikaa. Riski on siis mahdollisuus, mutta lopputulos voi olla negatiivinen tai positiivinen tavoitteiden saavuttamisen kannalta. Suomen kielessä riskin synonyymina voidaan pitää vahingonvaaraa tai vahingonuhkaa (Suominen 2003, 9).

Yrityksen riskejä on mahdollista luokitella riskilajeihin, mikä tarkoittaa mahdollisten samankaltaisuuksien ja eroavaisuuksien löytämistä riskien väliltä. Luokittelu on hyödyllistä, koska se mahdollistaa riskien vertailun keskenään ja myös parantaa organisaation riskitietoisuutta. (Ilmonen, Kallio, Koskinen, Rajamäki 2010, 70) Harrington ja Niehaus (2003, 4–5) jakavat yrityksen riskit yksinkertaisesti kahteen luokkaan, eli liiketoiminnan riskeihin ja henkilöstöön liittyviin riskeihin, kun taas Moeller (2007, 25) luokittelee riskit *strategisiin riskeihin, toimintariskeihin, taloudellisiin riskeihin* ja *tietoriskeihin*. Nämä riskilajit pitävät sisällään vielä lukemattomia riskejä.

Ilmosen ym. (2010, 70) mukaan yksi vakiintuneimmista tavoista jakaa riskit, on luokitella ne neljään riskilajiin niiden lähteen ja toisaalta niiden tyypin mukaan. Lähteellä tarkoitetaan tekijää, joka aiheuttaa riskin. Riskejä ovat strategiset riskit, operatiiviset riskit, taloudelliset riskit ja vahinkoriskit. Strategiset riskit liittyvät organisaation pitkän aikavälin tavoitteisiin. Strategisista riskeistä voidaan käyttää myös termiä liiketoimintariskit. Liiketoimintariskejä voivat olla muun muassa liiketoiminnan kehitykseen liittyvät riskit, markkinariskit, regulaatioriskit ja liiketoimintaympäristöön liittyvät riskit. Operatiivisilla riskeillä tarkoitetaan riskejä, jotka liittyvät yrityksen

päivittäisiin toimintoihin. Operatiiviset riskit voivat olla seurausta esimerkiksi riittämättömästä sisäisestä valvonnasta. Operatiivisia riskejä ovat esimerkiksi organisaatioon ja johtamiseen liittyvät riskit, tietoturvallisuusriskit ja tuottavuusriskit.(Ilmonen ym. 2010, 70–72)

Koska yrityksen päätehtävänä on kuitenkin usein rahan kerääminen ja voiton tavoittelu, yrityksen toimintaan sisältyy väistämättä huomattava määrä monenlaisia yrityksen rahaprosesseja uhkaavia riskejä, eli taloudellisia riskejä. Nämä voivat liittyä esimerkiksi yrityksen maksuvalmiuteen tai korkojen mahdolliseen nousuun. Taloudellisia riskejä ovat muun muassa korkoriskit, likviditeettiriskit, valuuttariskit, veroriskit ja sopimusriskit. Vahinkoriskeihin kuuluvat sen sijaan esimerkiksi työterveys ja työturvallisuusriskit, henkilöstöriskit, vahingoittumisriskit, luonnonkatastrofeihin liittyvät riskit ja ympäristöriskit. (Ilmonen ym. 2010, 71–75) Tämä riskien jaottelu neljään kategoriaan muistuttaa paljon Moellerin (2007) jaottelua. Moellerin jaottelussa vahinkoriskit on kuitenkin sijoiteltu muihin riskilajeihin, esimerkiksi toimintariskeihin.

Kuusela ja Ollikainen (2005, 33–34) jakavat riskit sen sijaan dynaamisiin ja staattisiin riskeihin. Heidän mukaansa *Dynaamiset* riskit muuttuvat suhdanteiden ja olosuhteiden mukaan ja toimija voi itse vaikuttaa riskeihin, kun taas *staattiset* riskit eli vakuutusriskit ovat yrityksen tai yksilön tahdosta riippumattomia. Riskit on mahdollista jakaa erilaisesta näkökulmasta käsin myös ulkoisiin ja sisäisiin riskeihin, operatiivisiin ja strategisiin riskeihin, tietoisiin ja tiedostamattomiin ja välillisiin ja välittömiin riskeihin (Erma, Rasila & Virtanen 2010, 49).

Pienten ja keskisuurten yritysten tulisi tunnistaa riskejä, koska se parantaa riskitietoisuutta eli käsitystä yritystä uhkaavien riskien olemassaolosta. PK- RH:n www-sivujen (2013) mukaan riskien luokittelu auttaa yritystä myös riskien tunnistamisessa ja niiden hallinnassa. Sivusto on luonut käytännönläheisen katsauksen pk-yritysten riskilajeihin. Riskit on lajiteltu liikeriskeihin, henkilöriskeihin, sopimus ja vastuuriskeihin, tietoriskeihin, tuoteriskeihin, ympäristöriskeihin, projektiriskeihin, keskeytysriskeihin, rikosriskeihin ja paloriskeihin. Riskejä on mahdollista luokitella siis monin eri tavoin, eikä olekaan olemassa mitään absoluuttista mallia riskiluokittelulle. Monet riskit ovat lähellä toisiaan ja voivat kuulua samoihin riskilajeihin yhtä aikaa. Pääasia on, että yrityksessä tunnistetaan ja luokitellaan riskejä.

3.5 Vaihtoehtoisia riskienhallintaprosesseja

Olen koonnut tähän kappaleeseen tekemäni kirjallisuustutkimuksen pohjalta riskienhallinnan prosessimalleja ja näkökulmia. Mallit saattavat aluksi muistuttaa paljon toisiaan, mutta niissä on myös ainutlaatuisia eroja. Olen käsittelyt muutamaa mallia myös tarkemmin. Luvussa 3.5.2 Risk management in the public services käsittelen Iso-Britannialaisen The Chartered institute of public finance and accountancy:n julkaisemaa riskienhallinnan teosta ja sen ajatuksia riskienhallinnasta. CIPFA on johtava instituutti Isossa-Britanniassa ja on keskittynyt nimenomaan julkisen sektorin laskentatoimeen, kirjanpitoon ja julkaisuihin. Luvussa 3.5.3 käsittelen yleistä riskienhallinnan standardia AS/NZS 4360:2004, jonka on valmistellut riskienhallintaan erikoistunut komitea Joint Technical Committee OB-007. Standardi hyväksyttiin riskienhallintaan erikoistuneissa neuvostoissa vuonna 2004, niin Australiassa kuin myös Uudessa-Seelannissa. Standardi julkaistiin 31. elokuuta vuonna 2004. Luvussa 3.5.4 Käsittelen organisaation riskienhallintaprosessia ORM eli Organization Risk Management. Viimeisenä käsittelen vielä maailmanlaajuisia COCO- ja ISO 31000- standardeja. Mielestäni kaikkia näitä riskienhallinnan prosesseja ja näkökulmia voi soveltaa myös yritysmaailmassa. Näiden kirjallisuuskatsauksien tarkoituksena on selventää erilaisia riskienhallinnan lähestymistapoja. Mielestäni on olennaista esitellä COSO:n lisäksi myös muita riskienhallinnan lähestymistapoja ja näkökulmia.

3.5.1 Kirjallisuuskatsaus riskienhallintaprosesseista

Ilmonen ym. (2010, 91) esittävät yksinkertaisempia malleja organisaation riskienhallinnalle. Yksinkertaisimmillaan riskienhallintaprosessi voisikin koostua riskien tunnistamisesta, arvioinnista, riskienhallintatoimenpiteiden suunnittelusta ja toteutuksesta sekä riskienhallinnan kokonaisvaltaisesta arvioinnista. Prosessia on vielä mahdollista pelkistää tai laajentaa. Tästä voi päätellä, että riskienhallinta voi olla pelkistetympää ja yksinkertaisempaa, jos organisaatio niin haluaa. Tämä voisi tulla kyseeseen nimenomaan mikroyritysten tai pienten yritysten kohdalla.

Ilmosen ym. (2010, 95) mukaan riskienarviointi ja tunnistaminen kannattaa kuitenkin tehdä systemaattisesti. Riskejä voidaan tunnistaa työryhmissä, ja apuna voidaan käyttää erilaisia riskimatriiseja, joiden avulla organisaation on mahdollista löytää

merkittävimmät ja rahamääräisesti suurimmat ja uhkaavimmat riskit. On myös sovittava kuinka monta riskiä on tarkoituksenmukaista tunnistaa ja kartoittaa. Organisaatiossa on siis löydettävä riskit, jotka ovat organisaation kannalta merkittävimmät ja uhkaavimmat riskit ja joiden varalta on pakko suojautua. Riskienarvioinnissa ja riskienhallintatoimenpiteissä on säilytettävä tehokkuus ja tarkoituksenmukaisuus. (Ilmonen ym. 2010, 95–96)

Vaughn (1997, 34) tarkastelee riskienhallintaa portaikollisena prosessina, jonka jokainen askel on yhteydessä toisiinsa. Teoria sisältää kuusi vaihetta, jotka ovat riskienhallinnan tavoitteiden määrittely, riskien tunnistaminen, riskien arviointi, riskeihin vastaaminen ja vaihtoehtojen valitseminen, päätösten toimeenpano ja jatkuva arviointi sekä seuranta. Mielestäni Vaughn (1997, 34) esittelee klassisen riskienhallinnan teorian, jonka keskeinen idea koostuu kolmesta tärkeästä riskienhallinnan elementistä eli riskien tunnistamisesta, arvioinnista ja riskeihin vastaamisesta. Vaughn (1997) kuitenkin toteaa, että hyödyllinen riskienhallinta edellyttää myös suunnittelua ja seurantaa.

Harringtonin ja Niehausin (2003, 8) riskienhallintaprosessi muistuttaa myös perinteisiä riskienhallinnan osa-alueita. Harringtonin ja Niehausin (2003, 8–9) mukaan riskienhallinta muodostuu merkittävien riskien tunnistamisesta, riskien arvioinnista, riskienhallinta toimenpiteiden luomisesta ja niiden toimeenpanosta sekä jatkuvasta prosessin ja toiminnan seurannasta. Mielestäni on huomattavaa, että myös Harrington ja Niehaus (2003) korostavat riskienhallintaprosessissa merkittävimpien riskien tunnistamista eli tarkoituksenmukaisuuden ja tehokkuuden säilyttämistä.

Pickettin (2004, 262) ehdotus muistuttaa paljon ERM-mallin mukaista prosessia. Pickett (2004) tarkastelee prosessia kuitenkin sisäisen tarkastajan näkökulmasta. Riskit ensinnäkin arvioidaan ja niiden merkittävyys analysoidaan. Johdon tulee päättää niiden riskien määrä, jotka se on valmis hyväksymään. Riskienhallintakeinot suunnitellaan ja toimeenpannaan. Riskienhallintaprosessia tulisi seurata jatkuvasti, jotta voidaan varmistua muun muassa riskienhallintatoimenpiteiden tehokkuudesta. Mallissa johdon ja hallituksen tulee myös saada kausittain tietoa riskienhallintaprosessin onnistumisesta ja tuloksista. Mallin mukaan riskienhallinnasta, riskistrategioista ja toimenpiteistä riskeihin vastaamiseksi tulisi antaa kausittain tietoa myös osakkeenomistajille. (Pickett, 2004, 262)

Suomisen (2003, 98) mukaan perinteisen riskienhallinnan elementtejä ovat taas riskien arviointi, kontrollointi ja rahoitus. Riskit aluksi siis arvioidaan ja tunnistetaan riskianalyysin avulla, minkä jälkeen riskeihin vastataan parhain mahdollisin keinoin.

Rittenberg & Schwieger (2003, 122–123) esittelevät riskienhallintaprosessin, joka painottuu riskianalyysiin ja tarkastelee prosessia tarkastuksen näkökulmasta. Teoksessa riskianalyysi muodostuu kolmesta osa-alueesta, jotka kaikki sisältävät omat komponenttinsa. Riskianalyysi koostuu riskien arvioinnista, riskienhallinta tekniikoista, kommunikoinnista ja riskien seurannasta.

Isossa-Britanniassa the Institute of Risk Management (IRM), the Association of Insurance and Risk Managers (AIRMIC) ja the Association of Local Authority Risk Mangers (Alarm) ovat luoneet oman riskienhallinnan standardinsa vuonna 2002. The U.K. riskienhallinnan viitekehikko nostaa prosessin osaksi yrityksen strategista johtamista. Standardin mukainen riskienhallintaprosessi ei pääpiirteiltään eroa COSO-mallin mukaisesti riskienhallinnasta. Se kuitenkin keskittyy enemmän johdon tehtäviin, liiketoimintayksiköihin ja yksilöihin yrityksen riskienhallinnan onnistumisessa. Standardi esittelee myös riskikartan, jota yritys voi käyttää riskien hahmottamisessa. (Skipper & Kwon 2007,294)

Kun olen tutkinut riskienhallintaa ja sen prosesseja erilaisista tietolähteistä käsin, olen huomannut että riskienhallinnan erilaiset mallit ja ehdotukset muistuttavat enemmän tai vähemmän ERM-mallin mukaista prosessia. Riskienhallinnassa keskeistä ovat olleet klassiset elementit, eli riskien arviointi ja tunnistaminen, riskeihin vastaaminen ja jatkuva seuranta.

3.5.2 Risk management in the public services

CIPFAN (2001, 31) julkaisussa todetaan, että riskienhallinta tulisi liittää osaksi organisaatiota ja sen toimintoja. Riskienhallinnan tulisi olla osa normaaleja päivittäisiä toimintoja sekä operaatioita. Riskienhallinnassa tulisi julkaisun mukaan kuitenkin käyttää jotain mallia tai viitekehikkoa, koska muuten riskienhallintaa ei toteuteta välttämättä systemaattisesti. Riskienhallinnan vaiheet ja prosessit tulisi olla löydettävissä viitekehikosta. Julkaisussa luetellaan tehokkaan riskienhallinnan mallin (framework) elementeiksi tehokas valvontaympäristö, vastuunotto koko organisaatiossa,

hyvin hoidettu riskienarviointi, sisäisen tarkastuksen menetelmät, riskienhallinnan seuranta ja kommunikointiprosessit. (CIPFA 2001, 31)

CIPFAN (2001, 9) julkaisemassa teoksessa esitetään myös tehokkaan ja onnistumiseen pyrkivän organisaation elementtejä. Elementit liittyvät organisaation riskienhallinnan toteuttamiseen. Näitä ovat muun muassa yrityksen visio, sitoutuminen, omistaminen, politiikat ja suunnitelmat, toimiva rakenteellinen yhteisö, roolien selkeys, vastuun jakaminen, rahoitus, seuranta ja jatkuva arviointi, informaatio ja yhteisön kommunikaatio.

Ajattelutavan mukaan visio ja yhteisön toiminta-ajatus muodostuvat yrityksen ylimmän johdon kautta. Riskienhallinnalla tulee olla kattava ja vahva ylimmän johdon tuki ja rahoitus, jotta se toimii oikein ja riittävästi. Yhteisön politiikat ja suunnitelmat liittyvät riskienhallinnan toteuttamiseen ja suunnitteluun organisaatiossa. Yrityksellä tulee olla samanlainen näkemys, politiikka ja ajattelutapa, jonka avulla riskienhallintaa toteutetaan koko yhteisössä ja osana johdon toimintaa. Organisaatiorakenne liittyy taas työryhmien, työntekijöiden ja johdon henkilöiden oikein sijoittamiseen ja johtamiseen. Organisaation jäsenten roolit on oltava järjestyksessä ja selkeitä, jotta riskiä voidaan arvioida kaikilla johdon tasoilla.

Julkaisun mukaan toiminnassa tulisi jakaa vastuut, eli on tärkeää hajauttaa vastuulliset työt ja kiinnittää huomiota myös yhteistyöhön. Riskienhallinnan rahoittamisella on suuri merkitys riskien ennaltaehkäisyssä, koska rahoittamisen avulla voidaan kohdentaa resursseja riskienhallinnan toimintoihin ja asiantuntijoihin. Jatkuvalla seurannalla ja arvioinnilla taas varmistetaan oikeiden menettelytapojen, toiminnan hyödyllisyyden ja saavutettujen etujen jatkuva tarkkailu ja päivittäminen.

Laadukkaan informaation ja tiedon saanti on olennaista, jotta riskienhallinta- ja tutkimusinformaatiota voidaan hyödyntää ja käyttää toiminnan parantamiseksi. Kommunikaatio on myös tärkeä tekijä yrityksen riskienhallinnassa, koska se mahdollistaa helpon ja vaivattoman tiedonkulun alhaalta ylöspäin sekä edesauttaa yrityksen profiilin luomisessa. Tiedonkulun lähteitä voivat olla muun muassa intranetit, uutiset, kurssit, kokoukset ja tiimipalaverit. (CIPFA 2001, 9-11)

CIPFAN 2001 julkaisussa esitellään riskienhallintaprosessi, joka muistuttaa yleistä riskienhallinnan standardia AS/NZS 4360. Julkaisu esittelee riskienhallinnan syklin,

joka etenee asteittain riskien tunnistamisesta, analyysin ja arvioinnin kautta riskien käsittelemiseen. (CIPFA 2001, 25.27)

3.5.3 AS/NZS 4360:2004

Riskienhallinnan yleisen standardin AS/NZS 4360 (2004, 7–13) mukaan riskienhallinta koostuu kontekstin ja tavoitteiden luomisesta, riskien tunnistamisesta, riskianalyysista, riskien arvioinnista, riskeihin vastaamisesta, kommunikoinnista ja seurannasta. Standardin mukaan ne organisaatiot, jotka hoitavat riskienhallintaa tehokkaasti ja pätevästi, onnistuvat myös paremmin saavuttamaan tavoitteensa. Standardissa myös todetaan, että hyvin hoidettu riskienhallinta mahdollistaa tavoitteiden saavuttamisen kustannustehokkaasti. Standardin mukainen riskienhallinta muistuttaa kovasti luonteeltaan ERM-mallin mukaista riskienhallintaa. (Standards Australia/Standards New Zealand, 2004)

Standardin mukaisesti riskille on luotava konteksti, koska se luo perustan sille miten riskiä organisaatiossa käsitellään ja johdetaan. Konteksti muodostuu yrityksen ulkoisesta ja sisäisestä ympäristöstä. Ulkoinen ympäristö koostuu yrityksen toiminnasta, lainsäädännöstä, säännöistä, kulttuurista, kilpailusta, rahoituksellisesta ja poliittisesta ympäristöstä. Ulkoinen ympäristö muodostuu myös yrityksen vahvuuksista, heikkouksista, mahdollisuuksista ja uhista. Ulkoiseen ympäristöön kuuluvat myös sijoittajat ja päärahoittajat. Yrityksen kannalta on tärkeää, että rahoittajien ja sijoittajien toiveet ja tavoitteet huomioidaan riskienhallinnan suunnittelussa ja toteuttamisessa. (Standards Australia/New Zealand 2004, 27–29)

Sisäinen konteksti sen sijaan muodostuu organisaation pääalueista, eli sisäisistä osallisista, kulttuurista, rakenteesta, työntekijöistä, prosesseista, pääomasta ja tavoitteista. Sisäisen kontekstin luominen on tärkeää, koska riskienhallinta liittyy olennaisesti yrityksen tavoitteisiin ja päämääriin. Organisaation tavoitteet, politiikat ja päämäärät auttavat myös riskienhallinnan tavoitteiden luomisessa. Sisäisen ja ulkoisen kontekstin luomisen lisäksi, organisaatiossa on perustettava riskienhallintaan liittyvä konteksti, joka koostuu muun muassa organisaation omista tavoitteista, päämääristä, strategioista, prosessista, jossa riskit ovat mukana ja toiminnan osa-alueista. Kontekstin luominen helpottaa rajojen asettamista ja määrittelyä organisaatiossa. Kontekstien

luomisessa on tärkeää hahmottaa riskin ympäristö ja se tila, jossa riskiä käsitellään ja sen kanssa toimitaan. (Standards Australia/ Standards New Zealand 2004,27–29)

