TAMPEREEN YLIOPISTO
Johtamiskorkeakoulu

SISÄISEN VALVONNAN KEHITTÄMINEN – KONTROLLIEN INTEGROIMINEN OSAKSI YRITYKSEN PROSESSEJA

Case UPM-Kymmene Oyj

Yrityksen taloustiede, laskentatoimi
Pro gradu -tutkielma
heinäkuu 2013
Ohjaaja: Petri Vehmanen
Matti Anttila

TIIVISTELMÄ

Tampereen yliopisto	Johtamiskorkeakoulu; yrityksen laskentatoimi
Tekijä:	ANTTILA, MATTI
Tutkielman nimi:	Sisäisen valvonnan kehittäminen – kontrollien integroiminen osaksi yrityksen prosesseja, case UPM-Kymmene Oyj
Pro gradu -tutkielma:	81 sivua, 4 liitesivua
Aika:	Heinäkuu 2014
Avainsanat:	sisäinen valvonta, kontrolli, COSO, lisäarvo, johtamisjärjestelmä

Yritysten kasvanut koko, lisääntynyt monimutkaisuus ja kiristyvä maailmanlaajuinen kilpailu asettavat haasteita yritysten johtamiselle. Johto pyrkii varmistamaan toiminnan tarkoituksenmukaisuuden ja siitä annetun informaation luotettavuuden erilaisten johtamisjärjestelmien kuten sisäisen valvonnan avulla. Kun sisäinen valvonta pettää, voi siitä pahimmassa tapauksessa seurata Yhdysvalloissa 2000-luvun alussa koetun kaltainen skandaali, jossa pörssiyhtiöitä ajautuu konkurssiin ja sijoittajat menettävät miljardeja. Sisäinen valvonta on tämän jälkeen ollut hyvin edustettuna akateemisessa tutkimuksessa, mutta se on painottunut käsittelemään talousraportoinnin luotettavuuteen tähtäävää sisäistä valvontaa ja erityisesti Sarbanes-Oxley-lain vaikutuksia.

Tässä tutkimuksessa perehdytään toiminta-analyyttisen case-tutkimuksen avulla sisäisen valvonnan kehittämiseen. Akateemisen kirjallisuuden valtavirrasta poiketen tutkimus keskittyy kaikkien kolmen COSO:n sisäisen valvonnan viitekehyksen mukaisen tavoitteen kehittämiseen: yrityksen toiminnan tarkoituksenmukaisuuden varmistamiseen, talousraportoinnin luotettavuuteen sekä lakien ja säännösten noudattamiseen. Tutkimuksen tavoitteena on selvittää, miten COSO:n viitekehyksen mukainen riskianalyysi ja valvontatoimintojen suunnittelu tehdään käytännössä, mitä ongelmia käytännön sovelluksessa kohdataan ja miten havaitut ongelmat voitaisiin ratkaista. Tutkimuksen empiirisen osioin perusteella selvitetään myös, mitä sisäisen valvonnan kehittämisellä pyritään saavuttamaan case-yrityksessä.

Tutkimuksen aluksi pohditaan sisäisen valvonnan käsitettä ja sisäisen valvonnan tarkoitusta. Tämän jälkeen tutkitaan kirjallisuuden perusteella, mitä on tehokas sisäinen valvonta ja mitkä tekijät siihen ovat yhteydessä. Empiirisen aineiston perusteella etsitään käytännön vastinetta kirjallisuudessa mainituille tekijöille. Tutkimuksen tulokset on saatu kokoamalla sisäisen valvonnan tehokkuuteen vaikuttavat tekijät yhteen ja vertailemalla niitä teoreettisen ja empiirisen aineiston valossa. Tutkimuksen tulokset lisäävät ymmärrystä sisäisen valvonnan kehittämisen motiiveista, käytännön haasteista ja menetelmistä, joiden avulla sisäistä valvonta saadaan tehostettua.

SISÄLLYS

1. JOHDANTO

1.1. Tutkimuksen tausta

Sisäistä valvontaa on ollut olemassa yrityksissä ja muissa organisaatioissa jo kauan sitten johtamisen ja seurannan luontaisena osana. Yksinkertaisimmillaan kyse on siitä, että omistaja pyrkii varmistamaan, että palkolliset tekevät työtä tarkoituksenmukaisesti. (Leitch 2008, 13) Nykypäivän yritysmaailmassa sisäinen valvonta on yksi merkittävä keino, jolla tavoitellaan tehokkaampaa toimintaa organisaatiossa ja sitä kautta tavoitellaan kilpailuetua kilpailijoihin nähden. Sisäinen valvonta tuottaa myös läpinäkyvyyttä ehkäisten väärinkäytöksiä, joiden torjuminen on 2000-luvulla muodostunut sisäistä valvontaa käsittelevän kirjallisuuden tärkeimmäksi huomion kohteeksi.

Akateeminen kiinnostus sisäistä valvontaa kohtaan kasvoi, kun vuonna 1992 Committee of Sponsoring Organization of the Treadway Commissionin (jäljempänä COSO) julkaisi sisäisestä valvonnasta ensimmäisen viitekehyksen ”Internal Control – Integrated Framework” (jäljempänä IF tai COSO IF). COSO IF on luonteeltaan ohjeellinen viitekehys, joka ensimmäistä kertaa määrittelee sisäisen valvonnan käsitteet, tavoitteet, vastuurakenteet ja lisäksi se antaa muutamia käytännön esimerkkejä sisäisen valvonnan sovelluksista (Aldridge & Colbert 1994, 21; Lee & Colbert 1997, 682). Vuoden 1992 COSO IF:stä on sittemmin tullut hyvin laajalti käytetty sisäisen valvonnan viitekehys (COSO 2013). Sisäisen valvonnan tehostamista viitekehyksen avulla on perusteltu mm. yritysten koon kasvulla ja entisestään kasvaneella monimutkaisuudella (COSO 1992, 4).

Sisäisestä valvonnasta tuli kuitenkin hetkessä aktiivisesti kirjoitettu aihe akateemisessa kirjallisuudessa, kun 2000-luvuna alussa Yhdysvalloissa paljastui useamman pörssiyhtiön kirjanpitoskandaali. Skandaalia seuranneiden konkurssien myötä sijoittajille aiheutui arviolta 460 miljardin dollarin tappiot (Cotton 2002, 1). Skandaalin aiheuttaneissa yhtiöissä oli mm. toimittu vastuuttomasti sijoittajien varoilla ja peitelty toimintaa vilpillisellä raportoinnilla (Hemraj 2004, 268). Sisäinen valvonta ei ollut näissä yhtiöissä ollut riittävää (Benston 2006, 483) ja vastaavanlaisten skandaalien pelossa

sijoittajien luottamus markkinoihin heikkeni (Conyon, Judge & Useem, 2011). Pörssiyhtiöiden sisäisen valvonnan vahvistamiseksi ja sijoittajien luottamuksen palauttamiseksi Yhdysvaltain kongressi sääti vuonna 2002 lain ”Public Company Accounting Reform and Investor Protection Act”, joka yleisemmin tunnetaan nimellä Sarbanes-Oxley-Act (Sarbanes-Oxley-laki, jäljempänä SOX). Lain tarkoituksena on suojella sijoittajia varmistamalla, että markkinoilla julkistettu informaatio on tarkkaa ja luotettavaa (Sarbanes-Oxley Act of 2002, 1).

SOX:n voimaantulon jälkeen akateemista kirjallisuutta on julkaistu runsaasti ja suuri osa siitä käsittelee SOX:n vaikutuksia markkinoilla. Markkinoiden tehokkuutta ennen ja jälkeen SOX:n ovat tutkineet mm. Jain, Kim & Rezaee (2008). Hammersley, Myers ja Shakespeare (2007) sekä Kim ja Park (2009) ovat tutkineet, miten markkinat reagoivat SOX:n edellyttämään julkiseen tiedonantoon, jossa yhtiö raportoi havaitusta heikkoudesta sisäisessä valvonnassa. Lisäksi on tutkittu, miten raportoitu heikkous sisäisessä valvonnassa otetaan markkinoilla vastaan, kun tilintarkastaja on joko pieni tilintarkastusyhteisö tai joku neljästä suuresta tilintarkastusyhteisöstä (Hammersley ym. 2007).

SOX:ia ja erityisesti sen sisäisestä valvonnasta määräävää pykälää 404 on myös kritisoitu sen aiheuttamien suurten kustannusten vuoksi (Berlau 2005) ja siitä, että lain edellytysten mukaan laaditut kontrollijärjestelmät kehittävät suuren määrän talousraportoinnin luotettavuutta varmistavia kontrolleja (Tackett, Wolf & Claypool 2006). Tackett ym. (2006) päätyivät tutkimuksessaan johtopäätökseen, että SOX:n kustannukset ovat suuremmat kuin sen tuomat hyödyt.

Sisäisen valvonnan hyödyt eivät kuitenkaan jää vain sijoittajien luottamuksen palautumiseen (Campbell, Campbell & Adams 2006). Campbell ym. (2006) kirjoittavat, että hyvin toteutetun sisäisen valvonnan myötä yhtiön strategia on tehokkaasti jalkautettavissa, vilpillinen käytös ehkäistään, riskit havaitaan ja niihin vastataan, ja lisäksi sisäinen valvonta auttaa tehostamaan ja harmonisoimaan yhtiön liiketoimintaprosesseja. Nämä ovat kuitenkin hyötyjä, joita ei SOX:n yhteydessä juurikaan ole tutkittu, koska SOX edellyttää vahvaa sisäistä valvontaa talousraportoinnin osalta. Muilta osin COSO IF:stä julkaistu tutkimus on ollut vähäisempää. Ramos (2004) on analysoinut COSO-komponenttien merkitystä ja mitkä tekijät tekevät niistä tärkeitä.

Hermanson, Smith ja Stephens (2012) ovat edelleen analysoineet sisäisen valvonnan komponenttien tärkeimpiä ilmenemiskohtia, jotta näihin osattaisiin kiinnittää huomiota. Jokipii ja Agbejule (2009) ovat puolestaan tutkineet COSO IF:n mukaisen sisäisen valvonnan komponenttien painotuksen yhteyttä yrityksen strategiaan. Näistä tutkimuksista voidaan saada osviittaa siitä, mihin seikkoihin sisäisen valvonnan kehityksessä olisi syytä kiinnittää huomiota.

Jokainen sisäisen valvonnan järjestelmä on erilainen (COSO 1992, 14). COSO:n IF on kattava teoreettinen viitekehys sisäiselle valvonnalle, mutta teoreettisen ohjeistuksen soveltaminen käytäntöön edellyttää useiden sellaisten ongelmien ratkaisemista, joihin ei COSO:n ohjeistuksessa ole suoraa ratkaisua. Tässä tutkimuksessa etsitään ratkaisuja sisäisen valvonnan kehittämiseen kirjallisuudesta ja empiirisen aineiston perusteella. Empiirinen aineisto perustuu projektiin, jossa kehitetään olemassa olevaa sisäisen valvonnan järjestelmää yrityksessä, jota SOX ei velvoita.

1.2. Tutkimuksen tavoitteet ja odotetut tulokset

Tämän tutkimuksen tavoitteena on syventyä sisäisen valvonnan uudistamiseen COSO IF:n puitteissa kansainvälisessä pörssiyrityksessä ja analysoida kehitysprojektin vaiheita sekä mahdollisia haasteita. Kirjallisuuden avulla etsitään viitteitä siitä, mitä seikkoja tutkimuksen empiirisessä osiossa saattaa ilmetä. Empiirisen osan tutkimus suoritetaan case-yrityksessä, jonka käytössä on kontrollijärjestelmä, joka perustuu SOX:n edellytyksiin painottuen taloudellisen raportoinnin osaan COSO:n IF:stä. Uuden kontrollijärjestelmän ei tarvitse täyttää SOX:n edellytyksiä ja uudistettu sisäisen valvonnan järjestelmä laaditaan kattamaan kaikki kolme COSO:n sisäisen valvonnan tavoitetta täysipainoisesti. Muutoksen ansiosta kehityksessä voidaan keskittyä entistä perusteellisemmin kontrollijärjestelmän tehokkuuteen, tarkoituksenmukaisuuteen sekä integroimaan valvonta osaksi liiketoimintaprosesseja seuraten COSO:n vuonna 1992 julkaisemaa viitekehystä.

Useita suomalaisyrityksiä nähneen asiantuntijan mukaan suunnitelmallisten ja laajojen kontrollijärjestelmien hyödyntäminen ei ole Suomessa kovin yleistä (Kaski 8.4.2013). Case-tutkimuksen kohteena olevassa yrityksessä on verraten vahva sisäisen valvonnan kulttuuri, joka on peruja siltä ajalta, kun yhtiö oli vielä listautuneena Yhdysvaltalaisessa

pörssissä ja SOX velvoitti yhtiötä. Käytössä oleva sisäisen valvonnan järjestelmä on tarkasti dokumentoitu ja sitä sekä seurataan että tarkastetaan säännöllisesti ja kattavasti siitä huolimatta, että sisäistä valvontaa ei laki enää sääntele. Pörssiyhtiönä yhtiö noudattaa Suomen listayhtiöiden hallinnointikoodia vuodelta 2010, joka ei kuitenkaan ole vaatimuksiltaan läheskään yhtä vaativa kuin SOX. Tällaisessa ympäristössä sisäisen valvonnan kehittäminen ja COSO-mallin soveltaminen tehdään todennäköisesti keskimääräistä systemaattisemmin ja täsmällisemmin.

Tutkimuksessa selvitetään vastausta seuraaviin kysymyksiin:

1. Mitkä ovat ne tekijät, joiden vuoksi uuden kontrollijärjestelmän kehittäminen katsotaan tarpeelliseksi?
2. Mitä vaiheita kontrollijärjestelmän kehittäminen sisältää ja miten projekti toteutetaan käytännössä?
3. Mitä ongelmia kehityksessä ilmenee ja miten ne ratkaistaan?

Ensimmäinen kysymys edellyttää perehtymistä sisäisen valvonnan kehityksen lähtötilanteeseen, jotta ymmärretään, miksi sisäistä valvontaa kehitetään. Sisäinen valvonta ei ole vain dokumentoitu säännöstö, vaan myös organisaation toimintatavat vaikuttavat lopputukokseen. Tämän vuoksi kehitysprojektin lähtötilanteeseen vaikuttava case-yrityksen sisäisen valvonnan muutoksiin on tässä tutkimuksessa myös tutustuttava. Joitakin motiiveja sisäisen valvonnan kehittämiselle voi olla mahdollista löytää COSO IF:stä, jossa on määritelty sisäisen valvonnan tuomia mahdollisia hyötyjä. Käytännön tutkimuksen odotetaan osoittavan, mitkä näistä hyödyistä ovat case-yrityksen kannalta tärkeitä ja mahdollisesti löytää joitain viitekehyksessä mainitsematta jätettyjä seikkoja.

Toinen kysymys tarkastelee sisäisen valvonnan teoreettisen ohjeistuksen soveltamista käytännössä. On mahdollista, että sovellus poikkeaa huomattavasti siitä systemaattisesta kuvasta, jonka teoreettinen malli antaa ymmärtää. Tämän kysymyksen kohdalla on hyvä kiinnittää huomiota siihen, missä kontrollijärjestelmän kehittämiseen tarvittava tietotaito on ja miten se koostetaan tarkoituksenmukaiseksi kokonaisuudeksi.

Kolmas kysymys jatkaa toisen kysymyksen ajatusta, jonka mukaan teorian soveltaminen käytännössä ei todennäköisesti ole mutkatonta. Tässä vaiheessa erityisiä mielenkiinnonkohteita ovat kehitysprosessissa ilmenneet ongelmat, niiden

oletettavimmat syyt sekä ongelmien ratkaisut. Sisäistä valvontaa käsittelevä kirjallisuus tarjoaa vastauksia joihinkin ongelmiin, mutta on mahdollista, että myös uusiin ratkaisuihin päädytään.

Mikäli kaikkiin kysymyksiin löydetään sopivasti vastauksia, olisi mahdollista listata esimerkkejä koetuista haasteista, jotka voisivat tulla vastaan myös muissa vastaavanlaisissa sisäisen valvonnan kehitysprojekteissa. Mikäli todennäköisesti kohdattavat haasteet ovat sisäisen valvonnan kehittäjän tiedossa, on tämän mahdollista varautua niihin etukäteen ja minimoida haasteiden negatiiviset vaikutukset.

1.3. Aihealueen rajaus

Sisäinen valvonta on osa hyvää hallinnointitapaa eli Corporate Governancea. Tähän laajaan kokonaisuuteen ja sen ominaisuuksiin ei tutkimuksessa perehdytä. Case-yritystä sitoo suomalainen CG-ohje, Suomen listayhtiöiden hallinnointikoodi, mutta tämän suosituksen sisäistä valvontaa käsittelevä kohta on kokonaisuudessaan tämä: ”Yhtiön on määriteltävä sisäisen valvonnan toimintaperiaatteet. Tuloksellinen liiketoiminta edellyttää, että yhtiö valvoo jatkuvasti toimintaansa. Hallitus huolehtii siitä, että yhtiössä on määritelty sisäisen valvonnan toimintaperiaatteet ja että yhtiössä seurataan valvonnan toimivuutta”. Case-yrityksen tilinpäätöksessä on lausunto sisäisen valvonnan olemassaolosta ja sen toimintaperiaatteista (UPM Oyj vuosikertomus 2012, 143), mutta raportoitujen toimintaperiaatteiden tutkiminen ja Suomen listayhtiöiden hallinnointikoodin edellytysten analysointi ei ole tutkimuksen kannalta keskeistä.

Riskienhallinta liittyy myös hyvään hallinnointitapaan, mutta riskienhallinta on lähtökohtaisesti olemassa eri tarkoitusta varten kuin sisäinen valvonta. Riskienhallinta katsoo pidemmälle tulevaisuuteen kuin johtamisprosessien kehittämiseen tähtäävä sisäinen valvonta. On toki kirjoittajia, joiden mukaan riskienhallinta ja sisäinen valvonta tulisi yhdistää toisiinsa (kuten Leitch 2008), mutta esimerkiksi COSO määrittelee ne erillisiksi kokonaisuuksiksi siten, että sisäinen valvonta on riskienhallinnan erityistapaus (ks. http://www.coso.org/erm-faqs.htm, viitattu 6.1.2014). Riskienhallinnan kokonaisuutta ei tässä tutkimuksessa käsitellä.

Sisäisen valvonnan kehittämistä tutkitaan COSO:n vuoden 1992 viitekehyksen puitteissa. Keväällä 2013 COSO julkaisi uudistetun viitekehyksen, mutta sitä käsittelevää kirjallisuutta on tutkimuksen kannalta julkaistu varsin vähän. Lisäksi uuden viitekehyksen määritelmät, elementit ja muut perusasiat ovat samat kuin alkuperäisessä viitekehyksessä, joskin COSO on selkiyttänyt viitekehyksen tekstiä ja panostanut enemmän sen sovellettavuuteen käytännössä (COSO 2013). Toisaalta, myös case-yrityksen kehitysprojekti perustuu vuoden 1992 viitekehykseen, joten tutkimuksen kannalta on perusteltua, että vuoden 2013 viitekehys jätetään tutkimuksen ulkopuolelle.

Sisäisen valvonnan komponentteja on COSO IF:n mukaan viisi. Komponentit ovat aina sidoksissa toisiinsa, mutta komponenteista kaksi on tutkimuksen empiirisen osan kannalta keskeisiä: riskianalyysi ja valvontatoiminnot. Kaikki IF:n komponentit käsitellään tutkimuksen teoriaosassa, jotta käsitys sisäisen valvonnan kokonaisuudesta saadaan tuotua tutkimuksessa esille. Näiden kahden elementin kehittämisestä ja käytännön sovelluksesta tutkitaan empiirisessä osassa siten, että riskianalyysin suunnittelu ja toteutus sekä valvontatoimintojen suunnittelu ovat tutkimuksen piirissä. Valvontatoimintojen toteutus- ja seurantavaihetta ei tutkita. Laadittavan kontrollijärjestelmän tarkastelu tutkimuksessa keskittyy operatiivisten prosessien ja tukitoimintojen prosessien valvontaan. Ylimmän johdon ja koko yhtiön tason valvontaan ei tutkimuksessa perehdytä.

1.4. Tutkimusmetodi

Tutkimus on tyypiltään laadullinen tapaustutkimus. Empiirinen data kerätään yhdestä kohdeyrityksestä ja tutkimusmenetelmänä käytetään haastattelujen ja dokumentoidun informaation analysointia. Tapaustutkimuksessa seurataan käytännön sovellusta sisäistä valvontaa ohjaavasta viitekehyksestä ja verrataan sovellusta muuhun viitekehyksen sovelluksesta kirjoitettuun kirjallisuuteen. Tämän tutkimuksen, kuten yleensäkin laadullisen tutkimusotteen, pääasiallisena tarkoituksena on yleensä lisätä ymmärrystä yritysten toiminnasta erittelemällä laadullista aineistoa, ei niinkään selittää ja kontrolloida yritysten toimintaa. (Koskinen, Alasuutari & Peltonen 2005, 16)

Neilimon ja Näsin (1980) rakentama luokittelu liiketalouden tutkimuksessa käytetyistä tutkimusotteista on usein käytetty. Jaottelun mukaiset tutkimusotteet ovat

käsiteanalyyttinen, nomoteettinen, päätöksentekometodologinen ja toiminta-analyyttinen tutkimusote. Luokittelua on myöhemmin täydennetty konstruktiivisella tutkimusotteella (Kasanen, Lukka & Siitonen 1991) Tämä tutkimus kuuluu luokittelun perusteella toiminta-analyyttisen tutkimusotteen piiriin. Toiminta-analyyttisen tutkimusotteen tavoitteena on tulkita ja ymmärtää yksittäistä tapausta laadullisin menetelmin.

Tässä tutkimuksessa tutkitaan monimutkaisen sisäisen valvonnan järjestelmän kehittämistä ja sen haasteita faktanäkökulmasta. Koskinen ym. (2005, 131) toteavat, että monimutkaisten ilmiöiden kuten toimintaprosessien tutkiminen on tarkoituksenmukaista suorittaa kirjallista aineistoa hyödyntäen. Harva ihminen esimerkiksi muistaisi kaikkia monimutkaisen prosessin osia yksityiskohtaisesti.

Sisäisen valvonnan kehittämisessä vaaditaan myös asiantuntemusta, joka ei aina ole dokumentoidussa muodossa. Riskien havaitsemisessa sekä olennaisten riskien identifioinnissa ovat kulloisenkin osa-alueen vastuuhenkilöt parhaita asiantuntijoita. Näitä henkilöitä haastattelemalla tämä hiljainen tieto saadaan tutkittavaan muotoon. Puolistrukturoitu haastattelu eli teemahaastattelu on tehokas väline kun kerätään tietoa ilmiöistä, joita ei voida täysin ennakoida valmiilla kysymyslistalla (Koskinen ym. 2005, 106).

Kirjoittaja ei itse ole osallistunut empiirisessä osiossa käsiteltävän kehitysprojektin kulkuun, mutta on ollut osana yrityksen taloushallinnon organisaation toimintaa ennen tätä projektia. Näin ollen kirjoittajalla on jonkinlainen käsitys case-yrityksen toimintatavoista ja valvontakulttuurista, mutta kirjoittaja ei ole osa tutkimuksen kohteena olevaa ilmiötä.

1.5. Tutkimusraportin kulku

Tutkimuksen toisessa luvussa syvennytään sisäisen valvonnan käsitteeseen ja lähtökohtiin sekä kirjallisuudessa hyvin keskeisessä asemassa olevaan COSO:n sisäisen valvonnan viitekehykseen. COSO IF:n osat käsitellään, jotta tutkimuksen myöhemmässä vaiheessa voidaan palata näistä tutkimuksen kannalta keskeisimpiin komponentteihin, eli riskianalyysiin ja valvontatoimintoihin.

Kolmannessa luvussa selvitetään sisäistä valvontaa käsittelevän kirjallisuuden avulla, miten sisäistä valvontaa voisi kehittää. Tässä luvussa selvitetään mitä on tehokas sisäinen valvonta ja miten se ilmenee organisaatiossa. Toisaalta selvitetään myös heikon sisäisen valvonnan ominaisuudet, sekä sellaiset erityiset olosuhteet, joissa sisäisen valvonnan toiminta on tyypillisesti uhattuna. Kolmannen luvun lopuksi syvennytään tyypilliseen sisäisen valvonnan kehitysprosessiin sekä käsitellään vielä kolme mallia, joita sisäisen valvonnan kirjallisuudessa ehdotetaan ratkaisumalleiksi sisäisen valvonnan käytännön toteutuksessa.

Neljännessä luvussa syvennytään sisäisen valvonnan kehittämiseen empiirisen aineiston avulla ja seurataan, miten COSO IF:n mukaiset riskianalyysi ja valvontatoimintojen suunnittelu toteutetaan käytännössä. Empiirisessä aineistossa esitetään kaksi erilaista lähestymistapaa sisäisen valvonnan kehittämiseen, kun olemassa olevan kontrollijärjestelmän kehityshistoria käydään läpi.

Viidennessä luvussa kootaan yhteen luvuissa kaksi, kolme ja neljä käsitellyt tavoitteet sisäisen valvonnan kehittämiselle ja verrataan näitä toisiinsa. Luvussa käsitellään empiirisen aineiston keräämisen yhteydessä ilmenneet valinnat, jotka on jouduttu tekemään sisäisen valvonnan viitekehyksen soveltamisessa ilmenneiden haasteiden ratkaisemiseksi.

Kuudennessa luvussa on tutkimuksen tulosten yhteenveto sekä tutkimuksen perusteella tehdyt johtopäätökset ja tutkimuksen kriittinen arviointi jatkotutkimusmahdollisuuksineen.

1.6. Käsitteet tässä tutkimuksessa

Corporate governance. Yleisesti Corporate Governancella tarkoitetaan yhtiön hallinnointijärjestelmää, joka määrittelee hallituksen ja palkattujen johtajien roolit, velvollisuudet ja heidän suhteensa osakkeenomistajiin (Ahokas 2012 145). Lisäksi Corporate governance määrittelee ne keinot, joiden avulla yhtiö pyrkii saavuttamaan asettamansa tavoitteet, ja se viitoittaa myös ne periaatteet, joiden avulla toimintaa seurataan (OECD 2004, 11).

Kontrolli on mikä tahansa toimenpide, jolla pyritään varmistamaan toiminnan oikeellisuus. Kontrollit voivat olla ehkäiseviä tai paljastavia ja automaattisia tai manuaalisia. (Ahokas 2012, 147)

Riski tarkoittaa tässä tutkimuksessa tapahtumaa, joka koostuu kahdesta tekijästä, todennäköisyydestä ja seurauksesta (Kaplan 1981). Seuraus voi Kaplanin (1981) mukaan olla positiivinen tai negatiivinen, mutta sisäisen valvonnan yhteydessä seuraus on lähtökohtaisesti negatiivinen. COSO (2004, 16) määrittelee riskin mahdollisuudeksi, että toteutuu tapahtuma, jolla on haitallinen vaikutus organisaation tavoitteiden saavuttamiseen. Tässä tutkimuksessa termiä ”riski” käytetään COSO:n määritelmässä merkityksessä.

Sarbanes-Oxley -laki eli SOX on vuonna 2002 säädetty laki Public Company Accounting Reform and Investor Protection Act, joka laadittiin “suojelemaan sijoittajia parantamalla yritysten julkistamien tietojen tarkkuutta ja luotettavuutta arvopaperilain tarkoittamiin ja muihin tarkoituksiin” (Sarbanes-Oxley Act of 2002, 1). Lakiin viitataan lakitekstin johdannossa annetun ohjeen mukaan ”Sarbanes-Oxley act of 2002”, joka vakiintuneen käytännön mukaan on edelleen lyhennetty muotoon ”SOX”. Laki astui voimaan Yhdysvalloissa vuonna 2002, mutta sen noudattaminen tuli pakolliseksi Yhdysvaltain arvopaperimarkkinoilla listatuissa yhtiöissä vuonna 2004. Muualla kuin Yhdysvalloissa kotipaikkaansa pitävien yhtiöiden siirtymäaikaa jatkettiin myöhemmin yhdellä vuodella. SOX:n määräykset koskevat mm. johdon raportointia, tilinpäätöstietojen julkistamista, tilintarkastajien vastuuta ja sisäisen valvonnan järjestämistä. Laissa on kaiken kaikkiaan 11 lukua ja 70 alalukua. (Ahokas 2012, ss. 132–133) Tämän tutkimuksen case-yrityksen kannalta olennaisin pykälä on SOX 404, joka määrää pörssiyhtiön sisäisen valvonnan järjestämisestä, velvoittaa johdon luomaan ja ylläpitämään tehokasta taloudellisen raportoinnin sisäistä valvontaa ja menettelytapoja. Yhtiön tulee vuosittain tilinpäätöksen yhteydessä antaa raportti, jossa johto toteaa vastuunsa, että talousraportoinnissa käytetään sisäistä valvontaa ja riittäviä menettelytapoja. Tämän lisäksi johdon tulee arvioida sisäisen valvonnan menettelytapojen tehokkuutta sekä osoittaa, että tilintarkastaja on vahvistanut arvion sisäisestä valvonnasta ja antanut siitä lausunnon. (Ahokas 2012, 139)

Sisäinen tarkastus on organisaatiossa riippumaton toimija, jonka tehtävänä on arvioida organisaation riskienhallinta-, valvonta-, johtamis- ja hallintoprosessien riittävyyttä ja tehokkuutta. Sisäisen tarkastuksen työtä ohjaa alan kansainvälinen ammatillinen viitekehys, joita ovat mm. eettiset säännöt, ammattistandardit ja käytännön ohjeet. (Sisäiset tarkastajat ry, http://www.theiia.fi/, viitattu 12.7.2014)

Sisäinen valvonta tarkoittaa yleensä organisaation sisäisiä menettely- ja toimintatapoja, joiden avulla pyritään varmistamaan toiminnan laillisuus ja tuloksellisuus. Käsitteeseen syvennytään tarkemmin luvussa 2.1 Sisäisen valvonnan käsite.