Standardin mukainen riskienhallintaprosessi edellyttää myös riskien tunnistamista. Riskien tunnistamisen tarkoituksena on tunnistaa ne riskit, jotka olennaisesti liittyvät yritystoimintaan ja joita varten yrityksessä on varauduttava. Yrityksessä on arvioitava mitä voi tapahtua, missä voi tapahtua ja milloin voi mahdollisesti tapahtua. Yrityksessä on siis arvioitava ne tapahtumat, jotka voivat aiheuttaa tuhoa, vahingoittaa yritystä tai estää sen tavoitteiden saavuttamista. Arvioinnissa tehdään lista riskien mahdollisista lähteistä. Jotta voidaan arvioida mahdollisia riskeihin liittyviä tapahtumia, on myös ymmärrettävä miksi niin voi tapahtua. Yrityksen on siis tärkeä ymmärtää tapahtumien syyt ja lähteet. Riskien tunnistamista varten organisaation on valittava ne työvälineet ja tekniikat, joiden avulla se tunnistaa riskejä. Standardin mukaisia keinoja ovat muun massa tarkistuslistat, kokemukseen perustuvat arvioinnit, aivoriihi (brainstorming), systemaattiset analyysit, skenaarioanalyysit ja kehittyneet analyysit Riskien tunnistaminen liittyy olennaisesti riskikontekstiin, eikä niitä tule erottaa toisistaan. Organisaation on mietittävä, mikä on riskin aiheuttaja, mitä voi mahdollisesti tapahtua, mitä tapahtuman vaikutukset olisivat, missä tapahtuisi, milloin tapahtuisi, ketkä olisivat tapahtumaan osallisina, mitkä toiminnot estävät riskitapahtumia, mikä on tiedon luotettavuus organisaatiossa, onko tarkemmalle riskeihin liittyvälle tutkimukselle tarvetta ja ovatko päämäärät ja toiminnot riittäviä. (Standards Australia/Standards New Zealand 2004, 37–39)

Riskin analysoinnissa on kyse riskin kokonaisvaltaisesta ymmärtämisestä. Standardin mukaan riskianalyysi auttaa organisaatiota kustannustehokkaassa riskienhallintamenettelyssä. Riskianalyysin avulla on mahdollista luokitella riskit niiden merkittävyyden mukaan. Riskianalyysiä voidaan tehdä kvalitatiivisin, puolikvantitatiivisin ja kvantitatiivisin keinoin. Kvalitatiivisessa analyysissa riskiä, riskin aiheuttajaa, riskin vaikutuksia ja sen seurauksia saatetaan kuvata monin kirjallisin keinoin, mutta pyritään välttämään numeraalista esittämistapaa. Kvantitatiiviset riskianalyysit taas perustuvat numeraaliseen esittämiseen ja kuvantamiseen. Molemmissa riskianalyysin keinoissa on kuitenkin perustana riskin todennäköisyyden ja seurauksen välinen suhde. Riskianalyysin avulla riskit voidaan luokitella esimerkiksi mataliin riskeihin, keskitason riskeihin ja korkeisiin riskeihin. Tämä edesauttaa yritystä

keskittämään voimavaransa ja resurssinsa olennaisimpiin riskeihin. (Risk management guidelines, companion to AS/NZS 4360:2004, 43–59)

Riskien arviointi onkin riskianalyysin jälkeinen riskienhallintaprosessin vaihe, jonka tarkoitus on standardin mukaan arvioida riskien merkittävyyttä ja auttaa organisaatiota riskejä koskevassa päätöksenteossa. Yrityksessä tehdään päätöksiä riskianalyysin pohjalta. Riskianalyysi antaa siis perustan ja pohjan riskiarvioinnille. Standardin mukaan riskiarviointi koostuu riskinhallintakeinojen suunnittelusta, riskien luokittelusta merkittäviin, riskitoimenpiteiden resurssien suunnittelusta ja riskin kokonaisvaltaisesta arvioinnista. Riskiarviointia voidaan tehdä myös kvalitatiivisin tai kvantitatiivisin keinon. Riskejä voidaan luokitella siedettäviin ja sietämättömiin, ja tämän luokittelun avulla valitaan ne keinot, joiden avulla vastataan riskeihin. (Risk management guidelines, companion to AS/NZS 4360:2004, 63–67)

Standardissa esitellään vielä riskeihin vastaaminen ja toimiminen osana riskienhallintaprosessia. Riskeihin vastaamisessa on tärkeää, että yritys arvioi riskeihin vastaamiskeinoja niin, että riskeistä voisikin muodostua positiivisia vaikutuksia. Riskeihin vastaaminen vaatii jatkuvaa mahdollisuuksien ja keinojen etsimistä. Yritys voi yrittää muuttaa tapahtumien mahdollisuuksia, edesauttaen positiivisia tuloksia. Yritys voi myös muuttaa odotettua lopputulosta tai jakaa mahdollisuutta. Riskienhallintakeinoja ovat muun muassa riskin välttäminen, muuttaminen, jakaminen ja myös siedettävien riskien säilyttäminen. Pääasia on, että riskeihin vastataan mahdollisimman tehokkaasti. Riskeihin vastaamisessa on kuitenkin huomioitava ehdotetut toiminnot, resursseihin liittyvät rajoitteet, aikataulu, vastuut, toimenpiteet ja raportointiin liittyvät vaatimukset. Riskeihin vastaamisessa tulisi hyödyntää mahdollisimman hyvin suunniteltua riskisuunnitelmaa. (Risk management guidelines, companion to AS/NZS 4360:2004,69–79)

AS/NZS 4360:2004 standardi painottaa kommunikaation ja tiedonkulun tärkeyttä, kuten myös monet muut riskienhallinnan teoriat ja prosessit. Standardin mukaan kommunikaatio ja oikea-aikainen tiedonkulku ovat tärkeitä koko riskienhallintaprosessin ajan ja jokaisella sen askeleella. Riskienhallintaprosessissa tulisi tiedottaa sijoittajia, sisäisiä ja ulkoisia toimijoita tehokkaasti ja koko ajan. Yrityksen on hyvä muodostaa myös tiedonkulkusuunnitelma. Tiedonkulku ja kommunikaatio

mahdollistavat riskienhallintaprosessin tehokkaan toiminnan ja myös prosessin toimenpiteiden riittävyyden. (Standards Australia/Standards New Zealand 2004, 19)

3.5.4 Organization Risk Management

Williams ym. (1998, 27) tarkastelevat sen sijaan organisaation riskienhallintaa (ORM). ORM yhdistää perinteisen riskienhallinnan ja riskienhallinnan yleisiä näkemyksiä. Organisaation johtaminen perustuu mallin mukaan kolmelle funktiolle, jotka ovat yhteydessä toisiinsa. Nämä funktiot ovat strateginen johtaminen, operatiivinen johtaminen ja riskienhallinta. Organisaation riskienhallinta koostuu ORM-mallissa viidestä elementistä, jotka ovat tehtävän tunnistaminen, riskien arviointi, riskien kontrollointi, riskien rahoitus ja suunnitelman tai ohjelman hallinta. (Williams ym. 1998, 27–29)

Williams ym. (1998,27) mukaan strateginen johtaminen koostuu niistä toimenpiteistä, joiden avulla organisaatio määrittelee toiminta-ajatuksena, tavoitteensa ja päämääränsä. Strategisella johtamisella tarkoitetaan siis johtamistapaa, jonka tarkoituksena on pitkän aikavälin suunnittelu ja yrityksen strategian ja mission luominen. Strategisesta suunnittelusta vastaa yleensä yrityksen ylin johto. Operatiivisella johtamisella tarkoitetaan johtamistapaa, jonka tarkoitus on viedä yritystä käytännössä lähemmäs kohti tavoitteita. Operatiiviseen johtamistapaan kuuluvat siis kaikki ne käytännön toimenpiteet, joiden avulla yritys saavuttaa lopulta tavoitteensa. Riskienhallinta sen sijaan kattaa kaikki ne toimenpiteet, joiden avulla yritys yrittää toteuttaa ja saavuttaa toiminta-ajatuksensa. (Williams ym. 1998,27–28)

ORM-mallissa on paljon samankaltaisuuksia myös moniin muihin riskienhallinnan teorioihin, mutta se on silti ainutlaatuinen. Tehtävän ja toiminta-ajatuksen tunnistaminen on ensimmäinen riskienhallintaprosessin askel. Tehtävän tunnistaminen liittyy olennaisesti yrityksen tavoitteisiin, päämääriin, toiminta-ajatukseen ja pääasialliseen tehtävään. Yrityksen on siis tunnistettava mitä se tekee, milloin se tekee ja miksi se tekee. Tämä osa-alue koostuu myös niistä toimenpiteistä, joiden avulla yritys pyrkii tunnistamaan toiminta-ajatuksensa. Tehtävän tunnistamista helpottavat muun muassa yrityksen sisäiset toimintatavat, politiikat ja menettelyt. ORM-mallin mukaan tehtävien ja tavoitteiden tunnistaminen ovat perustana yrityksen riskienhallintaprosessille ja riskienhallinnan toimenpiteille.

ORM-mallin mukaan riskienarviointi muodostuu kolmesta vaiheesta. Ensin yrityksen johdon tai riskienhallinnasta vastaavan yksikön on tunnistettava ja arvioitava ne riskit, jotka mahdollisesti vaikuttavat yrityksen päämäärien ja tavoitteiden saavuttamiseen. Tunnistaminen liittyy yleensä niin vaarojen kuin myös näiden kohteiden arvioimiseen. Vaarojen ja kohteiden tunnistamisella, voidaan tarkoittaa riskitekijöiden (risk factors) tunnistamista. Vaaralla tarkoitetaan ORM-mallissa tilaa, joka lisää tai vähentää riskin mahdollisuutta. Kohde voi olla esimerkiksi ihminen, tila tai esine, jolle vahinkoa aiheutuu. (Williams ym.1998)

ORM-mallin mukaan pelkkä riskien ja riskitekijöiden tunnistaminen ei ole riittävää, vaan riskejä tulee analysoida. Mallin mukaa riskin merkittävyyttä täytyy luokitella ja analysoida. Ensisijaisesti yrityksen tulee miettiä, miten riskin aiheuttama tila vaikuttaa tuotteisiin, työntekijöihin ja muihin osallisiin. Analysointi liittyy myös viimeiseen arviointivaiheeseen eli riskien mittaamiseen. Riskien mittaamisella tarkoitetaan riskin saattamista mitattavaan muotoon ja matemaattisten sekä kvalitatiivisten riskimallien hyödyntämistä. ORM-mallikin asettaa riskin todennäköisyyden yhdeksi riskin mittariksi ja huomioi riskin todennäköisyyden osana riskin määrittämistä. (Williams ym. 1998)

Riskin kontrollitoiminnot voidaan jakaa riskin välttämiseen, estämiseen, vähentämiseen tai riskin ja epävarmuuksien hallitsemiseen. Riskin kontrollitoimenpiteet voidaan esittää yksinkertaisesti. Kontrollitoimenpide voi olla esimerkiksi turvallinen palovaroitinjärjestelmä. Toimenpiteet voidaan kuitenkin esittää myös monimutkaisemmin. Kontrollitoimenpiteitä varten voidaankin rakentaa monipuolinen riskisuunnittelu ja valvontajärjestelmä. Malli tarkastelee myös riskin rahoittamista osana riskienhallintajärjestelmää. Riskin rahoittamisella voidaan tarkoittaa yksinkertaisuudessaan rahallisia vakuutuksia. (Williams ym. 1998, 29–31)

ORM-mallissa suunnitelman ja ohjelman hallinta on viimeinen riskienhallintaprosessin vaihe, mutta sitä tulee kuitenkin toteuttaa koko riskienhallintaprosessin ajan jokaisella portaalla. Hallinta tulisi kytkeä jokapäiväisiin operatiivisiin johtamistoimenpiteisiin. Suunnitelman tai ohjelman hallinnassa on kyse erilaisten toimenpiteiden ja järjestelmien luomisesta, esimerkiksi ohjelman tai toimenpideohjelman kokonaisvaltaisen seurannan järjestämisestä. Yrityksen toimintaa voidaan myös hallita erilaisten tiedonkulkujärjestelmien tai riskienhallintajärjestelmien avulla. Toiminnan hallinta ja suunnittelu ovat tiukasti yhteydessä organisaation kontekstiin, missioon ja tavoitteisiin,

koska hallinta edellyttää johdolta tietoa miten yritys toimii, mikä on sen historia, mitkä ovat sen tavoitteet ja millaisia ovat yrityksen työntekijät. (Williams ym. 1998, 29–31)

3.5.5 COCO-malli

COCO-malli on kanadalaisen Criteria of Control Committee of the Canadian Institute of Chartered Acoountants:n (CICA) julkaisema malli, joka muistuttaa paljon perinteistä COSO-mallia. Ensimmäisen kerran malli julkaistiin vuonna 1994 *Guidance on Criteria of Control* nimisessä oppaassa ja vuoden 1995 marraskuussa oppaasta julkaistiin lopullinen versio – *Guidance of Control.* (Sisäiset tarkastajat ry 1999,1)

Sisäiset tarkastajat ry on laatinut alkuperäisen Cuidance on Criteria of Control – oppaan pohjalta muistion, joka käsittelee mallin valvontakriteerejä ja osa-alueita. Muistion mukaisesti valvonnalla on kolme keskeistä tavoitetta, jotka liittyvät toimintojen tehokkuuteen ja tarkoituksenmukaisuuteen, liiketaloudellisen informaation ja johdon informaation luotettavuuteen sekä lakien, säännösten ja sisäisten ohjeiden noudatettavuuteen. Mallin mukaiset tavoitteet ovat samanlaisia COSO-mallin tavoitteiden kanssa. (Sisäiset tarkastajat ry 1999, 2)

COCO-mallissa valvonta muodostuu monista yhteen sovitettavista toimintaketjuista, joiden tarkoituksena on organisaation tavoitteiden saavuttaminen. Valvonnasta vastaavat kaikki organisaation jokaisella tasolla ja johto on ensisijaisesti vastuussa tavoitteiden saavuttamisen edellyttämistä valvontaprosesseista. Mallin mukaan valvontaprosessin tulee olla organisaatiossa dynaaminen, koska prosessit ovat jatkuvassa vuorovaikutussuhteessa keskenään. COCO-mallin mukaan valvonnalla ei voida saavuttaa ehdotonta varmuutta, vaan vain kohtuullinen varmuus toiminnasta ja sen luotettavuudesta. Kaikkien organisaation työntekijöiden jokaisella tasolla tulisi osallistua valvontaprosessiin, ja hallituksen vastuulle jää organisaation johtaminen. Organisaation johtaminen muodostuu esimerkiksi, strategiasta päättämisestä, henkilöstöresurssien jatkuvuuden varmistamisesta, yrityksen viestintäpolitiikan luomisesta ja organisaation valvonta- ja tietojärjestelmien eheyden muodostamisesta. (Sisäiset tarkastajat ry 1999, 6)

Tämän tutkimuksen kannalta mielenkiintoisin alue COCO-mallissa on sen valvontakehikko. COCO-mallin valvontakehikko tai viitekehys muistuttaa COSO-mallia, mutta myös muita riskienhallinnan yleisiä näkemyksiä. COCO-mallissa

viitekehikko muodostuu valvontaympäristöstä, tavoitteista ja riskeistä, valvontatoimista sekä seurannasta ja muutoksesta. Valvontaympäristön muodostumista ja osa-alueita käsittelen luvussa 4.

3.5.6 ISO 31000- standardi

Maailmanlaajuinen standardisointiorganisaatio ISO on julkaissut kansainvälisen standardin ISO 31000:20009 Risk management, joka kuuluu Management Systems – standardiperheeseen. Standardin lähtökohtana olivat monet muut riskienhallinnan viitekehikot, kokemukset ja riskienhallinnan näkemykset. ISO 31000- standardin valmistuminen onkin laajan taustatyön tulos. ISO 31000 – standardi kuvaa riskienhallinnan periaatteet, puitteet, käsitteet sekä riskienhallintaprosessin. Standardin tavoitteena on sen sisällyttäminen kaikkeen organisaation toimintaan ja johtamisprosessiin. Standardin mukaan tehokkaan riskienhallinnan ominaisuuksia ovat jatkuva kehittäminen, täysi vastuu riskeistä, jatkuva tiedonvaihto ja riskienhallinnan soveltaminen kaikessa päätöksenteossa. Riskienhallinta tulisikin liittää yrityksen hallintorakenteeseen. (Veijola 2012, 48–49)

Iso standardin mukainen riskienhallintaprosessi muistuttaa ERM-mallin mukaista riskienhallintaprosessi ja varsinkin AS/NZS 4360:2004 standardia. Iso 31000 standardin mukainen prosessi muodostuu kontekstin luomisesta, riskien tunnistamisesta, riskianalyysista, riskiarvioinnista, riskeihin vastaamisesta, kommunikaatiosta ja konsultoinnista sekä jatkuvasta seurannasta. Tiedon tulisi kulkea prosessissa jatkuvasti. En käsittele näitä riskienhallinnan osatekijöitä tarkemmin, koska niiden sisältö on samankaltainen kuin muissa vastaavissa riskienhallintaprosesseissa. Iso 31000 standardin mukaan riskienhallinnan tulisi muun muassa luoda lisäarvoa, olla olennainen osa yrityksen hallintokulttuuria, olla osa päätöksentekoprosessia, vähentää epävarmuustekijöitä, olla aikataulutettua ja systemaattista sekä perustua saatavilla olevaan informaatioon. (Purdy 2010)

3.6 Yrityksen riskienhallintaprosessi COSO-viitekehikon avulla

COSO-IC-viitekehikon perusperiaatteet ja tavoitteet käsittelin jo luvussa 2.3, joten tässä luvussa keskitytään COSO-IC-viitekehikon mukaiseen valvonta- ja riskienhallintaprosessiin. COSO-IC-viitekehikossa sisäinen valvonta muodostuu viidestä toisiinsa yhteydessä olevista osa-alueista. Näitä ovat sisäinen valvontaympäristö, riskien arviointi, kontrollitoiminnot, tieto ja viestintä, sekä seuranta.

Valvontaympäristö on valvonnan lähtökohta ja asettaa ehdot riskin käsittelylle yhteisössä. Valvontaympäristö luo myös säännöt, rakenteet ja pohjan yrityksen riskienhallintaprosessille. En esittele COSO-IC mallin mukaista valvontaympäristöä nyt tarkemmin, koska valvontaympäristö on luvun 4. aihe. Riskien arviointi on COSO-IC mallin toinen vaihe. Mallin mukaan riskien arvioinnissa on kyse, olennaisten riskien tunnistamisesta, analysoinnista ja arvioinnista. Riskien arviointi on tärkeää, jotta mahdolliset riskit eivät estä yrityksen tavoitteiden saavuttamista. (COSO 1992, 2)

Mallin kolmas vaihe on kontrollitoiminnot, joiden avulla riskeihin vastataan. Toimintojen avulla yritys varmistuu myös siitä, että tarvittavat toimenpiteet riskeihin vastaamiseksi on tehty ja ne ovat riittäviä. Kontrollitoimenpiteitä tulisi olla jokaisella organisaation tasolla. Kontrollitoiminnat voivat liittyä yrityksessä esimerkiksi, toimivaan hyväksymis-, tunnistamis- ja valvontamenettelyyn. Mallin neljäs vaihe on tieto ja viestintä, ja sen tarkoituksena on selventää tiedonkulun tärkeyttä organisaatiossa. Yrityksen tulisi tunnistaa olennainen tieto, säilyttää se ja välittää oikea-aikaisesti myös eteenpäin. Tiedon tulisi kulkea jokaisella organisaation tasolla aina ylhäältä alaspäin. Johdon tulee välittää työntekijöilleen selkeä viesti siitä, miten valvontajärjestelmä toimii ja miten siihen suhtaudutaan. Jokaisen tulisi tietää oma paikkansa yrityksen valvontaorganisaatiossa. Tieto ja sen kerääminen tuottaa hyödyllisiä raportteja ja tarjoaa operatiivista ja taloudellista tietoa yrityksen johdolle. Tiedon avulla yritys pystyy hoitamaan liiketoimintaa koskevat velvoitteensa ja toimenpiteensä. (COSO 1992, 2)

Mallin viimeinen komponentti on valvonta. Valvonnan tulisi olla ensisijaisesti jatkuvaa, mutta myös erillisiä arviointeja on mahdollista toteuttaa. Johdon tulisi valvoa yrityksen toimintaa päivittäin, mutta myös yrityksen työntekijöiden pitäisi noudattaa valvontatoimenpiteitä omassa työssään. Tehokas ja toimiva valvontaprosessi auttaa toiminnan laadun varmistamisessa myös pitemmällä aikavälillä. Yrityksen tulee myös

hyödyntää valvonnan tuloksia ja ne tulisi raportoida yrityksen johdolle ilman viivästyksiä. (COSO 1992, 3)

COSO julkaisi vuoden 2013 toukokuussa päivitetyn version sisäisen valvonnan perusmääritelmästä ja mallista Sisäisen valvonnan perusmääritelmä ja rakenteet eivät ole päivityksen myötä muuttuneet, mikä kertoo mallin alkuperäisestä hyödyllisyydestä. Päivitys on sen sijaan tuonut parannuksia ja selkeytyksiä, joiden tarkoituksena on helpottaa mallin soveltamista organisaatioissa. Päivityksen ansiosta sisäisen valvonnan viiden pääkomponentin rinnalle on luotu 17 pääperiaatetta, joiden tarkoitus on selkeyttää sisäisen valvonnan suunnittelua, toteutusta ja käyttöä. Pääperiaatteet selkeyttävät sitä, mitä eri komponentit todellisuudessa pitävät sisällään. (COSO 2013)

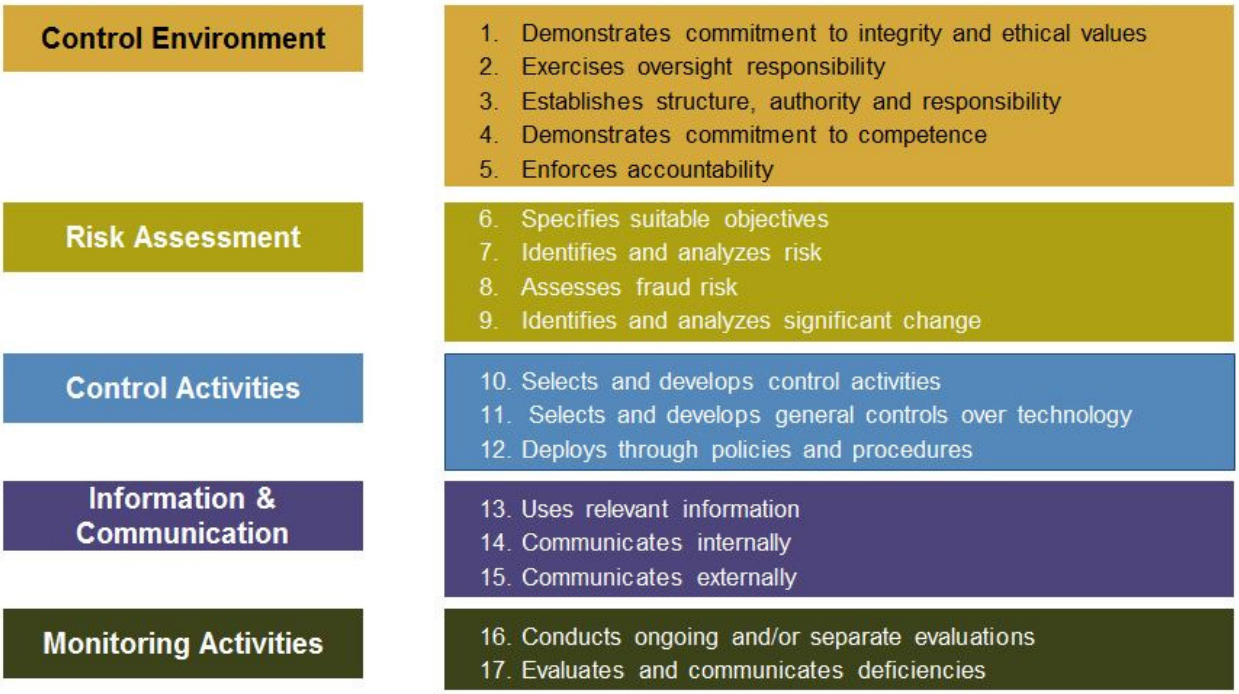
Valvontaympäristön osalta periaatteet liittyvät siihen, että yritys ensinnäkin sitoutuu rehellisyyteen ja eettiseen toimintaan kaikissa toiminnoissaan. Hallituksen tulisi olla tarpeeksi riippumaton muusta johdosta ja järjestää tehokkaan sisäisen valvonnan kehittäminen ja toimeenpaneminen. Johdon tulee perustaa rakenteita, linjauksia, velvollisuuksia ja vastuita tavoitteiden saavuttamiseksi. Yrityksen tulee olla myös sitoutunut siihen, että se huolehtii työntekijöidensä koulutuksesta ja kyvykkyydestä. Työntekijöiden ja johdon tavoitteiden tulee kulkea linjassa, jotta tavoitteet voidaan oikeasti saavuttaa. Valvontaympäristön tehtävänä voidaan nähdä myös tilivelvollisuuden valvominen ja ylläpitäminen. (COSO 2013, 6)

Uusien pääperiaatteiden mukaisesti riskien arviointi tulisi liittää yrityksen tavoitteisiin. Riskejä tulisi arvioida ja analysoida kokonaisvaltaisesti tavoitteet silmällä pitäen. Periaatteiden mukaisesti johdon tulisi kiinnittää erityistä huomiota väärinkäytösriskin arvioimiseen. Johdon tulee huomioida järjestelmän luomisessa myös jatkuva muutos ja muutostarpeet, jotka asettavat uusia vaatimuksia yrityksen sisäisen valvonnan järjestelmille. (COSO 2013,7)

Kontrollitoimintojen pääperiaatteet liittyvät kontrollitoimintojen järjestämiseen ja huomioimiseen sisäisen valvonnan järjestämisessä. Yrityksen on valittava tarvittavat kontrollitoimenpiteet, jotta se voi välttyä mahdollisilta riskien tuottamilta vahingoilta. Kontrollitoimintoihin liittyy myös tarvittavien poliitikkojen, toimintamallien ja ohjeiden luominen. Tieto ja viestintä komponentti pitää pääperiaatteiden mukaisesti sisällään laadukkaan tiedon hyväksikäyttämisen, mikä on olennaista laadukkaan sisäisen valvonnan järjestelmän tukemisessa. Valvontajärjestelmä edellyttää kommunikaatiota

niin yrityksen sisällä kuin myös ulkona. Valvontaan liittyvien pääperiaatteiden mukaan yrityksen tulee suorittaa jatkuvaa seurantaa ja arviointia, mutta tehtävä myös erillisiä laajempia arviointeja onnistumisesta. Puutteiden monipuolinen arviointi ja oikea-aikainen kommunikointiprosessi ovat tärkeitä sisäisen valvonnan toimivuuden turvaamiseksi. (COSO 2013,7)

Kuva 3. Uudistuneen COSO-mallin 17 pääperiaatetta. (COSO 2013)



COSO-ERM-viitekehikko on laajentanut alkuperäistä COSO-IC mallia ja nostanut riskienhallinnan keskeiseksi elementiksi. ERM-viitekehikon riskienhallintaprosessi muodostuu sisäisestä ympäristöstä, tavoitteenasettelusta, tapahtumien tunnistamisesta, riskienarvioinnista, riskeihin vastaamisesta, kontrollitoiminnoista, tiedosta ja viestinnästä sekä jatkuvasta seurannasta. (Moeller, 2007) Vuoden 2013 COSO-IC mallia koskevat päivitykset ja pääperiaatteet soveltuvat mielestäni myös ERM-mallin osatekijöihin, jotka ovat samoja kuin alkuperäisessä COSO-IC mallissa.

Koska IC-kehikko on ennen kaikkea sisäisen valvonnan perusmalli, eikä tuo riskienhallintaa ERM-malliin verrattuna laajasti esille, on mielestäni mielekkäämpää soveltaa ja käyttää ERM-kehikon mukaista riskienhallintaprosessia. Moeller (2007) toteaa, että ERM-kehikon mukaista riskienhallintaprosessia on mahdollista soveltaa ja käyttää kaikissa organisaatioissa, joilla vain on tavoitteellista toimintaa niin julkisella kuin myös yksityisellä sektorilla. Moellerin (2007) ajattelun mukaan pienten ja keskisuurten yhtiöiden riskienhallinta voikin siis perustua ERM-viitekehikon mukaiseen riskienhallintaprosessiin, tai ainakin mallin mukaista riskienhallintaa voi hyödyntää pk-yrityksissä soveltuvin osin.

Kokonaisvaltainen riskienhallinta (ERM) voidaan nähdä ennen kaikkea systemaattisena prosessina (Ilmonen ym. 2010, 93). Prosessin aikana yritys asettaa tavoitteensa, tunnistaa sekä ulkoisia että sisäisiä tapahtumia, arvioi riskejä, vastaa riskeihin, perustaa ja päivittää kontrollitoimenpiteitä, raportoi ja kommunikoi riskeistä ja seuraa riskienhallintaa jatkuvasti.

The Committee of Sponsoring Organizations of the Treadway Comission on julkaissut alkuperäisestä ERM-mallista tiivistelmän (2004), jonka mukaan riskienhallintaprosessin perusta on vahva sisäinen valvontaympäristö, eli organisaation asenteet ja toimintakulttuuri vaikuttavat koko riskienhallintaprosessin toteutumiseen. Valvontaympäristöä voi siis luonnehtia koko prosessin lähtökohdaksi ja moottoriksi. Jos yrityksen valvontaympäristö on sellainen, ettei se ole kiinnostunut riskienhallinnasta ja sillä on negatiivinen asenne prosessiin, yritys tuskin edes tunnistaa tai arvioi riskejä. Jos taas yrityksen johdolla ja koko henkilöstöllä on myönteinen suhtautuminen prosessiin, yritys luultavammin myös käyttää tehokasta ja monipuolista riskienhallintamenettelyä.

Jos organisaatiossa halutaan noudattaa ERM-mallin mukaista riskienhallintaprosessia, organisaatiossa on laadittava ensin tavoitteet. Organisaatiolla on oltava tarkoitus, joka osakeyhtiöissä yleensä on voiton tuottaminen osakkeenomistajille. Tarkoituksen löytymisen jälkeen, organisaatiossa on perustettava sarja strategisia tavoitteita, jotka kattavat organisaation raportoinnin, operaatiot ja lainkuuliaisuuden. Organisaation tavoitteiden toteutumiseen vaikuttavat ulkoiset tai sisäiset tapahtumat on tunnistettava. Tapahtumat voivat olla muun muassa taloudellisia tapahtumia tai luonnontapahtumia, esimerkiksi tulvia tai maanjäristyksiä. (Moeller 2007, 60–70; ks. myös COSO-ERM 2004, 3)

Riskien tunnistaminen ja arviointi on mallin keskiössä ja aina riskienhallinnan perus elementti. Moellerin (2007, 73) mukaan riskienarvioinnissa on tärkeää arvioida riskejä, jotka voivat vaikuttaa organisaation tavoitteiden saavuttamiseen. Näitä riskejä tulisi arvioida kahden tekijän perusteella, jotka ovat riskin *todennäköisyys ja vaikuttavuus*. Todennäköisyydellä tarkoitetaan mahdollisuutta riskin tapahtumiselle. Toteutuneen riskin vaikutukset voivat olla merkittäviä organisaation toiminnan kannalta. Organisaatio voi arvioida niin vaikutuksia kuin myös riskin todennäköisyyttä kvantitatiivisten analyysien avulla. Analyysissa riskin merkittävyyttä arvioidaan sen todennäköisyyden ja vaikutusten avulla. Riskit voidaan luokitella muun muassa numeroin, tai ne on myös mahdollista luokitella sanallisesti korkeisiin, keskitasoisiin ja mataliin riskeihin. (Moeller 2007, 74–75) Moeller toteaa myös, että riskien arvioinnissa voidaan käyttää molempia eli kvalitatiivisia että kvantitatiivisia menetelmiä yhtä aikaa.

Kun riskit on arvioitu niin todennäköisyyden ja vaikutusten avulla, johdon on mahdollista arvioida, miten se hallitsee riskejä ja miten se vastaa niihin. Keinoja ovat riskin välttäminen, hyväksyminen, jakaminen tai vähentäminen. Valvontatoimenpiteet luodaan sitä varten, että organisaatiossa voidaan varmistua siitä että riskeihin vastataan organisaatiossa tehokkaasti. Tarvittavan tiedon on kuljettava vaivattomasti eli organisaatiossa on oltava vahva viestintäjärjestelmä. Tarvittava tieto poimitaan, tunnistetaan ja viestitään organisaation sisällä mahdollisimman nopeasti. ERM-mallissa organisaation joka tasolla on seurattava riskienhallintaprosessia jatkuvasti ja prosessia tulee myös päivittää. Johdon on siis tehtävä tarpeellisia muutoksia riskienhallintaprosessiin. (COSO-ERM 2004, 4; Moeller 2007, 77–93)

Vaikka ERM on maailmanlaajuinen kokonaisvaltainen riskienhallinnan malli, siitä on tehty myös sovelluksia. KPMG on esimerkiksi luonut oman ERM-mallinsa, joka on strategialähtöinen. Malli on tehty alkuperäisen riskienhallinnan mallin pohjalta ja se eroaa pienin osin alkuperäisestä. Mallissa ydin on liiketoimintastrategia, joka liittää riskienhallinnan yrityksen toimintaan ja päätöksentekoon. Riskienhallinta liitetään siis osaksi yrityksen toiminnallisia tavoitteita ja strategioita. Mallissa kiinnitetään huomiota merkittävimpiin riskeihin, ja kaikki ovat vastuussa riskienhallintaprosessista ja sen onnistumisesta. Malli edellyttää organisaation johdon sitoutumista riskienhallintaprosessin toteutumiseen.(Alftan 2008, 87–89)

3.7 Riskienhallinta pk-yrityksissä ja mallien soveltaminen

Pk-yritysten kohdalla on olennaista tarkastella, voidaanko ERM-mallin mukaista riskienhallintaa todellisuudessa edes soveltaa pk-yrityksissä, tai onko se kuitenkaan kannattavaa? Jos yrityksessä halutaan noudattaa voimassa olevaa lainsäädäntöä, säännöksiä, suosituksia ja eettisiä vaatimuksia, sillä tulisi olla halu suojautua mahdollisilta riskeiltä ja yrityksellä olisi myös myönteinen ote riskienhallintaan. Voidaan ajatella myös, että riskienhallinta osana sisäistä valvontaa on nykypäivän liiketoimintaa ja välttämätöntä. Voihan kuitenkin olla, että vaikka yrityksessä haluttaisiin noudattaa tehokasta riskienhallintaa, ei varsinkaan pienessä yrityksessä välttämättä ole resursseja eli aikaa tai rahaa toteuttaa riskienhallintaprosessia.

Ensinnäkin Moellerin (2007) mukaan ERM auttaa kaikkia organisaatioita pienimmästä suurimpaan riskienhallinnan ymmärtämisessä, riskienhallintaympäristön hallinnassa ja riskejä koskevassa päätöksenteossa. Tämän mukaan ERM-viitekehikkoa voidaan siis soveltaa myös pk-yritysten riskienhallinnassa. Tämä ei kuitenkaan vastaa kysymykseen, onko ERM- mallin soveltaminen pk-yrityksissä kannattavaa?

Erman ym. (2010, 48) mukaan listayhtiöiden sisäinen valvonta ja tarkastus tulee olla hyvin organisoitu, mutta sama pätee toisaalta myös pk-yrityksiin. Menettelyllä mahdollistetaan, että yrityksen toiminta ja informaatio on luotettavaa, säännöksiä ja toimintaperiaatteita noudatetaan ja toiminta on tehokasta ja tuloksellista. Listaamattomissa ja pienemmissä yrityksissä sisäinen valvonta ja riskienhallinta suhteutetaan yrityksen kokoon. Pienissä yrityksissä esimerkiksi kaikki taloushallinnon tehtävät voivat olla keskittyneitä yhdelle ihmiselle, jolloin tarvitaan hyvin toimiva raportointijärjestelmä. Hyvällä ja toimivalla raportointijärjestelmällä on mahdollista parantaa riskienhallintaa. (Erma ym. 2010, 48–49) Pk-yritysten riskienhallintaa on mahdollista siis toteuttaa suhteessa yhtiön kokoon, mutta yhtiössä tulisi olla joka tapauksessa hyvä tiedonkulku ja kommunikointijärjestelmä.

Ilmosen ym. (2010, 43) mukaan yrityksen tavoitteet vaikuttavat ennen kaikkea siihen millä tavoin riskejä yhtiössä käsitellään. Riskienhallinnan menettelytavat tulisi pitää riittävän yksinkertaisina ja selkeinä, jottei yhtiön todellinen tarkoitus ja tehtävät unohdu. Riskienhallinnan teorioilla ja menettelyillä on ennen kaikkea välineellinen arvo, ja monimutkaisista teorioista seuraakin usein se, että koko riskienhallinta ja

riskienhallintaprosessi alkaa tuntua organisaatiossa taakalta. Tuolloin yhtiössä ei enää nähdä riskienhallinnan tuottamia hyötyjä ja etuja. Riskienhallintaa ei tulisi jättää irralliseksi vaan, menettely tulisi viedä yrityksen päivittäisiin prosesseihin ja päätöksentekoon. Riskienhallinnan roolit ja vastuut tulisi olla yhtiössä selkeitä. (Ilmonen ym. 2010, 43–44)

Suominen (2003, 97) taas toteaa, että suurissa yrityksissä riskienhallinta on mahdollista erottaa muusta taloushallinnosta, jos toiminta on erikoisluonteista tai riskienhallinnan menettelytavat sitä edellyttävät. Pienissä yrityksissä sen sijaan ei tarvita erillistä riskienhallintatoimintoa vaan asiat tulisi hoitaa muiden tehtävien ja päivittäisten toimintojen yhteydessä. Riskienhallintaa ei tuolloin erikseen korosteta yrityksessä. (Suominen 2003, 97)

Sutinen & Antikainen (1996, 272–283) esittelevät pk-yritysten riskienhallinnan vaiheita. Heidän mukaansa pk-yritysten tulee varautua vahinkoriskien ja liikeriskien varalta. Heidän mukaansa yrityksen tulisi kartoittaa riskit, arvioida taloudellisia seuraamuksia ja valita sopivat riskienhallintakeinot. Prosessi muistuttaa mielestäni perinteisiä riskienhallinnan elementtejä eli riskiarviointi, riskianalyysia ja kontrollitoimenpiteitä, jotka ovat sovellettavissa myös pk-yrityksien riskienhallintaa.

Kupi, Keränen ja Lanne (2009, 48–49) esittävät tutkimuksessaan, jossa selvitettiin riskienhallinnan yhteyksiä toiminnan ohjaukseen ja johtamiseen, että riskienhallinta on kiinteä osa pk-yrityksen johdon päivittäisiä toimintoja, mutta sen vaiheita on lähes mahdotonta erotella. Tutkimuksessa todetaan, että riskienhallinta tulisi integroida osaksi yrityksen strategiaa ja yhteisössä tulisi luoda riskit tiedostavaa kulttuuria. Tutkimuksen mukaan täysin epämuodollisen riskienhallinnan laatua ja laajuutta on kuitenkin vaikea arvioida. Riskienhallinnan tulisikin olla kiinteä osa johtamista, budjetointia ja suunnittelua, mutta dokumentointi ja prosessikuvauksien ja vastuiden määrittäminen on myös tärkeää. Tutkimuksen johtopäätöksenä myös todetaan, että hyvin hoidettu ja järjestelmällinen riskienhallinta tuo lisäarvoa ja jopa kilpailuetua pk-yritykselle (Kupi ym. 2009, 49).

Alftan ym. (2008, 84) toteavat, että yrityksen ylin johto on vastuussa toimivasta riskienhallinnan järjestämisestä ja johtamisesta. Heidän mukaansa riskienhallinnasta vastaavien elinten tulee ohjata, koordinoida, valvoa sekä seurata toimintaa. Julkaisussa todetaan, että riskienhallinnan vastuiden ja omistajuuksien määrittäminen tukee kattavaa

sisäistä valvontaa ja riskienhallintaa. Alftan ym. (2008, 84–85) toteavat myös julkaisussaan, että riskienhallinta on tehokkaimmillaan silloin kun se on liitetty osaksi tavanomaista, päivittäistä johtamista ja johtamisen prosesseja. Riskienhallinnan ottaminen osaksi strategiaa voi tarkoittaa käytännössä sitä, että epävarmuustekijöitä mietitään jo strategiaa valmisteltaessa. Alftan ym. (2008, 85) kuitenkin myöntävät, että riskienhallinnan integroiminen osaksi johtamista voi olla haastavaa ja siksi riskienhallinta voi usein jäädä irralliseksi kokonaisuudeksi.

Australian ja Uuden-Seelannin standardisointiorganisaatioiden laatimassa riskienhallinnan yleisessä standardissa AS/NZS 4360 (2004) todetaan, että riskienhallinta on tehokkainta, jos se on liitetty osaksi organisaatiokulttuuria. Standardin mukaan riskienhallinta tulee olla integroituna organisaation filosofiaan, toimintoihin ja liiketoimintaan. Riskienhallinnan integroiminen toimintoihin mahdollistaa standardin mukaan myös sen, että jokainen organisaatiossa ottaa vastuuta riskienhallinnasta. Standardin mukaan riskienhallinta täytyy nähdä osana johtamistoimintoa, hyvää johtamista ja hyvää hallinnointitapaa.