Suomen listayhtiöiden hallinnointikoodi on Suomen pörssissä listattuja yhtiöitä koskeva suositus. Sen tavoitteena on, että suomalaiset yhtiöt noudattavat korkeatasoista kansainvälistä hallinnointitapaa. Koodi yhtenäistää listayhtiöiden toimintatapoja sekä osakkeenomistajille ja muille sijoittajille annettavaa tietoa samoin kuin lisää avoimuutta hallintoelimistä, johdon palkkioista ja palkitsemisjärjestelmistä. (Arvopaperimarkkinayhdistys ry 2010, 6)

Väärinkäytös on laaja käsite, joka yleensä viittaa tarkoituksenmukaiseen pyrkimykseen saavuttaa laiton hyöty. Väärinkäytökset ovat jaettavissa karkeasti neljään tyyppiin: talousraportoinnin tahallinen virheellisyys, vastaavien väärinkäyttö tai anastus, laiton kulujen tai velkojen aiheuttaminen ja petoksellinen tulojen hankinta tai menojen välttäminen. (PWC 2003, 1–2) Väärinkäytökseen liitetään kolme tekijää: motivaatio, tilaisuus ja persoonallisuus. Näistä helpoimmin hallittava tekijä yritysympäristössä on tilaisuus. (Hightower 2008, 12)

2. MITÄ ON SISÄINEN VALVONTA?

2.1. Sisäisen valvonnan käsite

Sisäinen valvonta eli internal control tarkoittaa organisaation eri tasoille rakennettuja toimenpiteitä ja toimintatapoja, jotka muodostuvat useista osa-alueista, kuten hyväksymisvaltuuksista, työtehtävien jaosta sekä laskenta- ja ohjausjärjestelmien sisältämistä kontrolleista (Ahokas 2012, 11). COSO:n (1992, 3) määritelmän mukaan sisäinen valvonta tarkoittaa yhtiön hallituksen, johdon ja muun henkilöstön toteuttamaa prosessia, joka on suunniteltu tuottamaan riittävän varmuuden sisäiselle valvonnalle asetettujen tavoitteiden saavuttamisesta. Nämä tavoitteet ovat: 1) toimintojen tehokkuus ja tarkoituksenmukaisuus 2) taloudellisen raportoinnin luotettavuus 3) lakien ja säädösten noudattaminen (COSO 1992, 13) COSO:n lähtökohta on tiukasti tavoitteissa. Ahokas (2012, 12) toteaa, että sisäiselle valvonnalle ei ole yleisesti hyväksyttyä yksiselitteistä määritelmää. Yleisimmin sisäisestä valvonnasta näkee käytettävän COSO:n määritelmää enemmän ja vähemmän sanatarkasti, mikä kertoo COSO:n merkittävästä asemasta sisäisen valvonnan alalla (Leitch 2008, s.14; PwC 2003; Ahokas 2012)

Vaikka sisäinen valvonta keskittyy määritellyn tavoitteen saavuttamiseen, joka saattaa olla riskin ehkäiseminen, sisäinen valvonta ei tarkoita samaa kuin riskienhallinta. Riskienhallinta on COSO:n mukaan laajempi käsite. (COSO, http://www.coso.org/erm-faqs.htm) Riskienhallinta käsittelee riskejä laajemmin kuin sisäinen valvonta, jossa keskitytään pääasiassa negatiivisiin riskeihin. Riskienhallinta puolestaan sisältää myös ne riskit, että jokin positiivisen lopputuleman sisältämä mahdollisuus jätetään käyttämättä. Riskienhallinta lähtökohtaisesti pyrkii hallitsemaan liiketoiminnan kokonaisriskiä, ja esimerkiksi omistajan näkökulmasta yhtiön riskiprofiilia. (COSO 2004, 4–6) COSO linjaa, että sisäinen valvonta on riskienhallinnan erityistapaus, jossa riskejä hallitsemaan kehitetään kontrolleja (COSO, http://www.coso.org/erm-faqs.htm). COSO:n näkemyksen alleviivaa sen julkaisema viitekehys riskienhallinnalle (COSO 2004: Enterprise Risk Management, jäljempänä ERM). Sisäisen valvonnan ja riskienhallinnan erillisyydestä ei kuitenkaan olla kirjallisuudessa aivan yksimielisiä. Leitch (2008) kirjoittaa, että mikäli sisäinen valvonta nähdään laajemmin kuin vain COSO:n

määrittelemien tavoitteiden tähtäävänä kokonaisuutena, on ero riskienhallintaan jo häviävän pieni. Toisaalta, mikäli yrityksessä on tarkoitus toteuttaa sekä määrätietoista riskienhallintaa että sisäistä valvontaa, on näitä hankala erottaa toisistaan. (Leitch 2008 16) COSO:n (2004, 8) Enterprise Risk Management -viitekehyksessä linjataan, että sisäinen valvonta on integraali osa riskienhallintaa muodostaen kätevän työkalun yrityksen johdon käyttöön. Määritelmien perusteella voidaan yhteenvetona todeta, että sisäinen valvonta voi olla ilman riskienhallintaa, mutta riskienhallinnan yksi osa-alue tulisi olla sisäinen valvonta.

Sisäisen tarkastus saatetaan usein liittää kuuluvaksi sisäiseen valvontaan. Tiivistetysti voidaan sanoa, että sisäinen valvonta luo kontrollit ja varmistusmenetelmät, joiden toimivuutta ja olemassaoloa sisäinen tarkastus testaa. Jotta sisäinen tarkastus toimii riippumattomasti, sen ei tulisi olla liian aktiivisesti kehittämässä sisäistä valvontaa, vaan keskittyä testaamaan sen toiminnan tehokkuutta ja raportoida mahdollisista puutteista. Sisäinen tarkastaja on kuin yrityksen sisäinen konsultti. Sisäisen tarkastuksen toimintaa säätelevät kansainväliset laatustandardit ja toimintaohjeet, joita sisäinen tarkastus noudattaa. (COSO 1992, ss. 6–7) Sisäisen tarkastus on lähes poikkeuksetta tekemisissä sisäisen valvonnan kanssa, kun sisäisen valvonnan kehittämät ratkaisut vaativat objektiivisempia näkemyksiä päätöksenteon tueksi. (Ahokas 2012, ss. 12–13)

Koska sisäinen tarkastus ei voi osallistua aktiivisesti sisäisen valvonnan kehittämiseen, voi yrityksessä olla erillinen sisäisen valvonnan organisaatio, jonka vastuulla on sisäisen valvonnan kehittäminen ja ylläpitäminen. Sen asema organisaatiossa ei ole samalla tavalla riippumaton kuin sisäisen tarkastuksen asema, joka on yleensä suoraan toimitusjohtajan alaisuudessa. Sisäinen valvonta palvelee yrityksen johtoa, joten se on yleensä sisällytettynä organisaatiokaavioon ylimmän johdon alapuolelle. Ahokkaan mukaan (2012, 12) sisäisen valvonnan organisaatio on kuitenkin aina erilainen eri organisaatioissa riippuen mm. yrityksen koosta, omistussuhteista, rakenteessa, toimialasta ja toimintojen luonteesta.

2.2. Sisäinen valvonta ja agenttiteoria

Sisäistä valvontaa on ollut organisaatioissa aina olemassa aina siitä asti, kun työssä on ollut jonkinlaista vastuuhierarkiaa. Tämä on todennäköisesti todettu tarpeelliseksi, kun

ensimmäinen väärinkäytös on havaittu. Silloin on ollut kyse siitä, että varmistetaan, että työ tehdään oikein ja sovittujen sääntöjen mukaan. Sisäistä valvontaa on ollut mm. muiden työn valvominen tuotannossa, kahdenkertainen kirjanpito taloudenpidossa ja yksinkertaiset tarkistuslistat projekteissa. Yritysten koon kasvaessa monimutkaisuus on kasvanut ja sisäiseen valvontaan on jouduttu käyttämään entistä enemmän resursseja. (Leitch 2008, 13) Sisäinen valvonta aiheuttaa kuitenkin kustannuksia, jotka viime kädessä tulevat yrityksen omistajien maksettaviksi. SOX:n voimaanastumisen jälkeen on esitetty erinäisiä laskelmia, kuinka kalliiksi kyseisen lain vaatimusten täyttäminen on tullut (mm. Berlau 2005; Tackett ym. 2006). Miksi sisäistä valvontaa tarvitaan ja mikä selittää lisääntynyttä sisäisen valvonnan sääntelyä?

Väärinkäytöksinä nähtävä toiminta ei välttämättä tarkoita sitä, että toimitaan tahallisesti väärin oman edun saavuttamiseksi (Fama 1980, 295). Ongelma voi olla myös motivaation taso. Ei ole tavatonta, että työssä tulee vastaan tilanne, jossa organisaation kannalta edullisin ratkaisu ei ole helposti havaittavissa. Tällöin päätöksentekijä saattaa todeta, että parhaan vaihtoehdon selvittämiseksi joutuu näkemään paljon vaivaa. Jos päätöksentekijän oma etu, esimerkiksi palkka ei ole suoraan riippuvainen ratkaisun onnistumisesta, päätöksentekijä saattaa valita intuitiivisesti parhaalta vaikuttavan ratkaisun ja säästää lisätiedon hankkimiseen vaadittavan vaivannäön.

Eisenhardtin (1989) mukaan Organisaation edun ja oman edun eron aiheuttamaa ongelmaa sekä erilaisten johtamisjärjestelmien, kuten sisäisen laskentatoimen tai sisäisten kontrollijärjestelmien olemassaolo on perusteltavissa agenttiteorian avulla. Agenttiteoria sai alkunsa 1960- ja 1970-luvuilla, kun taloustieteilijät tarkastelivat tuottavuutta ja riskin jakamista yksilöiden ja ryhmien välillä. Tarkastelussa havaittiin nykyisen agenttiteorian taustalla vaikuttava ongelma, kun yhteistyössä toimivilla osapuolilla on erilainen asenne riskiä kohtaan. Agenttiteorian tutkijat sittemmin laajensivat tätä ongelmaa koskemaan myös tavoitteiden ja työnjaon eriävyyden ongelmaa, ja alkoivat käyttää tämän suhteen metaforana sopimusta. (Eisenhardt 1989, 58)

Omistajan eli päämiehen ja toimivan johdon eli agentin välille muodostuu motiiviristiriita kahdesta syystä. Toisaalta ristiriita perustuu erilaiseen suhtautumiseen riskiin ja toisaalta ristiriita perustuu osapuolten erilaisiin henkilökohtaisiin preferensseihin. (Holmström 1979, 74) Käytännön toiminnassa ongelmassa on kaksi osatekijää, toiminta ja toiminnan

raportointi. Agentti ei välttämättä toteuta päämiehen tahtoa tämän haluamalla tavalla tai saattaa jättää sen omien intressiensä vastaisiksi kokemiaan osia toteuttamatta. Agentti voi myös antaa toiminnastaan todellisuudesta poikkeavan kuvan raportoidessaan suoritetuista toimenpiteistä. (Eisenhardt 1989, 58)

Agenttisuhde saa aikaan sellaisia kustannuksia, jotka syntyvät pyrittäessä takaamaan, ettei agentti toimi päämiehen edun vastaisesti. Tällaisia kuluja syntyy esimerkiksi sopimusten tekemisestä ja tilintarkastajien käytöstä. Jensen ja Meckling (1976, 6) määrittelevät näiden kustannusten koostuvan kolmesta osatekijästä: valvonnasta aiheutuneet kustannukset, agentin sitouttamisesta aiheutuvat kustannukset ja lisäksi se päämiehen hyvinvoinnin lasku, joka aiheutuu agentin ei-optimaalisista toimenpiteistä (residual loss). Agenttikustannuksiksi katsotaankin edellä mainittujen kustannusten summa. Jos konsernijohto haluaa tarkkailla tulosyksikköjohtajan toimintaa perinpohjaisesti, joutuvat he hankkimaan saman määrän informaatiota tulosyksikön toiminnasta kuin tulosyksikköjohtajalla on käytössään. Agenttikustannukset nousevat korkeiksi silloin, kun päämiehen ja agentin intressit eroavat huomattavasti, sillä hyvin kattavan informaation hankkiminen aiheuttaa kustannuksia. (Lumijärvi 1987, ss. 15–16) Agenttikustannusten myötä tullaan samalla mitanneeksi myös informaation arvo, eli kuinka paljon lisäinformaatioon on järkevää investoida resursseja (Holmström 1979, 89).

Kun agentin toiminta aiheuttaa agentille negatiivisen marginaalihyödyn, agentin motivaatio valita päämiehen kannalta epäedullinen ratkaisu kasvaa. Päämiehen näkökulmasta agentti valitsee siis liian alhaisen toiminnan tason, jota agentti puolestaan voi selittää itsestään riippumattomilla tekijöillä, kuten epäedullisella toimintaympäristöllä. Tätä agenttiteorian käsittelemää ongelmaa kutsutaan moral hazardiksi. (Wright, Mukherji & Kroll 2001, 415; Lumijärvi 1987, 16) Moral hazardin aiheuttaman ei-optimaalisen toiminnan ehkäisemiseksi yritys tarvitsee kattavaa seurantamenetelmää, kuten sisäistä laskentaa tai muuta informaatiojärjestelmää (Holmström 1979, 89).

Kuten vuosituhannen vaihteen talousskandaalit osoittavat, aikaisemmat keinot organisaation toiminnan todenmukaisen raportoinnin varmistamiseksi eivät olleet riittäviä. Skandaaleihin sekaantuneiden yritysten johto ei kyennyt vastaamaan omistajien odotuksiin, mutta kuitenkin todennäköisesti tulospalkkauksella heitä motivoitiin

ottamaan korkeampia riskejä parempien tulosten toivossa. Kun todellinen suorituskyky jäi toivotusta tasosta, annettiin taloudellisesta suorituskyvystä heidän motiiviensa eduksi muokattua informaatiota siinä toivossa, että omistajien käytössä olevan informaation perusteella petos ei paljastu. Toisin sanoen agentti toimi päämiehen kannalta ei-optimaalisella tavalla, mutta raportoi asiasta siten kuin todellista tehokkaampi toiminnan taso olisi saavutettu.

Sisäisen valvonnan ensimmäisen tavoitteen mukaisesti toiminnan tehokkuus ja tarkoituksenmukaisuus pyrkii varmistamaan agentin toiminnan olevan mahdollisimman optimaalista tai vähintäänkin tuottamaan informaatiota siitä, mikäli näin ei ole toimittu. Sisäisen valvonnan toinen tavoite, taloudellisen raportoinnin luotettavuus, varmistaa agentin antavan todenmukaisen raportin toiminnastaan tai ainakin se pyrkii tuottamaan informaatiota siitä, mikäli raportin sisältämä informaatio ei ole luotettavaa. Sisäisen valvonnan kehittäminen ja ylläpitäminen aiheuttaa kustannuksia, jotka voidaan edellä esitettyjen seikkojen valossa laskea myös agenttikustannusten valvontakustannusten joukkoon.

2.3. Sisäinen valvonta sääntelyn edellyttämänä

Vaikka COSO:n IF julkaistiin jo kauan ennen SOX:n voimaantuloa, ei systemaattisia ja dokumentoituja kontrollijärjestelmiä ollut yhtä merkittävissä määrin käytössä kuin lain voimaantulon jälkeen. SOX:n voidaan ajatella olleen tärkein kattavaa sisäistä valvontaa yleistänyt tekijä. (Leitch 2008, 4–5) Kuten edellisessä kappaleessa todettiin, aiheuttaa sisäisen valvonnan kattava järjestäminen kustannuksia yrityksille. Mikä sitten motivoi markkinat ja lainsäätäjät säätämään lain, joka tekee sisäisen valvonnan järjestämisestä pakollista?

Vuosituhannen vaihteen talousskandaalit olivat Yhdysvaltain sijoitusmarkkinoille valtava isku. Se kaatoi suuria pörssiyhtiöitä, merkittävän tilintarkastusyhteisön ja asetti kyseenalaiseksi myös muiden kuin skandaaliin sekaantuneiden yhtiöiden tilinpäätösinformaation luotettavuuden. Sijoittajat pelkäsivät, milloin seuraava vakaana pidetty yritys kaatuisi. Joidenkin tutkijoiden mukaan Yhdysvaltain arvopaperimarkkinoiden toiminnan tehokkuus heikkeni talouskriisin myötä siten, että markkinoiden likviditeetti heikkeni, josta indikaattoreina olivat mm. hitaampi reagointi

informaatioon, laajempi hintahajonta sekä haitallinen valikoituminen (adverse selection) (Jain ym. 2008; Hammersley ym. 2008; Beneish al. 2008). Tämän syyksi esimerkiksi Jain ym. (2008, 361) arvelivat sitä, että sijoittajien luottamus markkinoihin oli mennyt kriisin myötä. SOX:n ensimmäisillä riveillä kerrotaan lain laadinnan tavoitteena olleen tarve suojella sijoittajia parantamalla yritysten tuottaman informaation tarkkuutta ja luotettavuutta (http://www.sec.gov/about/laws.shtml). Kansantalouden perusteista jo tiedämme, että tehottomat markkinat ovat haitaksi koko taloudelle, kun pääoma ei allokoidu markkinoilla tehokkaasti niihin investointeihin, jotka tuottavat sijoittajalle parhaan hyödyn.

Jain ym. (2008, 380) esittävät, että SOX onnistui tavoitteessaan palauttaa sijoittajien luottamus sillä perusteella, että markkinoilla on havaittavissa merkkejä tehokkuuden palaamisesta lain voimaantulon jälkeen. Lakia on kuitenkin kritisoitu sen aiheuttamista kustannuksista (Berlau 2005; Tackett ym. 2006). Koska lain vaatimukset jouduttiin täyttämään suhteellisen lyhyessä ajassa, ei kenelläkään ollut todellista tietämystä siitä, mitä lain vaatimusten täyttämiseksi tarvitsisi todella käytännössä tehdä (Cenker & Nagy 2004). Näin ollen sisäisen valvonnan asianmukaisen järjestämisen ja kontrollijärjestelmän kehittämiseen tähtääviin hankkeisiin palkattiin konsultteja, usein suurista tilintarkastusyhteisöistä kertomaan näkemyksensä vaadittavista toimenpiteistä. (Leitch 2008, s 3) Tällaisessa tilanteessa vaarana oli, että konsultin asema asiakasorganisaation ulkopuolisina toimijoina aiheutti erisuuntaisen motivaation kuin jos he olisivat työskennelleet asiakasyrityksen päämiehen alaisuudessa. Berlau (2005, 40) kirjoittaa, että heidän tavoitteenaan oli, että asiakasyritys tekee varmasti riittävän määrän toimenpiteitä lain vaatimusten täyttymiseksi, jotta konsultti varmasti hoitaa vastuunsa. Konsulttiyhtiölle ei koitunut kustannuksia siitä, että laadittu kontrollijärjestelmä oli mahdollisesti liian yksityiskohtainen, jolloin sen pyörittämiseen kului turhaan resursseja. Liian runsaan kontrolloinnin ylimääräiset kustannukset jäivät asiakasyhtiöön (Berlau 2005, 40). Sisäisen valvonnan tarkoitus on COSO:n (1992, 4) mukaan kuitenkin tuottaa vain kohtuullinen varmuus sisäisen valvonnan tavoitteiden saavuttamisesta, kuten seuraavassa kappaleessa selviää.

2.4. Sisäinen valvonta COSO-mallin mukaan

2.4.1. Sisäisen valvonnan pääpiirteet

COSO IF on ensimmäinen yleisesti tunnettu sisäisen valvonnan malli, joka esittää sisäisen valvonnan määritelmän ja sen osatekijöiden kuvaukset (Ahokas 2008, 24). COSO IF on yleisimmin sovellettu viitekehys SOX:n vaatimusten täyttämiseksi., joten se on vakiintunut käyttöön erityisesti Yhdysvalloissa kotipaikkaansa pitävissä yrityksissä ja siirtymäajan jälkeen myös niissä ulkomaisissa yhtiöissä, jotka olivat listautuneena jossakin Yhdysvaltalaisessa pörssissä. (Jeffrey 2008; Jokipii & Agbejule 2009) Sisäisen valvonnan viitekehyksistä on olemassa muitakin malleja kuin COSO IF, mutta tutkimuksen empiirisessä osassa tutkitaan tapausta, jossa on sovellettu nimenomaan COSO IF:ia vuodelta 1992. Tässä kappaleessa käydään läpi tämän tutkimuksen kannalta keskeisimmät asiat COSO IF:stä.

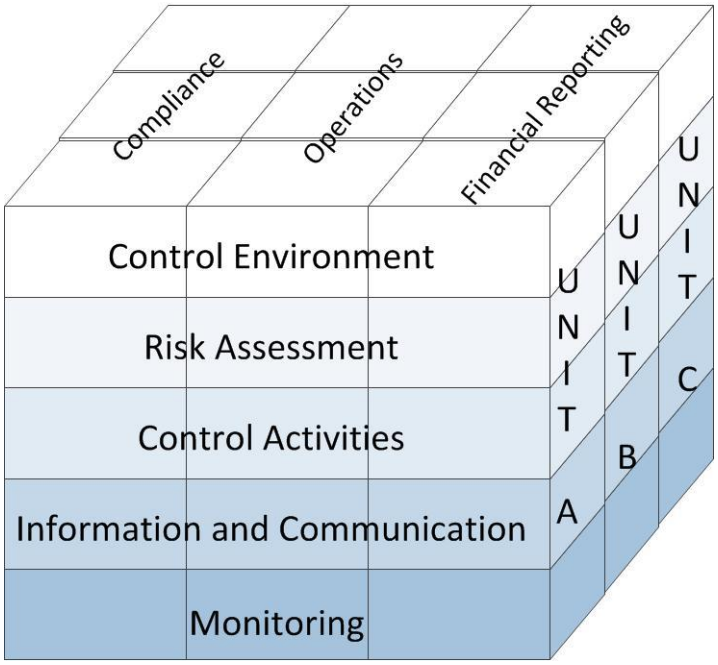
Sisäinen valvonta on luonteeltaan jatkuva prosessi. COSO:n IF:n mukaan sisäinen valvonta ei ole vain yksittäinen tapahtuma tai tilanne, vaan sisäinen valvonta on sarja tapahtumia, jotka levittyvät kaikkiin yrityksen aktiviteetteihin. Sisäinen valvonta on integroitu osa kaikkia yrityksen tavanomaisia prosesseja, joiden toiminnan tarkoituksenmukaisuutta se yhtenä johdon käyttöön soveltuvana työkaluna varmistaa. Ei ole olemassa yhtä mallia sisäisestä valvonnasta, joka soveltuisi kaikkien yritysten käyttöön, joten sisäinen valvonta tulee järjestää kussakin yhtiössä siten kuin se siihen parhaiten sopii. (COSO 1992, 14)

Sisäistä valvontaa toteuttavat ihmiset. Sisäinen valvonta koskettaa organisaation kaikkia henkilöitä yhtiön hallituksesta lähtien. Ihmiset kehittävät sisäisen valvonnan järjestelmän mekanismit, määrittelevät sen tavoitteet ja varmistavat, että sisäinen valvonta toimii parhaalla mahdollisella tavalla. Tärkeätä on määritellä ihmisten roolit, vastuut ja oikeudet, jotta kaikki toimivat tehokkaasti tavoitteiden saavuttamiseksi. (COSO 1992, 15)

COSO (1992, 15) huomauttaa, että hyväkin sisäisen valvonnan järjestelmä voi tarjota vain kohtuullisen varmuuden toiminnan tavoitteenmukaisuudesta. Tähän on monia syitä, kuten ihmisen päätöksentekokyvyn rajoitteet ja mahdolliset virheet, ja lisäksi on kontrollien suunnittelussa otettava huomioon myös kustannusnäkökulma.

Kontrollit on myös mahdollista kiertää, jos useampi henkilö toimii yhteistyössä ja organisaation ylimmällä johdolla voi olla mahdollisuus toimia virheellisesti kontrolleista huolimatta. (COSO 1992, 15)

COSO tiivistää näkemyksensä sisäisestä valvonnasta kuvion 1 mukaiseen kuutioon. Kuution kukin osa-alue käsitellään seuraavissa alaluvuissa tarkemmin. Kuvio havainnollistaa sisäisen valvonnan tavoitteiden, viiden sisäisen valvonnan elementin ja organisaation eri tasojen suhdetta. Kunkin organisaation osan tavoitteet voidaan jakaa COSO:n määrittelemään kolmeen kategoriaan (compliance, operations ja financial reporting) ja näihin tavoitteisiin pääsemiseksi tulee hyödyntää kaikkia sisäisen valvonnan elementtejä. (COSO 1992 s.18 – 19)



Kuvio 1. COSO Relationship of Objectives and Components

2.4.2. Sisäisen valvonnan tavoitteet

COSO:n mukaan sisäisen valvonnan tavoitteet on johdettavissa organisaation toiminnan tavoitteista joko koko yhtiön tasolla tai alemmilla tasoilla erikseen. Kuitenkin COSO toteaa, että käytännössä kaikkia organisaatioita yhdistää seuraavat pyrkimykset: säilyttää positiivinen maine toimialalla ja asiakaskunnassa, tuottaa luotettavia raportteja

sidosryhmille sekä toimia toimintaa koskevien lakien ja säännösten puitteissa. Näin ollen pyrkimykset voidaan yhdistää kolmeen tavoitteeseen:

1) yrityksen toiminnan tarkoituksenmukaisuus ja tehokkuus
2) taloudellisen raportoinnin luotettavuus
3) lakien ja sääntöjen mukainen toiminta

Tätä jaottelua COSO perustelee sillä, että se auttaa keskittymään sisäisen valvonnan eri osa-alueisiin ja siten vastaamaan erilaisiin tarpeisiin. On tosin mahdollista, että jotkin tavoitteet voidaan lukea useampaan kuin yhteen yllä esitetyistä kategorioista. (COSO 1992, 16; Ahokas 2012, 25)

Edellä esitettyjen tavoitteiden saavuttaminen ei COSO:n (1992, 16) mukaan kuitenkaan takaa sitä, että organisaatiossa ei tehtäisi huonoja päätöksiä tai estä organisaation ulkopuolisten tekijöiden negatiivista vaikutusta liiketoiminnan tavoitteiden saavuttamiseen.