Standardissa todetaan, että se soveltuu monenlaisiin toimintoihin, päätöksentekoprosesseihin, kaikkiin yksityisen tai julkisen sektorin organisaatioihin ja yrityksiin pienimmästä suurimpaan. (Standards Australia/Standards New Zealand 2004,1)

CIPFAN (2001,35–43) mukaan riskienhallinta osana päivittäistä johtamista tuottaa hyötyjä kaikenkokoisille organisaatioille. Monipuoliset ja toimivat tiedonkulku- ja päätöksentekotoiminnot voivat vähentää vahinkoja ja haitallisia tapahtumia, mutta samalla auttaa yritystä sen mission täyttämisessä tai päämäärien saavuttamisessa. Riskienhallintaa toimii osana päivittäisiä rutiineja, jos hallintajärjestelmä on sidoksissa kaikkiin yrityksen toimintoihin ja kaikki yrityksen työntekijät ja johtoon kuuluvat ovat tietoisia riskienhallinnasta ja omasta osastaan riskienhallinnan edesauttamisessa. (CIPFA 2001, 35–43)

Williams ym.(1998,21–22) esittävät, että riskienhallinnan merkitys kaikenkokoisissa organisaatioissa on lisääntynyt. Heidän mukaansa riskienhallinnan perusta on kuitenkin muuttunut vakuutuslähtöisestä riskienhallinnasta kohti monipuolisempaa ja kattavampaa järjestelmää. He toteavat, että riskienhallintayksikön tai riskienhallinta managerin rooli

on sidoksissa yrityksen kokoon. Pienillä yrityksillä ei yleensä ole resursseja palkata kokoaikaista riskeistä vastaavaa manageria, työntekijää tai yksikköä.

Sen sijaan suuryrityksissä saattaa olla kokoaikainen riskienhallinnasta vastaava yksikkö tai henkilö. Suuryrityksillä on heidän mukaansa myös enemmän resursseja monipuolisten riskienhallintakeinojen käyttämiseen. Sen sijaan riskienhallinnan laatukysymys on heidän mukaansa epäselvä. Pienyrityksissä ei välttämättä olekaan vaikeaselkoisia riskienhallintakehikkoja ja kokoaikaisia riskienhallinnan toimijoita, mutta yrityksessä saatetaan silti toteuttaa edistynyttä ja laadukasta riskienhallintamenettelyä. Pienissä yrityksissä riskienhallinta voi olla sidottu päivittäisiin johtamistapoihin ja menettelyihin, mikä saa aikaan positiivisen ja laadukkaan riskienhallintaprosessin. Sen sijaan suuryrityksissä riskienhallinnasta saattaa vastata riskienhallintaan palkattu erityinen henkilö tai yksikkö, jonka liiketaloudellinen ja tekninen osaaminen on kuitenkin heikkolaatuista. (Williams ym. (1998, 21)

Pk-yritysten riskienhallintastrategian ja viitekehikon soveltaminen ei siis aina ole systemaattista, mutta sen ei välttämättä tarvitsekaan olla. Pk-yrityksen ei välttämättä kannata tuhlata tuhansia euroja ja luoda raskaita riskienhallinnan lähestymistapoja. Valvontajärjestelmän valinnassa tulisi ensisijaisesti huomioida yrityksen koko ja sen tarpeet. Yrityksen tulisikin valita sellainen riskienhallinnan viitekehys tai työväline, joka vastaa sen riskienhallinnan tarpeita. Myös pienten yritysten tulisi kuitenkin olla kiinnostuneita riskienhallinnasta, koska sen avulla yritys voi pienentää väärinkäytösriskiä ja luoda yhteisöön varmuutta. Oli yritys miten pieni tahansa, hyvin järjestetty valvontaprosessi auttaa muun muassa kavallusten havaitsemisessa, väärinkäytösten ehkäisemisessä ja täsmällisen taloudellisen tiedon saannissa. Ennen kaikkea yrityksen johdolla tulisi olla ymmärrys riskienhallinnan viitekehikoista ja niiden hyödyistä. (Ahokas 2013, 53–55)

Yrityksen riskienhallinta edellyttää sen johdolta myös eettistä johtamistapaa, filosofiaa sekä kontrollien luomista. Monet pk-yritykset ovat ulkoistaneet taloushallintonsa tilitoimistolle, eikä yrityksen johto välttämättä ole yhteydessä tilitoimistoon ja kirjanpitäjään kuin ongelmatilanteissa. Riskienhallinnan kannalta myös pienten yritysten tulisi olla kiinnostuneita taloudestaan. Yrityksen johdon tulisikin hankkia tarvittaessa taloudellista osaamista ja käydä lävitse yrityksen raportteja ja tunnuslukua.

Johdon tulisi olla kiinnostunut yrityksen taloutta koskevista asioista, jotta yrityksessä vältyttäisiin ikäviltä taloutta koskevilta yllätyksiltä. (Ahokas 2013, 53–55)

Johdon tehtävä on myös viestiä henkilöstölle valvontaa koskevista ohjeista ja menettelytavoista. Johdon asennoituminen valvontaprosessiin määrittelee koko organisaation sitoutumisen valvontaan. Pientenkin yritysten olisi hyvä tehdä kirjalliset toimintaohjeet yrityksen valvonnasta. Yrityksessä on kuitenkin varmistettava, että kaikki organisaation kuuluvat ymmärtävät toimintaohjeet ja niiden merkityksen. Pienissä yhtiöissä tulisi kiinnittää huomiota tietojärjestelmiin liittyviin kontrolleihin, muun muassa käyttöoikeuksiin ja järjestelmien käyttöoikeuksiin. Yrityksen tulisi huomioida myös salasanat, asiakirjojen ja dokumenttien säilytys, ovien lukitseminen, turvajärjestelmät, vakuutukset, salasanat, palomuurit, valvontakamerat ja monet muut kontrollit toiminnassaan. Hyvin usein varsinkin käyttöoikeuksia koskevissa kontrolleissa on puutteita. Pienessä yrityksessä tehtävien eriyttäminenkin on tärkeää, vaikka yrityksessä ei olisi kuin muutama henkilö. (Ahokas 2013,53–55)

Sisäiset tarkastajat ry:n julkaisemassa COCO-mallia koskevassa valvontakriteerioppaassa (1999) todetaan, että CICA:n julkaisemaa Guidance on Criteria of Control- opasta, joka esittelee COCO-mallin pääperiaatteet, on mahdollista soveltaa kaikenlaisiin organisaatioihin tai jopa niiden osiin. COCO-mallin soveltaminen pk-yrityksien riskienhallinnassa olisi siis tämän mukaan mahdollista. Valvontakriteerioppaassa huomioidaan kuitenkin myös se, että mikään valvontakehikko ei sovellu suoraan mihinkään organisaatioon, vaan ohjeita tulisi tulkita ja soveltaa joustavasti. Oppaan mukaan jokaisen yrityksen on itse luotava sellainen valvontakehikko, joka vastaa parhaiten sen olosuhteita, tai yritys voi myös yhdistellä erilaisia valvontakehikoita. Yrityksen ei siis suinkaan tarvitse luopua omista valvontakäsitteistään, vaan se voi poimia erilaisista malleista niiden hyödylliset puolet. (Sisäiset tarkastajat ry 1999,7)

Riskienhallinnan merkitys organisaatioiden menestyksen kannalta on siis suuri ja sen vuoksi on kehitelty riskienhallinnan tueksi joukko välineitä, työkaluja, käsitteitä ja laajoja viitekehyksiä. Mielenkiintoinen kysymys onkin, kannattaako yrityksen sitoutua vain yhden standardin käyttämiseen? Ylimmän johdon tulisi riittävän arvioinnin perusteella valita itselleen sopivin strategia riskienhallinnan toteuttamiseen. Strategian tulisi olla yrityksen mahdollista menestystä tukeva viitekehikko. Yhtenä

lähestymistapana voidaan käyttää organisaatiosta saatua kokemusta. Yrityksessä voidaan valita sellainen riskienhallintamalli, joka vastaa organisaation tarpeita kustannustehokkaasti. Mallin tulisi samalla kuitenkin varmistaa, että organisaatiota pakollisesti koskevaa sääntelyä noudatetaan. (Veijola 2012,27–28)

Yrityksen on mahdollista sitoutua parhaaksi koettuun standardiin, jotta se ei luopuisi hyvistä käytännöistä. Standardin valinnassa tulee huomioida myös sidosryhmien tarpeet. On olennaista, että monipuolinen ja julkisesti tunnettu viitekehikko antaa sidosryhmille sellaista informaatiota, jota sidosryhmien on helppo arvioida olemassa olevien arviointikriteerien perusteella. Standardin valinnassa tulisi myös huomioida sen käyttäjät ja sen kehittämisestä vastaavat tahot. On siis huomioitava, mitkä ovat taustavoimien intressit sekä millainen on viitekehyksen hallinnointimalli. Monimutkainen riskienhallintastandardi saattaa nopeasti kasvattaa asiantuntijatarvetta ja samalla riskienhallinnan kustannuksia. Paras pk-yrityksen riskienhallintastandardi näyttäisi olevan viitekehys tai työväline, joka kulkee linjassa yrityksen johtamisjärjestelmän kanssa. Malli tulisi valita selkein perustein ja riittävän arvioinnin perusteella yrityksen ylimmässä johdossa. (Veijola 2012, 27–28)

Nämä ajatukset ja tulokset vahvistavat näkemystäni siitä, että riskienhallinta pk-yrityksissä voi olla epämuodollisempaa ja yksinkertaisempaa kuin suuryrityksissä sekä poiketa ERM-mallin mukaisesta riskienhallintaprosessista. Pienissä ja keskisuurissa yrityksissä riskienhallinta voisikin perustua klassisen riskienhallinnan elementeille, eli riskejä tunnistetaan, arvioidaan ja lopuksi niihin vastataan osana päivittäistä liiketoimintaa (Harington & Niehaus 2003, 8–9; Vaughn 1997, 34).

Ilmosen ym. (2010, 44) mukaan riskienhallinta ei ole henkilöresurssien kannalta kovin kallis osa-alue, jos sen menettelytavat on toteutettu yhtiössä käytännönläheisesti ja järkevästi ja jos voimavarat kohdennetaan niihin riskeihin, joiden merkitys on yrityksen tavoitteiden kannalta suurin. Pienissä ja keskisuurissa yrityksissä erityisen tärkeäksi elementiksi nousevat siis tarkoituksenmukaisuus ja tehokkuus.

Riskienhallinnan ei kuitenkaan tulisi olla täysin epämuodollista, vaan joka tapauksessa tarvitaan raportointia, määrittelyä ja dokumentointia (Kupi ym. 2009, 48–49). Williams ym. (1998, 53) toteavat myös, että tehokas raportointi ja kommunikointi koskien riskienhallintaprosessia ovat yksi tärkeimmistä riskienhallinnan elementeistä niin pienissä kuin myös suurissa organisaatioissa, koska kommunikoinnin avulla voidaan

vähentää yritystä uhkaavia epävarmuuksia. Riskienhallinta edellyttääkin perinteisten elementtien lisäksi aina tehokasta raportointia, mutta myös jatkuvaa seurantaa.

Vaikka ERM-mallin mukaista riskienhallintaa on mahdollista käyttää ja soveltaa pk-yrityksissä, riskienhallinnan menettelytavat kannattaisi ainakin pienissä yrityksissä pitää mahdollisimman selkeinä ja käytännönläheisiä sekä osana päivittäisiä rutiineja. Monimutkaisen teorian luominen ei ole kannattavaa ja hyödyllistä, jos teoria tuntuu pikemminkin taakalta kuin organisaatiota hyödyttävältä välineeltä. Riskienhallintaa tulisi siis hoitaa osana päivittäistä johtamista. Pk-yrityksissä riskienhallintaa ei kannata välttämättä irrottaa omaksi toiminnokseen, vaan erillisen riskienhallintatoiminnon tarve riippuukin yrityksen toiminnan luonteesta, laajuudesta, laadusta, riskeistä ja riskeihin liittyvistä tavoitteista (Alftan ym. 2008, 84). Erillinen riskienhallintatoiminto soveltuukin pääasiassa siis suuryrityksiin.

Kuten jo luvun aluksi totesin, Moellerin (2007) mukaan ERM-kehikko siis soveltuu kaikkiin yrityksiin aina pienimmästä suurimpaan. Yrityksissä on kuitenkin tehtävä yrityskohtaisia valintoja riskienhallinnassa, koska ERM-kehikon soveltamista ei voi pitää itsestään selvyytenä, vaikka Moeller (2007) antaakin näin ymmärtää. ERM-viitekehikon soveltaminen ei näyttäisi olevan kannattavaa ainakaan pienissä yhtiöissä. Riskienhallinnan toteuttamista onkin mahdollista miettiä suhteessa pk-yrityksen kokoon. Jos yritys on esimerkiksi mikroyritys, ei kannata soveltaa ERM-viitekehikon mukaista riskienhallintaa. Jos taas yritys on pieni tai keskisuuri, voi ERM-viitekehikon soveltaminen olla joissain tapauksissa hyödyllistä ja kannattavaa.

4 VALVONTAYMPÄRISTÖN MERKITYS RISKIENHALLINNASSA

4.1 Valvontaympäristö

Valvontaympäristössä on kyse siitä, miten organisaatio ja sen johto suhtautuvat riskeihin ja sisäiseen valvontaan kaikessa toiminnassaan. Itse asiassa valvontaympäristö on koko ERM-viitekehyksen perusta ja kivijalka. Sisäinen valvontaympäristö sisältää organisaation ilmapiirin ja se asettaa perustan sille, miten riskit nähdään koko yhteisössä. (Journal of Accountancy, 2008) ERM-mallista julkaistussa tiivistelmässä (2004, 3) todetaan, että valvontaympäristö ja sen ilmapiiri määrittävät myös sen, miten koko henkilöstö suhtautuu riskeihin ja riskienhallintaan organisaatiossa. Henkilöstö käsittelee riskejä ja toimii valvontaympäristön ilmapiirin ja asenteiden pohjalta. Valvontaympäristö vaikuttaa siis koko henkilökunnan toimintaan.

Sisäinen valvontaympäristö on nimenomaan COSO-mallin luoma käsite organisaation riskienhallinnan mallissa ja se on tärkeä osa niin COSO-IC-kehikkoa kuin myös COSO-ERM-kehikkoa. COSO-IC-viitekehikko on asettanut valvontaympäristön alimmalle tasolle, kun taas COSO-ERM-viitekehikossa sisäinen ympäristö on ylimpänä, muiden osatekijöiden päällä. Viitekehikot tarkastelevat organisaation valvontaympäristöä eri nimityksillä. COSO-IC kutsuu sitä sisäiseksi valvontaympäristöksi (Internal control environment), ja COSO-ERM-viitekehikossa sitä käsitellään sisäisenä ympäristönä (Internal environment). Molemmissa viitekehikoissa on kuitenkin sama ajatus siitä että, sisäinen valvontaympäristö luo perustan ja pohjan koko mallille ja muille riskienhallinnan vaiheille. (Moeller, 2007)

Valvontaympäristö koostuu monista toisiinsa linkittyvistä alueista. Näitä ovat riskienhallinta-ajattelu, johdon periaatteet, toimintatavat ja asenteet, rehellisyys ja eettiset arvot, henkilöstön pätevyys, organisaatiorakenne, valtuuksien ja velvollisuuksien jakaminen ja henkilöstöhallinnon menettelytavat (Moeller 2007; ks. myös Holopainen ym. 2006).

4.2 Johtamistapa ja valvontakulttuuri kirjallisuuskatsaus

Valvontaympäristö tarkoittaa pohjimmiltaan yrityksessä vallitsevaa johtamis- ja valvontakulttuuria ja luo perustan koko riskienhallintaprosessille sekä sisäisen valvonnan ja riskienhallinnan malleille. (Alftan ym. 2008, 38). Organisaation johdon esimerkit ja kommunikointi vaikuttavat olennaisesti siihen, miten organisaatiossa suhtaudutaan valvontaan ja rehellisyyteen. Organisaatiossa tulisikin siis olla selvä johdon viesti siitä, että yhteisössä toimitaan rehellisesti ja oikeudenmukaisesti. (CIPFA 2001, 31)

Sisäinen valvonta ilmentää pohjimmiltaan organisaation arvoja, periaatteita, rakenteita ja sen organisaatiokulttuuria kokonaisuutena. Eli sisäinen valvonta ilmentää organisaation valvontaympäristöä. Organisaatio, jossa toimitaan sisäisen valvonnan periaatteiden mukaisesti, päätökset tehdään myös hyvien periaatteiden mukaisesti. Valvontaympäristössä tulee puuttua kuitenkin myös epäkohtiin toiminnan tehostamiseksi. (Hightower 2009)

Yrityksen johtamistapa ja organisaatiokulttuuri antavat suunnan koko yrityksen toiminnalle. Näin ollen yrityksen valvontaympäristö vaikuttaa myös liiketoimintaan. Valvontaympäristö edellyttää ennen kaikkea järjestystä, sääntöjä ja rakenteita. Valvontaympäristöllä on suuri vaikutus siihen, miten koko yrityksen toiminta järjestetään, miten yritys asettaa tavoitteensa ja arvioi riskejä. Yrityksen johtamistapa ja valvontakulttuuri vaikuttavat myös siihen, miten yrityksen valvonta järjestetään, miten toimintaa seurataan ja miten yhteisössä kommunikoidaan.(Holopainen ym. 2010, 55) Kuten jo aikaisemmin totesin, valvontaympäristöä voidaan pitää koko riskienhallintaprosessin lähtökohtana ja moottorina, joka laukaisee prosessin.

Jos yrityksessä toimitaan vilpittömästi, ja yrityksen johto ja henkilöstö noudattaa voimassaolevaa lainsäädäntöä, eettisiä vaatimuksia, standardeja ja ohjeita, se luultavasti suhtautuu myös myönteisesti riskienhallintaan ja sen toteuttamiseen. Valvontaympäristön ja riskienhallinnan suhteen taustalla on *pyrkimys* noudattaa näitä vaatimuksia, eli yrityksen johdolla on halu toimia rehellisesti. Tämän pyrkimyksen vastakohtana voidaan nähdä yritys, jonka johto ja henkilöstö ovat alttiita väärinkäytöksille ja vilpilliseen toimintaan. Vilpillisessä yrityksessä ei ole edes halua toimia rehellisesti, noudattaa lainsäädäntöä tai voimassaolevia suosituksia. Koska

valvontaympäristö edellyttää rakenteita, sääntöjä ja lainmukaisuutta, mielestäni osakeyhtiön toimielinten lakisääteisten tehtävien toteutumisella on riskienhallinnan ja sisäisen valvonnan kannalta suuri rooli.

The chartered institute of public finance and accountancy:n (2001, 32) julkaisemassa teoksessa luetellaan valvontaympäristön keskeisiä ominaisuuksia, joista valvontaympäristö ja sen elementit koostuvat. Ominaisuuksien tarkoitus on selventää, mistä riskienhallinnan valvontaympäristöön kuuluu. Näitä ominaisuuksia ovat muun muassa johdon asettama ilmapiiri organisaatiossa, henkilöstön menettelytavat ja politiikat, henkilöstön tiedot ja kokemus, johdon tasapainoisuus, organisaatiokulttuuri, selkeästi määritellyt tehtävät, asenteet, organisaation moraali, tehtävien hajauttaminen, suunnittelu, valvonta, seurantamenetelmät, vahva ja laadukas sisäinen tarkastus ja tilintarkastus, ulkoiset lainsäädännön vaatimukset ja eettisten arvojen sekä oikeudenmukaisuuden viestintä henkilöstölle.

Teos nostaa esille myös johtamisen tärkeyden ja tehtävien suunnittelun, asettamisen ja organisoinnin merkityksen riskienhallinnan onnistumisessa. Valvontaympäristön valvonnan kannalta keskeistä on myös johtaminen ja johtajan ominaisuudet. Riskienhallintaan vaikuttaa olennaisesti se, miten organisaation ylin johto, eli yleensä hallitus ja toimitusjohtaja koordinoivat töitä ja tehtäviä. Valvontaympäristö voi olla erilainen sellaisessa organisaatiossa, jossa tehtäviä on hajautettu ja niistä vastaavat useammat tahot. Toisaalta teos ei puolla tai kiellä myöskään yksinjohtamista. (CIPFA 2001, 32)

CIPFAN (2001,3 2-33) julkaisun mukaan valvontaympäristö muodostaa perustan sisäiselle valvonnalle ja riskienhallinnan määrittelylle. Julkaisussa todetaan, että sisäisen valvonnan järjestäminen auttaa organisaatiota sen rakenteiden, tavoitteiden ja tehtävien määrittelyssä. Julkaisussa painotetaan myös johdon esimerkin tärkeyttä koko organisaation kannalta. Johto ja johdon asenne vaikuttavatkin suoraan henkilöstön suhtautumiseen riskienhallintaa kohtaan. Nämä valvontaympäristön ominaisuudet ovat mielestäni tiukasti yhteydessä Moellerin (2007) luokittelemiin ERM-mallin osatekijöihin.

Valvontaympäristöä voidaan mielestäni myös verrata yrityksen kontekstiin ja sen rakenteisiin. Sisäistä valvontaa ja riskienhallintaa voidaan tarkastella myös kontingenssiteorian kannalta. Teorian ajatus on, että yhteisön prosessien ja toimintojen

on sovelluttava organisaation konteksteihin. Jotta yritys voisi menestyä, täytyy yrityksen toimintojen siis soveltua yrityksen kontekstiin tai valvontaympäristöön. (Jokipii, 2006) Tässä tutkielmassa luvussa 3.5.2 käsiteltiin AS/NZS 4360 standardia, jonka mukaan riskienhallintaprosessin ensimmäinen vaihe on yrityksen kontekstin luominen ja sen hahmottaminen. Yrityksen kontekstihan muodostuu standardin mukaan ulkoisesta ja sisäisestä ympäristöstä ja niihin liittyvistä osatekijöistä. Tämä konteksti muodostaa mielestäni myös perustan yrityksen valvontaympäristölle. Kontekstin eli valvontaympäristön ulkoisia tekijöitä ovat standardin mukaan, esimerkiksi lainsäädännölliset velvoitteet, ohjeet, suositukset ja viitekehikot. Ulkoinen konteksti muodostuu myös rahoittajien vaatimuksista, viranomaisten ohjeista sekä muista ulkoisista pakotteista. Sisäinen konteksti sen sijaan muodostuu yrityksen omasta organisaatiokulttuurista, periaatteista ja ohjeista. Sisäinen konteksti antaa siis yrityksen johdolle tilaa päättää yrityksen valvontaympäristön luomisesta.

Yrityksen johto siis viime kädessä määrää, miten yrityksessä suhtaudutaan ulkoisiin velvoitteisiin, eli esimerkiksi lainsäädäntöön ja viranomaisten määräyksiin. Valvontaympäristö muodostuu siis ulkoisesta ympäristöstä, joka asettaa ehdot yrityksen toiminnalle sekä sisäisestä ”vaihtoehtoisesta” ympäristöstä. Se millaisen sisäisen kontekstin yrityksen johto muodostaa, voi vaikuttaa suoraan riskienhallinnan toteuttamiseen yrityksessä.

4.3 Valvontaympäristön osatekijät ERM-mallissa

Moeller (2007, 54–57) luokittelee ERM-mallin sisäisen valvontaympäristön osatekijöiksi *riskienhallintafilosofian, riskinottohalukkuuden, johdon asenteet, rehellisyyden ja eettiset arvot, pätevyyteen sitoutumisen, organisaatiorakenteen, vastuiden ja velvollisuuksien jakamisen ja henkilöstöhallinnon menettelytavat.* IC-mallin valvontaympäristön osatekijät poikkeavat ERM-mallin osatekijöistä vain pienin osin. Periaatteet molemmissa malleissa ovat kuitenkin samat. Valvontaympäristön osatekijät ovat sellaisenaan sovellettavissa pk-yritysten valvontaympäristöön, mutta elementtejä tulee arvioida kuitenkin jokaisen yrityksen kohdalla erikseen ja tapauskohtaisesti.

Riskienhallintafilosofia on valvontaympäristön keskeinen elementti. Moellerin (2007, 54) mukaan riskienhallintafilosofia sisältää asenteita ja uskomuksia, jotka vaikuttavat

organisaatiossa siihen, miten se suhtautuu riskeihin kaikessa mitä se tekee. Riskinottohalukkuus taas kertoo sen riskien määrän, jonka organisaatio on valmis hyväksymään. Johdon asenteilla on valvontaympäristössä suuri asema, koska yrityksen johto ohjaa ja johtaa yritystä ja näin ollen vaikuttaa suoraan myös henkilöstön asenteisiin. Jos yrityksen johdolla on negatiivinen asenne riskeihin, asenne välittyy myös helposti organisaation muille tasoille. Rehellisyys, oikeudenmukaisuus ja eettiset arvot tarkoittavat paljon muutakin kuin kirjoitettuja sääntöjä. Rehellisyyteen ja eettisiin arvoihin liittyy vahva ohjaus ja tunne siitä, miten yrityksessä tulisi toimia ja käyttäytyä. Yrityksessä tulisi olla myös vahva yhteistoiminnan ja oikeudenmukaisuuden tunne. (Moeller 2007, 54–55)

Pätevyys ja siihen sitoutuminen tarkoittaa sitä, että yrityksessä on tarpeellinen määrä tietoa ja taitoa, jotta yrityksessä voidaan suorittaa toimintaan liittyvät tehtävät. Yrityksessä tulisi olla ammattitaitoa, ja ammattitaitoisten ihmisten tulisi hoitaa vaativia ja strategisia tehtäviä. Organisaatiokulttuuri on yksi valvontaympäristön tärkeimmistä elementeistä ja on kiinteästi yhteydessä myös velvollisuuksien ja vastuiden jakamiseen. Organisaatiokulttuurissa onkin kyse siitä, miten organisaatiota johdetaan, ja miten vastuut ja velvollisuudet organisaatiossa jakaantuvat. (Moeller 2007, 56–57)

Henkilöstöhallinnon menettelytavoilla sen sijaan tarkoitetaan kaikkia henkilöstöön liittyviä toimenpiteitä. Työntekijöiden palkkaaminen, perehdytys, kannustaminen, ylentäminen, palkitseminen kurinpito ja muut henkilöstöön liittyvät toimet ovat menettelyjä, jotka väistämättä kertovat henkilöstölle siitä, mikä yrityksessä on sallittua, suositeltavaa, siedettyä ja kiellettyä. Henkilöstöhallinnon osalta organisaatiossa tulisikin olla vahvat standardit ja selkeät ohjeet siitä miten missäkin tilanteessa toimitaan. (Moeller 2007, 56–57)

4.4 Valvontaympäristön elementit riskienhallinnan toteuttamisessa

Tässä osiossa sovellan aikaisemman kappaleen valvontaympäristön osatekijöitä pk-yrityksen valvontaympäristöön riskienhallinnan toteuttamisen kannalta. Jos pk-yritys toimii rehellisesti, noudattaa lainsäädäntöä, suosituksia ja sillä on siis myönteinen ote ja asenne riskienhallintaan, yrityksen riskienhallintafilosofia muodostuu myönteisistä asenteista ja uskomuksista, jotka liittyvät riskienhallintaan. Valvontaympäristö voi siis olla positiivinen ja edesauttaa riskienhallinnan toteuttamisessa. Jos johdon asenteet

riskienhallintaan ovat myönteiset, se heijastuu organisaatiossa koko henkilöstöön. (COSO, 2004; ks. myös Moeller 2007)

Yrityksessä on tällöin etusijalla rehelliset arvot, oikeudenmukaisuus ja vahva yhteistoiminnan kulttuuri. Pk-yrityksessä on tällöin myös vahvat käyttäytymisen standardit ja ohjeet, jotka auttavat yritystä tekemään riskeihin liittyviä päätöksiä. Yrityksessä ollaan myös sitoutuneita pätevyyteen, ja ammattitaitoiset ihmiset hoitavat strategisia ja vaativia tehtäviä. Yrityksen organisaatiokulttuuri on vahva, ja velvollisuuksien ja vastuiden jako on yrityksessä hoidettu selkeästi. Henkilöstöhallinnon osalta yrityksessä on vahvat standardit ja ohjeet. Valvontaympäristössä on siis kaiken kaikkiaan selkeät rakenteet, määräykset, ohjeet ja säännöt. Valvontaympäristö muodostuu kokonaisuutena positiivisesta ilmapiiristä, jolla on myönteinen asenne pk-yrityksen riskienhallintaan.

4.5 Osakeyhtiön johto osana valvontaympäristöä

Osakeyhtiön johdon toimielinten voidaan katsoa olevan jopa tärkeimmässä osassa yhtiön riskienhallinnassa, koska yhtiön valvontaympäristön ilmapiiri eli johdon asenteet, eettisyys ja riskienhallinta-ajattelu vaikuttavat kokonaisuutena yhtiön riskienhallintaprosessiin ja sen onnistumiseen (Moeller 2007; ks. myös COSO-ERM tiivistelmä 2004). Osakeyhtiölaissa määrätään, että osakeyhtiöllä on oltava hallitus ja sillä voi olla myös toimitusjohtaja ja hallintoneuvosto (OYL 6:1). Kun siis puhutaan osakeyhtiön johdosta, tarkoitetaan osakeyhtiölaissa säädettyä hallitusta, toimitusjohtajaa ja hallintoneuvostoa. Hallitus on kuitenkin ainoa osakeyhtiön pakollinen toimielin. Jokainen yhtiö voi siis päättää, nimittääkö se toimitusjohtajan tai ottaako se käyttöön hallintoneuvoston. Pienissä yhtiöissä on mahdollista olla hallitus, jossa on vain yksi jäsen, joka useimmiten on myös koko yhtiön omistaja. Samainen henkilö on mahdollista nimittää myös yhtiön toimitusjohtajaksi, vaikka sitä ei tarvittaisikaan. (Norri 2006, 264) Mikroyrityksissä eli muutaman omistajan yrityksissä tämänkaltainen järjestely onkin usein mahdollista, mutta ei suinkaan välttämättä kannattavaa.

Ei ole olemassa mitään lakisääteistä estettä sille, että hallituksen jäsen ei voisi olla samalla yhtiön toimitusjohtaja tai toisin päin. Erman ym. (2010, 37) mukaan pienissä yhtiöissä usein ajatellaan, että toimitusjohtajan tulee automaattisesti olla mukana hallituksessa. Erma ym. (2010, 37) kuitenkin toteavat, että tämä asetelma voidaan

kyseenalaistaa ja miettiä miksi toimitusjohtajan ylipäätään pitäisi olla hallituksen rivijäsen. Erman ym. (2010, 37) mukaan hyvä hallinnointitapa ei suosittele tämänkaltaista roolikumulaatiota, koska vastuunjaon ja valvonnan tulisi olla toimivaa ja selkeää osapuolten välillä.

Pienissä ja keskisuurissa yrityksissä hallituksen ja toimitusjohtajan roolit tulisi siis erottaa, jotta valvontaympäristö olisi paras mahdollinen ja mahdollistaisi tehokkaan ja toimivan johtamistavan ja valvontakulttuurin. On kuitenkin huomattava, että muutaman tai pari omistajan mikroyrityksissä roolit ja vastuut voivat mennä väistämättä päällekkäin. Riskienhallinnan toteuttamisen kannalta pk-yrityksessä tulisi kuitenkin olla halu noudattaa suosituksia, järjestää johtonsa parhaalla mahdollisella tavalla sekä estää roolikumulaatiot. Moeller (2007, 13–14) toteaa myös, että vastuiden ja velvollisuuksien jakaminen on tärkeä osa valvontaympäristöä, eikä yhden ihmisen vastuulla saisi olla liikaa tehtäviä, vaan tehtävät tulisi sen sijaan jakaa useamman ihmisen kesken. Yrityksen taloushallinnon ei esimerkiksi tulisi koskaan olla pelkästään yhden ihmisen vastuulla. Jos tämänkaltainen järjestely on kuitenkin käytössä pk-yrityksessä, tulisi yrityksessä olla kattava ja tehokas raportointijärjestelmä.

Tässä tutkimuksessa olen kiinnostunut nimenomaan osakeyhtiön lakisääteisistä tehtävistä sekä muista tarkoituksenmukaisista tehtävistä, jotka voidaan mieltää myös osaksi organisaation valvontaympäristöä. Keskeistä onkin huomata, noudattaako yhtiö voimassaolevaa lainsäädäntöä ja suosituksia. Seuraavassa osiossa käsittelen aluksi hyvää hallintotapaa, ja sen jälkeen esittelen osakeyhtiön toimielinten eli hallituksen, toimitusjohtajan, ja hallintoneuvoston lakisääteiset tehtävät sekä muita oleellisia tarkoituksenmukaisuuteen perustuvia tehtäviä riskienhallinnan toteuttamisen kannalta.

4.6 Corporate Governance pk-yrityksissä

Corporate governancea voidaan pitää yritysmaailmassa keskeisenä johtamisen ja hallinnointitavan ohjenuorana sekä käyttäytymissääntönä, joka on lähinnä tarkoitettu julkisesti noteeratuille pörssiyhtiöille. Corporate governance voidaan suomentaa hyväksi hallintotavaksi, hyväksi hallinnointitavaksi tai omistajaohjaukseksi, mutta toisinaan sitä kutsutaan vain myös termillä ”corporate governance”. Corporate governacen alkuperä sijoittuu Yhdysvaltoihin ja se on tiukasti yhteydessä lisääntyneisiin avoimuuden ja tilivelvollisuuden vaatimuksiin. Suomessa arvopaperimarkkinayhdistys

on laatinut corporate governancen pohjalta Suomen listayhtiöiden hallinnointikoodin, joka ohjeistaa pörssiyhtiöiden hyvää hallintoa ja hyvää hallinnointitapaa. (Erma ym. 2010, 19–20)

Hyvälle hallintotavalle ei ole yksiselitteistä määritelmää. Kyse on kuitenkin johtamisjärjestelmästä, jonka avulla organisaatiota johdetaan ja valvotaan. Olennaista hyvän hallintotavan kannalta on tiedon antaminen myös ulkoisille sidosryhmille. Sisäinen valvonta ja riskienhallinta kuuluvat olennaisena osana myös hyvään hallintotapaan. (Alftan ym. 2008, 10–11) Sisäisen tarkastuksen ammattistandardit (2001) määrittelet hyvän hallinnon koostuvan hallituksen toimeenpanemista prosesseista ja rakenteista, joiden avulla hallitus ohjaa, informoi ja seuraa organisaation toimintaa.

Corporate governance ja hyvä hallintotapa liittyvät oleellisesti myös pienten ja keskisuurten yritysten johtamiseen ja johdon tehtäviin. Hyvä hallinnointitapa ja johtamiskulttuuri liittyvät valvontaympäristöön, koska kyseessä on keskeinen johtamista sääntelevä suositus. Erman ym. (2010, 20) mukaan corporate governance ei kuitenkaan sovi suoraan listaamattomille yhtiöille, kuten sukuyhtiöille tai pienyhtiöille. Näitä varten on kuitenkin julkaistu omia hyvän hallinnointitavan suosituksia. Keskuskauppakamari on muun muassa julkaissut vuonna 2006 vapaaehtoisuuteen perustuvan listaamattomien yhtiöiden asialistan, jonka tarkoitus on kehittää näiden yhtiöiden hallintoa (Alftan ym. 2008, 18).

Erma ym. (2010, 21) toteavat myös, että valtaosa hyvän hallinnointitavan suosituksista on yleispäteviä, mutta yrityksissä on mahdollista miettiä mitä niistä kannattaa omaksua ja soveltaa. Jos yritys on pieni, ei yrityksessä kannata käyttää monimutkaisia menettelytapoja. Jokaisen pk-yrityksen on siis mietittävä, millä tavoin yrityksessä voidaan käyttää ja soveltaa hyvän johtamis- ja hallinnointitavan periaatteita.

Mielestäni hyvälle johtamistavalle tai Corporate Governancelle ei ole yksiselitteistä määritelmää, vaan sillä voidaan tarkoittaa yleisesti yrityksen hallinnointijärjestelmää, joka määrittelee yrityksen johdon tehtävät ja velvollisuudet. Hyvä hallinnointitapa voi pitää sisällään muun muassa hallituksen ja muun ylimmän johdon päätöksenteon, talouden hoidon menettelyt, seuranta- ja arviointimenettelyt, prosessit ja ylimmän johdon toimintatavat ja ne menettelyt joiden avulla henkilöstölle viestitään johtamisesta.

4.7 Osakeyhtiön hallitus valvontaympäristön näkökulmasta

Osakeyhtiön hallituksella on lain mukaan yleistoimivalta, ja se vastaa yhtiön hallinnosta sekä sen toiminnan asianmukaisesta järjestämisestä. Hallitus vastaa lain mukaan myös siitä, että yhtiön kirjanpidon ja varainhoidon valvonta on asianmukaisesti järjestetty. (OYL 6:2) Enempää laissa ei hallituksen tehtävistä määrätä. Tiihonen (2007, 64) toteaakin, että hallituksen tehtävät muotoutuvat usein tilannetekijöiden mukaan. Hannulan (2003, 90) mukaan taas osakeyhtiön erilaiset tehtävien määrittelyt ja luokittelut ovat pikemminkin toisiaan tukevia kuin ristiriitaisia.

Hallituksen perinteisiin tehtäviin voidaan Tiihosen (2007, 101) mukaan laskea muun muassa yhtiön sisäinen hallinto, edustaminen, yhtiön tarkoituksen ja arvojen määrittely, yhtiön taloudellinen valvonta, laillisuuden ja eettisyyden valvonta, riskien hallinta ja yhtiön strategisen suunnan määrittely. Erma ym. (2010, 51) nostavat esille hallituksen strategisen ohjauksen ja valvontatehtävät. Heidän mukaansa yhtiön operatiiviset tehtävät tulee pääsääntöisesti jättää yhtiön toimitusjohtajalle. Erma ym. (2010, 48–49) toteavat myös, että hallituksen keskeisimpiä tehtäviä on huolehtia siitä, että yhtiön toiminta on lakien ja yhtiöjärjestyksen mukaan järjestetty, yhtiössä sisäinen tarkastus ja valvonta on organisoitu hyvin ja tehokkaasti, yhtiön antama informaatio on luotettavaa ja yhtiössä noudatetaan säännöksiä sekä määräyksiä. Samaan aikaan toiminnan tulisi olla kuitenkin tehokasta ja tuloksellista.

Hannulan (2003, 91–92) mukaan osakeyhtiön keskeisiksi ja yksityiskohtaisiksi tehtäviksi voidaan lukea, esimerkiksi yrityksen hallinta, kehittäminen, yrityksen tehtävän ja arvojen määritys, strategiaprosessin toteuttaminen, liiketoimintakäytännöistä päättäminen, yrityksen valvonta, omistusrakenteen kehittäminen, toimitusjohtajan ottaminen ja erottaminen ja yrityksen riskienhallinta.

Nämä luokittelut mielestäni kertovat siitä, että valvontaympäristön toimivuuden näkökulmasta pk-yrityksen hallituksen tulee varmistua ja huolehtia siitä, että osakeyhtiössä toimitaan lakin, määräysten ja säännösten mukaan. Tärkeää on kuitenkin toimia myös eettisesti ja toimintaa kehittäen. Hallituksella on mielestäni tärkeä osuus myös yhtiön arvojen ja strategian määrittelyssä. Yrityksen arvot vaikuttavatkin oleellisesti siihen, millainen valvontaympäristö ja johtamistapa yhtiöön muodostuu. Valvontaympäristö taas vaikuttaa riskienhallintaan ja riskienhallintaprosessin

onnistumiseen ja sen toteuttamiseen. Valvontaympäristön ja riskienhallinnan toteuttamisen näkökulmasta pienissä ja keskisuurissa osakeyhtiöissä hyvä hallitustyöskentely on siis tärkeää.

4.8 Toimitusjohtajan ja hallintoneuvoston tehtävät valvontaympäristön näkökulmasta

Osakeyhtiöllä on siis aina hallitus, mutta toimitusjohtajan valinta ei ole pakollista. Osakeyhtiöillä on kuitenkin yleensä sekä hallitus että toimitusjohtaja. Toimitusjohtajan tärkein tehtävä on hoitaa yhtiön juoksevaa, eli päivittäistä hallintoa hallituksen antamien ohjeiden ja määräysten mukaisesti. Toimitusjohtaja saa ryhtyä laajankantoisiin tai epätavallisiin toimiin vain, jos hallitus on toimitusjohtajan siihen valtuuttanut. Toimitusjohtaja vastaa myös siitä, että yhtiön varainhoito on järjestetty luotettavalla tavalla ja kirjanpito on lain mukaista. Toimitusjohtajan on annettava hallitukselle sellaiset tiedot, jotka ovat tarpeellisia hallituksen tehtävien hoidon kannalta. (OYL 6:17)

Toimitusjohtaja saa siis hoitaa tavanomaisia ja päivittäisiä toimia sekä tehdä tavanomaisia sopimuksia. Toimitusjohtaja voi myös edustaa yhtiötä, jos edustettava asia kuuluu hänen toimivaltaansa (Erma ym. 2010, 36). Hannulan (2003, 213) mukaan juokseviin ja rutiininomaisiin tehtäviin luetaan muun muassa yhtiön liiketoimintojen johtaminen ja valvominen, sopimusten solmiminen, rekrytointi ja henkilöstöhallinto.

Hannula (2003, 212) toteaa myös, että vastuiden ja velvollisuuksien jako hallituksen ja toimitusjohtajan välillä on tärkeää. Kuten jo aikaisemminkin totesin, vastuiden ja velvollisuuksien jakaminen organisaatiossa on myös tärkeä osa valvontaympäristöä COSO-ERM-viitekehikossa (Moeller 2007). Keskinäisten roolien ja vastuiden tulisi olla selkeästi määritelty, jotta vastuunjakoon ei tarvitsisi puuttua yhä uudelleen. Hallituksen tulee ohjeistaa ja kontrolloida toimitusjohtajaa, jottei toimitusjohtaja voi toimia päättömästi ja yksin. Hallituksen ohjeistus toimitusjohtajalle on syytä dokumentoida samoin kuin sellaiset asiat, joista on sovittu osapuolten välillä. (Hannula 2003, 212–213) Hallitusta voidaan pitää toimitusjohtajan ”esimiehenä”, ja siksi sen on seurattava toimitusjohtajan tehtävien hoitoa ja niistä selviytymistä.