2.4.3. Sisäisen valvonnan viisi komponenttia

COSO:n mukaan sisäinen valvonta koostuu viidestä toisiinsa liittyvästä komponentista. Ne on hahmoteltu sen mukaan, miten yritysjohto yleensä johtaa organisaatiota. (COSO 1992, 16)

Valvontaympäristö

Valvontaympäristöllä tarkoitetaan kaikkea sitä, minkä puitteissa liiketoimintaa harjoitetaan, kuten yrityksen kulttuuri, historia ja ihmisten asenteet. Se asettaa organisaation ”äänensävyn”, mikä vaikuttaa organisaation jäsenten tietouteen sisäisestä valvonnasta. Valvontaympäristö on kaikkien muiden komponenttien perusta tuoden organisaatioon kurin ja rakenteen. Avainasemassa valvontaympäristön kehittämisessä on yhtiön yli johto, joka omalla esimerkillään viestii muulle henkilöstölle, miten tärkeänä sisäistä valvontaa organisaatiossa pidetään. (COSO 1992, 23; Ahokas 2012, 27)

Valvontaympäristö on jaettavissa seitsemään osa-alueeseen: 1) rehellisyys ja eettiset arvot, 2) henkilöstön pätevyys, 3) hallituksen ja tarkastusvaliokunnan jakama huomio ja ohjaus, 4) johdon filosofia ja toimintatapa, 5) organisaatiorakenne, 6) työntekijöiden valta

ja vastuu, 7) henkilöstöhallinnon menettelytavat ja käytännöt. Kaikki osa-alueet ovat tärkeitä, mutta niiden soveltamisen laajuus eri organisaatioissa vaihtelee sen mukaan, miten organisaation rakenne ja yksiköiden ominaispiirteet vaihtelevat. (Ahokas 2012, 27)

Riskien arviointi

Jokainen organisaatio altistuu toiminnassaan sisäisille ja ulkoisille riskeille, joiden merkitys tulee arvioida. Riskeiltä ei voida sisäisen valvonnan avulla täysin välttyä, mutta niiden todennäköisyyttä ja mahdollista vaikutusta voidaan vähentää. Riskien arviointi tarkoittaa sellaisten riskien tunnistamista ja analysointia, jotka vaikuttavat olennaisesti organisaation tavoitteiden saavuttamiseen. Koska organisaation ympäröivät tekijät muuttuvat jatkuvasti ajan kuluessa, tulee riskien arvioinnissa kiinnittää erikseen huomiota myös muutoksen aiheuttamaan riskiin. Riskien tunnistaminen ja analysointi on jatkuva prosessi, joka on tehokkaan sisäisen valvonnan keskeinen osa. (COSO 1992, 33)

COSO:n mukaan tavoitteiden asettaminen on edellytys riskien arvioinnille, mutta tavoitteiden asettaminen ei ole luettu mukaan IF:n osaksi. Tavoitteet voidaan asettaa erikseen kullekin organisaation yksikölle ja lisäksi koko organisaatiolle. Tavallisesti tavoitteet seuraavat organisaation strategiaa ja tavoitteet ovat johdettavissa sieltä. COSO:n mukaan kaikkien tavoitteiden tulisi olla luokiteltavissa johonkin kolmesta IF:n tavoitteesta. Tavoitteiden perusteella on johdettavissa organisaation kannalta kriittiset menestystekijät, jotka voidaan mahdollisesti muotoilla mitattavaan muotoon. (COSO 1992, 33)

Riskin tunnistamista voidaan auttaa luokittelemalla riskejä eri tasoille organisaatiossa, kuten edellä mainittiin tavoitteiden määrittelyn yhteydessä. Lisäksi riskejä voidaan luokitella yritystason ja toimintatason riskeihin. Karkeasti yleistettynä yritystason riskit ovat ulkoisia riskejä, kuten teknologinen kehitys, asiakastarpeiden muuttuminen, kilpailu ja uusiutuva lainsäädäntö. Toimintatason riskit johtuvat pääsääntöisesti sisäisistä tekijöistä, kuten tiedonkulun katkeamisesta ja henkilöstön epäpätevyydestä. (COSO 1992, 33, 40–42; Ahokas 2012, 31–32)

Riskianalyysissa suoritetaan kolme arviota: riskin realisoitumisen todennäköisyyden arviointi, sen aiheuttamien vaikutusten arviointi ja millä keinoilla riskiä voidaan hallita. Mikäli sekä riskin todennäköisyys että vaikutus ovat pienet, riski ei todennäköisesti ole

olennaisen merkittävä. Yksi tapa on luokitella riskit asteikolla ”pieni – kohtalainen – suuri”. Onnistunut riskianalyysi on tärkeä, jotta sisäinen valvonta keskittyy kontrolloimaan oikeita asioita. Riskien hallitsemisessa voidaan käyttää muutamia menetelmiä vaikutusmahdollisuuksien mukaan. Organisaatio voi päättää olla ottamatta riskiä lainkaan, pyrkiä vähentämään sen todennäköisyyttä tai rajaamaan seurauksia. Joitakin riskejä voidaan myös yrittää siirtää muiden kannettavaksi esimerkiksi vakuutuksilla tai muilla suojausinstrumenteilla. (COSO 1992, 42–43)

Valvontatoiminnot

Valvontatoiminnot ovat toimintaperiaatteita ja toimintatapoja, jotka varmistavat, että organisaatio toimii johdon asettamien tavoitteiden mukaisesti. Ne auttavat varmistamaan, että tarvittaviin toimenpiteisiin on ryhdytty organisaation tavoitteiden toteutumista vaarantavien riskien hallitsemiseksi. Valvontatoimintoja suoritetaan kaikkialla organisaatiossa kaikilla toiminnan tasoilla ja toiminnoissa. Valvontatoiminnot koostuvat hyväksymisistä, valtuutuksista, todentamisista, täsmäytyksistä, toiminnan tarkastuksesta, omaisuuden turvaamistoimista ja työtehtävien eriyttämisestä. (COSO 1992, 49)

Valvontatoiminnot voidaan luokitella valvontatavoitteen mukaan tähtäämään johonkin kolmesta sisäisen valvonnan tavoitteesta. Valvontatoiminnot koostuvat yleensä kahdesta elementistä: toimintaperiaate ja kontrollitoimenpide. Toimintaperiaate määrittelee sen, miten asiassa pitäisi toimia ja kontrollitoimenpiteillä varmistetaan, että toimintaperiaatetta toteutetaan. Toimintaperiaatteita ei välttämättä ole dokumentoitu, eikä näin aina ole tarpeenkaan, jos toimintaperiaate on organisaatiossa vakiintunut ja hyvin sisäistetty. Toisaalta kirjoitettukaan toimintaperiaate ei takaa sitä, että sitä noudatetaan. Kontrollitoimenpiteet ovat usein niitä toimenpiteitä, joita ihmiset käytännössä tekevät. Kontrollitoimenpiteitä on tapana dokumentoida esimerkiksi työnkuvauksissa tai kontrollimatriisin muodossa. (COSO 1992, 51; Ahokas 2012, 34)

Valvontatoiminnot voidaan luokitella ehkäiseviin, paljastaviin, manuaalisiin, automaattisiin ja johtamiskontrolleihin (COSO 1992, 49). Ehkäisevät kontrollit tähtäävät virheiden ja väärinkäytösten ennaltaehkäisyyn. Ehkäisevät kontrollit voidaan rakentaa sisään toimintaperiaatteisiin ja ne ovat usein työläitä implementointivaiheessa, mutta ylläpitämiseen ei vaadita paljoa resursseja. Ennalta ehkäiseviä kontrolleja ovat

esimerkiksi työtehtävien eriyttäminen, laskujen tarkistus ennen maksamista, hyväksymisrajat maksuille, ostotilausten tekeminen ainoastaan hyväksytyille toimittajille, tietojen suojaaminen salasanoilla ja käyttöoikeusrajoitteilla sekä fyysiset kontrollit, joilla pyritään estämään tiedon tai omaisuuden tuhoutuminen, varastaminen tai vahingoittuminen. (Ahokas 2012, 35)

Paljastavat kontrollit on suunniteltu paljastamaan jo tapahtuneita virheitä ja poikkeamia. Paljastavia kontrolleja suoritetaan, jotta virheet havaitaan ajoissa ja ne ehditään parhaassa tapauksessa korjata jo ennen kuin mitään vahinkoa on tapahtunut. Paljastavat kontrollit ovat usein työläämpiä ylläpitää kuin ehkäisevät kontrollit, koska usein paljastavan kontrollin suorittaminen on ylimääräinen työvaihe aikaisempaan menettelyyn verrattuna. Esimerkkejä paljastavista kontrolleista ovat mm. kirjanpidon rahatilin täsmäyttäminen kassatiliotteeseen, varaston fyysinen inventointi, myyntisaamisten saldovahvistusten täsmäyttäminen, palkanmaksun oikeellisuuden pistokoetarkastus, analyyttiset tarkastukset ja monitorointikontrollit. Analyyttisia tarkastuksia ovat mm. erilaiset suhdelukuvertailut ja kehityssuuntien analysointi, joissa selvitetään muutosten syyt ja yhteydet, jotka ovat epäjohdonmukaisia muuhun informaatioon tai ennustuksiin nähden. Monitorointikontrollit ovat jälkikäteen tehtäviä tarkastuksia yksittäisten liiketapahtumien asianmukaisuudesta. Monitorointikontrolleja voidaan tehdä esimerkiksi satunnaisotannalla. (Ahokas 2012, 36)

Ennaltaehkäisevät ja paljastavat kontrollit voivat olla automaattisia tai manuaalisia kontrolleja. Manuaaliset kontrollit edellyttävät ihmisen osallistumista sen suorittamiseen. Esimerkiksi varmennukset ja analyysikontrollit ovat yleensä manuaalisia kontrolleja. Automaattisissa kontrolleissa puolestaan kontrolli suoritetaan tietokoneohjelman tekemänä ilman ihmisen osallisuutta. Automaattisia tarkastuksia ovat mm. asiakkaan luottorajan tarkistus ja järjestelmien väliset liittymätäsmäytykset. (Ahokas 2012, 37)

COSO esittää IF:ssä edellä esitetyn luokittelun, mutta ei ota kantaa luokittelun käsitteiden sisältöön. Sen sijaan COSO esittelee erityyppisiä valvontatoimintoja ilman täsmällistä luokittelua:

Top level reviews eli ylätason tarkistukset tarkoittaa analyyttista vertailua toteutuneiden ja budjetoitujen tai ennustettujen lukujen välillä. Tässä vertaillaan myös erilaisten

tehokkuudenkehitysprojektien tuloksia, markkinointi panostusten tuottamaa myynninlisäystä ja kululeikkausohjelmien tuloksia. (COSO 1992, 50)

Direct Functional or Activity Management muistuttaa hieman ylätason tarkistuksia, mutta on luonteeltaan täsmäytys. Toimintoja ja aktiviteetteja johtavat johtajat analysoivat oman osastonsa suorituskykyä. Vastaavasti heidän esimiehensä, jotka ovat vastuussa useammasta toiminnosta tai aktiviteetista, laativat yhteenvetoja saamansa datan perusteella ja täsmäyttävät saamansa datan osastoittain tai asiakassegmenteittäin. He kiinnittävät huomiota myös lain vaatimusten täyttymiseen. (COSO 1992, 50)

Information processing tarktoittaa, että varmistetaan tuotetun informaation tarkkuus, täydellisyys ja transaktioiden auktorisointi usean erilaisen kontrollin avulla. Kriittisen informaation muokkauksen tulee olla seurattavissa rekisteristä. Transaktiot on numeroitu juoksevasti. Tietueiden summia vertaillaan aikaisempien versioiden ja vertailuarvojen kanssa ja mahdolliset poikkeamat tutkitaan ja niistä raportoidaan. Uusien tietojärjestelmien suunnittelu, muutokset vanhoihin järjestelmiin ja pääsy dataan, tiedostoihin ja ohjelmiin on valvottua (käyttöoikeuksien valvonta). (COSO 1992, 50)

Physical controls tarkoittaa työkalujen ja tarvikkeiden, varastojen, arvopapereiden, käteisvarojen ja muun käyttöomaisuuden olemassaolo ja käyttökelpoisuus varmistetaan fyysisesti ja toistuvasti. Laskennan perusteella saatua tietoa verrataan vertailurekisteriin. (COSO 1992, 50)

Performance indicators eli suorituskyvyn mittarit muistuttavat hieman benchmarking-vertailua yrityksen sisäisesti. Samankaltaiset toiminnot organisaation eri osissa tuottavat samankaltaista toiminnallista tai taloudellista dataa. Näiden keskinäisten suhteiden analysointi ja yhdistely sekä poikkeamien korjaus toimivat valvontatoimenpiteinä. Suorituskyvyn mittareita voivat olla esimerkiksi ostojen hintavarianssi, kiireellisinä käsiteltyjen tilausten osuus kaikista tilauksista ja palautusten prosenttiosuus kaikista tilauksista. Analysoimalla odotusten vastaisia trendejä johto voi havaita sen tavoitteiden vastaisia toimintatapoja. Tämän kaltaista raportointia ja analyysia voidaan suorittaa sekä liiketoiminnan tarkoituksenmukaisuuteen tähtäävän valvontatavoitteen että taloudellisen raportoinnin oikeellisuuteen tähtäävän valvontatavoitteen hyväksi. (COSO 1992, 50)

Segregation of Duties (SoD) eli työtehtävien eriyttäminen on tärkeä keino ehkäistä väärinkäytöksiä. Työtehtävät jaetaan eri henkilöiden kesken siten, että riski yhden henkilön aiheuttamasta väärinkäytöksestä alenee. Tähän kontrolliin liittyy olennaisesti tietojärjestelmien auktorisointitoiminnot ja tehtyjen muutosten tallentaminen mahdollisten väärinkäytösten havaitsemiseksi. (COSO 1992, 51)

Infromaatio ja kommunikaatio

Jokaisen yhtiön tulee kyetä varmistamaan, että olennainen informaatio on sen työntekijöiden käytettävissä ja omaksuttavissa oikea-aikaisesti, jotta he pystyvät vastaamaan toiminnastaan ja olemaan osa sisäistä valvontaa. Organisaation tietojärjestelmät tuottavat liiketoiminnan tarkoituksenmukaisuuden, taloudellisen raportoinnin ja lain vaatimusten täyttämisen kannalta olennaista informaatiota, joka mahdollistaa organisaation tehokkaan johtamisen. Johdon tulee kyetä identifioimaan ja seuraamaan tätä informaatiota, jota käytetään paitsi päätöksenteossa sisäisesti, myös raportoidaan organisaation ulkopuolelle päätöksentekoa varten. Kommunikaation tulee olla tehokasta organisaatiossa horisontaalisesti ja vertikaalisesti, jotta tieto liikkuu organisaatiossa huipulta alas, käytännön tasolta ylös ja sivuttaissuunnassa eri osastojen välillä. Jokaisen henkilön organisaatiossa tulee ymmärtää johdon selvä viesti, että sisäisen valvonnan toimenpiteet tulee suorittaa vastuullisesti ja että jokainen työntekijä on osa sisäistä valvontaa omassa työssään, mitä heiltä odotetaan ja miten se vaikuttaa muiden työhön. Kommunikaation tulee olla tehokasta myös organisaation ulkopuolelle, kuten asiakkaiden, toimittajien, lainsäätäjien ja omistajien suuntaan. (COSO 1992, 59)

COSO (1992, 59–61) korostaa tietojärjestelmien tärkeyttä relevantin informaation tuottamisessa ja saattamisessa sitä tarvitsevien henkilöiden käyttöön. Tämä tarkoittaa sekä rahallisten että ei-rahallisten tietojen keräämistä asiakkaista, tuotannosta, tuotteista ja markkinoista. Informaation tuottamisen nopeus ja tehokkuus on edellytyksenä tarvittaville päätöksille, jotta kilpailuetua ei menetetä. Tehokas informaation tuottaminen palvelee kaikkia sisäisen valvonnan tavoitteita. Tuotetun informaation on kuitenkin oltava laadukasta, jotta johto voi hyödyntää sitä tehokkaasti organisaation toimintojen ohjaamisessa. COSO määritteleekin viisi tekijää, joilla voidaan arvioida tiedon laatua:

1) Sisältö on tarkoituksenmukaista – tarvitaanko juuri tätä informaatiota siellä?

2) Informaatio on oikea-aikaista – onko se perillä silloin kun sitä tarvitaan?
3) Informaatio on ajantasaista – onko se viimeisin saatavilla oleva tieto?
4) Informaatio on tarkkaa – onko data virheetöntä?
5) Informaatio on saatavilla – pystyvätkö oleelliset tahot saavuttamaan informaation?

Kommunikointi on keino siirtää informaatiota ja on siten yhtä tärkeää kuin relevantin informaation tuottaminen. Ongelmat havaitaan yleensä etulinjan työntekijöiden parissa, mutta usein vain ylempänä organisaatiossa olevilla on mahdollisuus vaikuttaa näihin ongelmiin. Mikäli ongelmista raportointia ei oteta vakavasti tai esimiehet toimillaan lannistavat ongelmista raportoivat työntekijät, on mahdollista, että kommunikointi ongelmista loppuu ja näin organisaation kyky toimia tehokkaasti vaarantuu. COSO mainitsee myös ”pilliin puhaltajan”, turvatun viestintäkanavan, jonka kautta kuka tahansa voi anonyymisti raportoida epäillyistä väärinkäytöksistä. Kommunikointimenetelminä COSO mainitsee ohjesäännöt, muistiot, sähköiset ilmoitustaulut ja videoidut viestit. Kun viestintää toteutetaan suullisesti suurelle tai pienelle yleisölle, tulee äänen ja kehonkielen alleviivata tarkoitettua viestiä. Myös johdon toiminta on osa viestintää. Esimerkki kertoo myös siitä, millainen toimintakulttuuri organisaatiossa halutaan olevan ja miten vastaavissa tilanteissa tulisi toimia. (COSO 1992, 64–66)

Seuranta

Sisäinen valvontajärjestelmä tarvitsee seurantaa, jonka avulla arvioidaan sen toimivuutta ja laatua ajan kuluessa. Seurannan tulee olla yksi sisäisen valvonnan prosessi, joka voidaan jakaa kahteen tasoon: jatkuvaan seurantaan ja erillisiin arviointeihin. Jatkuva seuranta tapahtuu tavallisen toiminnan yhteydessä sekä osana johtamisprosessia. Erillisten arviointien laajuus ja taajuus tulee suhteuttaa arvioituun riskitasoon ja suunniteltujen valvontatoimintojen tehokkuuteen nähden. Seuranta ei kuitenkaan pelkästään johda haluttuun tulokseen, vaan havaitut puutteet tulee myös raportoida asianmukaisesti ylöspäin organisaatiossa ja vakavat puutteet aina hallitukselle saakka. (COSO 1992, 69; Ahokas 2012, 42)

Seurannan ainoa tehtävä ei ole varmistaa, että valvontatoiminnot suoritetaan asianmukaisesti, vaan sen tehtävänä on myös varmistaa, että sisäisen

valvontajärjestelmän muut komponentit täyttävät yhä tehtävänsä tehokkaasti organisaation toiminnan tai toimintaympäristön muuttuessa. COSO:n mukaan jatkuvan seurannan ja erillisten arviointien sopiva yhdistelmä varmistaa valvonnan tehokkuuden ajan kuluessa. (COSO 1992, 69)

COSO pitää jatkuvaa seurantaa erillistä arviointia tehokkaampana siksi, että jatkuvan seurannan myötä mahdolliset virheet havaitaan pian niiden tapahtumisen jälkeen, jolloin ne voidaan vielä ajoissa korjata. Erilaisia jatkuvan seurannan toteutustapoja ovat esimerkiksi eri toimintojen johdon välinen yhteydenpito, raporttien informaation vertailu johdon käsitykseen tilanteesta, kommunikointi organisaation ulkopuolisten tahojen kanssa toimitusten tai laskutusten sujuvuudesta, sisäisen valvonnan koulutusseminaarien ja kokousten pitäminen henkilöstön kanssa. (COSO 1992, 70–71)

Erillisten arviointien vahvuus on siinä, että niiden yhteydessä on hyvä kyseenalaistaa rutiininomainen valvontatoiminta ja samalla varmistaa sisäisen valvontajärjestelmän tehokkuus. Arviointia toteuttava sisäinen tarkastus tekee tätä osana työtään, mutta sen tehtävän ei ole koko sisäisen valvontajärjestelmän erillisarviointi kerralla. Arvioinnin suorittajan tulee ymmärtää, miten sisäisen valvonnan järjestelmä toimii ja mitä järjestelmä on milloinkin rakennettu varmistamaan. Arvioinnin apuna voidaan käyttää haastatteluja ja tapaamisia valvontatoimintoja suorittavien henkilöiden kanssa, testejä dokumentaatiosta ja kyselyitä. (COSO 1992, 72–74)

Seurannan paljastamat ja muut havaitut puutteet sisäisessä valvonnassa tulee raportoida organisaatiossa ylöspäin sille tasolle, jolla on riittävästi auktoriteettia käynnistää korjaavat toimenpiteet. Pääsääntöisesti valvontatoiminnoista vastuussa oleva johto tulee saattaa tietoiseksi havaituista puutteista, jotta tällä on mahdollisuus arvioida asetettujen valvontatoimintojen riittävyyttä. Heidän on kyettävä arvioimaan uudelleen riski ja se, johtuuko havaittu puute virheestä kontrollin suunnittelussa vai onko ongelma siinä, että kontrollia ei ole noudatettu. (COSO 1992, 74–77)

3. SISÄISEN VALVONNAN KEHITTÄMINEN

3.1. COSO-mallin soveltaminen käytännössä

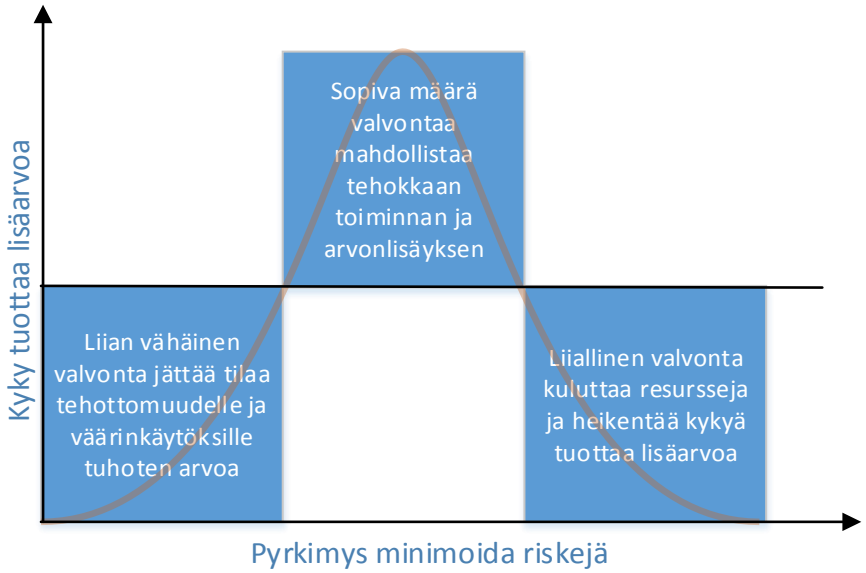
COSO:n sisäisen valvonnan malli on tarkoitettu yleiseksi ohjeeksi sisäisen valvonnan toteutuksen suunnitteluun. Se ei kuitenkaan anna paljoa tietoa siitä, miten sisäisen valvonnan soveltaminen käytäntöön tapahtuu. Kun teoreettisesta mallista tehdään sovellus käytäntöön, joudutaan usein ratkaisemaan liuta ongelmia, joihin COSO ei tarjoa suoraa ratkaisua (Hightower 2008, 8). Tästä syystä monet sisäisen valvontajärjestelmän kehittäneistä yhtiöistä turvautuivat konsulttien apuun (Leitch 2008, 3).

COSO (1992) toteaa, että sisäinen valvonta on erilainen jokaisessa yhtiössä, eikä yksi ratkaisumalli käy kaikkiin tilainteisiin. Kun kehitetään sisäisen valvonnan järjestelmää, voi siis olla hyödyllistä tutustua erilaisiin käytännön ratkaisuihin ja niitä kuvaileviin suuntaviivoihin, joilla ongelmia on pyritty ratkaisemaan. Vaikka sisäisen valvonnan malli toimiikin teoriassa, on käytännön sovelluksesta kiinni, tuleeko lopputuloksesta toimiva. Erilaisista vaihtoehdoista voidaan valita parhaiten tilanteeseen sopiva ratkaisuja siten päästä todennäköisemmin kohti tehokasta sisäistä valvontaa.

3.2. Tehokkaan sisäisen valvonnan tunnuspiirteet

Sisäinen valvonta on järjestetty tehokkaasti silloin, kun sen voidaan katsoa palvelevan liiketoiminnan tavoitteita ja että sisäinen valvonta tuottaa riittävän varmuuden siitä, että sisäinen valvonta toimii suunnitellulla tavalla (Hightower 2008, 27). Näin ollen hyvä sisäinen valvonta suhtautuu kriittisesti myös itseensä ja tuottaa valvonnan toimivuudesta raportteja. Hyvä sisäinen valvonta hallitsee riskiä, tuo läpinäkyvyyttä organisaation toimintaan ja raportoi organisaation valvonnan tilasta (Hightower 2008, 27). Hyvän sisäisen valvonnan myötä yrityksellä on mahdollisuus parantaa todennäköisyyttä saavuttaa asettamansa tavoitteet, tehostaa johdon ajankäyttöä keskittymällä olennaisiin asioihin, tehostaa johtamista muutostilanteissa, helpottaa strategian toteutusta ja laskea oman pääoman kustannusta (KPMG 1999, 17).

KPMG (1999, 14) toteaa, että sisäisen valvonnan ei tulisi muodostaa organisaatiolle taakkaa, vaan olla yhdessä riskienhallinnan kanssa yritykselle mahdollistavassa roolissa. Toisin sanoen valvontatoimintojen suorittaminen ei saa olla liian raskasta organisaation resursseille. Tässä on hyvä huomioida yllä todettu ”riittävän varmuuden” tavoittelu tavoitteiden saavuttamiseksi, sillä resurssien tuhlaaminen riittävän tason ylittävään varmuuteen ei ole mielekästä. Kuvio 2 havainnollistaa KPMG:n näkemystä optimaalisesta suhtautumisesta organisaation kohtaaman riskin hallitsemiseen.



Kuvio 2. Sisäisen valvonnan intensiteetin ja luodun arvon suhde. (Mukaillen: KPMG 1999, 15)

Kun sisäisen valvonnan lähtökohtana on täyttää lain tai muun säännön vaatimukset, voidaan helposti unohtaa, miksi kontrollointia ylipäätään tehdään. Kun ulkoinen ja sisäinen tarkastus painostavat vaatien uusia kontrolleja, jotta ”voidaan olla aivan varmoja”, saatetaan tällaisessa tilanteessa kehittää kontrolleja, jotka toki lisäävät varmuutta toiminnan suunnitelmanmukaisuudesta, mutta kontrollin suorittamiseen käytetyt resurssit ovat hyötyyn nähden liian suuret. (Leitch 2008, 4)

Sisäisen valvonnan tulee siis saavuttaa tavoitteensa, mutta siihen ei tule käyttää liiaksi resursseja. Ahokkaan (2012) mukaan sisäinen valvonta on prosessi, jonka aikaansaavat ihmiset. Parhaiten sisäinen valvonta toimii silloin, kun se on rakennettu osaksi liiketoimintaprosesseja ja sen komponentit ovat läsnä kaikilla organisaation tasoilla.

Mikäli valvontajärjestelmä rakennetaan olemassa olevien prosessien päälle, se jää irtonaiseksi, eivätkä siihen kuuluvat toiminnot sulaudu aidosti osaksi yksilöiden tehtäviä ja vastuita. (Ahokas 2012, 14)

COSO ei ohjeistanut, missä suhteessa sisäisen valvonnan resurssit tulee komponenttien kesken jakaa, mutta erilaisen painotuksen valinta valvontatoimintojen ja seurannan välillä on sidoksissa yrityksen strategiaan (Jokipii 2009; Agbejule & Jokipii 2009). Vaikka yleispätevää mallia ei voi luoda, on kuitenkin edullista tiedostaa, millaiseen strategiaan painotus sopii. Innovatiivinen ja uusia markkinoita etsivä strategia hyötyy suuremmasta valvontatoimintojen määrästä ja pienemmästä seurannan määrästä. Tämä asetelma tukee reaktiivista ja mukautumiskykyistä johtamista. Sen sijaan vakailla markkinoilla toimiva ja kustannustehokkuuteen tai laatuun perustuva strategia hyötyy sekä valvontatoimintojen että seurannan suuresta määrästä. Tämä tukee kustannusten hallintaa ja laadunvalvontaa. (Jokipii & Agbejule 2009)

Sisäisen valvonnan kokonaisuuden tehokkuutta on hankala arvioida kerralla, mutta sen osa-alueiden tehokkuuden arvioinnista on kirjallisuudessa muutama esimerkki. Valvontaympäristö on kirjallisuudessa nostettu COSO:n viidestä komponentista merkittävimmäksi (Ramos 2004; Hermanson ym. 2012). Ramos (2004) kirjoittaa, että vahvalla ja hyvin kommunikoidulla valvontaympäristöllä on merkittävin vaikutus siihen, että sisäinen valvonta koetaan tehokkaaksi ja myös ylimmän johdon toimet tulevat valvonnan piiriin. Myös PwC (2003) kiinnittää julkaisussaan suurimman huomionsa sisäisen valvontaympäristön ja sen osa-alueiden huolelliseen toteutukseen sisäisen valvonnan näkökulmasta.

Riskien arvioinnin ja valvontatoimintojen laatu kulkee käsi kädessä. Ensinnäkin, onko tunnistettu riski kyetty muotoilemaan niin tarkasti, että siihen kyetään suunnittelemaan täsmällisiä valvontatoimenpiteitä. Vastaavasti valvontatoimintojen eli kontrollien tulee vastata kattavasti siihen riskiin, jonka hallitsemiseen kontrolli on luotu. Tämän lisäksi kontrollin tulisi paljastaa oleellinen virhe kohtuullisen ajan kuluessa sen syntymisestä. (Ahokas 2012, 18) Vaikka tämä Ahokkaan esittämä huomio on hankala muuttaa sellaiseen muotoon, että sisäisen valvonnan onnistumista voitaisiin mitata, on kuitenkin hyvä huomata, että tämä on kriittinen osa-alue sisäisen valvonnan onnistumisen kannalta

ja siihen on hyvä kiinnittää erityistä huomiota sisäistä valvontajärjestelmää suunniteltaessa.

3.3. Tehokasta sisäistä valvontaa uhkaavat olosuhteet

Kirjallisuudessa on jonkin verran osviittaa siitä, mitkä tekijät ovat yhteydessä heikkoon sisäiseen valvontaan. Tässä kappaleessa kootaan yhteen merkit heikosta sisäisestä valvonnasta. Kirjallisuudessa suurimman huomion ovat saaneet SOX:n määritelmän täyttävä julkisuuteen raportoitu sisäisen valvonnan olennainen heikkous eli ”material weakness of internal control”. Tässä yhteydessä on huomattava, että nämä tutkimukset koskevat siis lähtökohtaisesti talousraportoinnin osuutta COSO:n mallista ja havaittuja väärinkäytöksi, sillä raporttien kohdeyleisö ovat sijoittajat ja muut ulkoiset sidosryhmät.

Ge ja McVay (2005) ovat osoittaneet, että SOX:n määritelmät täyttävät olennaiset heikkoudet sisäisessä valvonnassa ovat yleisempiä organisaatioissa, jotka ovat suhteessa monimutkaisempia, pienempiä ja taloudellisesti vähemmän kannattavia kuin ne organisaatiot, joissa havaittuja olennaisia heikkouksia ei esiinny. Etelä-Koreasta kerättyyn dataan perustuvan tutkimuksen mukaan sisäisen valvonnan parissa työskentelevien henkilöiden määrä on käänteisesti yhteydessä sisäisen valvonnan heikkouksien määrään (Choi, Choi, Hogan & Lee 2013). He tukevat Ge:n ja McVay:n (2005) päätelmää, että heikko sisäinen valvonta voi olla seurausta pätevän taloushallinnon henkilöstön riittämättömyydestä. Choi ym. (2013) päättelevät, että riittävä määrä pätevää henkilöstöä sisäisen valvonnan parissa mahdollistaa toimivan raportointiprosessin, riittävän tehtävien eriyttämisen ja asianmukaiset tilien täsmäytykset. Leitch (2008, 28) kirjoittaa, että sisäisellä valvonnalla on taipumus vähentyä siellä, missä on vähemmän tarvetta ja enemmän painetta kuluttaa valvontaan käytetty aika johonkin muuhun.

Doyle, Ge ja McVay (2007) kirjoittavat, että heikosta sisäisestä valvonnasta ovat taipuvaisia raportoimaan yritykset, jotka ovat nuorempia, monimutkaisempia, nopeasti kasvavia ja niissä on meneillään uudelleenjärjestelyitä. Nämä ovat tekijöitä, jotka voidaan yhdistää yhtiöihin, joilla on pulaa resursseista ja jotka joutuvat käsittelemään monimutkaisia raportointitapauksia sekä lisäksi joutuvat vastaamaan muuttuvaan toimintaympäristöön (Doyle ym. 2007).

Ahokkaan (2012, 22) mukaan virheiden ja väärinkäytösten riskiä lisäävät olosuhteet, joissa työtehtävien eriyttäminen on puutteellista, johtajien vaihtuvuus on tiuhaa, kassatilanne on huono, yhtiössä on kasvava vanha varasto ja lisääntyneet luottotappiot tai niiden uhka. Myös sisäisen tarkastuksen heikkous on merkittävä tekijä edesauttamaan sisäisen valvonnan heikkoutta. Sisäinen tarkastus kykenee havaitsemaan sääntöjen vastaista toimintaa ja mahdollisia puutteita kontrollien toimivuudessa ja niiden noudattamisessa tehden sisäisestä valvonnasta tehokkaampaa. (Ahokas 2012, 23)

Yllykkeenä väärinkäytökseen voi toimia myös esimiehiltä tuleva paine saavuttaa epärealistisia tavoitteita tai korkeat suoritukseen perustuvat palkkiot (Ahokas 2012, 22). Myös Hightower (2008, 28) mainitsee ongelman epärealististen tavoitteiden ja organisaation resurssien välillä ja esittää todennäköiseksi syyksi sen, että työntekijöillä ei ole käytettävissä riittävää tietoa ja resursseja. Hän mainitsee myös konkreettisen esimerkin tyypillisestä virheiden selittelystä: ”ihmiset tekevät erehdyksiä ja välillä niitä sattuu. Ei riskiä voi ennakoida tai poistaa”. Hermanson ym. (2012) kirjoittavat, että epärealististen tavoitteiden ja resurssien suhde muodostaa ongelman, joka kuuluu sekä valvontaympäristön että informaation ja kommunikaation komponenttien tehtäväkenttään. Hermanson ym. (2012) lisäävät, että ongelma on yleinen yritysmaailmassa. He ehdottavat ongelman parhaimmiksi indikaattoreiksi: 1) missä määrin analyytikkojen odotukset vastaavat todellista organisaation ilmapiiriä, 2) kuinka suuren pelon tai paineen alaisena organisaatiossa suhtaudutaan numeerisiin tavoitteisiin, 3) millaiset ovat organisaation käytössä olevat kannustimet ja kompensaatiot, jotka voivat johtaa ei-hyväksyttävään, epäeettiseen tai laittomaan käyttäytymiseen tuloksenhallinnassa. (Hermanson ym. 2012)

3.4. Esimerkkejä sisäisen valvonnan puutteista

Kaikki edellä esitellyt tutkimukset käsittelevät niitä yrityksen ominaispiirteitä, joiden perusteella on todennäköisempää, että yritys joutuu raportoimaan heikosta sisäisestä valvonnasta. Sisäisen valvonnan kehittämisen näkökulmasta kyseisen tyyppiset tutkimukset osoittavat ne olosuhteet, jolloin sisäisen valvonnan kehittämisessä on oltava erityisen tarkkana. Ne eivät kuitenkaan anna juurikaan tietoa siitä, mihin seikkoihin huomiota tulee kiinnittää.

Doyle ym. (2007, 220–221) ovat lisänneet tutkimuksensa liitteeksi esimerkkejä muutamista analysoimistaan sisäisen valvonnan heikkouksista. America West Airlines raportoi olennaisesta sisäisen valvonnan heikkoudesta polttoaineen hinnan suojausinstrumenttien US GAAP:n mukaisesta markkinaehtoisessa raportoinnissa. Syyksi tähän heikkouteen mainitaan puute suojausinstrumenttien transaktioiden dokumentaation seurannassa ja puute asianmukaisessa kvartaaleittain tehtävässä markkina-arvoon kirjauksessa. (Doyle ym. 2007, 220)

Comstock Homebuilding Company raportoi olennaisesta sisäisen valvonnan heikkoudesta tuottaa oikea-aikaisia ja täsmällisiä tilinpäätösraportteja. Yhtiön oli tehtävä muutoksia toimintaansa tilinpäätösinformaation tuottamiseen käytetyn datan täydellisyyden ja täsmällisyyden varmistamiseksi. Yhtiön tilintarkastaja suositteli lisäämään talousraportoinnista vastaavan henkilöstön määrää ja parantamaan tämän henkilöstön yleistä osaamistasoa. (Doyle ym. 2007, 220)

Hollinger International raportoi kolmesta olennaisesta sisäisen valvonnan toimintaympäristöön liittyvistä heikkoudesta. 1) Yhtiön aikaisemman johdon organisaatioon viestimä eettinen ilmapiiri ei ollut sellaista, jolla olisi edistävä vaikutus sellaisen toimintakulttuurin luomiseen, jossa sisäisen valvonnan järjestelmä toimenpiteineen ja paljastavine kontrolleineen olisi vahva. 2) Osa edellisestä johdosta oli johtavassa asemassa myös yhtiön osakkeenomistajina toimivissa yhtiöissä ja he eivät osallistuneet avoimeen ja oikea-aikaiseen viestintään talousraportoinnista vastaavien henkilöiden tai hallituksen riippumattomien jäsenten kanssa. 3) Yhtiön johto ja organisaatiorakenne edesauttoivat varojen siirtoa yhtiöstä omistusyhteysyritys-transaktioiden avulla hyödyttäen yhtiön suurimpia omistajia suoraan ja epäsuorasti. (Doyle ym. 2007, 221)

3.5. Tyypillinen sisäisen valvontajärjestelmän kehitysprojekti

COSO:n viitekehyksen mukaisen sisäisen valvontajärjestelmän kehittäminen käytännössä vaihtelee sen mukaan, minkä tavoitteen vuoksi järjestelmää kehitetään. Erilaisia tavoitteita ovat esimerkiksi lakisääteisten velvoitteiden täyttäminen tai prosessien laadun ja tehokkuuden parantaminen. Ahokas (2012) esittelee tyypillisen sisäisen valvontajärjestelmän kehitysprojektin kulun, kun kehittämisprojektin laajuutena

on koko sisäisen valvonnan kokonaisuus. Hänen mukaansa hankkeen laajuus on tärkeää hahmottaa jo alettaessa suunnitella projektia ja se tulisi nähdä osana koko organisaation hallinnointitapaa. Sisäinen valvonta voidaan nähdä hyvin eri tavalla eri puolella organisaatiota ja se on myös erilainen eri organisaatioissa. (Ahokas 2012, 64)

Sisäisen valvonnan kehitysprojekti noudattelee Ahokkaan (2012) mukaan pääsääntöisesti seuraavia vaiheita:

- sisäisen valvonnan tavoitteiden määrittely
- yritystason kontrollien tunnistaminen ja dokumentointi
- taloudellisten prosessien tunnistaminen ja dokumentointi
- avainkontrollien tunnistaminen ja dokumentointi
- puuttuvien kontrollien määrittely ja implementointi
- kontrollien arviointi tehokkuuden toteamiseksi
- kontrolliheikkouksien arviointi
- tulosten raportointi
- uudelleenarviointi
- jatkuva seuranta

Sisäisen valvonnan tavoitteet asettavat raamit projektille ja toisaalta määrittelevät johtoajatuksen projektin läpiviemiselle. Jos tavoitteeksi asetetaan vain lakisääteisten velvoitteiden täyttäminen, jotta sisäisestä valvonnasta voidaan antaa lausunto, valitaan yleensä ratkaisuja, jotka tuottavat edullisimman vaihtoehdon. Vaarana on, että sisäinen valvonta jää pintapuoliseksi ja mahdolliset hyödyt liiketoiminnassa jäävät saavuttamatta. Toinen vaihtoehto on asettaa tavoitteeksi saavuttaa prosessien parempi tuntemus, lisätä läpinäkyvyyttä ja mahdollisesti lisätä tehokkuutta. Tällainen projekti on suuri hanke ja se vaatii paljon resursseja. Tällöin vaarana voi olla, että kustannukset ylittävät hyödyt, etenkin jos järjestelmästä tulee liian byrokraattinen ja tarpeettomasti heikennetään organisaation joustavuutta. Jokaisen organisaation tulee määritellä tavoitteet itse, jotta ne rakentuvat organisaation prosesseihin ja tukevat liiketoimintaa. (Ahokas 2012, 65)

Yritystason kontrollien tunnistaminen tarkoittaa suuressa määrin COSO IF:n valvontaympäristön tunnistamista, määrittelyä ja implementointia. Näitä ovat mm. vastuiden ja tehtävien määrittely, johdon määrittelemät eettiset suuntaviivat ja sisäinen

toimintaohje, tarkastusvaliokunnan ja sisäisen tarkastuksen olemassaolo jne. (PwC 2003, 3–11) Yritystason kontrolleja yhdistää se, että ne eivät ole osa yksittäistä prosessia vaan ne vaikuttavat kaikkien prosessien taustalla. Yritystason kontrollien dokumentointi voidaan toteuttaa kätevästi esimerkiksi kontrollimatriisissa, jossa on määritelty itse kontrolli, sen tavoite, kontrollitoiminto ja kuvaus evidenssistä, joka osoittaa valvontatoiminnon olevan suoritettu. (Ahokas 2012, 68).

Taloudellisten prosessien tunnistaminen ja dokumentointi viittaa niihin prosesseihin, jotka ovat yhteydessä talousraportointiin. Tämä Ahokkaan (2012) rajaus on kuitenkin suppea, jos tavoitteena on kehittää koko sisäisen valvonnan järjestelmää, sillä myös rajauksen ulkopuolella olevien prosessien toimintaa voi olla mahdollista kehittää sisäisen valvonnan avulla. Pienissä yrityksissä prosesseja ei välttämättä ole formaalisti määritelty, eikä niitä aina ole suurissakaan yrityksissä dokumentoitu. Prosessien määrittely ja kuvaus voi olla avuksi päällekkäisyyksien eliminoinnissa ja auttaa osastoja ymmärtämään muiden osastojen toimintaa. (Ahokas 2012, 69–70)

Avainkontrollien tunnistaminen ja dokumentointi viittaa vaiheeseen, jossa aikaisemmin määriteltyjen prosessien kannalta kriittisimpien tavoitteiden saavuttamiseksi määritellään keskeiset kontrollit. Näiden kontrollien tulisi varmistaa, että prosessi toimii pääpiirteissään oikein, ja tuottaa riittävä kuva prosessin sen hetkisestä tehokkuudesta. Avainkontrollien tulisi tuottaa kattava kuva koko organisaation sisäisestä valvontajärjestelmästä ja kattaa kaikki merkittävimmät riskit. Avainkontrollit ovat keskeisessä asemassa testauksessa, koska niiden avulla saadaan nopeasti kuva kontrollien luotettavuudesta. (Ahokas 2012, 71)

Puuttuvien kontrollien määrittely ja implementointi -vaihe voidaan suorittaa avainkontrollien määrittämisen jälkeen. Johtoajatuksena tässä määrittelyssä on, mitä muita kontrolleja tarvitaan, jotta kontrolloitavan prosessin osa-alueet menevät olennaisilta osin oikein. Tässä vaiheessa on myös hyvä kyseenalaistaa mahdollisesti olemassa olevan kontrollijärjestelmän ominaisuuksia, tehdäänkö niitä tarkoituksenmukaisesti tai tehdäänkö jotain turhaan. Ahokas kirjoittaa, että tähän vaiheeseen tulee panostaa riittävästi, jotta kontrollit voidaan suunnitella osaksi organisaation toimintatapoja. (Ahokas 2012, 75) Kontrollien määrittelyyn ja dokumentointiin perehdytään tarkemmin seuraavassa alaluvussa.

Kontrollien arviointi tehokkuuden toteamiseksi viittaa kontrollitestaukseen, jolla varmistetaan kontrollien toimivan tarkoitetulla tavalla. Arvioidaan, onko esimerkiksi myyntihenkilöstö noudattanut määriteltyjä toimintaperiaatteita myöntäessään asiakkaille luottoa. Testauksen voi suorittaa ulkoinen tarkastaja, sisäinen tarkastus, vertaishenkilö, se voidaan suorittaa itsearviointina tai heikkouksista voidaan raportoida normaalin toiminnan yhteydessä esimerkiksi controllerin toimesta. Tilintarkastajan ja sisäisen tarkastajan arviointia voi pitää objektiivisimpana ja itsearviointia sekä rutiinin yhteydessä raportointia puolestaan subjektiivisimpana. Menetelmästä riippumatta arvioinnin tulisi noudattaa aina tarkoituksenmukaista kaavaa. Sen lähtökohta on aina riskien arviointi, jonka pohjalta arvioidaan testattavat kontrollit. Tilikauden loppuun mennessä tulisi olla selkeä kuva siitä, mitä kontrolliheikkouksia on vielä ratkaisematta, jotta näiden vaikutus tilinpäätökseen voidaan arvioida. (Ahokas 2012, 76–83)

Kontrolliheikkouksien arviointi keskittyy löydettyjen kontrollipuutteiden syiden analysointiin. Kontrolliheikkouden syitä voi olla monia. Esimerkiksi kontrollia ei ole suoritettu, se on suoritettu vain osittain, se ei estä virhettä, kontrollia ei ole suunniteltu kunnolla, kontrollin suorittamista ei ole dokumentoitu kunnolla tai kontrolli paljastaa olennaisen virheen tai puutteen. Analyysi antaa eväitä kontrollin kehittämiseen, jotta se toimisi siten kuin pitäisi. (Ahokas 2012, s.87)

Tulosten raportointi viittaa kontrollijärjestelmän testauksesta ja kontrolliheikkouksien arvioinnista saatujen tulosten raportointiin relevanteille tahoille. Raportissa esitetään havainnot ja niiden taloudelliset vaikutukset. Erityisen tärkeää on se, että kontrollipuutteet saadaan käsiteltyä ja kommunikoitua siten, että ne saadaan korjattua. Parannusehdotukset on hyvä esittää keinoina kehittää organisaation prosesseja, jolloin muutosten toteuttamiseen suhtaudutaan paremmin. (Ahokas 2012, 88)

Uudelleenarviointi tarkoittaa kehitystä edellyttäneiden kontrollitoimenpiteiden testaamista ja arvioimista uudelleen muutosten jälkeen, jotta näiden kontrollien laadusta voidaan varmistua. Uudelleenarviointia ei kuitenkaan voida suorittaa saman tien korjaavien toimenpiteiden jälkeen, jotta on ehtinyt kertyä tarpeeksi evidenssiä. (Ahokas 2012, 89)

Jatkuva seuranta tarkoittaa sisäisen valvontajärjestelmän kokonaisvaltaista arviointia, jotta se säilyy ajantasaisena. Seurannasta vastuussa on ylin johto, mutta sitä voi toteuttaa myös erillinen osasto, kuten riskienhallinta, sisäinen valvonta tai sisäisen tarkastuksen yksikkö. Myös itse valvonnan arviointiprosessin laatua ja tehokkuutta tulee arvioida, esimerkiksi arvioinnin dokumentaation laatua ja käytettyjen menetelmien riittävyyttä, jotta sen antamaan kuvaan sisäisen valvonnan tehokkuudesta voidaan luottaa. (Ahokas 2012, 89)

3.6. Menetelmiä riskianalyysin suorittamiseen ja kontrollitavoitteiden sekä valvontatoimintojen suunnitteluun

3.6.1. Menetelmistä yleisesti

Leitch (2008) kirjoittaa useasta erilaisesta lähestymistavasta riskianalyysin, kontrollitavoitteiden ja valvontatoimintojen kehittämisessä, jotka hänen mukaansa nivoutuvat tiukasti yhteen sisäisen valvontajärjestelmän kehitysprojekteissa. Hän yhdistelee sisäisen valvonnan ja riskienhallinnan keskeisiä piirteitä eri menetelmissä ja esittelee kaiken kaikkiaan kaksikymmentä erilaista menetelmää, joista muutamat soveltuvat paremmin juuri sisäisen valvonnan tarpeisiin keskittymättä sen enempää riskienhallintaan. Sisäisen valvonnan tarpeisiin parhaiten soveltuvista menetelmistä tutustutaan empiirisen osan kannalta tärkeimpiin kolmeen menetelmään: matrix mapping of risks and controls, process step analysis ja generic control design library. Nämä menetelmät auttavat tunnistamaan prosessitason riskit ja ideoimaan riskejä hallitsevat kontrollitavoitteet ja kontrollitoiminnot. Kukin menetelmä sisältää vahvuuksia ja heikkouksia, joten sopiva menetelmä tulee valita tilanteen mukaan (Leitch 2008).

3.6.2. Matrix mapping of risks and controls

Kontrollien dokumentointimenetelmällä on suuri vaikutus järjestelmän toimivuuteen ja käytettävyyteen. Leitch (2008, 71) kirjoittaa, että yleisin tapa dokumentoida riskit ja kontrollit, on laatia niistä lista, jossa suunnitellut kontrollit on lueteltu riskin kohdalla seuraavassa sarakkeessa. Dokumentaatiosta muodostuu siis kaksisarakkeinen taulukko. Riskit voidaan tunnistaa analysoimalla tärkeimpien yleisten prosessien päätavoitteen toteutumista uhkaavat riskit. Näitä yleisiä prosesseja ovat tulon- ja kulujen varmistus,

datan prosessointi, kannattavuuden varmistus, lakien ja säännösten noudattaminen, tukiprosessit, tietoturva- ja IT-riskit sekä liiketoimintayksikön yleiskuva. Leitch huomauttaa, että tämä menetelmä on mainittu myös COSO IF:n Evaluation tools -osassa. Kaksisarakkeinen lista tarjoaa kuitenkin vähän mahdollisuuksia tallentaa taulukkoon lisätietoja. Tämän lisäksi lista muuttuu hankalaksi lukea, jos yksi kontrolli vastaa useampaan riskiin samanaikaisesti aiheuttaen toistoa listan tietoihin. Taulukon epäselvyys aiheuttaa riskin, että jokin asia jää huomiotta suunnitteluvaiheessa tai myöhemmin kun listaa käytetään. Tämän lisäksi kontrollijärjestelmän hierarkia jää havainnollistamatta taulukon rakenteen vuoksi. Kontrollijärjestelmän tulisi olla kerrostunut eritasoisiksi kontrolleiksi, joiden avulla voidaan hallita kokonaisuutta tai puuttua prosessin osaongelmiin. (Leitch 2008, s.71)

Toistosta voidaan kuitenkin hyötyä, sillä joskus riskien tunnistaminen on helpompaa toisin päin, eli ajattelemalla ensin kontrollia ja sitten vasta riskiä. Tästä voidaan hyötyä erityisesti silloin, kun yhden kattavan kontrollin tiedetään vastaavan useaan riskiin. Analysoimalla kaikki mahdolliset riskit, joihin kontrolli vastaa, voidaan tunnistaa uusi riski. Joskus ihmiset ajattelevat tietämättään riskejä näin päin, eli riski löytyy vasta sitten kun joku ajattelee ensin kontrollia. Leitch kuitenkin varoittaa, että riski tulee aina arvioida sellaisenaan ja sitä vastaan tulee kehittää kontrollitavoite ja vasta sitten kontrolli. Muussa tapauksessa riskiä ei välttämättä arvioida sellaisenaan ja kehitetä siihen vastaavaa tehokasta kontrollia. (Leitch 2008, 72)

Kontrolli	Riski A	Riski B	Riski C	Riski D	jne.
Kontrolli 1		1	1		
Kontrolli 2			1		1
Kontrolli 3	1				1
Kontrolli 4			1	1	1
jne.					

Taulukko 1. Risk control matrix (Leitch 2008)

Listan sijaan muotoa voidaan laajentaa matriisiksi, jolloin kaksisarakkeisen listan heikkouksista päästään eroon, kun toisto voidaan välttää ja taulukkoon voidaan lisätä

enemmän tietoja. Leitch (2008, 73) esittelee taulukon 1 mukaisen matriisin mallin, jossa riskit on lueteltu sarakkeittain ja kontrollit riveittäin. Näin ollen lista kaikista käytössä olevista kontrolleista on selkeä, helposti luettava ja lisäksi taulukosta voi havaita, mihin riskiin kontrolli vastaa. Tällä menetelmällä kontrollijärjestelmän monikerroksisuus on huomattavasti helpommin havaittavissa. Kontrollit voidaan esimerkiksi ryhmitellä vielä kontrollityypeittäin alaotsikoiden alle, jolloin kaikki kontrollityypit pysyvät mielessä. (Leitch 2008, 73)

Matriisimuotoisen dokumentointimenetelmän vahvuuksia ovat siis luettavuus ja mahdollisuus tallentaa lisätietoja luettavuuden kärsimättä. Tämän lisäksi matriisimuotoinen informaatio on helppo järjestää taulukkolaskennassa raportointitarpeen mukaan ja erityisiä tarpeita varten. Hyödyllisiä lisätietoja, joita taulukkoon voi tallentaa, ovat mm. kontrollin suunnittelija ja vastuuhenkilö, kehitystarpeet ja kontrollifrekvenssi. Matriisimuoto on listaa helpompi muokata ohjelmistokehitystä varten, mikäli kontrollijärjestelmää varten kehitetään tietokoneohjelmisto. Koska kontrollin lisäksi myös riski on nähtävissä dokumentaatiossa, parantaa se henkilöstön näkemystä sisäisestä valvonnasta. Matriisimuodon heikkous on dokumentaation koko sekä leveys- että pystysuunnassa, jolloin matriisin tulostaminen on hankalaa ja usein dokumentaation luettavuus menetetään. Ongelmaa voidaan ehkäistä pitämällä dokumentaatio vain elektronisena ja piilottamalla epäolennaisia soluja tulosteita varten. (Leitch 2008, 74)

3.6.3. Process step analysis

Process step analysis eli prosessin vaiheiden analyysi on perusteellinen menetelmä yksittäisen prosessin sisältämien riskien etsimiseen. Tämä menetelmä sopii erityisen hyvin talousraportoinnin tavoitteita uhkaavien riskien kartoittamiseen. Prosessin kaikki vaiheet piirretään kaavioon, joka kuvastaa koko prosessia kaikkine vaiheineen. Kuhunkin vaiheeseen liittyy yleensä tavoite, jotta vaihe on merkityksellinen. Näin ollen jokainen vaihe–tavoite -pari muodostaa riskin, että tavoitetta ei saavuteta. (Leitch 2008, 75)

Prosessiksi kannattaa valita mahdollisimman laaja kokonaisuus, jotta vältytään ongelmilta prosessin jakamisessa, esimerkiksi ”ostot ja ostovelat” vs. ”ostot”, joihin luetaan mukaan palautukset ja muut korjauserät. Seuraavaksi kartoitetaan, miten

prosessin informaatiovirrat kulkevat ja näistä laaditaan diagrammi. Tässä avuksi voi olla tarpeen tutkia kaikkia tiedon tallennuspaikkoja, kuten paperikaavakkeita, tietokantoja ja tietokoneiden tiedostoja sekä datavirtoja kaikissa siirtovaiheissa, laskelmia ja tiedonkeruuta. Olemassa olevat kontrollivaiheet tulee jättää kartoituksen ulkopuolelle. Seuraavaksi muodostetaan tietovirroista vaiheita, jotka lopulta muodostavat prosessin kokonaisuuden. Yleensä vaiheet ovat luonteeltaan datan keräämistä, siirtämistä tai laskentaa ja yhteenvetoa. Seuraavana vaiheena on ottaa käyttöön geneerinen kontrollitavoitelista. Yleensä tällaisina tavoitteina käytetään informaation laadun kriteerejä: täydellisyys, tarkkuus, validiteetti ja näiden lisäksi ainutkertaisuus. Ainutkertaisuus viittaa siihen, että taloushallinnon maailmassa dataa pääsääntöisesti kopioidaan lähteestä kohteeseen. Data voi kopioitua muiden kriteerien mukaan oikein, mutta se voi kopioitua useammin kuin kerran. (Leitch 2008, 76)

Prosessin vaiheiden kontrolleissa korostuu vaiheiden ketjuluonteisuus, eli data siirretään ensin A:sta B:hen, sitten B:stä C:hen ja edelleen D:hen. Kontrolleja suunnitellessa tulee ottaa huomioon myös kontrollin jänne, eli kuinka monta vaihetta se kattaa. Täsmäytys voi kattaa vain yhden siirtovaiheen, mutta se voidaan suunnitella kattamaan myös neljän siirtovaiheen jänne. Toinen esimerkki on laatia yhteen ohjelmistoon kontrolli, joka paljastaisi tahallisen tai tahattoman muutoksen ohjelmassa. Tämä kontrolli parantaisi kaiken tämän ohjelman läpi kulkevan informaation luotettavuutta. Näin ollen kontrolleista voidaan tehdä monikerroksisia ja siten kehittää niihin hierarkia. (Leitch 2008, 77)

	Tä	Ta	V	A	Vaihe A	Vaihe B	Vaihe C	Vaihe D	Yht.
Kontrolli 1	1	1				1	1		2
Kontrolli 2	1	1	1				1		1
Kontrolli 3				1	1				1
Kontrolli 4		1	1				1	1	2
jne.									
Yhteenveto									
Täydellisyys					0	1	2	0	3
Tarkkuus					0	1	3	1	5
Validiteetti					0	0	2	1	3
Ainutkertaisuus					1	0	0	0	1

Taulukko 2. Prosessin vaiheet matriisissa geneerisillä kontrollitavoitteilla (Leitch 2008, 78).

Prosessin vaiheiden kartoitus kontrolleineen toimii hyvin yhteen edellä esitetyn Matrix mapping of risks and controls -menetelmän kanssa muodostaen kompaktin ja helposti luettavan dokumentaation. Matriisimuotoisesta taulukosta voidaan hyötyä myös silloin, kun kartoitetaan eri vaiheiden kontrollien kattavuutta kontrollitavoitteiden mukaan. (Leitch 2008, 78) Taulukossa 2 on esitetty yhden prosessin vaiheet sarakkeittain (A–D) ja kaikki kontrollit riveittäin (1–4) ja lisäksi taulukon alaosassa on riveittäin yhteenveto. Koska kontrollin tuoma varmuus on aina sama riippumatta siitä, missä vaiheessa se suoritetaan, voidaan sama kontrolli merkitä useaan eri vaiheeseen (vaakarivit 2–6). Kontrolli vastaa aina samoihin geneerisiin kontrollitavoitteisiin, joten ne on taulukoitu vasempaan yläkulmaan siten, että esimerkiksi kontrolli 1 vastaa täydellisyydestä ja tarkkuudesta. Yhteenveto paljastaa, että vaiheessa A on vain yksi kontrolli, joka vastaa datan ainutkertaisuudesta, mutta muita kontrollitavoitteita vastaamassa ei ole yhtäkään kontrollia. Sen sijaan vaiheessa C on kolme kontrollia, jotka kaikki varmistavat datan tarkkuutta, mutta yksikään kontrolleista ei vastaa datan ainutkertaisuudesta. Viimeisestä sarakkeesta nähdään, miten hyvin kontrollit vastaavat geneerisiä kontrollitavoitteita koko prosessin tasolla.

Leitch (2008, 79) kirjoittaa, että taulukossa 2 esitettyä matriisia voidaan vielä kehittää kontrollijärjestelmän toimiessa arvioilla kunkin kontrollin toimivuudesta ja niille asetetuista tavoitteista. Tämä tarkoittaa sitä, että jos kontrollin toimivuudelle asetetaan 100 %:n toimivuustavoite, se saa taulukossa arvon 1 tai vastaavasti 80 %:n tavoite saa arvon 0,8. Jos prosessista vastaavat henkilöt arvioivat kontrollin toimivuuden tasoksi 75 %, voidaan taulukkoon merkitä tavoitteen ja toteutuneen suorituskyvyn erotus, jolloin saadaan tuotettua informaatiota kontrollien luotettavuudesta kontrollitavoitteittain.