Lakisääteisten tehtävien lisäksi toimitusjohtajalla on suuri joukko käytännön tehtäviä, joiden luokittelu voi toisinaan olla haastavaa. Toimitusjohtajan käytännön tehtävinä ja

toimina voidaan kuitenkin pitää muun muassa yhtiöön ja sen toimintaan perehtymistä, toimia hallituksen toivomalla tavalla, itsenäisyyden säilyttämistä suhteessa hallitukseen, tutustua yhtiön hallituksen jäseniin, varmistaa oikea-aikainen tiedonkulku hallituksen ja toimitusjohtajan välillä, varmistaa että sovitut asiat toteutuvat ja hyväksyä toimisuhteen päättyminen. Toimitusjohtajan tulisi kuitenkin välttää epäselvää vastuunjakoa hallituksen kanssa, hallituksen ohjaamista, yksinäisyyttä ja keskustelun välttelyä, intressiriitaa ja sellaisten asioiden viemistä hallitukseen, jotka eivät sinne kuulu. (Hannula 2003, 215–216)

Muodollinen työnjako hallituksen ja toimitusjohtajan välillä on siis selvä. Hallitus keskittyy työskentelyssään suuriin, strategisiin, pitkänaikavälin toimiin ja asioihin, kun taas toimitusjohtaja hoitaa yhtiön juoksevaa hallintoa. Tiihosen ym. (2007, 65) mielestä hallituksen yhteistyö muun toimivan johdon, esimerkiksi toimitusjohtajan kanssa voi olla haasteellista, koska jos yhteistyö on liian läheistä, hallituksen valvontatehtävän hoitaminen vaarantuu. Hallitus ikään kuin yhdentyy muun johdon kanssa, ja tämän vuoksi hallitus ei enää kyseenalaista asioita. Valvontarooliin kuuluu läheisesti kommunikointi ja tehokas tiedon jakaminen. Jotta toimielimet voivat hoitaa tehtävänsä kunnolla ja mahdollisimman hyvin, tarpeellisen tiedon tulisi kulkea vaivattomasti ja oikea- aikaisesti. (Tiihonen ym. 2007, 65–67)

Valvontaympäristössä yhtiön toimitusjohtajan tulee siis hoitaa lakisääteiset tehtävänsä ja samalla hoitaa useita käytännön tehtäviä, jotka tulee olla dokumentoitu yhtiön johdon toimesta. Vastuunjaon yhtiössä tulee olla selkeää. Hallitus ja toimitusjohtaja eivät saa toimia liian läheisissä väleissä, jottei hallituksen valvontatehtävä vaarannu. Toisaalta toimiva yhteistyö osapuolten välillä on tehtävien suorittamisen kannalta olennaista. Avoimuus ja tilivelvollisuus lisäävät muutoinkin yhtiön luotettavuutta.

Osakeyhtiölain mukaan osakeyhtiön johtoon voi kuulua myös hallintoneuvosto. Hallintoneuvostosta tulee määrätä osakeyhtiön yhtiöjärjestyksessä. Hallintoneuvoston tärkein tehtävä on hoitaa hallituksen ja toimitusjohtajan vastuulla olevaa hallintoa. Hallintoneuvosto voi myös valita hallituksen, jos yhtiöjärjestys niin määrää. Yhtiöjärjestyksessä on mahdollista määrätä hallintoneuvostolle myös muita hallituksen yleistoimivaltaan kuuluvia tehtäviä ja sellaisia tehtäviä, joita ei ole säädetty muille toimielimille. Hallintoneuvosto ei voi kuitenkaan edustaa yhtiötä. (OYL 6:21)

Hallintoneuvoston on yleensä katsottu kuuluvan suuryhtiöiden toimielimeksi, ja siksi sitä harvemmin näkee pienissä ja keskisuurissa yhtiöissä. Toisaalta suuryhtiöissäkään ei välttämättä ole hallintoneuvostoa. Hallintoneuvostojen määrä onkin radikaalisti vähentynyt, koska toimielin on yhtiössä vapaaehtoinen ja sille ei ole löytynyt luontevaa roolia yhtiössä. (Hannula 2003, 26) Monissa pk-yrityksissä yhtiön johto siis muodostuu pelkästä hallituksesta tai hallituksesta ja toimitusjohtajasta. Joissain keskisuurissa yhtiöissä on mahdollista olla hallintoneuvosto, jos yhtiöjärjestyksessä on niin määrätty.

4.9 Osakeyhtiön valvonta valvontaympäristön näkökulmasta

Osakeyhtiön toimielinten ja johdon työskentelyä on pakko valvoa, jotta voidaan varmistua muun muassa toiminnan tuloksellisuudesta, tehokkuudesta, raportoinnin ja talouden lainmukaisuudesta. Seuranta ja valvonta on nostettu tärkeäksi osaksi myös sisäisen valvonnan prosessia COSO-IC-viitekehikossa ja osaksi riskienhallintaprosessia COSO-ERM-viitekehikossa (Moeller 2007).

The Institute of Internal Auditors (IIA), joka nykyisin painottaa entistä enemmän organisaation eettistä ilmapiiriä yhtiön toiminnassa on määritellyt johtamis- ja hallintotavan keskeisiksi toimijoiksi hallituksen, ylimmän johdon, sisäisen tarkastuksen ja ulkoisen tilintarkastuksen. Näitä toimijoita voidaan myös pitää keskeisinä toimijoina osakeyhtiön valvonnan kannalta. Näiden toimijoiden tehokas vuorovaikutus on perusta hyvälle yhtiön johtamiskulttuurille. Osakeyhtiön hallituksen tehtävänä on valvoa toimitusjohtajaa sekä vastata sisäisen valvonnan ja riskienhallintajärjestelmän olemassaolosta. Toimiva johto mukaan lukien toimitusjohtaja taas vastaa käytännön operatiivisesta johtamisesta, mutta myös riskienhallinnan suunnittelusta, toteuttamisesta ja seurannasta. Tilintarkastus perustuu lakisääteisyydelle, kun taas sisäinen valvonta on vapaaehtoista arviointi-, varmistus-, ja konsultointitoimintaa. (Holopainen ym. 2010, 19)

Sisäisen valvonnan ja tarkastuksen tukena ovat muun muassa IIA:n määrittelemät kansainväliset sisäisen tarkastuksen ammattistandardit, joiden avulla sisäinen tarkastus tulisi yhtiöissä suorittaa. Standardien noudattaminen osana tarkastusta on tärkeää, jotta tarkastustoiminto täyttää velvollisuutensa. (The Institute of Internal Auditors, 2013)

Lakisääteisellä tilintarkastajalla on tärkeä asema tarkastuselimenä, koska tarkastuksen avulla osakkeenomistajat saavat riippumattoman lausunnon yhtiön kirjanpidosta, tilinpäätöksestä ja hallinnosta. Sisäinen valvonta ja tarkastus taas varmistavat, että yhtiön toiminta on tehokasta ja tuloksellista, informaatio on luotettavaa ja säännöksiä noudatetaan. (Asialuettelo listaamattomien yhtiöiden hallinnoinnin kehittämiseksi, 2004) Asialuettelo listaamattomien yhtiöiden hallinnon kehittämiseksi on luotu yhtiöille, jotka haluavat aktiivisesti kehittää hallintoaan, valvontaansa ja muita toimintojaan hyvän hallinnointitavan mukaiseksi. Tästä voikin päätellä, että niissä yhtiöissä joiden valvontaympäristö on ”positiivinen”, on halu järjestää sekä ulkoinen että sisäinen valvontansa tehokkaasti, lakien ja muiden suositusten mukaan.

Uusi tilintarkastuslaki (2007/459) muutti pienten osakeyhtiöiden tilintarkastuksen vapaaehtoiseksi tietyin edellytyksin. Tilintarkastaja voidaan jättää yhteisössä valitsematta, jos sekä päättyneellä että sitä välittömästi edeltäneellä tilikaudella on täyttynyt enintään yksi seuraavista edellytyksistä: ensinnäkin taseen loppusumma ylittää 100 000 tai liikevaihto tai sitä vastaava tuotto ylittää 200 000 euroa tai yhtiön palveluksessa on keskimäärin yli kolme henkilöä. (Tilintarkastuslaki 2 luku 4§) Tämä tarkoittaakin, että liiketoiminnaltaan aivan pienissä parin tai kolmen hengen mikroyrityksissä ei välttämättä ole ulkopuolista valvontaa, koska yhtiössä ei ole valittu vapaaehtoisesti tilintarkastajaa. Tällöin yhtiössä tärkeää on eettisyys, rehellinen toimintatapa sekä tehokas sisäinen valvonta, vaikka myöskään erillistä sisäisen tarkastuksen toimintoa näissä yhtiöissä ei olisi.

Tilanteessa on keskeistä yhtiön toimielinten eli periaatteessa mikroyrityksissä hallituksen tai hallituksen ja toimitusjohtajan rehellinen toiminta ja valvontaympäristön eettisyyden lähtökohta. Tämän voidaan katsoa pätevän myös niihin mikroyrityksiin, joissa mahdollisesti syntyy roolikumulaatioita, eli esimerkiksi silloin kun yhtiön toimitusjohtaja on samalla myös hallituksen puheenjohtaja (Norri 2006, 264). Sellaisten yhtiöiden toimintaa, joissa ei ole valittu vapaaehtoisesti tilintarkastajaa on erityisen vaikeaa valvoa, mikä voikin taas johtaa epärehelliseen toimintaan ja väärinkäytöksiin, jos yrityksen perusta eli valvontaympäristö on ilmapiiriltään epärehellinen. Valvontaympäristön ilmapiirillä on siis suuri vaikutus siihen, millaista toimintaa yhtiössä harjoitetaan valvonnasta riippumatta. Positiivisen valvontaympäristön näkökulmasta yhtiössä tulisi kuitenkin olla halu vapaaehtoisesti valita yhtiölle

tilintarkastaja, jotta voidaan varmistua toiminnan, hallinnon ja talouden lainmukaisuudesta.

Jos ajatellaan kokonaisuutena pk-yritysten luokkaa, niin suurimmassa osassa yhtiöitä on kuitenkin tilintarkastusvelvollisuus, koska tarkastuksen rajat on tilintarkastuslaissa asetettu mataliksi. Sen sijaan mikroyhtiössä ei välttämättä ole sisäisen tarkastuksen toimintoa, koska yleisesti sisäinen tarkastus on ajateltu suurempien yhtiöiden menetelmäksi (Hannula 2003, 155). Kuten jo aikaisemmin totesin, jos yhtiössä ollaan kuitenkin aktiivisesti halukkaita kehittämään yhtiön valvontaa ja hallintoa hyvän hallinnointitavan mukaiseksi, yhtiössä ollaan myös positiivisia vapaaehtoisen sisäisen valvonnan ja tarkastuksen suhteen.

Sisäisen valvonnan COSO-IC-viitekehikossa organisaation tavoitteet luokitellaan kolmeen ryhmään. Ensinnäkin organisaatiolla on toiminnallisia tavoitteita, taloudelliseen raportointiin liittyviä tavoitteita ja lakien ja sääntöjen mukaisuuteen liittyviä tavoitteita. Toiminnalliset tavoitteet liittyvät yrityksen resursseihin ja niiden tarkoituksenmukaiseen käyttöön, kun taas taloudellinen raportointi liittyy taloudellisten raporttien luotettavuuteen. Lakien ja sääntöjen mukaisuus liittyy taas niihin tavoitteisiin joita yrityksellä on, jotta se voi toimia lakien ja sääntöjen mukaisesti. (Moeller 2007, 4; ks. myös Holopainen 2010, 54) Voidaan ajatella, että sisäinen valvonta auttaa yhtiöitä näiden tavoitteiden saavuttamisessa, mutta samalla se auttaa yhtiötä toimimaan myös rehellisesti. Sisäisellä valvonnalla voidaan ajatella olevan vain avustava ja välineellinen rooli, koska halu toimia rehellisesti syntyy yhtiön johdossa ja sen henkilöstössä yhtiön johtamis- ja valvontakulttuurin pohjalta. Tämä lisäksi sisäinen tarkastus osana sisäistä valvontaa auttaa yhtiötä ja sen johtoa saamaan reaaliaikaista tietoa yhtiön toiminnasta ja taloudesta. Voidaankin ajatella, että pelkkä tilintarkastajan suorittama jälkitarkastus ei ole riittävä turva väärinkäytösten ehkäisemiseksi. (Myllymäki 2007)

5 HAASTATTELUT

5.1 Haastattelun menetelmät

Suomen lainsäädäntö ei suoraan määrää yrityksen sisäisen valvonnan järjestämisestä. Osakeyhtiölain mukaan yrityksen hallitus on kuitenkin vastuussa siitä, että kirjanpidon ja varainhoidon valvonta on lainmukaista ja varainhoito on luotettavalla tavalla myös järjestetty. Yrityksen hallitus on siis osakeyhtiölainkin mukaan vastuussa sisäisen valvonnan asianmukaisesta järjestämisestä. Toimitusjohtajalla sen sijaan on kokonaisvastuu valvontajärjestelmän luomisesta ja ylläpitämisestä. Toimitusjohtaja vastaa myös organisaation valvontakulttuurin tiedottamisesta organisaatiossa ja sen eri tasoilla, eli niin sanotun ”tone at the top” – viestin kulkeutumisesta organisaatiossa. Yrityksessä saattaa myös olla oma sisäisen valvonnan ja tarkastuksen yksikkönsä, joka vastaa sisäisen valvonnan toteuttamisesta, implementoinnista ja ylläpitämisestä. Tällöin sisäisen valvonnan toteutumisen kannalta tärkeissä rooleissa ovat muun muassa controllerit, talouspäälliköt ja muut organisaation laskentaihmiset. Virallinen vastuu sisäisen valvonnan järjestämisestä kuuluu siis organisaation ylimmälle johdolle. Tämä ei kuitenkaan poissulje organisaation työntekijöiden vastuuta, koska jokainen organisaation työntekijä on omalta osaltaan vastuussa sisäisen valvonnan toimintaohjeiden ja periaatteiden noudattamisesta. (Ratsula 2011)

Valitsin haastattelun tutkimusmenetelmäksi, koska sisäisen valvonnan ja riskienhallinnan järjestäminen on yrityksen ylimmän johdon vastuulla. Mielestäni sisäisen valvonnan prosesseista ja toimintatavoista on vaikeaa saada kokonaisvaltaista käsitystä ilman, että haastattelee tutkimuskohteita. Mielestäni sisäisen valvonnan ja riskienhallinnan määrittely voi jäädä lomakehaastattelussa myös vajaaksi. Haastattelun avulla haastattelukohteet saavat paremman ja syvällisemmän kuvan tutkimusaiheesta ja sisäisestä valvonnasta. Haastatteluiden tarkoitus on täydentää aiempia kirjallisuudesta saamiani tuloksia.

Haastattelin kahdeksaa yritystä, jotka kaikki kuuluivat pk-yritysten joukkoon. Yritykset kuuluivat pk-yritysten luokissa mikroyrityksiin ja pieniin yrityksiin. Haastatteluiden perusteella ei voi siis tehdä laajamittaisia johtopäätöksiä koko pk-yritysten luokasta,

koska haastattelu kohdistui vain mikro- ja pienyrityksiin. Varsinaisina haastattelukohteina olivat pääasiassa näiden yritysten toimitusjohtajat ja hallituksien jäsenet. Tarkoitukseni oli valita haastateltaviksi henkilöitä, joiden vastuulla sisäisen valvonnan, tarkastuksen ja riskienhallinnan järjestäminen kyseisissä yrityksissä on.

Yritysten nimiä ei julkaista tutkielmassa, joten koodasin yritykset. Käytän yritysten analysoinneissa koodeja A, B, C, D, E, F, G JA H. Haastatteluja ei nauhoitettu, koska haastateltavat henkilöt suhtautuivat siihen negatiivisesti, ja yritysten tunnistamisesta täytyi tehdä mahdollisimman vaikeaa. Haastattelun purku perustuu muistiinpanoihini haastatteluista. Seuraavassa esittelen yritysten toimialat ja keskeiset tilinpäätöstiedot viimeisimmistä tilinpäätöksistä. Tietojen tarkoitus on selventää haastattelemieni yritysten suuruusluokkaa ja toimialoja. Tilinpäätöstietojen luvut ovat pyöristettyjä.

Yritys A:n liikevaihto oli viimeisimmässä tilinpäätöksessä noin 1 950 000 euroa, taseen loppusumma 14 100 000 euroa ja tilikauden tappio noin 270 000 euroa. Viimeisimmän tilinpäätöksen mukaan yrityksen palveluksessa henkilöstöä oli tilinpäätöshetkellä noin 5,5. Yritys A siis kuuluu pk-yritysten joukkoon, vaikka taseen loppusumma ylittääkin pk-yritysten 43 miljoonan euron taseen rajan. Sen sijaan henkilöstömäärä ja liikevaihto ovat pk-yritysten luokittelun rajoissa. Yritys A:n toimiala on muiden kiinteistöjen vuokraus ja niiden hallinta.

Yritys B:n liikevaihto oli viimeisimmässä tilinpäätöksessä 414 000 euroa, taseen loppusumma 240 000 euroa ja tilikauden tappio noin 26 000. Henkilöstömäärä yrityksessä oli tilinpäätöshetkellä 4 henkilöä. Yritys B: toimiala on rakennetekninen palvelu. Yritys B:n liikevaihto on kuitenkin huomattavasti kasvanut kuluvalla tilikaudella ja henkilöstöä on palkattu lisää. Yritys C:n liikevaihto oli viimeisimmässä tilinpäätöksessä 433 000 euroa, taseen loppusumma 231 000 euroa ja tilikauden voitto 25 000 euroa. Henkilöstömäärä yrityksessä oli tilinpäätöshetkellä keskimäärin 6 henkilöä. Yritys C:n toimiala on lvi-tekninen suunnittelu. Yritykset B ja C kuuluvat selkeästi mikroyritysten joukkoon.

Yritys D:n liikevaihto sen sijaan oli tilinpäätöshetkellä noin 5 680 000 euroa, taseen loppusumma 7 800 00 euroa ja tilikauden tulos 860 000 euroa. Henkilöstöä yrityksessä oli tilikaudella keskimäärin 41. Yritys kuuluu pk-yritysten joukossa pieniin yrityksiin. Yhtiön toimialana on ylläpitää rinnehiihtokeskusta ja harjoittaa alaan liittyvää liiketoimintaa. Yritys E kuuluu pk-yritysten luokittelussa myös pienten yritysten

joukkoon. Sen liikevaihto oli viimeisimmässä tilinpäätöksessä 4 170 000 euroa, taseen loppusumma 2 300 000 euroa ja tilikauden voitto 350 000 euroa. Työntekijöitä yrityksessä oli keskimäärin 35 tilikauden aikana. Yhtiön toimiala on metallirakenteiden ja niiden osien valmistus.

Yritys F:n liikevaihto oli viimeisimmässä tilinpäätöksessä 31.12.2012 noin 5 000 000 euroa. Taseen loppusumma yrityksessä F oli tilinpäätöshetkellä noin 4 000 000 euroa ja henkilöstön lukumäärä noin 45. Yhtiön toimiala on muualla luokittelemattomat rahoituspalvelut. Tarkemmasta toimialakuvauksesta selviää, että yhtiön toiminta liittyy elintarvikkeiden, kosmeettisten tuotteiden ja terveyttä ja hyvää oloa edistävien tuotteiden myyntiin ja vientiin. Yhtiö kuuluu pk-yritysten luokittelussa pieniin yrityksiin.

Yritys G:n taseen loppusumma oli viimeisimmässä tilinpäätöksessä noin 700 00 euroa, liikevaihto noin 250 000 euroa ja tilikauden tulos noin 4080 euroa. Yritys G kuuluu siis pk-yritysten luokassa selkeästi mikroyrityksiin. Yritys G:n toimiala on kultasepänteosten ja kellojen vähittäiskauppa. Henkilöstöä yrityksessä oli viime tilikaudella keskimäärin kaksi. Yritys H:n liikevaihto oli viimeisimmässä tilinpäätöksessä 30.6.2013 noin 800 000, taseen loppusumma noin 400 000 ja tilikauden voitto noin 75 000 euroa. Yritys H:n toimiala liittyy kirjanpito-, tilintarkastus-, toimisto- ja palkanlaskentatehtävien tuottamiseen. Yrityksessä oli henkilöstöä viimeisimmällä tilikaudella keskimäärin 10.