3.6.4. Generic control design library

Generic control design library -menetelmä auttaa kontrollijärjestelmän kehittäjiä ajattelemaan kaikkia kontrollijärjestelmän tärkeimpiä osia ja toimii ideoita stimuloivana viitekehyksenä. Sen taustalla on kolme keskeistä ajatusta. Ensiksi luodaan yleispätevä suunnitelma keskeisistä kontrolleista, joka asetetaan luettavaksi listana ajatusten stimuloijaksi. Toiseksi yhdistetään listaan laadittavat ohjeet, joiden avulla yleispätevää suunnitelmaa voidaan räätälöidä erilaisiin olosuhteisiin sopivaksi. Ohjeiden tulisi sisältää neuvoja siitä, mitä seikkoja tulee ottaa huomioon, ja muutama ohjenuora siitä, miten

voidaan vastata erilaisten tilanteiden vaatimuksiin. Kolmanneksi rakennetaan vähitellen tietokanta edellä mainituista ratkaisun ja ohjeistuksen sisältämistä skeemoista hyödyntäen aikaisempia kokemuksia. Alkuperäisiä skeemoja ei välttämättä tarvita aluksi kovinkaan montaa, mutta niiden tulee olla hyvin räätälöitävissä erilaisiin tilanteisiin, joista voidaan kerätä tietoa skeeman toimivuudesta ja tallentaa tiedot tietokantaan. (Leitch 2008, 88)

4. EMPIIRINEN AINEISTO: SISÄINEN VALVONTA CASE-YRITYKSESSÄ

4.1. Case-yrityksen esittely

UPM-Kymmene Oyj (jäljempänä UPM) on tunnettu suomalainen metsäteollisuuden konserni, joka on yksi alansa johtavia toimijoita. Vuonna 2011 liikevaihto oli 10,1 Mrd EUR (8,9 Mrd EUR vuonna 2010), josta kaksi kolmannesta on peräisin läntisen Euroopan valtioissa tapahtuvasta myynnistä. UPM:n tuotantoa on tällä hetkellä viidellä mantereella, Pohjois- ja Etelä-Amerikassa, Aasiassa, Afrikassa ja Euroopassa yhteensä 16 eri maassa. Henkilöstöä yhtiö työllistää n. 24 000 (2011) työntekijän verran. UPM:n organisaatiota voidaan luonnehtia laajaksi maantieteellisten ominaisuuksien vuoksi, mutta monimutkaisuutta lisää myös organisaation matriisimuoto, jossa useimmat tukifunktiot kuten taloushallinto on omana kokonaisuutenaan globaali. (UPM Annual Report 2012)

UPM:n liiketoiminta jaetaan kolmeen liiketoiminta-alueeseen, jotka ovat paperi, ”jalostetut materiaalit” ja ”energia ja sellu”. Paperiliiketoimintaan kuuluvat kaikki paperituotteet aikakauslehtipaperista sanomalehtipaperiin ja erikoispapereihin. Jalostetut materiaalit käsittävät tarramateriaali-, ja vaneriliiketoiminnan. UPM:n ”energia ja sellu” -liiketoiminta-alueeseen kuuluvat: energiantuotanto mukaan lukien ydinvoima ja bioenergia, sellu, metsätalous sekä sahatavaraliiketoiminta. Paperiliiketoiminta käsittää kuitenkin jopa 69 % yhtiön liikevaihdosta kun taas toiseksi suurimman eli tarraliiketoiminnan osuus on n. 11 %, joten yhtiön toiminta perustuu liikevaihdon valossa pitkälti paperiliiketoiminnan ympärille. Paperiliiketoiminnan suurta merkitystä on pyritty pienentämään kasvattamalla muita liiketoiminta-alueita, joista erityisesti energialiiketoiminta on kasvanut voimakkaasti. (UPM Annual Report 2011, 2–21) Uudet liiketoiminnat ovat myös merkitykseltään kasvavassa roolissa, sillä UPM hakee kasvua näiltä aloilta samalla kun paperiliiketoimintaa pyritään tehostamaan uuden kasvun keskittyessä lähinnä kehittyville markkinoille (UPM Group Presentation 2012).

UPM:ssä on riippumaton sisäisen tarkastuksen organisaatio, joka avustaa hallituksen jäseniä varmistumaan hallinnon tarkoituksenmukaisuudesta, sisäisen valvonnan

toiminnasta ja sääntöjen noudattamisesta. Sisäinen tarkastus toimii hallituksen puheenjohtajan ja toimitusjohtajan alaisuudessa, mutta sisäinen tarkastus raportoi myös suoraan tarkastusvaliokunnalle. Riittävän sisäisen valvonnan järjestämistä valvomaan on siis asetettu Suomen listayhtiöiden hallinnointikoodin edellyttämä tarkastusvaliokunta. Tarkastusvaliokunta koostuu hallituksen jäsenistä. Tarkastusvaliokunnan vastuulle kuuluvat mm. sisäisten kontrollien, sisäisen tarkastuksen ja riskienhallinnan toimivuuden ja tehokkuuden monitorointi sekä sisäisen valvonnan suorituskyvyn arviointi. (UPM Annual Report 2012, ss. 29 - 72)

Systemaattisen, tarkkaan dokumentoidun, laajan ja suunnitelmallisen sisäisen kontrollijärjestelmän hyödyntäminen ei ole Suomessa kovin yleistä (Kaski 8.4.2013). UPM on pyrkinyt noudattamaan sisäisen valvonnan vaatimuksia (kuten SOX) ja suosituksia minimivaatimustasoa paremmin. (Piikkilä 12.03.2013; Rainamaa 29.1.2013) Kirjoittaja on itse havainnut, että organisaation taloushallinnossa kunnioitetaan sisäisiä kontrolleja ja niiden suorittamista pidetään tärkeänä. Tämä havainto antaa viitteitä siitä, että yhtiössä on olemassa jonkinlainen valvontakulttuuri ja sisäisten kontrollien olemassaolo on yleisesti henkilöstön tiedossa. Edellä mainittujen seikkojen valossa yritystä voidaan pitää sopivana kohteena case-tutkimukselle, kun tutkitaan sisäisen valvonnan kehittämistä.

4.2. UPM:n olemassa oleva kontrollijärjestelmä

4.2.1. Nykyisen kontrollijärjestelmän perusta: SOX-vaatimukset täyttävä kontrollijärjestelmä

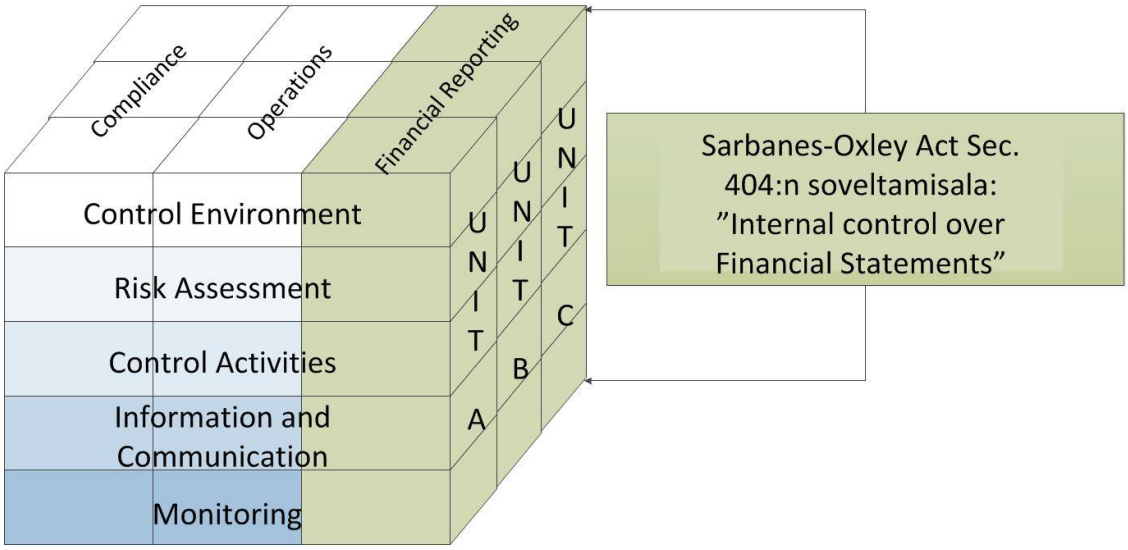
Helsingin pörssin lisäksi UPM oli listautuneena New Yorkin pörssissä vuodesta 1999 vuoteen 2007. Tänä aikana SOX tuli Yhdysvalloissa voimaan, joten listautuneena yhtiönä myös UPM:n oli täytettävä vuonna 2002 voimaan astuneen lain vaatimukset. Alkuperäistä kahden vuoden siirtymäaikaa pidennettiin ulkomaisten yhtiöiden osalta myöhemmin kolmeksi vuodeksi, joten SOX-vaatimukset täyttävän kontrollijärjestelmän tuli olla UPM:n käytössä vuoden 2005 loppuun mennessä. Tehdaskohtaisia johtamisjärjestelmiä lukuun ottamatta UPM:llä ei tätä ennen ollut käytössä keskitettyä sisäisen valvonnan järjestelmää, joten koko kontrollijärjestelmä luotiin täysin puhtaalta pöydältä (Piikkilä 12.3.2013).

Laajan kontrollijärjestelmän luominen oli kallis prosessi, eikä siitä haluttu luopua vuoden 2007 jälkeen, vaikka Yhdysvaltain laki ei UPM:ää tältä osin enää velvoittanutkaan. Syiksi kontrollijärjestelmän säilyttämiseen on mainittu olleen mm. laadukkaampi talousinformaatio, alemmas organisaatioon jalkautettu riskienhallinta ja kontrollointitrendin vahvistuminen myös Euroopassa (UPM Intranet, tiedote: ”Work with internal controls continues as planned”, päivämäärä ei alkuperäinen 23.02.2011).

UPM:n toistaiseksi käytössä olevan kontrollijärjestelmän kehitykseen tähtäävä projekti alkoi vuoden 2004 alussa. Projektin tavoitteeksi määriteltiin SOX 404 vaatimusten täyttäminen lain edellyttämällä tavalla, mutta UPM halusi täyttää lain vaatimukset minimivaatimustasoa kattavammin. Tämän projektin myötä luotiin perusta sisäisen valvonnan kokonaisvaltaiselle kehittämiselle, jonka myötä tuotetun talousinformaation luotettavuutta katsottiin parantuneen niin ulkoista kuin sisäistäkin päätöksentekoa varten. (Piikkilä 12.03.2013; Niiranen 2005)

SOX-kontrollijärjestelmäprojektia toteuttamaan asetettiin ryhmä henkilöitä useasta UPM:n eri organisaatiosta ja lisäksi konsulttiyhtiön edustajia, jotka kaikki olivat aktiivisessa roolissa kontrollijärjestelmää luomassa. Projektitiimin lisäksi projektin kehityksessä olivat mukana UPM:n valitseman tilintarkastusyhteisön edustajat, jotka ottivat projektin edetessä kantaa, täyttääkö järjestelmä heidän mielestään SOX:n vaatimukset. Projektitiimi koostui tiiminjohtajasta ja kahdesta jäsenestä, joita tukemassa ja valvomassa oli nelihenkinen ”steering group”. Molemmilla tasoilla oli lisäksi myös ulkopuolisen konsulttiyhtiön jäseniä. Projektitiimi hoiti pääsääntöisesti kaiken käytännön työn konsulttien avustamana. He olivat esimerkiksi kaikissa liiketoimintayksiköissä laatimassa kulloisenkin yksikön kontrolleja. Ulkoisen konsulttiyhtiön rooli oli tuoda SOX-osaamista projektitiimiin ja heidän kokemuksensa vastaavanlaisista projekteista Yhdysvalloissa. Heidän tehtävänä oli tukea kontrollien laadintaa siten, että ne täyttivät SOX:n normien ehdot. (Piikkilä 12.03.2013)

Kehitettävän kontrollijärjestelmän viitekehyksenä käytettiin COSO:n IF:ia, sillä se oli konsulttien mukaan SOX:n laadinnan taustalla vaikuttanut malli, jonka perusteella sisäinen kontrollijärjestelmä voidaan rakentaa. Viitekehyksen esittämää mallia ei kuitenkaan toteutettu kokonaisuudessaan, vaan ainoastaan COSO-kuution talousraportointia käsittävä osa, kuten kuviossa 3 havainnollistetaan.



Kuvio 3 SOX-kontrollijärjestelmän osuus COSO-kuutiosta käsittää vain talousraportoinnin osuuden (UPM Internal Control Development Project 2004)

Projektia varten kehitettiin tietokantapohjainen työkalu, Internal Control Handbook, johon koko kontrollointia ohjaava dokumentaatio koostettiin. Tietokantaan on koostettu viralliset SOX:n vaatimukset, riskiskenaariot, kontrollien kuvaukset ja harmonisoidut ohjeet eri liiketoimintayksiköille ja organisaation tasoille.

4.2.2. SOX-ajattelutapa ja kontrollijärjestelmän kehitys

Kontrollijärjestelmän taustalla oleva ajattelutapa seuraa projektin toteutuksen vaiheita. Kontrollijärjestelmää alettiin suunnitella huipulta alaspäin – loppusummasta kohti tilitasoa. Koska SOX-vaatimukset täyttävän kontrollijärjestelmän kehittäminen oli sekä UPM:lle että hanketta toteuttaneelle konsulttiyhtiölle ennestään lähes tuntematon tehtävä, päätettiin ensin toteuttaa pilottiprojekti ostoprosessista Rauman paperitehtaalla. Pilottiprojektin vaiheet ovat pääpiirteissään samat kuin varsinaisen SOX-projektin vaiheet, joten niitä ei tässä tutkimuksessa käsitellä erillisinä.

SOX-projektin tavoite oli täyttää lain vaatimukset, joten tehokkuuden nimissä ensin kartoitettiin ne yksiköt, joihin kontrollijärjestelmä joudutaan implementoimaan. Ensimmäisenä toimenpiteenä määritettiin konsernitason olennaisuusrajat, jotka määritettiin erikseen liiketulokselle sekä yksittäisille tilinpäätöksen riveille.

Olennaisuusraja määriteltiin yhdessä tilintarkastajien, projektitiimin ja konsulttien kesken viideksi prosentiksi liiketuloksesta. Olennaisuusrajalla tarkoitetaan suurinta virhettä, jonka johto on valmis hyväksymään ja silti toteamaan, että kontrollointitavoitteet on saavutettu. Aikaisemman kokemuksen ja sekä sisäisen että ulkoisen tarkastuksen kanssa käytyjen keskustelujen pohjalta projektitiimi arvioi, että tilinpäätöksen lukuihin sisältyy virheitä, joita ei heti havaita. Arvioinnin tuloksena oletettiin, että tilinpäätöksessä on mahdollisesti viisi virhettä. Tästä syystä yhden virheen olennaisuusrajaa joudutaan kiristämään siten, että yhteensä viisi virhettä muodostaa 5 prosenttia kokonaisuudesta, eli:

$Olennaisuusraja\ yksittäiselle\ virheelle$: $\frac{1}{5} * 5\ \% = 1\ \%$ (konsernin liiketuloksesta)

Konsernituloslaskelman ja taseen saldot koostuvat luonnollisesti tytäryhtiöiden vastaavista luvuista. Olennaisuusrajasta seuraa, että mikäli tytäryhtiön osuus konsernitason tilin saldosta on yli yhden prosentin, on kyseisen tytäryhtiön tili otettava mukaan kontrollijärjestelmän piiriin. Olennaisuusrajaan perustuvaa analyysiä nimitetään kvantitatiiviseksi analyysiksi, ja se perustellaan erityisesti riskin kvantitatiivisella merkittävyydellä, eli vaikuttavuudella.

Yksiköitä otettiin mukaan projektin piiriin myös kvalitatiivisen analyysin perusteella. Tämä ratkaisu perustui tavallista suurempaan riskiin sen todennäköisyyden osalta, kun liiketoimintaympäristö poikkeaa huomattavasti kapitalistisesta demokratiasta. UPM:n liiketoimintaa on useassa kehittyvän talouden valtiossa. Kvalitatiivisen analyysin tuloksena esimerkiksi Venäjän yksiköt otettiin mukaan kontrollijärjestelmän piiriin. (Niiranen 2005, 76)

Kontrollijärjestelmän piiriin valittiin yhtiöitä myös niiden liiketoiminnan kokonaisuuden muodostaman olennaisuuden perusteella, vaikka yksittäiset tytäryhtiöt eivät olisi kvantitatiivista olennaisuusehtoa täyttäneetkään. Yhdessä nämä yksittäiset yksiköt kuitenkin muodostivat sijoittajien kannalta mielenkiintoiseksi katsotun kokonaisuuden. (Niiranen 2005, 77)

Kontrollijärjestelmän piiriin valitut yksiköt jaettiin niiden merkittävyyden ja tyypin mukaan kolmeen eri kategoriaan: full scope entities (kaikki merkittävät riskit kontrollijärjestelmän piirissä), partial scope entities (vain jotkin riskit ja tilit

kontrollijärjestelmän piirissä) ja non-scope entities (kontrollijärjestelmän ulkpuoliset yksiköt). Pääperiaatteena oli, että kussakin tytäryhtiössä olisi vähintään yksi yksikkö, joka on full scope entity, mutta myös muiden yksiköiden tulee noudattaa samoja määriteltyjä prosesseja siitä huolimatta, että ne eivät ole kontrolloinnin piirissä. (Niiranen 2005, 77)

	Megaprocess	Procurement					
	Major process	Purchasing					Receiving
	Subprocess	Review and approve purchase requisition and create PO	Process incoming supplier credit notes	Purchase invoice handling	Make vendor payments	Maintain vendor master data	Receive goods and issue to warehouse
Sales							
External							
Other operating income							
Capital gains on disposal of fixed assets							
Costs and Expenses							
Change in stocks of finished goods and WiP							
Production for own use							
Materials							
Purchases during the period		X	X	X		X	X
Change in stock							X
External services							
External variable third party		X	X	X		X	X
Salaries and fees							
Indirect employee costs							
pension expenses							
Other indirect employee expenses							
Other operating costs and expenses		X	X	X		X	X
Financial income and expenses							
Financial income							
Interest income							
Interest income, derivatives							
Fair value changes, derivatives							
Exchange rate differences						X	
Financial expenses							
interest expenses							
interest expenses, derivatives							
Fair value changes, derivatives							
Exchange rate differences						X	
Intangible assets							
Intangible rights		X	X	X		X	X
Goodwill							
Other capitalized expenditure		X	X	X		X	X
Advance payments		X	X	X			

Taulukko 3. Esimerkki prosessien ja merkittävien tilien ristiintaulukoinnista (UPM SOX Project material 2004)

Merkittävien tilien määrittelyn jälkeen UPM:n prosessit käytiin läpi siten, että saatiin selville, mitä prosesseja kunkin tilin saldon takana on. Selvitys tehtiin ristiintaulukoimalla prosessi vs. ylätason tili, kuten taulukko 3 esittää. Taulukossa on kuvattu kokonaisuudessaan megaprosessitason hankintaprosessin (Procurement) vaikutus tuloslaskelman tileihin ja taseen osalta aineettomiin oikeuksiin. Tätä tietoa varten oli toki

ensin alustavasti kartoitettava ja dokumentoitava yhtiön prosessit, mikä suoritettiin pilottiyksikössä. (Piikkilä 12.03.2013)

SOX-projektin yhteydessä UPM:lle valittiin prosessimalli kontrollijärjestelmän perustaksi konsulttiyhtiön suosituksen mukaan, sillä heidän mukaansa kyseisen kaltaista prosessimallia oli käytetty esimerkiksi Yhdysvalloissa SOX-vaatimusten täyttämiseksi. Prosessimallissa prosessit jaetaan kolmeen eri tasoon: megaprosessitaso, pääprosessitaso ja alaprosessitaso (Megaprocess, Major process, Subprocess). Taulukko 3 havainnollistaa myös prosessihierarkiaa, joskaan se ei ole tyhjentävä. UPM:ssä ei ollut dokumentoitu prosesseja koko yhtiön tasolla aikaisemmin, joten käyttöön otettu malli ei aiheuttanut konflikteja minkään olemassa olevan mallin kanssa. Todellisuudessa kaikki yksiköt eivät toki toimineet samalla tavalla, mutta ilmeisesti SOX-vaatimusten täyttämiseksi valittu prosessimalli oli riittävän joustava vastaamaan erilaisten liiketoimintojen kuvaamisesta (Piikkilä 12.03.2013).

Prosessimallia syvennettiin kussakin kontrollijärjestelmän piiriin kuuluvassa yksikössä, ja näiden todellinen prosessikulku kartoitettiin ja dokumentoitiin paikallisten asiantuntijoiden kanssa. Projektitiimi ja paikallisten prosessien asiantuntijat yhdessä määrittelivät riskit, joita yksikön prosesseissa saattaa ilmetä. Riskit dokumentoitiin prosessien yhteyteen, ja näille suunniteltiin kontrollitoimenpiteet, joilla riskien vakavuutta voitiin rajoittaa. Projektitiimin kokemus useasta eri yksiköstä auttoi saamaan varmuuden, että kaikki olennaiset riskit tunnistettiin kussakin yksikössä, jossa riskikartoitus tehtiin. Kontrollitoimenpiteet kukin yksikkö sai kuitenkin laatia itse. (Piikkilä 12.03.2013; Niiranen 2005, 80-83).

Projektin lopputuloksena oli dokumentoitu kuvaus UPM:n SOX-relevanteista prosesseista, niihin liittyvistä riskeistä, ja niistä toimenpiteistä, joilla riskejä pyrittiin hallitsemaan. Kaikki tämä informaatio tallennettiin yhteiseen Lotus Notes -pohjaiseen Internal Control Handbook -tietokantaan. Paikalliset tahot huolehtivat käytännön työohjeiden tekemisestä aina yksittäisen työvaiheen tasolle, kuten millä asetuksilla tietty raportti pitää ajaa, jotta se voidaan täsmätä toiseen raporttiin kontrollitavoitteen saavuttamiseksi. Kontrolleja kertyi suunnilleen 400 kappaletta ja järjestelmää luonnehdittiin varsin tarkaksi ja kattavaksi (Rainamaa 20.03.2013).

4.2.3. Kontrollijärjestelmän nykytila

Kun SOX-vaatimukset lakkasivat olemasta sitovia New Yorkin pörssistä irtautumisen jälkeen vuonna 2007, ilmoitettiin koko organisaatiolle, että työ sisäisten kontrollien kanssa jatkuu niin kuin ennen pörssistä irtautumistakin (UPM Intranet, tiedote: ”Work with internal controls continues as planned” 23.2.2011). Vuonna 2008 kontrollijärjestelmälle tehtiin suunnitelmallisesti toteutettu läpikäynti. Tätä varten kootuissa asiantuntijaryhmissä käytiin läpi kaikki ne UPM:n prosessit, jotka SOX-projektissa oli määritelty. Prosesseja ei kokonaisuudessaan päivitetty, vaan joitakin prosesseja yhdistettiin ja joihinkin kohtiin tehtiin pieniä muutoksia. Prosessien nykytilaa on kuvattu liitteessä 1. Lisäksi työryhmässä käytiin läpi SOX-projektissa määritellyt riskit, lähinnä siinä mielessä olivatko ne enää todellisia tai oliko joitakin riskikuvauksia, joita jouduttiin muuttamaan todellisia riskejä vastaaviksi. Tämän kontrollijärjestelmän läpikäynnin tarkoitus oli tehostaa kontrollijärjestelmää, jotta se olisi yhä riittävän kattava, mutta se keskittyisi tarkemmin olennaisiin asioihin samalla keventäen jatkuvan kontrolloinnin ja tarkastuksen työtaakkaa. Tämän laajemman läpikäynnin tuloksena noin 100 kontrollia saatiin joko yhdistettyä tai eliminoitua kokonaan. Tehostuksen lisäksi kontrollijärjestelmään otettiin mukaan myös riskejä, joiden hallinnassa tähdättiin COSO-mallin toimintojen tehokkuuden ja tarkoituksenmukaisuuden varmistamiseen, mutta painopiste säilyi edelleen talousraportoinnissa. (Rainamaa 20.3.2013)

Työryhmät koottiin paikallisten prosessien asiantuntijoista kuten tehtaiden kontrollereista ympäri maailmaa UPM:n kannalta tärkeimmistä maista, joista mainittakoon Suomi, Ranska, Saksa ja Iso-Britannia. Näiden lisäksi työryhmiin pyrittiin saamaan mukaan aina vähintään yksi sisäinen tarkastaja, joka toi siis myös tarkastuksen näkökulman keskusteluun. Tällä haluttiin välttyä siltä, että jotain oleellista olisi jätetty kontrollijärjestelmän piiristä pois. (Rainamaa 20.3.2013)

Hankkeen myötä pyrittiin myös eroon joistakin SOX-kontrollijärjestelmään jääneistä epäkohdista. SOX-projektissa määritelty prosessirakenne osaltaan aiheutti sen, että periaatteessa sama kontrolli oli eri liiketoiminta-alueiden tarpeiden mukaisesti hieman erilainen. Kun kokonaisuuden hahmottaminen jäi hankalaksi, kontrollitoimenpiteiden

suorittajat eivät aina olleet varmoja mitä tarkkoja toimenpiteitä heidän tulisi tehdä. Mahdollisesti osittain tästäkin syystä kontrollijärjestelmä sai kritiikkiä, että kontrollit ovat liian raskaita toteuttaa tavallisten töiden ohessa ilman lisäresursointia ja lisäksi testata kontrollien toimivuus joka vuosi. (Rainamaa 20.3.2013)

Edellä kuvaillun kattavamman läpikäynnin jälkeen kontrollijärjestelmään ei ole tehty vastaavaan tapaan toteutettuja suuria muutoksia, vaan ainoastaan vuosittaista päivitystä. Vuosittain on käyty läpi, mitä muutoksia liiketoiminnassa on tapahtunut vuoden aikana, ja voidaanko näiden muutosten olettaa vaikuttavan kontrollien sisältöön, kontrollitoimenpiteisiin tai jopa riskeihin. Tämä seuranta on toteutettu systemaattisesti liiketoiminta-alue kerrallaan. Riskinä kyseisessä menetelmässä on ollut se, että tieto muutoksista ei aina kulkenut tai sitten tieto saatiin viiveellä vasta hieman muutosten jälkeen. Muutoksista perillä oleminen oli erityisen tärkeää automaattikontrollien osalta, kun järjestelmissä tehtiin muutoksia. (Raainamaa 20.3.2013) Kuitenkin kaikki järjestelmäkontrollit ja tehtävien eriytykset on pyritty käymään läpi kerran vuodessa, jotta kaikki ovat ajan tasalla – kuitenkin korkeintaan vuoden viiveellä. (Hankkio 14.3.2013)

4.3. Uuden kontrollijärjestelmän kehittäminen

4.3.1. Motiivit uuden kontrollijärjestelmän kehittämiseen

UPM:n olemassa olevaa kontrollijärjestelmää ei ole vuoden 2007 jälkeen täysin uudistettu. UPM:n liiketoiminnassa on tapahtunut monia muutoksia varsin lyhyessä ajassa, on hankittu uusia tuotantolaitoksia yritysostojen kautta ja perustettu kokonaan uusia liiketoimintoja. Toisin sanoen yrityksen keskeisissä prosesseissa on tapahtunut merkittäviä muutoksia, jotka on tarvinnut ikään kuin jälkikäteen lisätä prosessikaavioon ja siten prosesseihin liittyvät kontrollit kontrollijärjestelmään. Esimerkkejä näistä tapauksista on mm. liitteessä 1 mainittu Energy. Prosessien muodostaman kokonaisuuden tarkastelun myötä on mahdollisesti saavutettavissa tehokkuuden parannusta, kun jälkikäteen lisätyt prosessit saadaan yhdistettyä kokonaiskuvaan.

Prosessien muuttumisen lisäksi myös organisaatio on muuttunut. Vaikka UPM:llä on tuotantoa hajallaan ympäri maailmaa, on liiketoiminnan tukiprosesseja vahvasti keskitetty suuriin palvelukeskuksiin. SOX-projektin aikaan kaikki tukiprosessit kuten

kirjanpito, materiaalihankinta jne. sijaitsivat aina tuotantolaitoksen yhteydessä. Palvelukeskusten eduksi katsotaan toimintojen harmonisointi, parhaiden käytäntöjen hyödyntäminen, osaamisen keskittyminen ja siten osaamisen tehokkaampi allokointi. (Rainamaa 29.1.2013) Lisäksi keskitetyssä palvelukeskuksessa on mahdollista suorittaa monitorointia pienemmillä resursseilla kuin hajautetussa taloushallinnossa, kun kaikki tietovirrat kulkevat keskitetysti saman organisaation läpi ennen jatkojalostusta raportointia varten. Nykyinen kontrollijärjestelmä perustuu vielä hajautetun palvelumallin maailmaan, joten kontrollien määrää on pyritty rajoittamaan kustannusten pitämiseksi kohtuullisina. Hajautetut ja keskenään heterogeeniset raportointiprosessit eivät myöskään tuota niin luotettavasti vertailukelpoista raportointidataa kuin keskitetty ja harmonisoitu raportointiprosessi. Kun raportointi on viety kauemmas liiketoiminnasta, myös maantieteellisesti, voidaan olettaa, että tuotantoyksiköllä on pienemmät mahdollisuudet vaikuttaa oman toimintansa raportointiin ja siten parantaa vertailukelpoisuutta.

Olemassa olevan kontrollijärjestelmän puutteena on pidetty sen painottumista talousraportointinäkökulmaan, mikä johtaa siihen, että kontrollointitoimenpiteitä käytännössä tekevät henkilöt eivät yleensä hyödy kontrollien täyttämisestä ja dokumentoinnista omassa työssään. Koska SOX-kontrollijärjestelmän alkuunpanija oli ulkoinen pakko, oli erittäin todennäköistä, että järjestelmästä kehkeytyi toisenlainen kuin jos aloite kontrollijärjestelmän kehittämiselle olisi tullut yhtiön sisältä käsin. Siten lähtökohdaltaan ulkoa päin tulleen tarpeen täyttämiseksi luotu järjestelmä saattaa todennäköisesti sisältää epärationaalisuuksia, joita on jouduttu tekemään muodon vuoksi. vastaa organisaation sisältä päin tulevaa tarvetta. Jo SOX-projektin toteutusvaiheessa koettiin muutosvastarintaa liiketoimintaorganisaatioiden suunnalta, sillä kehitetty kontrollijärjestelmä koettiin ”ulkoa annetuksi” ja ”hallinnolliseksi harjoitukseksi” (Piikkilä 12.3.2013). Kontrolleja suorittava taho ei siis useinkaan suorittanut kontrollitoimenpiteitä osana omaa työtään, vaan tästä aiheutui ylimääräinen työtehtävä. Näin ollen kontrollointi nähtiin ylimääräisenä taakkana, eikä sen välittömiä hyötyjä havaittu käytännön työssä. (Rainamaa 29.1.2013)

4.3.2. Projektin lähtöasetelma ja toteutuksen laajuus

Business Process and Risk based Controls -projekti käynnistettiin 2012 päivittämään aikanaan SOX-vaatimuksiin kehitettyä kontrollijärjestelmää. Projektia johtaa päivittäisen työnsä ohessa sisäisen valvonnan päällikkö Maarit Rainamaa. Projektin toteutukseen on osallistunut aktiivisesti kustakin prosessista asiantuntijoita, jotka tuntevat oman alueensa prosessit tarkasti. Liiketoimintaan liittyvien pääprosessien osalta asiantuntijoina on pääsääntöisesti eri liiketoimintojen controllereja ja tukiprosessien asiantuntijoina on kyseisten toimintojen avainhenkilöitä. Varsinaista kiinteää projektitiimiä ei vielä kehitysvaiheessa ollut. (Rainamaa 20.3.2013)

Tämä projekti on suurin kontrollijärjestelmän kehittämiseen tähtäävä projekti sitten SOX-projektin, jossa kontrolloinnille luotiin vahva perusta. Projektissa on alettu laatia uudistettua kontrollijärjestelmää ns. puhtaalta pöydältä, eli työpajoissa on mietitty alusta alkaen kunkin prosessin riskipisteet ja niihin kontrollitavoitteet. (Rainamaa 29.1.2013)

4.3.3. Projektin tavoitteet

Kehitettävän kontrollijärjestelmän taustalla on käytetty viitekehyksenä COSO-mallia vuodelta 1992, mutta SOX-kontrollijärjestelmästä poiketen, tällä kertaa mukaan on otettu systemaattisesti kaikki COSO-mallin tavoitteet, Financial Reporting, Operations ja Compliance. (Rainamaa 20.3.2013) Nykyisessä kontrollijärjestelmässä joitakin kontrolleja olisi voitu sijoittaa myös näiden kahden muun tavoitteen alle, mutta järjestelmää ei ollut suunniteltu lähtökohtaisesti palvelemaan muuta kuin taloudellisen raportoinnin luotettavuuden tavoitetta. COSO-elementeistä projektin fokus on erityisesti Risk Assessment, Control Activities ja Monitoring -elementeissä. Muut elementit toki säilyvät sisäisen kontrollijärjestelmän osana, mutta niiden osalta projekti aiheuttaa vain vähäisiä systemaattisia muutoksia.

Projektin tavoitteena on luoda UPM:lle uudistettu ja ajantasainen kontrollijärjestelmä, joka on kattava ja tehokas. Kontrollijärjestelmä rakennetaan uudesta näkökulmasta, joka seuraa yhtiön oikeita prosesseja, eikä perustu pelkästään taloushallinnon näkökulmaan. Tällä tavoin liiketoimintojen on helpompi hyväksyä kontrollit omakseen ja käyttää valvontaa palvelemaan itse liiketoimintaa. Sisäisen kontrolloinnin suorittaminen liiketoimintatasolla antaa lisäksi business controllereille työkaluja varmistaa

määriteltyjen prosessien toteutuminen ja legitimoida tämän toteuttama toiminnan valvonta. Tämän myötä tavoitellaan liiketoimintaprosessien strategianmukaista ja tehokkaampaa jalkauttamista. Uusi näkökulma johtaa siihen, että myös riskianalyysi seuraa todellisten liiketoimintaprosessien virtaa. Prosessiajattelussa organisaatiorajoja ei ole, vaan työvaiheet etenevät järjestyksessä organisaatiosta riippumatta. (Rainamaa 29.1.2013)

Yksi tärkeä tehokkuutta tukeva tekijä on informaatioteknologian tuoma mahdollisuus automatisoida kontrollointia. Nykyaikaiseen sisäisen valvonnan työkaluohjelmistoon on mahdollisuus koodata valmiiksi mm. riskit ja kunkin yksikön merkittävyyden määrittävät tekijät. Tästä seuraa mahdollisuus analysoida sisäisen ja ulkoisen kontrollitestauksen tarvittava laajuus, jotta testataan vain oleelliset yksiköt. Tämän lisäksi automaattiset jatkuvan valvonnan ohjelmistot suorittavat reaaliaikaista analyysia valittujen kontrollien osalta ja siten antavat jatkuvasti tietoa niiden toimivuudesta. Automaattisen tarkastuksen etuna on tarkastajan resurssien säästyminen havaintojen analysointiin ja toiminnan kehittämiseen varsinaisen tarkastuksen sijaan, sillä suurin osa tarkastuksessa läpikäytävästä datasta on virheetöntä. (Rainamaa 29.1.2013)

Uusi kontrollijärjestelmä luodaan koko UPM:n tasolle maailmanlaajuisesti. Globaali taso on tarkoitettu soveltuvaksi kaikille liiketoiminta-alueille. Malli on kaikille liiketoiminta-alueille sama, mutta siitä voidaan joitakin osia jättää pois, jos kyseistä riskin taustalla olevaa prosessia ei ole lainkaan, mutta toisaalta yhteiseen sapluunaan ei tarvitse tehdä erityisiä lisäyksiä. Jotta kontrollitavoite ja riski saadaan jalkautettua aivan alimmalle käytännön tasolle, kirjoittaa kontrollia suorittava organisaatio ainoastaan yksityiskohtaisen kontrollikuvauksen, kuinka se suorittaa kontrollin. Jäljempänä tätä kuvausta kutsutaan työohjeeksi. Työohje saattaa sinällään olla jo olemassa, jos kyseinen työvaihe on jo nykyisin osa toimintaa, mutta ei osa virallista kontrollijärjestelmää. (Rainamaa 29.1.2013)

4.3.4. Projektin kulku

4.3.4.1. SoD- ja järjestelmäriskien hallinta

Kontrollijärjestelmäprojektin riippumattomana alaprojektina vedettävä tietojärjestelmien kehittämiseen tähtäävä SoD- ja järjestelmäriskien uudelleenkartoitusprojekti käynnistyi samoihin aikoihin kuin kontrollijärjestelmäprojekti. Projektin tavoitteena on selkeyttää käyttäjäoikeuksien hallintaa, ehkäistä eri järjestelmäympäristöjen rinnakkaisuutta, systematisoida käyttäjäoikeuksien hallintaa. Tämä keventää manuaalisen työn taakka, kun vuosittain arvioidaan kunkin käyttäjän käyttöoikeuksien aiheuttamat työyhdistelmäriskit. Projektin pidemmän tähtäimen tavoitteena on mahdollistaa CA/CM-ohjelmiston[1] käyttöönotto osana GRC-ratkaisua[2]. Tämä mahdollinen ratkaisu sisältää systemaattisen käyttöoikeuksien hallinnan, hälytykset vaarallisista työyhdistelmistä ja automaattisen data- ja poikkeama-analyysin, jolla voidaan havaita esimerkiksi poikkeuksellisia tapahtumia. (Hankkio 15.3.2013)

Jo nykytilanteessa kaikki käyttöoikeudet haetaan keskitetysti käyttöoikeusportaalin kautta, joten tiedot tallentuvat rekisteriin automaattisesti. Ongelma ei kuitenkaan ole tiedon olemassaolo vaan sen tehokas käsittely. Ennen projektin alkua käyttäjäoikeuksien aiheuttamia vaarallisia työyhdistelmiä seurattiin Excel-taulukossa kerran vuodessa täysin käsityönä. Tämä oli Hankkion mukaan erittäin työläs ja hidas prosessi, eikä siltikään päästy hyvään varmuuteen siitä, että käyttäjäoikeuksien yhdistelmistä aiheutuneet riskit on havaittu ja turhat käyttöoikeudet poistettu. Epävarmuus johtuu siitä, että käyttöoikeuksia haetaan jatkuvasti ja ihmiset vaihtavat paikkaansa suuressa organisaatiossa. Tämän vuoksi kerran vuodessa toteutettu riskikartoitus voi olla jo huomattavalta osaltaan vanhentunut puolen vuoden kuluttua. Riski väärinkäytöksestä muodostuu kuitenkin saman tien käyttöoikeuden myöntämisen jälkeen, minkä vuoksi käyttöoikeuksia myöntävät esimiehet ovat hankalassa asemassa, kun heillä ei nykyisellään ole selkeää näkyvyyttä muodostuvista työyhdistelmistä. (Hankkio 15.3.2013)

[1] CA = Continuous Auditing, jatkuva tilintarkastus; CM = Continuous Monitoring, jatkuva valvonta. Ks. KPMG 2012

[2] GRC: Governance, Risk and Compliance. Viittaa kokonaisvaltaiseen riskienhallintajärjestelmään ATK-ohjelmana.

Uudet tietotekniset sovellukset mahdollistavat käyttäjäoikeuksien automaattisen seurannan ja ohjelman generoimat hälytysraportit ilmoittavat uusista vaarallisista käyttäjäoikeusyhdistelmistä. Tällöin raportteja seuraava henkilö voi tarkastaa kohteena olevan henkilön esimiehen kanssa, luoko yhdistelmä tosiasiassa riskin väärinkäytökseen ja sen jälkeen arvioida, tarvitseeko henkilö oikeasti nämä käyttöoikeudet. (Hankkio 15.3.2013)

Projektin myötä käydään läpi kaikki yksittäiset toisistaan selkeästi erotettavissa olevat työtehtävät, esimerkiksi maksatusajon suorittaminen, pääkirjaan kirjaaminen jne. Nämä työtehtävät on helppo koota taulukkoon matriisimuotoon (Kuvio 4), vaaka- ja pystyakselille, jolloin rivin ja sarakkeen leikkauskohta tarkoittaa näiden työtehtävien yhdistelmää. Näin voidaan määritellä helposti ne työtehtävät, joiden tulisi olla eri henkilöiden suorittamia, jolloin SoD-riskit on havaittu.

	Down payment request	Down payment release	Clear down payment	Approve invoices	Payment proposal	Payment run	Process manual outgoing payment	Customer down payment request	Post customer down payment	Clear customer down payment	Raise customer invoice	Match receipts to invoices
Down payment request												
Down payment release	x											
Clear down payment	x	x										
Approve invoices	x	x	x									
Payment proposal				x								
Payment run				x	x							
Process manual outgoing payment	x	x	x	x	x							
Customer down payment request		x	x				x					
Post customer down payment							x	x				
Clear customer down payment							x		x			
Raise customer invoice	x						x			x		
Match receipts to invoices							x				x	

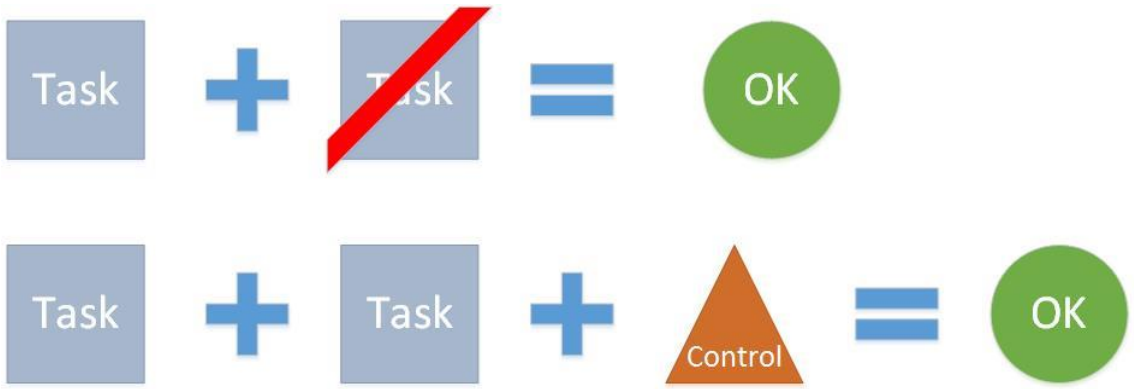
x = SoD conflict

Kuvio 4. Esimerkki SoD-matriisista. (Mukaillen, Deloitte 2007)

Riskiä voidaan kohtuullistaa kontrolloimalla, mitä työtehtäviä työntekijät suorittavat. Koska osa riskipitoisista työtehtävistä edellyttää tietojärjestelmien käyttämistä, voidaan järjestelmien käyttöoikeuksia rajaamalla tehokkaasti kontrolloida työtehtäviä, joita yhden työntekijän on mahdollista suorittaa. Kun edellä mainitut SoD-riskit on havaittu, voidaan tämä sama matriisi siirtää käytännön ympäristöön, jossa suurempien tietojärjestelmien osat, tai suppeampien ohjelmien tapauksessa koko ohjelma, vastaavat yksittäistä matriisin

mukaista työvaihetta. Näin päästään tehtävien eriyttämisen hallinnasta käyttöoikeuksien hallintaan. (Hankkio 15.3.2013)

Käyttöoikeuksien hallinta voidaan automatisoida silloin, kun käyttöoikeuksien hakeminen integroidaan SoD-matriisiin. Tätä varten tarkoitetusta järjestelmästä on mahdollista ajaa raportteja vaaralliseksi määriteltyjen työyhdistelmien esiintymisestä ja niihin voidaan tehokkaasti puuttua paitsi jälkikäteen, myös reaaliaikaisesti käyttöoikeuden myöntämisvaiheessa, mikäli järjestelmä ilmoittaa käyttöoikeuden myöntäjälle mahdollisesta SoD-riskistä. (Hankkio 15.3.2013)



Kuvio 5. SoD-riskin hallintaperiaate: vaarallisten työyhditelmien eriyttäminen ja riskin kohtuullistaminen lisäkontrollilla. (Mukaillen, Hankkion laatima esitysmateriaali)

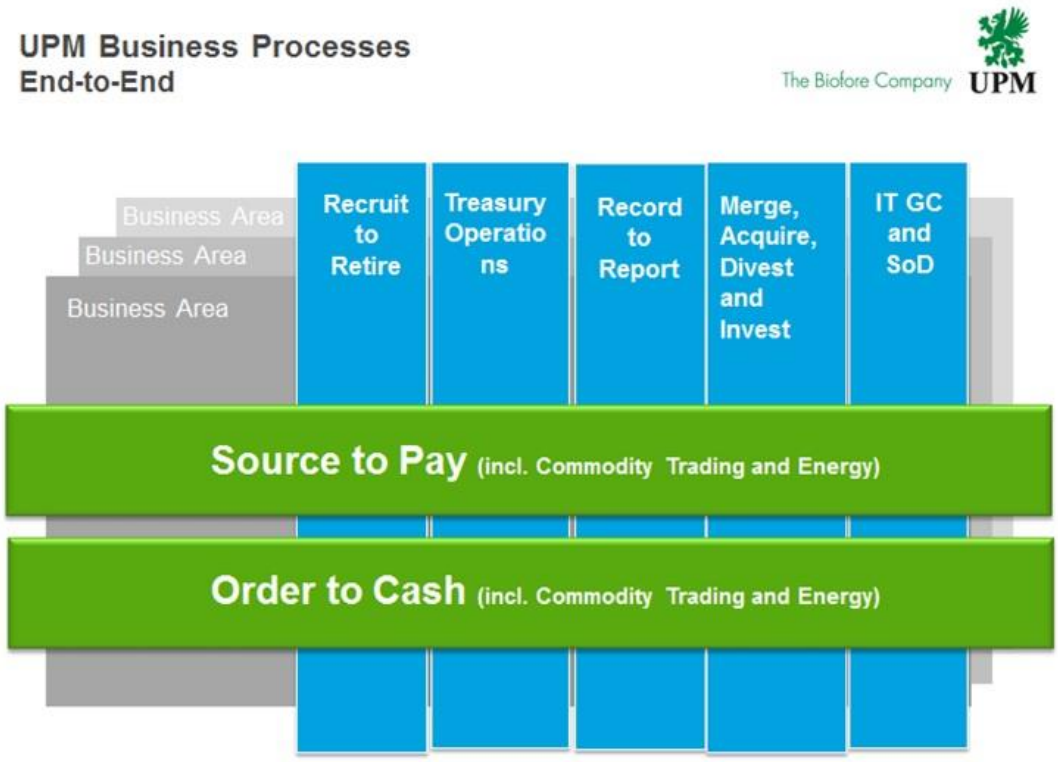
Kaikissa tapauksissa tehtävien eriyttäminen ei ole kuitenkaan mahdollista, jos tehtäviä hoitava tiimi on esimerkiksi niin pieni, että jonkun henkilön on suoritettava vaaralliseksi määritetty työyhdistelmä. Näissä tapauksissa voidaan erikseen arvioida, onko riski tässä tapauksessa olennainen, tai voidaanko riskiä alentaa jollakin erikseen suoritettavalla kontrollilla (ks. kuvio 5). Esimerkki lisäkontrollista laskun kirjaamisen ja maksatusajon tapauksessa on jonkun toisen henkilön hyväksyntä maksuajolle. Tavoitteena on joka tapauksessa vain kohtuullisen riskitason saavuttaminen, sillä turhan tarkka kontrollointi lisää SoD-riskin hallinnan kustannuksia ja siten vähentää tavoiteltua tehokkuutta. (Hankkio 15.3.2013)

4.3.4.2. Prosessien määritys

SOX-kontrollijärjestelmä lähti liikkeelle talousraportoinnin osa-alueiden riskeistä, joista kontrollit pyrittiin jalkauttamaan prosessitasolle ilman, että prosessitasolla kuvatut

kontrollit kuitenkaan vastaisivat todellista prosessivirtaa. Uudistettu kontrollijärjestelmä sen sijaan lähtee liikkeelle toisesta suunnasta eli liiketoiminnan prosesseista, ja niihin liittyvistä riskeistä. Tämän kaltaisen lähestymistavan ensimmäinen vaihe on kartoittaa liiketoiminnan prosessit. UPM:llä ei ennen projektin aloittamista ollut olemassa kaikki liiketoiminnot kattavaa ja riittävän tarkkaa prosessikarttaa, jota projektissa olisi voitu hyödyntää. (Rainamaa 30.9.2013).

Prosessikaaviota lähdettiin laatimaan ns. puhtaalta pöydältä. Prosessien suunnittelussa on lähdetty liikkeelle näkökulmasta, jossa kaikki prosessit seuraavat päätasolla samaa kaavaa liiketoiminnosta riippumatta. Tämän näkökulman tarkoituksena on mahdollistaa lopullisen prosessimallin monistaminen kaikkiin liiketoiminta-alueisiin soveltuvin osin ja näin välttää luomasta erityistapauksia. Ylimpänä prosessimallissa ovat pääprosessit ”Order to Cash” ja ”Source to Pay”. Nämä prosessit muodostavat yrityksen perusfunktiot: myyntifunktion ja ostofunktion (ks. kuvio 6). Nämä ovat yrityksen varsinaisen liiketoiminnan kannalta välttämättömiä prosesseja. Tukiprosessit nimensä mukaisesti tukevat pääprosessien toimintaa ja mahdollistavat pääprosessien tehokkaan toiminnan. Kaikki tukiprosessit ovat määritellyin rajapinnoin yhteydessä pääprosesseihin ja lisäksi usein toisiinsa. Yhdessä nämä prosessit muodostavat prosessien päätason. (Rainamaa 20.3.2013)

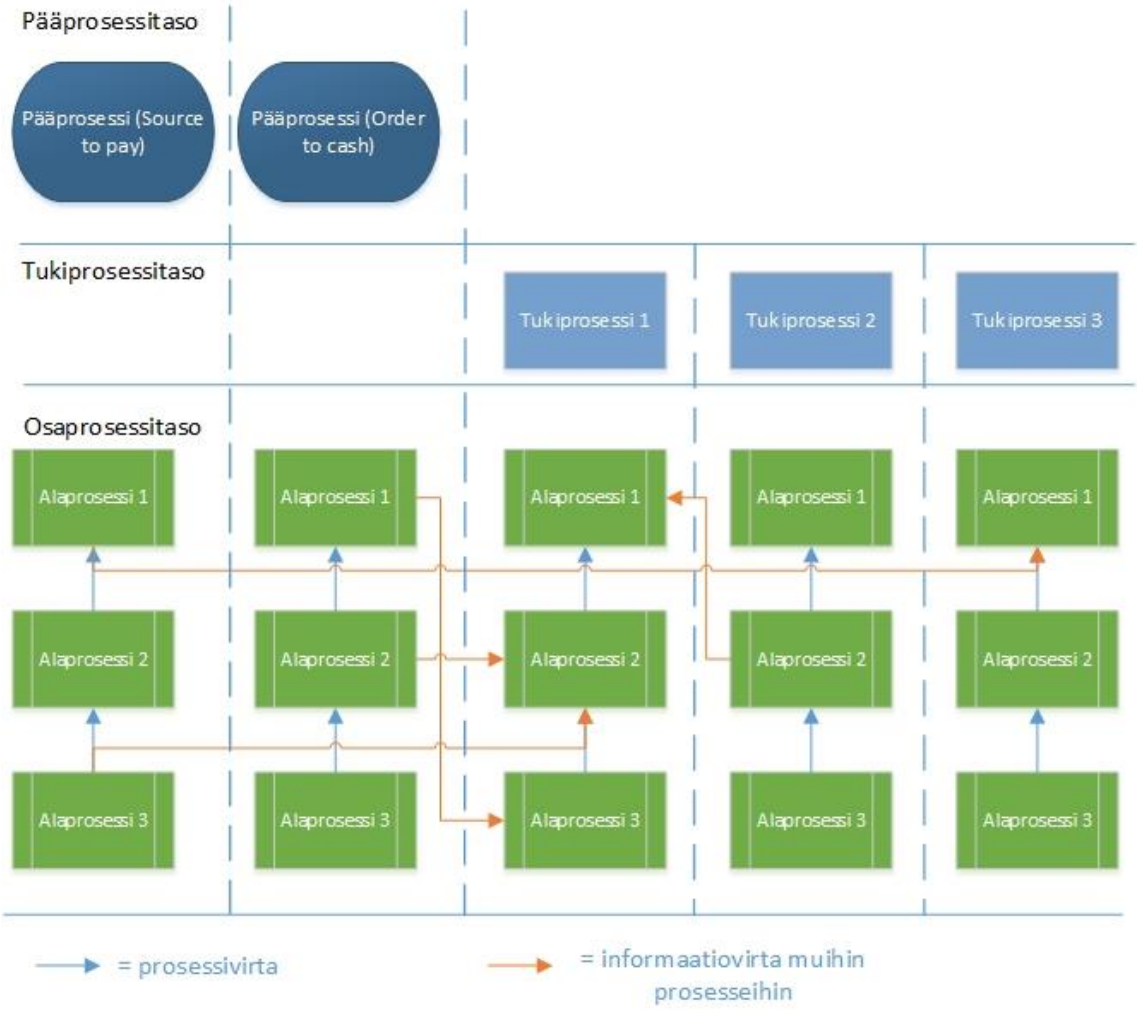


Kuvio 6. UPM:n pää- ja tukiprosessit (UPM, projektimateriaali 2013)

Käytännössä prosessimallin ylin taso eli päätaso suunniteltiin yhdessä kokouksessa, jossa oli riittävän päätösvaltainen kokoonpano liiketoiminta-alueiden ja tukitoimintojen avainhenkilöitä. Tässä tilaisuudessa yhteisesti visioitiin kuvion 6 mukainen prosessikartta, ja päätettiin suurin piirtein, mitä toimintoja kukin tukiprosessi sisältää ja samalla pohdittiin, ketkä ovat ne henkilöt, jotka kutakin tukiprosessia voivat kartoittaa tarkemmin. Vielä myöhemmin prosessilaatikoiden sisältöä on tarkennettu ja muiden muassa energialiiketoiminta erityslaatuisuudestaan huolimatta päätettiin sisällyttää samaan prosessimuottiin. (Rainamaa 20.3.2013)

Ylätason suunnittelun jälkeen alkoi pienryhmätyöskentely kunkin päätason prosessin asiantuntijoiden kesken. Suunnitteluun valittiin erityisesti asiasta kiinnostuneita ja motivoituneita henkilöitä sen sijaan, että olisi määrätty suoraan vastuuhenkilöt. Jokaisen pää- ja tukiprosessin sisältö määriteltiin yhdellä virkkeellä ja prosesseille määriteltiin alku- ja loppupisteet. Tämän lisäksi kuhunkin pää- ja tukiprosessiin kuuluu joukko pienempiä osaprosesseja, joista itse päätason prosessi muodostuu. Esimerkiksi Record to

Report -prosessi (jäljempänä RtR) koostuu seitsemästä osaprosessista, joita ovat esimerkiksi välillisen verotuksen prosessi, pääkirjaprosessi ja sisäisen raportoinnin prosessi. Merkittävää prosessimallissa on se, että sen jaottelu ei seuraa millään tavalla UPM:n organisaatiota, joten yhdessä organisaatiossa saatetaan osallistua usean osaprosessin suorittamiseen. (Rainamaa 20.3.2013; Rainamaa 30.9.2013) Näin ollen prosessihierarkia on kontrollijärjestelmää silmällä pitäen kolmitasoinen kuvion 7 esittämällä tavalla.



Kuvio 7. Prosessimallin kolme tasoa (mukaillen, UPM Projektimateriaali 12.3.2013)

Kun prosessit oli määritelty, laadittiin kaikista pää- tuki- ja osaprosesseista kaaviot, joihin merkittiin liittymäpinnat muihin prosesseihin hahmottamisen helpottamiseksi.

Varsinaisen prosessikartan kehittäminen ei kuitenkaan ollut tämän työvaiheen tarkoitus, vaan osaprosessien mahdollisimman tarkka rajaaminen. Kukin osaprosessi otettiin syvennettyyn käsittelyyn seuraavassa vaiheessa, riskien ja kontrollitavoitteiden määrittelyn yhteydessä. (Rainamaa 20.3.2013; Projektimateriaali 2013) Määriteltyjen osaprosessien joukossa on myös sellaisia osaprosesseja, joilla ei ole selkeää liittymäpintaa taloushallintoon, mikä on selvä muutos olemassa olevaan kontrollijärjestelmään.

4.3.4.3. Riskien kartoitus ja kontrollitavoitteiden määritys

Riskien kartoitusta ja kontrollitavoitteiden laadintaa alettiin toteuttaa työryhmissä, joihin oli koottu henkilöitä, joilla oli riittävä tietämys prosessin eri osa-alueista, jotta koko prosessin riskit saataisiin kartoitettua. Työryhmien kokouksissa oli läsnä sparraajana ja kirjurina myös kontrolliprojektin vetäjä Maarit Rainamaa, jolla näin ollen olisi projektin lopuksi näkemys prosessien horisontaalisesta kokonaisuudesta. Tällä mallilla käytiin läpi kaikki prosessit osaprosesseja myöten globaalilla tasolla, joten yksittäisiin liiketoiminta-alueisiin ei puututtu eikä mitään työryhmän tuloksia myöskään jätetty kirjaamatta siksi, että se ei olisi johonkin liiketoiminta-alueeseen sopiva. (Rainamaa 20.3.2013)

Riskien kartoituksessakaan ei käytetty mitään olemassa olevan kontrollijärjestelmän materiaalia tai riskilistausta, vaan kartoitus lähti täysin puhtaalta pöydältä. Apuna oli ainoastaan määritelty osaprosessi tai osaprosessit alku- ja päätepisteinen, jos käsittelyssä oli samalla kerralla useampi osaprosessi. Riskien kartoitus toteutettiin ryhmissä keskustellen ja yhdessä ideoiden. Usein joku asiantuntijoista alkoi ikään kuin ajatella prosessia ääneen alusta loppuun ja muut saivat tästä ideoita mahdollisista riskeistä. Kristiina Kaski (8.4.2013) kertoi tiiviin esimerkin RtR-prosessin ideoinnin yhteydessä käydyn keskustelun kulusta:

> Pääkirjanpitoprosessiin siirtyy liittymien kautta dataa, jota me alamme analysoida. Mikä voi mennä väärin? Liittymästä tulee vääränlaista dataa, epätäydellistä, huonolaatuista, kahteen kertaan tai se tulee väärään aikaan. Miten tätä valvotaan? Tehdään liittymätäsmäytyksiä. Sen lisäksi pääkirjanpitoon on kirjattava tapahtumia, joista ei saada tietoa liittymien kautta. Meidän on siis tehtävä jotakin. Miten me

> huomaamme ja tunnistamme ne asiat, jotka eivät tule liittymien kautta? Me tarvitsemme kommunikaatiota liiketoimintayksiköiden kanssa. Me tarvitsemme mahdollisesti joitakin tarkistuslistoja, joissa on listattuna ne yleisimmät asiat, jotka meidän pitäisi saada. Täytyykö näille asioille tehdä jotakin? Onhan kaikki huomattu tehdä? Sitten on vielä analysoitava ulos lähtevät numerot ja arvioida, ovatko ne järkeviä. Näiden riskien lisäksi asiaan liittyy myös muita riskejä, kuten virheitä järjestelmässä, virheellistä master dataa, virheellisiä koodeja jne. Miten me huomaamme nämä virheet?

Esimerkissä edetään loogisesti riskistä tavoitteen kautta kontrollitoimenpiteen ideointiin. Rainamaan mukaan joskus keskustelu oli luonnollisempaa aloittaa kontrollitavoitteesta ja etsiä varsinainen riski tämän jälkeen. Riskien havaitsemisessa pyrittiin ikään kuin brainstorming-menetelmällä ensin kattamaan yleistaso ja toteamaan, että riskit on mahdollisimman kattavasti tunnistettu. Tämän jälkeen riskejä alettiin tarkastella ja monesti niitä voitiin niputtaa yhteen, kun toisinaan sama riski oli ilmaistu hieman eri muodoissa useampaan kertaan. (Rainamaa 20.3.2013)

Riskien alustavan kartoituksen ja päällekkäisyyksien poistamisen jälkeen riskejä analysoitiin Excel-taulukon avulla kartoittaen riskin realisoitumisen vaikutuksia (taulukko liitteessä 2). Ensiksi otetaan kantaa siihen, onko kyseessä liiketoiminnan riski vai talousraportoinnin riski. Toiseksi otettiin kantaa siihen, sisältyykö riskiin mahdollisuutta petokseen kolmen eri vilppityypin perusteella. Nämä yleiset vilppityypit ovat vilpillinen raportointi (myös ei taloudellinen raportointi), yhtiön varojen väärinkäyttö (sisältäen varkaudet ja rahanpesun) ja korruption. Edellä luetellut vilppityypit on määritelty COSO:n vuoden 2013 viitekehyksessä. Kolmanneksi määriteltiin ne tilinpäätöksen tilit, joihin riski voi vaikuttaa.