Toteutin haastattelun puolistrukturoituna teemahaastatteluna. Lähetin kysymykset vastaajille etukäteen, jotta heillä oli aikaa syventyä aiheeseen ennen varsinaista haastattelua. Teemahaastattelussa edetään keskeisten etukäteen valittujen teemojen varassa ja näitä teemoja sitten tarkennetaan erilaisilla kysymyksillä. Teemahaastattelu korostaa tulkintoja tilanteesta, ihmisten antamia merkityksiä ja asioiden välisiä vuorovaikutussuhteita. (Tuomi & Sarajärvi 2003, 77)

Teemahaastattelussa ei tarvitse edetä suunnitelmien mukaan. Kysymysten järjestystä on mahdollista vaihdella ja johonkin alueeseen voi syventyä tarkemmin. Teemahaastattelun onnistumisen kannalta on tärkeää, että haastattelija antaa tilaa vastaajille ja heidän tarpeilleen. Teemahaastattelun avulla on mahdollista saada syvällisempää, monimuotoisempaa ja tarkempaa tietoa haastateltavista ja tutkimusongelmista verrattuna esimerkiksi lomakehaastatteluun. Teemahaastattelun tarkoitus on kuitenkin

löytää vastaukset asetettuihin tutkimuskysymyksiin ja tutkimusongelmiin, joten teemahaastattelussa ei voi kysellä mitä tahansa. Haastatteluun valitut teemat perustuvat tutkimusongelman viitekehykseen ja siihen mitä aiheesta jo ennalta tiedetään. (Tuomi & Sarajärvi 20013, 76–78)

Lähdin purkamaan haastatteluaineistoani sisällönanalyysin avulla. Sisällönanalyysi perustuu laadullisen aineiston analysointiin. Sisällönanalyysin tarkoitus on löytää olennainen tarkasteltavasta aineistosta. Sisällönanalyysin avulla pyritään saamaan kuvaus tutkittavasta aiheesta. Kerätty aineisto saadaan analyysin avulla järjestetyksi johtopäätöksien tekoa varten. Ensin on päätettävä se mikä aineistossa eniten kiinnostaa. Tämän vaiheen jälkeen aineisto käydään lävitse ja siitä erotellaan merkitykselliset ja merkityksettömät asiat. Aineiston analysoinnin ja kuvailun avulla tutkijan on mahdollista muodostaa aineistosta kattava yleiskuva. Tutkimusprosessin lähtökohtana on ensisijaisesti monimutkaisen tutkimuskohteen ymmärtäminen. (Lillis & Mundy 2009, 138) Kaikki epäolennainen jää siis pois aineistosta. Merkityt asiat kerätään yhteen ja aineistoa tyypitellään ja luokitellaan. Lopuksi aineistosta kirjoitetaan yhteenveto. (Tuomi & Sarajärvi 2003,104)

5.2 Haastatteluaineisto ja sen analysointi

Ajatukset riskienhallinnasta

Johdon ajatukset riskienhallinnasta, johtamistapa johtamisfilosofia ja johtamiskulttuuri ovat tiukasti sidoksissa yrityksen valvontaympäristöön ja sen perustaan. Haastattelussa haluttiin selvittää, minkälaisia ajatuksia riskienhallinta haastateltavissa herättää ja miten haastateltavat suhtautuvat riskienhallintaan ja sen metodeihin.

Haastateltavista viisi yritystä piti riskienhallintaa tärkeänä osana yritysten johtamista ja osana johdon päivittäisiä toimintoja. Nämä viisi yritystä (A, B, C, F ja H) totesivat, että yrityksen riskienhallinta on positiivinen asia. Näiden haastateltavien mukaan riskienhallinnan avulla voidaan varautua epävarmuuksiin. Näiden kaikkien haastateltavien mukaan riskienhallinta on tärkeää myös silloin, kun pyritään ennakoimaan toimialalla tapahtuvia muutoksia tai muutoksia liiketoimintaympäristössä. Haastateltavien (A, B, C, F ja H) mielestä riskienhallinta on tärkeä osa yrityksen laatujohtamista.

Vain kaksi yritystä (D ja E) haastateltavista myönsi, että riskienhallintaan liittyy myös negatiivisia ajatuksia ja tuntemuksia. Nämä negatiiviset ajatukset liittyvät riskienhallinnan aiheuttamaan lisätyöhön. Näiden kahden yrityksen mukaan, riskienhallinnan kustannukset ja siihen käytettävissä olevat resurssit aiheuttavat negatiivisia ajatuksia. D:n ja E:n mukaan riskienhallinta vaatii yrityksen johdolta päivittäisten rutiinien lisäksi paljon lisätyötä ja tutustumista aiheeseen. Heidän mukaansa riskienhallinta aiheuttaa siis enemmän kuormitusta yrityksen johtamiseen ja sen osa-alueisiin. D:n ja E:n mukaan riskienhallinta on kuitenkin tärkeää ja sen avulla on mahdollista varautua myöhempiin ja odotettavissa oleviin vaurioihin ja epäsuotuisiin tapahtumiin. Eli vaikka D:n ja E:n mukaan riskienhallinta on osittain negatiivinen yrityksen johtamisen osa-alue, on sen huomioiminen heidän mukaansa kuitenkin tärkeää.

Haastateltavista yritys G:n toimitusjohtaja oli ainoa, joka ei pitänyt riskienhallintaa tärkeänä elementtinä yrityksen johtamisen kannalta. Yritys G:n toimitusjohtajan mukaan riskienhallinta on ylimääräinen johtamisen osa-alue, jota ei voi soveltaa pienessä yrityksessä, koska se aiheuttaisi yritykselle kustannuksia ja lisätyötä. Yritys G:n toimitusjohtaja oli haastattelussa epäileväinen myös riskienhallinnan hyötyjen suhteen. Yritys G:n toimitusjohtajan mukaan riskienhallinta ei aiheuta positiivisia, mutta ei myöskään negatiivisia tuntemuksia.

Riskienhallinnan toteuttaminen yrityksissä

Haastattelussa minua kiinnosti se, miten yrityksissä toteutetaan riskienhallintaa, ja jos riskienhallintaa toteutetaan, niin millä laajuudella sitä toteutetaan. Halusin myös tietää, että onko riskienhallinta osana yritysten johtamista säännöllistä vai epäsäännöllistä.

Kaikissa haastattelemissani yrityksissä toteutetaan riskienhallintaa jollain tasolla. Kaikissa yrityksissä on vakuutuksia, kontrolleja ja arviointeja. Mielestäni on olennaista, että yritykset A, B, C, D, E, F, ja H pitävät vakuuttamista tärkeänä elementtinä riskienhallinnassa. Puran tässä aineistossa vain parin yrityksen vakuuttamistapaa.

Haastatteluiden perusteella yrityksissä A, B, E ja F riskienhallintaa toteutetaan säännöllisesti, jatkuvasti ja osana johdon päivittäisiä toimintoja. Yrityksessä A riskienhallintaa toteutetaan koulutuksen, järjestelmien, prosessien ja asiantuntijalausuntojen kautta. Käytännössä yrityksessä A on paljon vakuutuksia ja

kontrolleita. Yritys A mainitsi myös taloudellisten raporttien merkityksen kvalitatiivisten ja kvantitatiivisten arviointien apuna. Yrityksessä A siis arvioidaan riskejä raporttien avulla kvalitatiivisin ja kvantitatiivisin metodein. Yritys A:n mukaan riskienhallinnasta vastaa keskitetysti toimitusjohtaja, mutta haastateltavan mukaan jokaisen henkilön panos riskienhallinnan kannalta on tärkeä. Yritys A:ssa seuranta on toteutettu omavalvontana.

”*Kukin vastaa riskienhallinnasta omassa työssään”*
Yritys A:n toimitusjohtaja

Haastattelussa selvisi, että yritys B:ssä riskienhallintaa toteutetaan ensisijaisesti vakuuttamisen ja sopimusehtojen avulla. Yritys B:n toimitusjohtajan mukaan sopimusehtojen ja vakuutusten avulla voidaan varautua muun muassa välillisten vahinkojen varalta. Yritys B:llä on muun muassa tuotevastuu-, palo-, varkaus-, oikeusturva - ja ilkivaltavakuutus. Yrityksessä on varauduttu myös patenttiriitoihin ja kilpailukieltoihin. Yrityksessä on käytössä myös kulunvalvontaa, varoituskylttejä, aidatut alueet, kameravalvonta, palomuurit, murtohälytykset ja sopimus vartiointiliikkeen kanssa. Henkilöstöriskeihin yrityksessä on varauduttu esimerkiksi varamiesjärjestelmän avulla, henkilöstön pakollisilla ja vapaaehtoisilla vakuutuksilla sekä terveydenhuoltosuunnitelmilla. Yritys B:n toimitusjohtaja piti tärkeänä myös sisäisiä kontrolleja, esimerkiksi tehtävien hajauttamista, salasanojen käyttöä ja valtuuksien määrittelyä.

Riskien arviointi ja analysointi on toteutettu yrityksessä B toiminnan virheiden läpikäynnin ja minimoinnin avulla. Yrityksessä B on kattavat tilitoimistopalvelut, jotka tuottavat kuukausittain raportteja päätöksenteon ja arvioinnin tueksi. Näiden lisäksi yrityksessä B on käytössä kustannus- ja kuormituslaskentamalli, jonka avulla yritys pystyy ennustamaan tulevaa toimintaa ja sitä kautta varautumaan muutoksiin. Riskejä arvioidaan yrityksessä aina uusien asiakassuhteiden ja projektien alkaessa. Yritys B:n mukaan riskienhallinta kuuluu päivittäiseen johtamiseen ja sitä pyritään yrityksessä toteuttamaan määräajoin ja tarvittaessa. Haastattelun perusteella yrityksessä B riskienhallintaa arvioidaan ja tarkastellaan kuukausittain. Yrityksen toimitusjohtajan mukaan riskienhallinta on ensisijaisesti toimitusjohtajan ja yrityksen omistajien

vastuulla, mutta myös yritys B:n toimitusjohtaja muistuttaa koko henkilöstön osallisuudesta riskienhallinnan toimivuuden kannalta.

Yrityksessä E riskienhallintaa toteutetaan vakuuttamisen ja kontrollien lisäksi riskikartoituksen, kvalitatiivisten ja kvantitatiivisten metodien avulla. Yrityksessä E tehdään riskikartoitus jokaiselle projektille ja asiakkaalle. Haastattelussa selvisi, että riskikartoitus on kirjallinen ja esimerkiksi yrityksen tarjouskatselmuksissa huomioidaan mahdolliset riskit. Yrityksessä on käytössä myös laatujärjestelmä riskienhallinnan tukena ja mahdollisten riskien minimoimisen apuna. Yritys E:n toimitusjohtajan mukaan yrityksen riskienhallinta on säännöllistä ja yrityksen toimintaa sekä laatujärjestelmän tuloksia seurataan tiiviisti. Huomioimisen arvioista mielestäni on, että yrityksessä E on riskienhallinnasta vastaava projektipäällikkö. Yritys E ei huomioinut varsinaisesti siis toimitusjohtajan tai hallituksen vastuuta riskienhallinnan toteuttamisessa.

Yrityksessä F riskienhallintaa toteutetaan seuraamalla jatkuvasti ja aktiivisesti sisäisen verkon kautta tulevia lainsäädännöllisiä ja poliittisia ehdotuksia sekä muutoksia. Yritys F arvioi mahdollisia riskejä myös tilitoimistolta saamiensa raporttien, esimerkiksi tuloslaskelman ja taseen perusteella. Yritys F:n toimitusjohtajan mukaan yhteistyö tilitoimiston ja tilintarkastajan kanssa on yrityksen taloudellisten muutosten ja liiketoiminnansuunnittelun kannalta tärkeää. Toimitusjohtajan mukaan yhteistyön hyötyjä ovat myös mahdollisten tappioiden välttäminen ja taloudellisten riskien tiedostaminen etukäteen. Riskien arviointi on yrityksessä kvantitatiivista ja perustuu raporteista saataviin tunnuslukuihin ja niiden analysointeihin. Yrityksen tietoturvavastaava tekee yrityksen sisällä pistokokeita yrityksen tietoturvaan liittyvistä kontrolleista ja niiden toimivuudesta.

Haastattelun perusteella voin todeta, että yritys F luottaa riskienhallinnan toteuttamisessa etukäteissuunnitteluun ja ennakointiin. Yrityksessä varaudutaan käytännössä riskeihin vakuutusten, hälytinjärjestelmän, sisäisen tiedonkulun ja henkilöstön kattavan ohjeistuksen avulla. Yritys F:n toimitusjohtajan mukaan henkilöstön kouluttamisella, ohjeistuksella ja yrityksen pelisääntöjen tiedottamisella voidaan ehkäistä väärinkäytöksiä ja vääränlaisten toimintatapojen aiheuttamat riskit.

Yrityksessä H riskienhallintaan suhtaudutaan positiivisesti, mutta varsinaisen riskienhallintaprosessin luominen on kesken. Yrityksessä riskeihin vastataan vakuuttamisella, käyttäjätunnuksilla, salasanoilla, hyväksymismenettelyillä, valtuuksilla, varallisuuden turvaamisella ja kontrolleilla. Riskien arviointi ja analysointi on yrityksessä hallituksen analysoinnin vastuulla. Kvalitatiivisten ja kvantitatiivisten arviointitapojen käyttäminen on yrityksessä vielä alkeellista. Yrityksessä kuitenkin tehdään monipuolista ja kattavaa analysointia yrityksen taloudellisesta tilanteesta kuukausittaisten tuloslaskelma - ja taseraporttien perusteella.

Toimitusjohtajan mukaan yrityksen valvonta on ensisijaisesti hallituksen vastuulla, mutta myös tiiminvetäjien ja henkilöstön panos sisäisen valvonnan ja riskienhallinnan seurannassa on toimitusjohtajan mukaan merkittävä. Toimitusjohtaja kertoi haastattelussa, että yrityksen palvelukseen oli palkattu controller, jonka toimenkuvaan riskienhallintaprosessin luominen ja sen kehittäminen olisi kuulunut. Controller kuitenkin irtisanoutui, joten riskienhallinnan kehittäminen on jäänyt yrityksessä kesken.
Yrityksissä C,D ja G riskienhallinnan toteuttaminen on heikommalla tasolla. Yritys C:n toimitusjohtajan mukaan yritys toteuttaa riskienhallintaa säännöllisen epäsäännöllisesti. Yrityksessä C ei tehdä kvantitatiivisia eikä kvalitatiivisia riskiarviointeja. Riskejä arvioidaan epäsäännöllisesti, eikä riskikartoitusta tehdä kirjallisena. Yritys C:n toimitusjohtaja myönsi haastattelussa, että yrityksen harjoittama riskiarviointi on puutteellista ja riittämätöntä. Yritys C:n riskienhallinta perustuu vakuuttamiseen ja töiden ohessa tapahtuvaan käytännön työhön. Yrityksen toimitusjohtajan mukaan hallituksen puheenjohtaja ja toimitusjohtaja ovat vastuussa riskienhallinnan toteuttamisesta.

Yrityksessä D ei myöskään ole varsinaista riskienhallintaprosessia, eikä riskienhallinnan tukena käytetä vaativia riskiarviointeja. Yritys D:n toimitusjohtajan mukaan yrityksen riskienhallintaa toteutetaan tilannekohtaisesti ja epäsäännöllisesti. Haastattelun perusteella yrityksessä D ei tehdä minkäänlaisia analysointeja riskeistä. Toimitusjohtajan mukaan kuitenkin tilitoimistopalvelut ja laadukas yhteistyö kirjanpitäjän kanssa takaavat kattavan turvan mahdollisilta riskeiltä. Yritys D:n toimitusjohtajan mukaan vakuuttamisen avulla voidaan suojautua riskeiltä, ja siksi yrityksen vakuutuksen pidetään ehdottomasti kattavasti ja harkitusti kunnossa.

Yrityksessä pidetään vuosittain myös tilannekohtainen päivitystapahtuma, jossa käydään lävitse olennaisia toiminnan muutoksia ja ajankohtaisia asioita.

Yritys G:ssä riskienhallintaa ei toteuteta ollenkaan. Haastattelussa yritys G:n toimitusjohtaja vastasi kysymyksiin lyhyesti. Yrityksessä ei tehdä arviointeja, eikä kvalitatiivisia eikä kvantitatiivisia analysointeja. Riskejä ei arvioida edes epäsäännöllisesti. Yrityksessä G riskienhallinta ei kuulu johdon päivittäisiin toimintoihin. Yrityksen toimitusjohtajan mukaan yrityksessä on kuitenkin huolehdittu keskeisistä vakuutuksista, joten yrityksessä harjoitetaan riskienhallintaa ainakin minimalistisella tasolla.

COSO-viitekehikoiden tunnettavuus ja riskienhallinnan kehittäminen

Halusin selvittää haastatteluiden avulla, ovatko pk-yritykset tietoisia sisäisen valvonnan ja sisäisen tarkastuksen viitekehikoista. Ensisijaisesti minua kiinnosti, ovatko pk-yritykset tietoisia COSO-viitekehikoista. Olennainen kysymys haastattelussa oli, olivatko yritykset kuulleet sisäisen valvonnan viitekehikoista ja ensisijaisesti riskienhallinnan COSO-ERM-mallista. Selvensin haastattelussa, että COSO-ERM koostuu valvontaympäristöstä, tavoitteenasettelusta, tapahtumien tunnistamisesta, riskien arvioinnista, riskeihin vastaamisesta, kontrollitoiminnoista, informaatiosta ja kommunikaatiosta ja jatkuvasta seurannasta.

Mielenkiintoinen havainto haastatteluissa oli, että kukaan haastateltavista ei ollut kuullut aikaisemmin COSO-viitekehikoista tai COSO-ERM-mallista. Yritys A:n toimitusjohtajan mukaan mallin osatekijät ovat kuitenkin hyödyllisiä. Yritys A:n toimitusjohtaja selvensi, että mallin osatekijöitä toteutetaan yrityksessä käytännössä. Yrityksessä A on siis valvontaympäristö, joka antaa perustan riskienhallinnalle. Sen lisäksi yrityksessä asetetaan keskeisiä toiminnallisia ja taloudellisia tavoitteita, tunnistetaan olennaisia tapahtumia, tehdään riskiarviointia, vastataan riskeihin, luodaan kontrollitoimenpiteitä, huomioidaan informaation ja tiedonkulku organisaatiossa sekä seurataan toimintaa jatkuvasti. Vaikka yritys A:n toimitusjohtaja ei siis ollut kuullut COSO-viitekeihkoista tai COSO-ERM-mallista, totesi hän kuitenkin hyödyntävänsä näitä mallin osatekijöitä käytännön työssään ja johtamisessaan.

Yritys B:n toimitusjohtaja ei myöskään ollut kuullut ennen haastattelua COSO-viitekehikoista tai COSO-ERM-mallista. Haastattelun perusteella yritys B:ssä ei ole käytössä mitään tietynlaista sisäisen valvonnan tai riskienhallinnan mallia, mutta toiminnassa on pyritty toteuttamaan omaa yksinkertaista järjestelmää. Tämä osittainen laatu- ja ympäristöjärjestelmä ottaa toimitusjohtajan mukaan huomioon COSO-ERM-mallin osa-alueet. Yritys B:n toimitusjohtaja ei osannut arvioida COSO-ERM mallin hyödyllisyyttä, mutta totesi osa-alueiden olevan sovellettavissa myös pk-yrityksiin.

Yritys C:n toimitusjohtaja ei muiden tapaan ollut aiemmin kuullut COSO-malleista, mutta huomioi kuitenkin mallin osa-alueiden tunnettavuuden. Yritys C:n toimitusjohtajan mukaan riskien arviointi, niihin vastaaminen, tiedonkulku ja seuranta ovat olennaisia osa-alueita yrityksen riskienhallinnassa. Yritys C:n toimitusjohtaja totesi haastattelussa, että komponentit ovat sovellettavissa käytännön työhön.

Yritykset D, E, F, G ja H eivät olleet kuulleet COSO-viitekehikoista, mutta yritys E:n toimitusjohtaja totesi haastattelussa, että osa-alueet ovat tuttuja ja ymmärrettäviä. Yritys F:n toimitusjohtajan mukaan malli voisi olla jopa hyödyllinen ja sovellettavissa yritykseen ja sen toimintaan. Yritys G:n toimitusjohtajan mukaan malli voisi olla sovellettavissa aivan pienimuotoisesti yrityksen toimintaan. Yritys H:n toimitusjohtaja sen sijaan totesi haastattelussa, että on nähnyt COSO-kaavion aiemminkin. Yritys H:n toimitusjohtajan mukaan mallin osa-alueet ovat hyvin sovellettavissa yrityksen riskienhallintaan. Yritys H:n toimitusjohtajaa arvelutti vain mallin soveltaminen ja sen tuomat rajoitteet käytännön työssä.