Rainamaan mukaan tämä tarkempi riskien analysoiminen auttoi monessa tapauksessa huomaamaan, että riski ei todennäköisesti ole hyvin muotoiltu, jos työryhmällä oli vaikeuksia liittää käsiteltävää riskiä mihinkään näistä kategorioista. Toisaalta, jos riskillä ei arvioitu olevan realisoituessaan mitään vaikutusta tilinpäätöksen kannanottoihin, voitiin kyseenalaistaa vaikutus tilinpäätökseen ja pohtia uudelleen muiden kategorioiden soveltuvuutta. (Rainamaa 20.3.2013)

Samassa työryhmässä pohdittiin riskeihin riskikartoituksen yhteydessä myös kontrollitavoitteet. Kuten edellä todettiin, käytännössä kokouksessa ehdotettiin toisinaan kontrollitavoitetta ensin ja sitten vasta ikään kuin takaperin etsittiin riski. Riski ja kontrollitavoite suunniteltiin vastaamaan toisiaan ja ne syötettiin liitteen 2 mukaiseen Excel-taulukkoon riskin numeron mukaiseen sarakkeeseen. Mikäli riski on monitahoinen, voitiin samaan riskiin liittää useita kontrollitavoitteita. Esimerkiksi UPM:n projektimateriaalin perusteella pääkirjaprosessiin liittyvään riskiin ”incomplete / insufficient / unpunctual period end closing activities” liitettiin kolme kontrollitavoitetta: 1) ”Relevant closing activities in SAP are performed and in correct sequence” 2) ”Relevant information is available within the given time schedules” 3) ”No accounting postings to old periods”. Kontrollitavoitteiden merkitys projektin edetessä oli erityisesti kontrollitoimenpiteiden suunnittelun ohjaaminen määrättyyn tarkasti mitattavaan tavoitteeseen. Kontrollitavoitteet auttavat paitsi kontrollitoimenpiteiden suunnittelua, ne myös toimivat johtoajatuksena ja motivaationa kontrollitoimenpiteen suorittajalle. (Rainamaa 20.3.2013; Kaski 8.4.2013)

Jotta Compliance-tavoite saatiin entistä vahvemmin mukaan kontrollijärjestelmään, määritettiin myös Compliance-riskit, joiden määrittely poikkesi hieman edellä kuvatusta. Compliance-riskeistä huomattava osa muodostuu talousraportoinnin eri maiden raportointivaatimuksista, kuten verokäytännöistä ja paikallisen lain vaatimuksista. UPM:n organisaatiossa talousraportoinnin paikallisista erityispiirteistä vastaa LCF-organisaatio (IFRS-vaatimuksista vastaa Global Finance -organisaatio), jolla on osaamista paikallisesti kussakin merkittävässä maassa, jossa UPM:llä on liiketoimintaa. Riskien kartoittamiseksi merkittävimpien maantieteellisten liiketoiminta-alueiden paikallisesta talous- ja veroraportoinnista vastaaviin henkilöihin oltiin yhteydessä projektin kuluessa ja kommunikoitiin, mitä oltiin tekemässä ja nyt siihen olisi mahdollisuus vaikuttaa ja saada paikalliset erityisvaatimukset huomioitua. Paikallisraportoinnin vastuuhenkilöt ja asiantuntijat ottivat projektin innokkaasti vastaan, ja toimittivat sähköpostitse luonnokset omista riski- kontrollitavoite- ja kontrollitoimenpide-ehdotuksistaan. Näiden ehdotusten pohjalta järjestetyissä kokouksissa asiat vielä keskusteltiin läpi jo edellä esiteltyyn tapaan. (Rainamaa 20.3.2013)

4.3.4.4. Kontrollitoimenpiteet ja olennaisten kontrollien rajaus

Tutkimuksen kohteena olevan projektin puitteissa määritellään vielä globaalilla tasolla kontrollitoimenpiteet vastaamaan kunkin kontrollitavoitteen asettamaan haasteeseen. Nämä kontrollitoimenpiteet suunniteltiin suuremmilta osin samoissa työryhmissä kuin riskikartoitus ja kontrollitavoitteiden kehityskin tehtiin, mutta mukana voi olla myös muita käsiteltävän prosessin asiantuntijoita, joilla on syvää asiantuntemusta esimerkiksi jostakin pienemmästä prosessin osasta. Työryhmiin perustuvien kokousten lähestymistapa kontrollitoimenpiteiden suunnitteluun oli samantapainen kuin riskikartoituksen yhteydessä, eli ideointi toteutettiin avoimen keskustelun avulla. Projektin puitteissa ei sen sijaan perehdytä kontrollitoimenpiteiden yksityiskohtaiseen ohjeistamiseen, vaan siitä vastaavat kunkin prosessin vastuuhenkilöt kontrollia suorittavassa organisaatiossa ja kussakin liiketoimintayksikössä. He toteuttavat kontrollijärjestelmän jalkautuksen käytännön tasolle huomioiden oman prosessinsa erityispiirteet. Tämä lähestymistapa valittiin, sillä vain näillä henkilöillä on riittävän syvä tuntemus tarvittavista yksityiskohdista. (Rainamaa 20.3.2013)

Kontrollitoimenpiteet määriteltiin projektin workshopeissa yleisellä tasolla siten, että määritelmää voidaan soveltaa jokaisella liiketoiminta-alueella. Määritelmät koodattiin riskimatriisiin, jonka malli on liitteessä 3. Riskimatriiseja on osaprosessia kohti yhtä monta kuin siinä on määriteltyjä riskejä. Yhteen riskiin voi olla liitetty useampi eri kontrollitavoite, jotka on listattu taulukon sarakkeessa ”Control Objectives”. Vastaavasti kuhunkin kontrollitavoitteeseen pääsemiseksi voidaan käyttää useampaa kontrollia, jotka on listattu seuraavaan sarakkeeseen ”Control Activities”. Seuraavaan sarakkeeseen linkitetään kontrolliin suorittamiseen liittyvät yksityiskohtaiset työohjeet, jotka laatii vastuunalainen organisaatio, joka on mainittuna seuraavassa sarakkeessa. Vastuunalaisia organisaatioita voi olla myös useampi kuin yksi. Seuraavan sarakkeen kontrollifrekvenssi määritellään tapauskohtaisesti kontrolloitavan asian perusteella. Kontrollityyppiä määritellään seuraavissa kahdessa sarakkeessa ”Control rating type” ja ”Detective/Preventative”. (UPM Projektimateriaali; Rainamaa 29.1.2013) Kontrollityypin merkitys on sikäli olennainen, että erilaisten kontrollointityyppien tuottama varmuus prosessin toiminnasta nähdään erisuurena. Täsmäytys (Reconciliation) tuottaa varsin yksiselitteisen lopputuloksen: täsmää tai ei täsmää, mutta esimerkiksi management review on vahvasti riippuvainen kontrollin suorittajan osaamisesta.

Manuaaliset kontrollit on helppo jättää suorittamatta tai ymmärtää väärin. Automaattinen ehkäisevä kontrolli on usein kaikista luotettavin, jos sitä ei pysty kiertämään. Paljastavat kontrollit pystyvät sen sijaan havaitsemaan myös odottamattomat poikkeukset, kuten odottamatonta kautta tulleen datan. Se, että data siirtyy järjestelmästä A kohti järjestelmää B liittymässä suunnitellusti, ei varmuudella vielä tarkoita sitä, että sekä lähtevä että kohteessa lopulta oleva data olisi yhtenevää. Varmuuden saamiseksi tulisi siis verrata, että kaikki järjestelmässä B oleva data on samaa kuin järjestelmässä A. (Kaski 8.4.2013)

Taulukkomuotoinen koodausmenetelmä mahdollistaa sen, että prosessikartat, riskimatriisit ja työohjeet on mahdollista linkittää toisiinsa tietokantaohjelmassa tai erityisesti tähän tarkoitukseen laaditussa GRC-ohjelmistossa. Tämä rakenne mahdollistaa työohjeiden päivitykset tietokantaan, johon sekä kontrollin suorittajalla että tarkastajalla on pääsy. Työohjeet laaditaan siten, että niissä on tarkalleen määritelty ne toimenpiteet, joita kontrollin suorittajan tulee tehdä. Tämä palvelee paitsi kontrollin suorittajaa, kun hän tietää millä toimenpiteillä kontrollin edellytykset täyttyvät, myös sisäistä tai ulkoista tilintarkastajaa, kun hänellä on käytettävissään tarkka kuvaus kontrollin suorittamisesta. Jos kontrolli on esimerkiksi liittymätäsmäytys, työohjeissa määrätään millä järjestelmäraportilla ja millä parametreilla raportti ajetaan kussakin järjestelmässä ja miten kontrolli dokumentoidaan. Mikäli työvaiheet on mahdollista koodata GRC-ohjelmistoon samalla rakenteella, kuin riskimatriisin kontrollitoimenpiteet on koodattu, on mahdollista suorittaa reaaliaikaista kontrollitoimenpiteiden suorittamisesta. Kun kontrollitoimenpiteen yksittäinen työvaihe on suoritettu, käyttäjä voi merkitä tehtävän tehdyksi ja näin ollen kontrollien suorittamista voidaan seurata riskitasolta, millä toimenpitein riskiä on hallittu. (Hankkio 15.3.2013; Rainamaa 20.3.2013)

Kontrollitoimenpiteitä suunnitellessa pyrittiin siihen, että mahdollisimman moni jo olemassa oleva työvaihe, joka ehkäisee riskiä, voidaan ottaa osaksi dokumentoitua ja testattavaa kontrollijärjestelmää. Business controllereiden keskeisimpiä työtehtäviä ovat erilaiset tarkistukset, analyysit ja täsmäytykset, joita he tekevät normaalissa työssään. Pyrittiin siihen, että näiden tehtävien lisäksi heidän ei tarvitsisi tehdä vielä erikseen standardoituja tarkistuksia ja analyyseja. Päällekkäisyydestä pyrittiin eroon. Tässä lähestymistavassa on kuitenkin törmätty ongelmaan, jossa olemassa olevat yksittäiset työvaiheet sisältävät kontrolliaspektin, mutta ne liittyvät epäolennaiseen riskiin. Toisaalta

joissakin tapauksissa yksittäisiä kontrolliaspektin sisältäviä työvaiheita olisi ollut mahdollista ottaa dokumentoidun kontrollijärjestelmän piiriin useampi kuin todettiin tarpeelliseksi. (Kaski 8.4.2013)

4.3.4.5. Kokonaisuuden arviointi ja korjaavat muutokset

Koska jokainen osaprosessia työstävä ryhmä koostuu hieman eri henkilöistä, on kokonaiskuva projektista vain projektinvetäjällä. Hänen tärkeäksi tehtäväkseen tuli seurata erityisesti prosessikuvauksia, kontrollitavoitteita ja kontrollitoimenpiteitä, jotta niiden keskinäinen rajanveto oli paitsi aukotonta myös havaita mahdolliset kahdesti mukaan luetut riskit. Rainamaan mukaan näin oli toisinaan käynyt tahattomasti, kun sama riski oli muotoiltu hieman eri tavalla. Toisaalta riskien sijoittaminen oikeiden prosessien yhteyteen tuli varmistaa. (Rainamaa 20.3.2013)

Kun prosessien riskit ja kontrollitavoitteet oli määritelty, oli tehtävä arviointi, jossa kukin riski arvioitiin uudelleen ja varmistettiin, että se on sijoitettu oikeaan prosessiin ja että sama riski oli huomioitu vain yhdessä prosessissa. Tässä yhteydessä käytiin myös läpi kaikki päällekkäiset ja kahteen kertaan mukaan lasketut riskit, jotka riittävän asiantuntemuksen prosessista omaavan ryhmän kesken määriteltiin uudelleen. Tuplasti mukana olleet riskit selvitettiin vielä sen ideoineen pienryhmän kanssa kommunikoiden, että riskin kuvaus on projektijohdossa ymmärretty oikein ja kyseessä on todella tupla. (Rainamaa 30.9.2013)

Riski- ja kontrollikartoituksen päätteeksi otettiin ensimmäisen kerran esille olemassa olevan kontrollijärjestelmän riski- ja kontrolliviitekehysmääritelmät. Näitä määritelmiä verrattiin projektin tuloksena kartoitettuihin riskeihin ja varmistettiin, että yhtään olennaista riskiä tai kontrollia ei ole jäänyt puuttumaan. Tämä arviointi suoritettiin kussakin asiantuntijaryhmässä riski- ja kontrollitavoitemäärittelyn lopuksi. Tässä vaiheessa myös sisäisen tarkastuksen edustajat olivat neuvoa antavassa roolissa mukana siten, että heidän riskilähtöisellä ajattelulla varmistettiin, että kontrollijärjestelmään ei jää vahingossa aukkoja. Joitakin olemassa olevan kontrollijärjestelmän riskejä todettiin voitavan yhdistää toisiinsa ja joidenkin riskien todettiin menettäneen merkitystään liiketoiminnan muutosten vuoksi. (Rainamaa 20.3.2013)

4.3.4.6. Testauksen huomioon ottaminen kontrollijärjestelmää suunniteltaessa

Kontrollijärjestelmän kehitysprojektin suunnitteluvaiheessa päätettiin, että kontrollien tarkastuksen suunnittelu ei ole osa tätä kehitystyötä. Se, miten kontrollien käyttöönottoa ja toimivuutta voidaan testata, suunnitellaan vasta kuin malli on muutoin valmis. Testattavuutta ei pidä sekoittaa kontrollitoimenpiteiden toteutettavuuden ja toimivuuden kanssa, vaan se, miten kontrollien toimivuudesta ja luotettavuudesta saadaan varmuus, on oma asiakokonaisuutensa. Sisäisen valvonnan kannalta tärkeintä on se, että laadittu kontrollijärjestelmä toimii. Tarkastuksen tehtävä on pystyä toteamaan kontrollijärjestelmän toimivuus. (Kaski 8.4.2013)

Tästä ajatustavasta, että ”tarkastusta ei vielä mietitä” on kuitenkin tehty muutama poikkeus. Ensiksikin hyvin dokumentoitu kontrollijärjestelmä palvelee paitsi kontrolleja suorittavaa organisaatiota, myös tarkastusta. Tästä syystä dokumentaatioratkaisu haluttiin saada sellaiseksi, että myös tarkastajat saavat sen vaivatta käsiinsä. (Rainamaa 20.3.2013)

Toiseksi, tietotekniikan kehityksen myötä mahdollistunut automatiikan lisääminen on haluttu ottaa huomioon kontrollitoimenpiteitä suunniteltaessa. Erityisesti SAP-ympäristössä on mahdollista suorittaa automatisoituja data-analyysiohjelmia, jotka käyvät läpi tietyn aikavälin kaikki transaktiot, ja ilmoittavat poikkeavista tapahtumista. Nämä automatiikan suorittamat analyysit ovat toimenpiteitä, joita tilintarkastajat suorittaisivat normaalisti vuosittaisen tarkastuksen yhteydessä. Näin ollen on mahdollista, että tilintarkastajat voivat hyödyntää automatiikan tuottamia raportteja tarkastuksen yhteydessä. (Rainamaa 29.1.2013)

Kolmanneksi, projektin fokusalueeseen kuuluvaksi osaksi on otettu kartoitettujen ja dokumentoitujen riskien olennaisuuden määritys, joka liittyy olennaisesti testaukseen. Määritysprosessista on kerrottu tarkemmin seuraavassa luvussa. Perusteluksi tälle valinnalle voitaneen nähdä se, että ne henkilöt, jotka riskit parhaiten tuntevat, ovat mukana projektin työryhmissä ja ovat siten parhaita henkilöitä arvioimaan kunkin riskin todennäköisyyttä ja mahdollisia seurauksia. Tilintarkastaja on toki riskienhallinnan ammattilainen yleisemmällä tasolla, mutta hänellä ei välttämättä ole riittävää teknistä ja yksityiskohtaista tietoa erityisistä riskeistä.

4.3.4.7. Riskien olennaisuustason määritys

Kun edelliset vaiheet on saatu tehtyä, perehtyivät työryhmät riskien merkittävyyden arviointiin. Tavoitteena oli liittää kuhunkin riskiin sen toteutumisen arvioitu todennäköisuus ja mahdolliset seuraukset sen realisoituessa. Näitä ei kuitenkaan kirjattu mihinkään lopputulokseen mukaan tulevaan taulukkoon, vaan työpaperiksi myöhempää varten. Myöhemmin näitä tuloksia suunniteltiin hyödynnettävän, kun työryhmä suorittaa riskien olennaisuuden arvioinnin kaikille prosesseille. Tämän työryhmän kokoonpanossa kiinnitettiin erityistä huomiota laajaan prosessituntemukseen ja kokemukseen riskienhallinnasta ja tarkastamisesta. (Rainamaa 20.3.2013)

Tehtävässä pidettiin tärkeänä sitä, että samat henkilöt arvioivat kaikki riskit, jotta linja olisi horisontaalisesti yhtenevä, jolloin esimerkiksi kohtalaiseksi arvioitu riski prosessissa A on yhtä merkittävä kuin kohtalaiseksi arvioitu riski prosessissa B. Epäyhtenäinen linja riskin olennaisuuden arvioinnissa on ollut erityisesti nykyisen kontrollijärjestelmän kohdalla ongelma, jolloin määriteltyä riskin olennaisuustasoa ei ole voitu täysipainoisesti hyödyntää tarkastuksessa. (Rainamaa 20.3.2013)

Asteikko on kolmiportainen: low (matala) – medium (kohtalainen) – high (korkea). Tämän lisätiedon tehtävänä on ohjata paitsi kontrollifrekvenssiä myös kontrollijärjestelmän testausta. Kun riskitaso yhdistetään riskimatriisissa määritettyyn tiliin, voidaan esimerkiksi testausta suunniteltaessa valita vähämerkityksiseksi arvioituun tiliin liitetyistä riskeistä testaukseen vain korkean merkittävyyden riskit. Vastaavasti voidaan arvioida, että matalan merkittävyyden omaavat riskit voidaan testata harvemmin, kuten vain joka kolmas vuosi. (Rainamaa 20.3.2013)

Kolmiportaisesta riskimäärittelystä kuitenkin luovuttiin projektin myöhemmässä vaiheessa. Riskeistä joitakin pidettiin edelleen merkittävinä ja joitakin vähemmän merkittävinä, mutta riskien olennaisuustason määrittelyä ei toteutettu alkuperäisen suunnitelman mukaan. Sen sijaan riskejä analysoitiin edellä mainittujen vilppityyppien perusteella, jotka määriteltiin yhdessä sisäisen tarkastuksen edustajan kanssa. (Rainamaa 16.7.2014)

Riskien olennaisuudella on merkitystä myös kontrollitestauksen jälkeen. Mikäli todetaan, että riskiä ehkäisemään laadittu kontrolli on suoritettu puutteellisesti tai sitä ei ole suoritettu lainkaan, auttaa olennaisuustaso arvioimaan korjaavien toimenpiteiden laajuutta. Mikäli riskiä ei ole ehkäisty kontrollilla, voidaan joutua kehittämään muita keinoja jälkikäteen riskin pienentämiseksi. Tässä tilanteessa mahdollisuutena on välttää turhaa lisätyötä, mikäli on jo tiedossa, että riski ei ole merkitykseltään korkea.

4.3.4.8. Jalkautus

Projektin kehitystiimeissä oli osaajia organisaation lähes kaikilta osa-alueilta, joilla kontrollointia aletaan jalkauttaa. He voivat siten toimia tämän prosessin alkuunpanijoina ja neuvonantajina omalla osa-alueellaan ja seurata kontrollien jalkautusta käytännön ohjeistuksiksi. Vastuu on paikallisesti kunkin prosessin organisaatioissa, joissa kontrollitoimenpiteitä suoritetaan. Jokainen kontrollitoimenpide pohditaan kyseisen relevantin liiketoiminnon kohdalla, ja selvitetään ne konkreettiset toimenpiteet, kuten valitut raportit, joilla kontrollitoimenpide suoritetaan käytännössä. Kuten edellä todetaan, tästä työvaihekohtaisesta dokumentaatiosta tulee kontrollijärjestelmän dokumentaatiohierarkian alin taso, lähimpänä käytäntöä. Kaikki tämä luotu dokumentaatio tallennetaan samaan tietokantaohjelmaan (joko dokumenttina tai linkitettynä), johon koko kontrollijärjestelmän hierarkia on tallennettu. Näin on mahdollista lähteä ylhäältä riskistä seuraamaan päättelyketjua kontrollitavoitteen ja kontrollitoimenpiteen kautta aina käytännön työvaiheen ohjeistukseen saakka tai päinvastoin. Tämä mahdollisuus palvelee sekä käytännön kontrollointia toteuttavan henkilön tarpeita, että tilintarkastajan tai sisäisen tarkastajan tarpeita. (Rainamaa 20.3.2013) Tämä dokumentointiprosessi ei kuitenkaan kuulu tämän tutkimuksen piiriin, sillä siinä tuotetaan valtava määrä erilaisia kontrollitoimenpiteitä, joiden teoreettinen tausta ja kontrollin tavoite eivät kuitenkaan poikkea tässä tutkimuksessa jo käsitellystä.

5. TUTKIMUSTULOKSET

5.1. Kehitystyön motiivit ja tavoitteet

UPM:n käytössä on ollut kattava talousraportoinnin sisäisen valvonnan järjestelmä, jota on tarvittaessa päivitetty ajantasaiseksi. Koska sisäinen valvonta on prosessi, on luonnollista, että toisinaan on tehtävä perusteellisempia päivityksiä sisäiseen valvontaan. Vaikka sisäisen valvonnan ylläpitämisen velvoitteet poistuivat, kattavasta sisäisestä valvonnasta ei kuitenkaan haluttu luopua. Näin ollen voidaan päätellä, että käytössä olleesta sisäisen valvonnan järjestelmästä on koettu olleen hyötyä.

Alun perin sisäisen valvonnan järjestelmä laadittiin kattamaan vain talousraportoinnin osa-alue, joka on yksi COSO:n määrittelemästä sisäisen valvonnan tavoitteesta. Tämän tutkimuksen tarkasteleman projektin myötä sisäinen valvonta ulotetaan kuitenkin täysipainoisesti kaikkiin kolmeen COSO:n määrittelemään tavoitteeseen. Suurin muutos lähestymistavassa on siis myös toimintojen tehokkuuden varmistamisen ja normien noudattamisen varmistaminen talousraportoinnin oikeellisuuden lisäksi. Kirjallisuuden perusteella tällä muutoksella pitäisi olla positiivinen vaikutus erityisesti johtamisen tehokkuuteen ja strategian tehokkaaseen toteuttamiseen. Muita tehokkaan sisäisen valvonnan kokonaisuuden tuomia hyötyjä ovat mahdollisuus tehokkaammin integroituun sisäisen valvonnan järjestelmään, lisääntynyt läpinäkyvyys organisaatiossa ja pienemmän riskin myötä alentunut pääoman kustannus. Taulukossa 4 on tiivistettynä sisäisen valvonnan motiivit ja tavoitteet agenttiteorian, COSO:n, muun kirjallisuuden ja case-yrityksen mukaan. Taulukko havainnollistaa teorian, kirjallisuuden ja käytännön tason suhdetta, miten johtamisjärjestelmiä ja erityisesti sisäisen valvonnan järjestelmän kehittämistä perustellaan. Taulukon perusteella voidaan todeta, että case-yrityksen tavoitteet ovat samansuuntaiset kuin kirjallisuuden perusteella voidaan ennustaa.

Case-materiaalin perusteella UPM:n sisäisen valvontajärjestelmän kehittämisen motiiveja olivat perinpohjaisen uudistuksen tarve, jotta valvontajärjestelmä vastaisi yhtiön ajanmukaisia prosesseja ja sopiva ajankohta, kun sisäisen valvonnan ohjelmisto oli uusittava joka tapauksessa. Liiketoiminnan tavoitteiden lisäys olemassa olleeseen kontrollijärjestelmään nähden nähtiin mahdollisuutena jalkauttaa yhtiön strategiaa liiketoiminta-alueille ja alemmas organisaatiossa. Case-materiaalin perusteella ei ilmene,

aiotaanko strategiaa jalkauttaa systemaattisin keinoin kontrollitavoitteiden ja kontrollitoimintojen lisäksi, mutta Jokipiin ja Agbejulen (2009) mukaan jo valvonnan ja seurannan välisellä painotuksella on yhteys strategiaan.

	agenttiteoria	COSO	lisäksi muualla kirjallisuudessa	case-yritys
motiivit	• päämiehen hyvinvoinnin optimoiminen	• tehokkaampi johtaminen • yllätysten minimointi	• strategian toteutus • läpinäkyvyyden parannus yli prosessien • alempi pääoman kustannus	• olemassa olevan valvontajärjestelmän kehittäminen • mahdollisuus jalkauttaa strategiaa
tavoitteet	• agentin tehokkaan toiminnan varmistaminen • agentin toiminnasta raportoivan informaation luotettavuus	• varmistaa prosessien tarkoituksenmukainen toiminta • talousraportoinnin luotettavuus • lakien, säännösten ja toimintatapojen noudattaminen	• havaita tehottomuudet vertailemalla eri toimintoja luotettavasti	• valvonnan integrointi osaksi prosesseja • talousraportoinnin kontrollien kerroksellisuus • globaali, yhteinen toimintamalli

Taulukko 4. Sisäisen valvonnan motiivit ja tavoitteet teoriassa ja käytännössä (Holmström 1979; COSO 1992; KPMG 1999; PWC 2003; Hightower 2008; Ahokas 2012).

Tärkeimpinä muutoksen mukanaan tuomina tavoitteina mainitaan mahdollisuus integroida sisäisen valvonnan toiminnot tehokkaammin liiketoiminnan prosesseihin, jotta liiketoimintayksiköt kokevat kontrollit hyödyllisiksi eivätkä vain taloushallinnon järjestämäksi lisätyöksi. Tavoitteena oli integroida riskiajattelu ja kontrollit liiketoimintayksikköjen päivittäiseksi työksi. Olemassa olleen kontrollijärjestelmän heikkoutena oli pidetty sen aiheuttamaa lisätyötä, sillä useimmat kontrollitoimenpiteet olivat suorittajilleen ylimääräisiä työvaiheita, eivätkä he usein itse hyötyneet suorittamastaan valvontatoimenpiteestä omassa työssään. Valvonnan integroiminen prosesseihin pitäisi Ahokkaan (2012, 65) mukaan olla parannus tähän ongelmaan, joskin itse sisäisen valvonnan kehitysprosessi on laajempi ja näin ollen kalliimpi toteuttaa ja laajempi järjestelmä mahdollisesti kalliimpi ylläpitää.

Toiseksi talousraportoinnin osalta tavoitteena oli kehittää valvontajärjestelmän kerrostuneisuutta, jotta poikkeamat havaittaisiin nopeasti ylemmällä tasolla, ja ongelmiin voitaisiin porautua tutkimalla tarkemmin yksittäisiä kapea-alaisia kontrolleja. Tämän tavoitteen taustalla on ajatus luoda valvontamenetelmiä, joiden avulla voidaan tehdä automaattisia täsmäytyksiä ja automaattisia poikkeamalistoja, joiden myötä kontrollien manuaalisen suorittamisen sijaan resursseja voidaan ohjata löydösten tarkempaan analysointiin. Kerrostuneen valvonnan hyötyjä luetaan myös ulkoisen tarkastuksen hyväksi, kun heille on esitettävissä kattava, mutta rajattu määrä valvontatoimintoja, joilla voidaan päästä kohtuulliseen varmuuteen talousraportoinnin luotettavuudesta.

Kolmas merkittävä muutos käytössä olleeseen kontrollijärjestelmään verrattuna on täysin erilainen lähestymistapa implementointiprosessiin kuin alkuperäisessä SOX-kontrollijärjestelmän implementoinnissa. SOX-kontrollijärjestelmä pyrittiin implementoimaan mahdollisimman kevyesti eli vain olennaisiin tytäryhtiöihin ja yksiköihin, kuten luvusta 4.2 ilmenee. Sen lähtökohta ei ollut ulottautua kaikkiin prosesseihin eikä puuttua muiden kuin olennaisten tilien taustalla oleviin raportointiprosesseihin. Ajatuksenjuoksun etenemisjärjestys oli ylätasolta tilinpäätöksen tileiltä olennaisuusrajaa noudattaen alaspäin yksittäisiin yhtiöihin, yksiköihin ja prosesseihin. Uusi kontrollijärjestelmä lähtee siis päinvastaisesta suunnasta liikkeelle kartoittamalla ensin prosessit, analysoimalla niiden riskit ja siten lopulta päätyy myös tilinpäätöksen lukuihin. Sama lähtökohdan muutos pätee myös itse kontrollitoimenpiteisiin, sillä kehitettävän järjestelmän valvontatoimenpiteet pyritään määrittämään niin, että tavalliset työvaiheet, joilla on kontrolliaspekti, luetaan järjestelmän puitteissa hyväksytyksi kontrolliksi. Näin ollen kehitettävä kontrollijärjestelmä ulottuu kaikkiin riskipitoisiin toimintoihin ja prosesseihin riippumatta siitä, aiheuttavatko riskit olennaisen virheen riskin talousraportoinnissa.