Olennainen johtopäätös haastatteluissa oli, että kaikkien haastateltavien mukaan yrityksien riskienhallintaprosesseissa on kehitettävää. Haastatteluiden perusteella voidaan todeta, että suuruusluokaltaan pienissä yrityksissä ja mikroyrityksissä riskienhallinnan tuomat haasteet liittyvät ensisijaisesti pienten- ja mikroyritysten resursseihin. Näissä yrityksissä ei välttämättä ole henkilöstöä, aikaa, osaamista tai ylimääräistä rahaa riskienhallintaprosessin luomiseksi.

6 JOHTOPÄÄTÖKSET JA YHTEENVETO

Tämä kappaleen tarkoitus on tiivistää tutkielman keskeisimmät johtopäätökset ja havainnot. Tutkielman edetessä olen jo tehnyt johtopäätöksiä ja havaintoja tutkimusongelmista. Johtopäätöksenä voin todeta, että pienissä ja keskisuurissa yrityksissä riskienhallinta kannattaa järjestää käytännönläheisesti. Johdon kannattaa integroida riskienhallinta osaksi pk-yrityksen päivittäisiä johtamistapoja ja rutiineja. Riskienhallinnan tulisikin olla yrityksessä osa organisaatiokulttuuria, strategiaa, johtamista ja yrityksen filosofiaa.

Mikro- ja pienyrityksissä ei välttämättä kannata soveltaa ERM-viitekehikon mukaista riskienhallintaa, koska monimutkaiset teoriat ja käytännöt voivat tuntua pitkällä aikavälillä puuduttavilta. Tämä taas johtaa siihen, että yrityksessä ei enää nähdä riskienhallinnan tuottamia etuja ja hyötyjä. Yrityksen johdon tulisi kuitenkin hankkia ymmärrys riskienhallinnan viitekehikoista. Yritys voi valita sellaisen riskienhallinnan standardin tai viitekehikon, joka soveltuu yrityksen johtamisjärjestelmään. Joka tapauksessa yrityksen johdon tulisi olla kiinnostunut riskienhallinnasta ja sen toteuttamisen vaihtoehdoista.

Riskienhallinta ei saisi kuitenkaan olla pk-yrityksissä liian epämuodollista, koska silloin riskienhallinnan laatua ja laajuutta on vaikea arvioida, kuin myös sitä miten riskienhallintaprosessissa on onnistuttu, ja mitä prosessissa pitäisi kehittää. Riskienhallinnan apuvälineenä on mahdollista käyttää vastuiden ja prosessikuvauksien määrittämistä sekä oikea-aikaista ja tarkoituksenmukaista dokumentointia. Johto vastaa riskienhallinnasta ja sen toimeenpanosta. Riskienhallinnan vastuiden ja velvollisuuksien määrittelyistä tulisi olla yrityksessä selkeä ohjeistus ja viesti koko yhteisölle.

Riskienhallinta on tärkeä johtamisen osa-alue myös mikro- ja pienyrityksissä, koska riskienhallinnan avulla yritys voi pienentää väärinkäytösriskiä ja luoda yhteisöön varmuutta. Vaikka yritys olisikin siis kuinka pieni tahansa, hyvin järjestetty valvontaprosessi auttaa yritystä muun muassa väärinkäytösten ehkäisemisessä ja täsmällisen taloudellisen tiedon saannissa.

ERM-viitekehikon käyttö on kuitenkin pk-yrityksissä mahdollista, ja jokaisessa yrityksessä on mietittävä, onko sen käyttö juuri sen yrityksen kohdalla kannattavaa.

ERM-viitekehikko voikin soveltua joihinkin keskisuuriin yrityksiin varsin hyvin. Lisäksi mallia on mahdollista soveltaa yrityksen edellyttämässä mittakaavassa ja mallista voi ainakin poimia hyödyllisiä vinkkejä ja ideoita. Pk-yrityksissä riskienhallinta tulee kohdentaa yrityksen kannalta merkittävimpiin riskeihin, joten riskienhallinnan kokonaisuudessaan tulisi olla pk-yrityksissä tarkoituksenmukaista. Riskienhallinnan tehokas toteuttaminen vaatii kuitenkin kattavaa ja toimivaa raportointijärjestelmää. Tarvittavan tiedon tulisi siis kulkea yhtiössä sujuvasti ja oikea- aikaisesti. Riskienhallintaprosessin toteuttaminen ja päivittäminen vaatii yrityksen johdolta myös jatkuvaa seurantaa.

Haastatteluiden perusteella voidaan todeta, että riskienhallinta voi perustua klassisille elementeille, eli riskien tunnistamisella, riskiarvioinnille ja riskeihin vastaamiselle. Tehokas ja toimiva riskienhallinta tuo lisäksi kilpailuetua ja lisäarvoa myös pk-yritykselle. Riskienhallintaprosessista ei kuitenkaan saa tehdä liian kaavamaista ja hankalaa. Tutkimuksen kohteena olevissa yrityksissä riskeihin vastattiin pääasiassa vakuuttamisen avulla. Tämä kertookin siitä, että yrityksissä arvioidaan mahdollisia epävarmuuksia ja uhkia ja niihin etsitään vastaamis- ja kontrollitoimenpiteitä. Haastatteluiden perusteella voin todeta, että pienten yritysten riskienhallinta muodostuu riskiarvioinnista, analysoinnista, riskeihin vastaamisesta ja muun muassa taloudellisten raporttien hyödyntämisestä. Haastateltavissa yrityksissä tiedonvaihtoa yrityksen johdon ja tilitoimiston välillä pidettiin tärkeänä. Yrityksen johdon tulisikin olla kiinnostunut talouteen liittyvistä raporteista ja tunnusluvuista, jotta ikäviltä ja odottamattomilta yllätyksiltä vältyttäisiin.

Haastatteluiden perusteella voin myös todeta, että COSO-viitekehikoiden tunnettavuus mikro- ja pienyrityksissä on heikkoa. Kukaan haastateltavista ei ollut kuullut riskienhallinnan teorioista, eikä COSO-malleista. Haastateltavat kuitenkin pitivät COSO-mallien osa-alueita käytännöllisinä ja olennaisena osana riskienhallintaprosessia ja johtamista. Haastatteluista tekemieni johtopäätösten perusteella, yritysten riskienhallintaprosessit koostuvat myös COSO-mallien elementeistä. Haastattelemissani yrityksissä riskejä arvioidaan, riskeihin vastataan ja johto myös seuraa riskienhallintaa. Yrityksien riskienhallintaprosesseissa oli osa-alueita, jotka löytyvät COSO-malleista. Haastatteluiden perusteella COSO-mallien osatekijöitä on siis mahdollista soveltaa pk-yritysten riskienhallinnassa.

Pienten ja keskisuurten yritysten valvontaympäristö koostuu riskienhallintafilosofiasta, riskinottohalukkuudesta, johdon asenteista, rehellisyydestä ja eettisistä arvoista, pätevyyteen sitoutumisesta, organisaatiorakenteesta, vastuiden ja velvollisuuksien jakamisesta ja henkilöstöhallinnon menettelytavoista. Valvontaympäristöllä on suuri merkitys yrityksen riskienhallinnassa ja sen toteutumisessa. Valvontaympäristön ilmapiiri määrittelee pitkälti sen, miten yritys ja sen johto suhtautuu riskeihin ja riskienhallintaprosesseihin.

Osakeyhtiön johto kuuluu olennaisesti yrityksen valvontaympäristöön, koska johto määrittelee sen, miten koko yrityksen henkilöstö suhtautuu riskienhallintaan. Sillä miten johto hoitaa lakisääteiset ja tarkoituksenmukaiset tehtävänsä on suuri merkitys, koska johdon toiminta näyttäytyy esimerkkinä koko muulle organisaatiolle. Johdon toiminta vaikuttaa näin koko yrityksen ilmapiiriin ja valvontaympäristöön.

Sellaisessa valvontaympäristössä, jonka johdolla on positiivinen suhtautuminen riskienhallintaan, riskejä halutaan tunnistaa ja arvioida tarkoituksenmukaisesti ja tehokkaasti. Valvontaympäristö on koko riskienhallinnan lähtökohta ja niin sanotusti ”käynnistysmoottori”. Voidaan siis todeta, että positiivisessa valvontaympäristössä riskienhallintaan suhtaudutaan paremmin ja sitä myös hoidetaan paremmin kuin valvontaympäristössä, jonka ilmapiiri on kokonaisuudessaan negatiivinen. Riskienhallinnasta saatavat hyödyt voivat olla suuremmat sellaisessa organisaatiossa, jossa on positiivinen valvontaympäristö ja myönteinen ilmapiiri.

Haastatteluiden perusteella voidaan myös todeta, että yrityksen valvontaympäristö ja sen sisältö vaikuttavat riskienhallintaprosessiin ja sen toteuttamiseen. Yrityksissä, joiden johto suhtautui myönteisesti riskienhallintaprosessiin, toteutettiin myös riskienhallintaa ja riskienhallintaprosessia.

7 LÄHTEET

Kirjallisuus ja lehtiartikkelit:

Ahokas, Niina. Kuinka järjestää pienen yhtiön sisäinen valvonta? Balanssi 03/2013

Ahokas, Niina. 2012. Yrityksen sisäinen valvonta. Helsinki: Edita

Alasuutari,P. 1995. Laadullinen tutkimus. Jyväskylä: Vastapaino

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. Helsinki:Edita.

Australian/New Zealand Standard, Risk management 2004 (AS/NZS 4360:2004).

Chambers, A.D 1996. Internal auditing. Aldershot: Darthmouth, cop. 1996.

Crouhy, Michel, Galai, Dan, Mark, Robert 2001. Risk management. United States of America: McGraw-Hill

Erma, Juhani, Rasila, Tommi, Virtanen, Olli V. 2010. Hyvä hallitustyö. Helsinki: Helsingin kamari Oy.

Eskola, J. & Suoranta, J. 1998. Johdatus laadulliseen tutkimukseen. Jyväskylä: Vastapaino

Hannula, Antti 2003. Hallitustyöskentelyn käsikirja. Helsinki: WSOY.

Harrington, Scott E., Niehaus, Gregory R. 2003. Risk management & insurance. Second edition. New York: McGraw-Hill/Irwin.

Hightower, Rose 2009. Internal control policies and procedures. Hoboken NJ USA: Wiley Agrawal R.C 2009. Risk Management Jaipur India: ABD Publishers

Hirsjärvi, Sirkka, Remes, Pirkko, Sajavaara, Paula. 2009. Tutki ja kirjoita. Helsinki:Kustannusosakeyhtiö Tammi.

Holopainen, Atte, Koivu, Eila, Kuuluvainen, Antero, Lappalainen, Keijo, Leppiniemi, Jarmo, Mikola, Matti, Vehmas, Keijo. 2010. Sisäinen tarkastus. Helsinki: Tietosanoma Oy.

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

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

Immonen, Raimo, Nuolimaa, Risto. 2007. Osakeyhtiöoikeuden perusteet. Helsinki: Talentum.

Jokipii, A. 2006. The Structure and Effectiveness of Internal Control. Vaasan yliopisto. Acta Wasaensia No. 166.

Journal of Accountancy, 2008. COSO´s Eight Components of Enterprise Risk Management. Vol.205, Issue 4, p50-50, 1/2p.

Kuusela, Hannu, Ollikainen, Reijo 2005. Riskit ja riskienhallinta. Tampere: Tampereen Yliopistopaino Oy.

Lillis, A. & Mundy, J. 2009. Cross-Sectional Field Studies in Management Accounting Research – Closing the Gaps between Surveys and Case Studies. Journal of accounting Research, 17, 119-141.

Listaamattomien yhtiöiden hallinnoinnin kehittäminen. Asialuettelo listaamattomien yhtiöiden hallinnoinnin kehittämiseksi. 2006. Helsinki: Keskuskauppakamari.

Maijoor, S. 2000. The Internal Control Explosion. Internal Journal of Auditing 4, 101-109)

Marttila, Veikko 1998. Tehokas sisäinen tarkastus yritysjohdon tukitoimintona. Tampere: Pk-Paino Oy.

Metsämuuronen, J. 2006. Tutkimuksen tekemisen perusteet ihmistieteissä. Jyväskylä: International Methelp Ky.

Myllymäki Arvo 2007. Finanssihallinto-oikeus Valtion ja kuntien varainkäyttö ja varainkäytön valvonta. Juva:WSOY

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

Norri, Matti 2006. Osakeyhtiö. Helsinki: Rakennustieto Oy.

Pickett, K.H. Spencer 2004. The internal auditor at work. New Jersey: John Wiley & Sons.

Risk management in the public services. 2001. London: The chartered institute of public finance and accountancy. CIPFA.

Rittenberg, Larry E, Schwieger, Bradley J 2003. Auditing: concepts for a changing environment. Mason (Ohio): Thomson/South-Western

Sisäiset tarkastajat ry. Ammatillisten asioiden toimikunta. COCO-malli-opas valvontakriteereistä. muistio. 1999

Sisäisen tarkastuksen kansainväliset ammattistandardit 2013. The Institute of Internal Auditors

Sisäisen tarkastuksen kansainväliset ammattistandardit 2011. The Institute of Internal Auditors.

Skipper, Harold D, Kwon, Jean W 2007. Risk management and insurance: perspectives in a global economy. Malden: Blackwell Pub

Standards Australia/Standards New Zealand. 2004 Risk management guidelines, companion to AS/NZS 4360:2004. NSW 2001 and Standards New Zealand

Suominen, Arto 2003. Riskienhallinta. Helsinki: WSOY.

Sutinen, Mika, Antikainen, Ahti. 1996. PK-yrittäjän käsikirja. Helsinki: Kauppakaari Oy

Tiihonen, Timo 2007. Hallitus vai toimitusjohtaja- työnjako ja vastuut. Boardman Oy.

Tuomi, Jouni, Sarajärvi Anneli. 2003. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Tammi

Vaughn, Emmet J. 1997. Risk management. Canada: john Wiley & Sons, Inc.

Veijola Risto. Sitoutuako vain tiettyyn riskienhallinnan standardiin? Tilintarkastus 04/2012

Veijola Risto. Iso 31000-standadri- riskienhallinta tulee osaksi organisaation kaikkea toimintaa. Tilintarkastus 4/2012

Williams JR, C Arthur, Smith, Michael L, Young, Peter C 1998. Risk management and insurance, eight edition. Singapore: Irwin/McGraw-Hill.

Verkkolähteet:

Committee of Sponsoring Organizations of The Treadway Comission. 2013. COSO Issues Updated Internal Control-Integrated Framework and Related Illustrative Documents
http://www.coso.org/documents/COSO%20Framework%20Release%20PR%20May%2014%202013%20Final%20PDF.pdf 10.1.2014

COSO ERM. Enterprise Risk Management – Integrated Framework. Executive summary 2004. Committee of Sponsoring Organizations of the Treadway Commission (COSO)
http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf 27.1.2011.

COSO ERM. Enterprise Risk Management- Integrated Framework (Kokonaisvaltainen ajatusmalli organisaation riskienhallintaan) Tiivistelmä. 2004
http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Finnish.pdf 27.1.2011.

COSO. Internal Control- Integrated Framework, Executive Summary (1992)
Committee of Sponsoring Organizations of the Treadway Commission (COSO)
http://www.coso.org/ic-integratedframework-summary.htm luettu 13.2.2013

COSO. Internal Control-Integrated Framework, (2013)
Committee of Sponsoring Organizations of The treadway Comission (COSO)
http://www.coso.org/ luettu 13.8.2013

COSO:n internet-sivut. http://www.coso.org/ 10.11.2013

EK 2013. Elinkeinoelämän Keskusliitto: PK-yritykset EK:ssa. http://www.ek.fi/www/fi/yrittajyys_ja_pk/pk_yritykset/pk_yritykset_ekssa.php 15.7.2013

EK 2013. Elinkeinoelämän Keskusliitto: PK-yritysten merkitys kansantaloudessa ja EU:ssa. http://www.ek.fi/ek/fi/yrittajyys_ym/yrittajyys/tietoa_pk-yrityksista/index.php 15.7.2013

EK 2013. Elinkeinoelämän Keskusliitto: Tietoa PK-yrityksistä. http://www.ek.fi/www/fi/yrittajyys_ja_pk/pk_yritykset/index.php 15.7.2013

Euroopan komission suositus 2003/361/EY/2003/361/EY:Mikroyritysten ja pienten ja keskisuurten yritysten määritelmästä.
http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:fi:PDF 13.1.2011.

Euroopan Komissio, 2006. Pk-yritysten uusi määritelmä. Käyttäjän opas ja ilmoitusmalli http://ec.europa.eu/enterprise/policies/sme/files/sme_definition/sme_user_guide_fi.pdf 30.1.2014

Journal of accountancy, 2013. Newly released COSO framework a fresh look at internal control, http://www.journalofaccountancy.com/News/20137970 14.5.2013

Kupi, Eija, Keränen, Jaana, Lanne, Marinka 2009. Riskienhallinta osana pk-yritysten strategista johtamista. http://www.vtt.fi/inf/pdf/workingpapers/2009/W137.pdf 11.1.2014

Osakeyhtiölaki21.7.2006/624
http://www.finlex.fi/fi/laki/ajantasa/2006/20060624?search[type]=pika&search[pika]=osakeyhti%C3%B6laki 20.12.2013

Pk-yrityksen riskienhallinta. Riskilajit http://www.pk-rh.fi/riskilajit. 5.1.2013

Purdy Grant. ISO 31000:2009-Setting a new standard for risk management. Risk analysis,vol.30,no6,2010.
http://www.broadleaf.com.au/pdfs/articles/art_riskanalysis_iso31000.pdf. 15.8.2013

Ratsula Niina 23.8.2011 Kuka on vastuussa organisaation sisäisestä valvonnasta?
http://www.codeofconduct.fi/kuka-on-vastuussa-organisaation-sisaisesta-valvonnasta/
10.11.2013

Tilintarkastuslaki13.4.2007/459
http://www.finlex.fi/fi/laki/ajantasa/haku.php?search[type]=pika&search[pika]=tilintarkastuslaki&submit=Hae 20.12.2013

TK 2009. Tilastokeskus: Katsaus yrityksiin ja toimipaikkoihin. http://www.stat.fi/til/syr/2009/syr_2009_2010-11-26_kat_001_fi.html 13.1.2013

Varjo, Pirkko 2006. Selkeämpi ja ystävällisempi pk-yrityksille. Varsinais- Suomen yrittäjä, 09/2006.http://www.y-lehti.fi/arkisto/artikkeli/965 11.1.2014

LIITTEET

LIITE 1: Haastattelukysymykset

Riskienhallinta pk-yrityksissä

1. Minkälaisia ajatuksia teillä on sisäisestä valvonnasta ja riskienhallinnasta?

- Positiivisia vai negatiivisia ajatuksia?
- Onko riskienhallinta tuttua?
- Miten tärkeänä pidätte riskienhallintaa?

2. Toteutetaanko yrityksessänne riskienhallintaa?

- Miten riskienhallintaa toteutetaan?
- Säännöllisesti vai epäsäännöllisesti?
- Kuka riskienhallinnasta vastaa?

3. Arvioidaanko yrityksessänne mahdollisia riskejä?

- Miten riskejä arvioidaan ja analysoidaan?
- Onko käytössä kvalitatiivisia tai kvantitatiivisia analysointeja?

4. Miten yrityksessänne vastataan riskeihin?

- Millaisia kontrollitoimenpiteitä yrityksessänne on? Kontrollitoimenpiteitä ovat mm. vakuutukset, käyttäjätunnukset, salasanat, hyväksymismenettelyt, varallisuuden turvaaminen, valtuuksien määrittelyt, tehtävien hajauttaminen, ym.?
- Miten yrityksenne valvonta ja jatkuva seuranta on toteutettu?

4. Oletteko kuulleet sisäisen valvonnan ja riskienhallinnan COSO-viitekehikoista?

Riskienhallinnan COSO-ERM viitekehikko koostuu valvontaympäristöstä, tavoitteenasettelusta, tapahtumien tunnistamisesta, riskien arvioinnista, riskeihin vastaamisesta, kontrollitoiminnoista, informaatiosta ja kommunikaatiosta ja jatkuvasta seurannasta

- Muut mahdolliset tunnetut mallit?
- Mallien käytettävyys ja soveltuvuus?
- Mallin hyödyllisyys?

5. Tuottaako tai tuottaisiko mahdollinen riskienhallinta mielestänne lisäarvoa yritykselle?

- Uskotteko riskienhallinnan olevan hyödyllistä?
- Riskienhallinnan muut vaikutukset?

6. Onko riskienhallintaan mielestänne tarpeeksi resursseja esimerkiksi henkilöstöä, rahaa, aikaa?

7. Olisiko riskienhallintaprosessianne mahdollista kehittää?

8. Jotain lisättävää?