5.2. Organisaation ominaisuuksista riippuvat haasteet riskianalyysin ja valvontatoimintojen suunnittelun yhteydessä

Sisäisen valvonnan kehitysprojekti voidaan itsessään nähdä haasteena toteuttaa teoreettinen malli käytännössä. Mallin toteuttamisen yhteydessä joudutaan ratkaisemaan useita ongelmia, joita COSO:n sisäisen valvonnan viitekehyksessä ei mainita. COSO

(1992) mainitsee, että ongelmien erittely viitekehyksen yhteydessä ei ole mielekästä, sillä jokainen organisaatio on erilainen. Moneen ongelmaan voitaisiin kuitenkin varautua etukäteen ja näin sisäisen valvonnan kehittäjän olisi mahdollista välttää pahimmat sudenkuopat.

Case-yrityksen sisäisen valvonnan kehitysprojektin yhteydessä törmättiin haasteisiin. Osaan näistä oli osattu varautua ja osaan ei, mutta haasteita yhdistivät karkeasti muutama tekijä: tietotaidon huono saatavuus, tarvittavan tietotaidon puute, sisäisen valvonnan tuntemus, kehitysprojektin resursointi ja muut organisaation ominaisuuksista johtuvat haasteet.

Tietotaidon huono saatavuus aiheutti ongelmia projektin lopputuloksen laatuun ja aikatauluun. Prosessien kartoituksessa, riskianalyysissa ja kontrollitavoitteiden määrittelyssä tarvittiin toisinaan asiantuntijoita, joilla oli tarvittava tarkempi tuntemus jostakin prosessin osasta. Muutamien asiantuntijoiden kanssa oli vaikeuksia saada sovittua yhteistä aikaa, jolloin asiat olisi saatu selvitettyä, ja usein ne, joilta aikaa oli hankalinta saada, heillä oli usein myös vähiten tietämystä sisäisestä valvonnasta. Vastaavasti joiltakin asiantuntijoilta aikaa liikeni kiireisyydestä huolimatta, koska he pitivät sisäisen valvonnan kehittämistä tärkeänä. Toisin sanoen ongelma ei ole se, että organisaatiossa ei olisi tarvittavaa tietotaitoa, vaan se, että tietotaito ei ole kontrollijärjestelmän kehittäjän käytettävissä. COSO (1992) painottaa sisäisen valvonnan kehityksessä johdon tuen tärkeyttä, jotta organisaation jäsenet saadaan motivoitua mukaan kehitykseen ja ymmärtämään sisäisen valvonnan merkitys. Johdon tuki tarkoittaa johdon alaisilleen välittämää viestiä, josta selviää mitä on tarkoitus tehdä, ja että kyseessä on koko organisaatiota koskeva projekti.

Edellä kuvailtu ongelma oli vahvasti läsnä prosessikartoituksessa, jossa prosessien eri vaiheita jouduttiin kehittämään pala kerrallaan niiden asiantuntijoiden kanssa, jotka tunsivat yleensä käsiteltävän prosessin osan. Kaikissa prosesseissa on kuitenkin liittymäpintoja muihin prosesseihin, joten prosessien raja-alueet edellyttivät dialogia muiden prosessien asiantuntijoiden kanssa. Koska kaikki tarvittavat henkilöt eivät olleet yhtä aikaa paikalla, jäi usein jokin prosessin osa, jota ei tunnettu kunnolla. Projektipäällikön mielestä asioiden sopiminen olisi ollut huomattavasti helpompaa, jos kaikki henkilöt olisivat olleet paikalla yhtä aikaa samassa paikassa työrutiinien

ulkopuolella. Koska suuren yhtiön prosessit ovat vaihetasolla varsin mutkikkaita ja kokonaisuuden hahmottaminen on vaikeaa, asetti tämä ”pala kerrallaan” -lähestymistapa haasteita projektille, jotta kokonaisuudesta tulisi ehyt. Tähän ongelmaan case-organisaatiossa vastattiin siten, että sama henkilö oli mukana koko prosessin kartoituksessa, jotta yleiskuva todennäköisemmin säilyisi.

Toinen ongelma oli tietotaidon saatavuuden sijaan se, että organisaatiosta ei löytynyt henkilöä, jolla olisi riittävän tarkka ja laaja tietämys yksittäisen prosessin vaiheista. Muutamassa tapauksessa projektin alusta asti mukana ollut asiantunteva henkilö oli lähtenyt organisaatiosta kesken projektin, eikä korvaajaksi ollut saatavilla vastaavan tietotaidon omaavaa henkilöä. Mikäli prosessikartoitus ei ole riittävän tarkka ja kattava, on riski, että jonkin vaiheen riski jää tunnistamatta ja näin ollen kyseisen vaiheen sisäiseen valvontaan saattaa jäädä aukkoja. Projektin arviointivaiheessa case-yrityksen sisäinen tarkastus kommentoi mm. tietojärjestelmien master datan eli perustietojen hallintaprosessista, että sen toiminnasta tarvitaan vielä vahvempi asiantuntijalausunto. Ongelma johtuu osin myös organisaation rakenteesta. (Rainamaa 30.9.2013) Tietojärjestelmien perustiedot ovat äärimmäisen kriittistä dataa, joten niiden tarkka valvonta on tärkeää. Tietojärjestelmien valvontaan on kehitetty jopa oma sisäisen valvonnan viitekehys (ks. Chang, Yen, Chang & Jan 2014) auttamaan tietojärjestelmien sisäisen valvonnan kehittämisessä.

Useammassa haastattelussa (Kaski 8.4.2013; Rainamaa 30.9.2013; Piikkilä 12.3.2013) kävi ilmi, että sisäisen valvonnan käsitteitä ei tunnettu organisaatiossa kunnolla, vaikka henkilöt olivat mukana kartoittamassa riskejä ja laatimassa kontrollitavoitteita sekä kontrolleja. Erityisesti kontrollitavoite ja kontrollitoimenpide sekoitettiin toisiinsa, jolloin kontrollitavoite oli jo itsessään kontrollitoimenpide. Ongelma oli havaittu jo ennen kehitysprojektia käytössä olleessa kontrollijärjestelmässä, ja ongelmaan oli osattu varautua (Kaski 8.4.2013), mutta tästäkin huolimatta kontrollitavoitteen määrittely tuotti ongelmia. Case-yrityksessä ongelma ilmeni, kun projektitiimi selvitti kysymällä ”mitä tehdään kontrollitavoitteen saavuttamiseksi”, jolloin vastauksena oli sama sisältö, joka oli dokumentoitu kontrollitavoitteeksi. COSO:n (1992) mukaan kontrollitavoite tulisi johtaa organisaation strategiasta, jotta sisäinen valvonta tukisi strategiaa. Mikäli kontrollitavoitetta ei määritellä, on riski, että tämä linkki kontrollitoimenpiteen ja

strategian välillä katkeaa. Case-yrityksessä opittiin, että puutteellisesti määritellyt kontrollitavoitteet voidaan havaita tarkistamalla, että kontrollitavoitteet ja kontrollitoimenpiteet eivät ole yhtenevät. Ongelmia oli myös riskin käsitteen määrittämisessä perimmäiseen seuraukseen saakka eli ei ajateltu loppuun asti ”mitä voi mennä pieleen?”. Haastattelussa (Kaski 8.4.2013) esiin tulleen esimerkin mukaan riskiksi oli määritelty, että organisaatiossa tehdään hankintoja, jotka ovat yhtiön ohjesäännön vastaisia. Kontrollitavoitteeksi oli määritelty, että kaikkien ostojen tulee olla ohjesäännön mukaisia. Tässä tapauksessa ongelma on riskin määrittelyssä, sillä vaikka ostoja tehdään sääntöjen vastaisesti, ei se tarkoita sitä, että olisi aiheutettu vahinkoa omistajille. Riskin ja kontrollitavoitteen ollessa toistensa peilikuvia, on todennäköistä, että vähintään toinen on pielessä (Kaski 8.4.2013). COSO:n (1992, 56) viitekehyksessä mainitaan, että riskien ja valvontatoimintojen muodostamaa paria tulee arvioida erikseen jokaisessa liiketoiminnossa. Case-yrityksessä riskin ja kontrollitoiminnon paria arvioitiin erikseen vielä hienojakoisemmin. Valvontatoimintojen arvioinnissa tärkeää on muodostaa käsitys siitä, vastaavatko valvontatoiminnot riskejä (COSO 1992, 57). Case-yrityksen kokemusten perusteella tämän COSO:n huomautuksen toteuttaminen on todettu hyödylliseksi.

Case-yrityksen organisaation muutamat erityispiirteet asettivat haasteita. UPM:n käytössä on kymmeniä tietojärjestelmiä, joista osa on päällekkäisiä järjestelmiä, mutta niitä käytetään eri liiketoiminta-alueilla. Järjestelmät eivät ole integroituja, eivätkä ne logiikaltaan toimi samalla tavalla. Tietojärjestelmäriippuvaisten riskien analysoinnissa ja kontrollitoimenpiteiden suunnittelussa jouduttiin siis käsittelemään moni järjestelmä erikseen. Tämä lisäsi työmäärää paitsi suunnittelussa myös myöhemmin seurannassa ja kaikkien muutosten tekeminen on hitaampaa fragmentoituneessa järjestelmäympäristössä (Rainamaa 30.9.2013). Toinen organisaation erityspiirteiden aiheuttama haaste oli määritellä riskit, kontrollitavoitteet ja kontrollit siten, että maantieteellisesti laajassa organisaatiossa kaikissa maailmankolkissa sanoma ymmärretään. Yhtiön kieli on englanti, joten samoja määritelmiä käytetään maanosasta riippumatta. Ongelma ei siis ole varsinaisesti kielitaito, vaan se, että sama viesti ymmärretään eri tavalla eri puolilla maailmaa. Syinä tähän voivat olla kulttuuri ja viestintäkulttuuri työpaikalla, mutta asiaa ei ole tarkemmin selvitetty.

5.3. Valitun menetelmän ja käytännön aiheuttamia haasteita

5.3.1. Riskianalyysi ja kontrollitoimenpiteet käytännössä

Luvussa neljä esitelty menetelmä riskianalyysin suorittamiselle ja kontrollitavoitteiden sekä kontrollien määrittelylle on case-organisaation kehittämä ratkaisu ongelmaan, miten toteuttaa yllä mainitut COSO IF:n mukaiset toimenpiteet. Ratkaisun aikaansaamiseksi on jouduttu tekemään linjauksia ja päätöksiä, jotta käytännön aiheuttamat ongelmat saadaan ratkaistua. Kohdatut haasteet on jaettavissa sen perusteella, missä projektin vaiheessa haaste tulee ilmi, eli riskianalyysin suorittamisessa vai kontrollitavoitteiden ja kontrollitoimintojen dokumentoinnin suunnittelussa.

5.3.2. Kontrollijärjestelmän arkkitehtuuri

Arkkitehtuurilla tarkoitetaan tässä sitä, millainen rakenne kontrollijärjestelmälle päätetään luoda, miten vastuu jaetaan globaalisti ja paikallisesti sekä missä muodossa dokumentaatio on. Arkkitehtuurin ongelmaan törmätään jo riskianalyysivaiheessa, kun liiketoiminnoilla on toisistaan poikkeavia riskejä tai on olemassa maantieteellisiä eritysriskejä. Jos kaikki erilaiset riskit otettaisiin huomioon ja tehtäisiin kullekin liiketoiminta-alueen organisaatiolle niille olennaisten riskien kontrollijärjestelmä, tehtäisiin kontrollijärjestelmiä juuri yhtä monta kuin on kyseisiä organisaatioitakin. Jotta suuri yhtiö välttyisi tuottamasta useita kontrollijärjestelmiä, joiden kaikkien seuranta olisi monimutkaista, on keksittävä keino yhdistää erilaiset ympäristöt yhteisen nimittäjän alle. Case-organisaatiossa ongelma ratkaistiin suorittamalla riskianalyysit riittävän yleisellä tasolla, jotta se kattaa mahdollisuuksien mukaan kaiken edellä mainitun variaation. Ratkaisun kääntöpuolena on riskimääritelmien jääminen yleisiksi, jolloin paikallisten riskien tunnistaminen yleisen määritelmän perusteella vaatii osaamista.

Projektin aikana esille nousivat joidenkin maiden, varsinkin Kiinan, muutamat erityiset riskit, joiden huomioon ottamista omana erityisriskilistana paikalliset asiantuntijat pitivät perusteltuna. Projektijohto ei kuitenkaan nähnyt ongelmaksi sijoittaa näitä erityisriskejä jo määriteltyihin globaaleihin riskeihin, jos niiden dokumentoidun kuvauksen muotoilee sopivalla tavalla. Näin ollen mitään erityslistaa ei tarvita, mutta maantieteellisten riskien mukaan ottaminen on tehty silti mahdolliseksi. Esimerkiksi palkkahallinnossa on paljon

maakohtaista erityssäännöstöä, joka on otettu huomioon riskikuvauksessa. Riskikuvauksessa todetaan, että palkkahallinto on järjestetty ”paikallisten vaatimusten mukaan”. Paikallisen johdon vastuulla on määritellä, mitä ”paikalliset vaatimukset” ovat ja dokumentoida ne riskimatriisiin (vrt. liite 3).

Valitun arkkitehtuurin myötä seuranta on helpompaa kuin usean erilaisen kontrollijärjestelmän, ja tämän lisäksi myös kontrollijärjestelmän pitäminen käytännön tasolla ajantasaisena on mahdollista toteuttaa muuttamalla vain paikallisen vastuun piiriin kuuluvaa dokumentaatiota. Kontrollijärjestelmän luotettavuuden kannalta on tärkeää, että dokumentaatioon ei tehdä harkitsemattomia muutoksia, mutta liian jäykkä muutosprosessi voi toimia myös tarkoitustaan vastaan. Case-yrityksen tekemä valinta tähtää siihen, että muutokset voidaan tehdä siellä, missä ne parhaiten tunnetaan.

Luvussa 3.2 mainitaan ongelma optimaalisen kontrolloinnin määrästä. Jos käyttöön otetaan liian paljon kontrolleja, on riski, että hyödyt jäävät kontrolloinnin aiheuttamia kustannuksia pienemmiksi. Case-yrityksessä törmättiin tilanteisiin, jossa tehtiin rajanvetoa työvaiheen ja kontrollitoimenpiteen välillä. Tärkeimpänä kriteerinä kontrollitoimenpiteelle pidettiin sitä, että toimenpiteellä oli ns. kontrolliaspekti eli kontrollitavoitteen suuntainen varmistava vaikutus. Erityisen suurta tarkkuutta edellytettiin kontrollitoimenpiteiltä, joilla kontrolloitiin rahan kanssa tapahtuvaa toimintaa. Toisaalta vähämerkityksisiä asioita jätettiin kontrollijärjestelmän ulkopuolelle, kuten ”asiakirjojen pitää olla allekirjoitettuja ja arkistoituja”, mikäli laki ei sitä vaatinut. Eräs konkreettinen esimerkki rajanvedosta kontrollin panoksen ja tuotoksen suhteessa oli ongelmallinen varaston hävikin valvonta. Varastossa oli pienikokoista tavaraa, jota usein hävisi. Kontrollia suunniteltaessa todettiin, että tehokas valvonta vaatisi investointeja, kuten valvontakameroita ja työntekijöiden toistuvia satunnaistarkastuksia. Näiden investointien arvioitiin maksavan enemmän kuin jatkuva, vähäinen hävikki. COSO:n (1992) mukaan kaikkea ei tarvitse, eikä voikaan, valvoa valvontatoimenpiteillä, vaan valvontaympäristöä ja toimintakulttuuria pitää pyrkiä kehittämään siihen suuntaan, että haitallisen toiminnan riski pienenee.

5.3.3. Kontrollijärjestelmän laatimisprosessi

Keinoksi riskianalyysin toteuttamiseen löytyy vinkkejä kirjallisuudesta, kuten Leitch (2008) ja Hightower (2008). Case-yrityksen kehittämä menetelmä yhdistelee jossain määrin luvuissa 3.6.2–3.6.4 esiteltyjä menetelmiä. Projektin riskianalyysi suoritettiin kartoittamalla prosessin yksittäiset vaiheet ja niihin liittyvät riskit, jotka dokumentoitiin matriisimuotoiseen taulukkoon. Yleiselle tasolle maailmanlaajuiseen käyttöön laadittu kontrollijärjestelmä puolestaan muistuttaa ideansa puolesta generic control design library -menetelmää, koska projektin myötä on määritelty yleiset riskit yleisimmille toiminnoille, joita paikallinen osaaminen hyödyntää kontrollitoimenpiteiden määrittelyssä ja työohjeiden dokumentoinnissa.

Riskianalyysia laadittaessa todettiin, että prosessikuvausten on oltava laadukkaita, koska muuten prosessin vaiheiden riskit on hankala sijoittaa oikeaan prosessiin ja siten pitää vastuu aukottomasti kyseisen prosessin osasta vastaavan tahon kannettavana. Projektijohto oli huolissaan, että prosessin vaiheiden alku- ja loppupisteiden määritysten sanamuotojen vuoksi on vaarana, että jotkin työvaiheet jäävät ikään kuin kahden prosessin vaiheen väliin. Tämä tarjoaisi prosessin vaiheesta vastaaville henkilöille mahdollisuuden välttää vastuuta ongelmatilanteissa. Process step analysis -menetelmää muistuttavan vaiheen toteutuksessa koettiin hankalaksi säilyttää kokonaiskuva prosessista, kun prosessia analysoitiin pala kerrallaan. Potentiaalinen ongelma ovat myös prosessin vaiheiden kokonaisuuden mahdollisesti muodostamat riskit, joita kyseinen menetelmä ei sinällään analysoi.

5.3.4. Kontrollijärjestelmän dokumentointi

Kehitetyn kontrollijärjestelmän dokumentointi on toteutettu matriisimuotoisina Excel-taulukoina, joissa Matrix mapping of risks and controls -mallista poiketen on riskit ja niitä vastaavat kontrollitavoitteet (ks. liite 2). Kussakin Excel-työkirjassa on toinen taulukko, jossa on pureuduttu vain yhteen riskiin kerrallaan ja dokumentoitu kontrollitoimenpiteet aina työohjeisiin asti (ks. liite 3). Tällä menetelmällä valvontatoimenpiteen koko ketju aina riskistä konkreettiseen työohjeeseen on nähtävissä kerralla. Case-yrityksen aikaisemman kokemuksen perusteella kontrolleja suorittava työntekijä ei aina ole tiennyt, miksi kontrolli suoritetaan, eli ei tiedetty, mitä riskiä pyritään hallitsemaan. Leitchin

(2008) esittelemässä mallissa käytettyä numeerista analyysia kontrolleista ei case-yrityksen kontrollijärjestelmän suunnitteluvaiheessa ole käytetty.

Dokumentointimenetelmä, jossa kontrollitoimenpiteet ja niiden työohjeet laaditaan paikallisesti, mahdollistaa kontrollijärjestelmän dokumentaation muutosten joustavuuden. Tämän ratkaisun potentiaalinen ongelma on kuitenkin se, että dokumentoinnin laatijalta vaaditaan paljon osaamista paitsi omasta prosessin osastaan, myös tietoa sisäisen valvonnan toiminnasta, jotta dokumentaatio olisi laadukas ja myös esimerkiksi tarkastuksen näkökulmasta käyttökelpoinen. Ongelmaan on pyritty löytämään ratkaisu määrittelemällä, mitä yksityiskohtaisen kontrollitoimenpidekuvauksen tulee sisältää. Nämä kriteerit auttavat dokumentaation laatijaa luomaan laadukkaan kontrollitoimenpidekuvauksen. Tasaisen laadukkaan dokumentaation olemassaolo kautta koko organisaation on yksi edellytys sille, että kontrollijärjestelmä on luotettava. Kuten luvussa 5.2 todetaan, sisäisen valvonnan tuntemus ei ole itsestäänselvyys.

6. YHTEENVETO JA JOHTOPÄÄTÖKSET

Tutkimuksen tavoitteena oli syventyä sisäisen valvonnan kehitykseen, sen tärkeimpiin osa-alueisiin ja yleisimpiin heikkouksiin kirjallisuuden perusteella sekä analysoida havaittuja seikkoja käytännössä tutkimukseen valitussa case-yrityksessä. Tavoitteen saavuttamiseksi tutustuttiin ensin sisäisen valvonnan määritelmään ja ominaisuuksiin sekä sisäisen valvonnan laajempaan teoreettiseen kontekstiin. Tämän jälkeen etsittiin kirjallisuudesta viitteitä, millä keinoilla sisäisen valvonnan kehittäminen voitaisiin toteuttaa COSO IF:n puitteissa mahdollisimman hyvin ja mitä virheitä sisäisen valvonnan kehityksessä tulee välttää. Seuraavaksi perehdyttiin tyypilliseen sisäisen valvonnan kehitysprojektiin sekä muutamaan riskianalyysissa ja kontrollitoimenpiteiden määrittelyssä käytettävään menetelmään. Tutkimuksen empiirisessä osassa seurattiin teoriaosassa käsiteltyjen seikkojen toteutusta käytännössä COSO IF:n riskianalyysin ja valvontatoimenpiteiden suunnittelun osalta.

Tutkimuskysymykset ennen tutkimuksen laatimista olivat seuraavat:

1. Mitkä ovat ne tekijät, joiden vuoksi uuden kontrollijärjestelmän kehittäminen katsotaan tarpeelliseksi?
2. Mitä vaiheita kontrollijärjestelmän kehittäminen sisältää ja miten projekti toteutetaan käytännössä?
3. Mitä ongelmia kehityksessä ilmenee ja miten ne ratkaistaan?

Tutkimuksen tulosten perusteella tutkimusongelman ensimmäiseen kysymykseen on saatu vastauksia sekä teorian että käytännön tasolla. Motiivit ja tavoitteet sisäisen valvonnan kehittämiseksi ovat sekä kirjallisuudessa että case-yrityksen motiivien perusteella samansuuntaiset, joskin case-aineiston perusteella ilmenee yksityiskohtaisempia perusteluja sisäisen valvonnan kehittämiselle. Esimerkkinä yksityiskohtaisemmasta perustelusta mainittakoon valvonnan integroiminen osaksi prosesseja, jonka taustalla on ajatus motivoida valvontatoimintoja suorittavat henkilöt kokemaan sisäisen valvonnan paremmin omakseen.

Toiseen tutkimuskysymykseen vastaus löytyy yksityiskohtaisesti vertailemalla lukujen 3 ja 4 sisältöä. Tutkimuksen empiirisen osuuden ja kirjallisuuden antaman kuvan väliltä ei löytynyt ristiriitoja, joskin kirjallisuus käsittelee pääasiassa sisäisen valvonnan kehittämistä yrityksessä ensimmäistä kertaa. Vaikka prosessien määritys ei ole osa sisäistä valvontaa tai COSO IF:ia, se on kuitenkin edellytys sisäisen valvonnan kehittämiselle, mikäli sisäinen valvonta on osa prosesseja. Case-yrityksen kokemusten perusteella prosessimäärityksen merkitys korostuu vahvemmin kuin kirjallisuuden perusteella voisi ymmärtää ja prosessien määritys vaati myös huomattavasti resursseja.

Kolmanteen tutkimuskysymykseen on koottu yksityiskohtaisempi vastaus luvuissa 5.2 ja 5.3. Tulosten perusteella voidaan sanoa, että kysymykseen on saatu vastauksia erityisesti empiirisen aineiston perusteella. Tutkimuksessa käsitellyn kirjallisuuden perusteella kaikkiin havaittuihin haasteisiin ei ollut valmista ratkaisua tarjolla. Erityisesti henkilöstön tietotaitoon liittyvien haasteiden ratkaisemista oli analysoitu myös akateemisessa kirjallisuudessa ja ratkaisuna tähän oli ehdotettu henkilöstön kouluttamista. Resurssien lisääminen toisaalta kasvattaa myös kustannuksia, jolloin sisäisen valvonnan hyöty voi olla vaarassa jäädä kustannuksia pienemmäksi. Optimaalisen valvonnan tason löytäminen on siksi keskeistä. Case-yrityksessä kontrollien aiheuttamat kustannukset pyrittiin pitämään kohtuullisina uusia työkaluja ja automaatiota hyödyntämällä. Rajanveto olennaisen ja epäolennaisen kontrollitoimenpiteen välillä on kuitenkin harkittava aina tapauskohtaisesti, mikä edellyttää sisäisen valvonnan tuntemusta organisaatiossa.

Vaikka tutkimuksen tuloksista voidaan saada osviittaa haasteista myös muissa sisäistä valvontaa kehittävissä yrityksissä, ei tutkimuksen tuloksia voida kuitenkaan yleistää muihin tapauksiin. Kuten yleensä laadullisissa tapaustutkimuksissa, tämänkin tutkimuksen pääpaino ei ole yleistettävyydessä, vaan tutkitun ilmiön analysoimisessa ja siihen vaikuttavien seikkojen ymmärtämisessä. On mahdollista, että toinen saman kokoinen vastaavilla toimialoilla toimiva yhtiö kokee samanlaisia haasteita sisäisen valvonnan kehityksessä, mutta tämän tutkimuksen perusteella ei voida sanoa tämän olevan sen enempää todennäköistä kuin epätodennäköistäkään.

Yleistettävyyden lisäksi tutkimuksen tuloksiin sisältyy rajoitteita myös tulosten täydellisyyden osalta, sillä empiiristä dataa ei ollut mahdollista kerätä koko projektin loppuun saakka saati sen jälkeen, jolloin kontrollijärjestelmää parannetaan seurannassa

ilmenneiden seikkojen avulla. On mahdollista, että kehitysprojektin jalkautusvaiheessa kohdataan myös haasteita, joita ei tässä ole huomioitu. Tutkimus on kuitenkin keskittynyt sisäisen valvonnan kehityksen suunnittelun, joten käytännön työohjeiden dokumentointi ja muut jalkautukseen liittyvät vaiheet eivät ole teoreettisesti yhtä mielenkiintoisia.

Tutkimuksessa on tuotu esille muutamia käytännössä havaittuja haasteita, joita tutkimuksen empiirisessä osiossa käsitelty yritys on kohdannut. Osa näistä haasteista oli mainittu kirjallisuudessa, joten on perusteltua sanoa, että nämä haasteet olivat ainakin jossain määrin tyypillisiä. Tutkimuksen tuloksista voidaan saada osviittaa myös siihen, mitä muut yritykset voivat joutua kohtaamaan kehittäessään sisäistä valvontaa. Tutkimusta voisi edelleen kehittää keräämällä vastaavanlaista aineistoa useammista käytännön tapauksista ja koostamalla näissä ilmenneitä ongelmia ja niiden ratkaisuja toimintamalleiksi sisäisen valvonnan kehityksen tueksi. Tutkimuksen tulokset eivät myöskään kerro mitään havaittujen haasteiden merkittävyydestä. Kun mahdolliset haasteet on kartoitettu, olisi kvantitatiivisin menetelmin mahdollista selvittä, mitkä näistä haasteista on yrityksissä koettu merkittävimpinä sisäisen valvonnan tehokkuutta vähentävinä tekijöinä.

Sisäisen valvonnan merkitys tuskin vähenee tulevaisuudessa. Kun informaatioteknologia kehittyy entisestään, on entistä suurempien yritysten keskitetty hallinta entistäkin yleisempää. Suuremmat organisaatiot hyötyvät tutkitusti enemmän systemaattisesta sisäisestä valvonnasta kuin pienemmät organisaatiot. Tämän lisäksi nykyinen trendi, jossa tukifunktioita kuten taloushallintoa, tietohallintoa ja logistiikka tuotetaan entistä enemmän ulkoistettuina ja alihankittuina palveluina, yrityksen toiminnan tarkoituksenmukaisuuden varmistaminen ja raportointiprosessin laadun varmistaminen tulevat entistäkin tärkeämmiksi.

LÄHTEET

Kirjallisuus:

Agbejule, A. &, Jokipii, A. 2009. Strategy, control activities, monitoring and effectiveness. *Managerial Auditing Journal*, 24, 500–522.

Ahokas, N. 2012. *Yrityksen sisäinen valvonta.* Jyväskylä: Edita Publishing Oy

Aldridge C., & Colbert, J. 1994. Management's Report on Internal Control, and the Accountant's Response. *Managerial Auditing Journal*, 9, 21–28.

Arvopaperimarkkinayhdistys ry 2010. Suomen listayhtioiden hallinnointikoodi (Corporate Governance) 2010. <www.cgfinland.fi> 06.02.2012

Beneish, M.D., Billings, M. & Hodder L. 2008. Internal Control Weaknesses and Information Uncertainty. *The Accounting Review*, 83 (May), 665–703.

Berlau, J. 2005. A Tremendously Costly Law. *National Review*, 11 (April).

Campbell, D., Campbell, M. & Adams, G. 2006. Adding Significant Value with Internal Controls. *The CPA Journal*, (June), 20–25.

Chang, S., Yen D., Chang, I-C. & Jan, D. 2014. Internal control framework for a compliant ERP system. *Information & Management*, 51, 187–205.

Cenker, W. & Nagy, A. 2004. Section 404 implementation Chief audit executives navigate uncharted waters. *Managerial Auditing Journal*, 19, 1140–1147.

Choi, J-H., Choi, S., Hogan, C. E., & Lee, J. 2013. The Effect of Human Resource Investment in Internal Control on the Disclosure of Internal Control Weaknesses. *Auditing: A Journal of Practice & Theory*, 32 (November), 169–199.

Conyon, Judge & Useem, 2011. Corporate Governance and the 2008–09 Financial Crisis. *Corporate Governance: An International Review*, 19, 399–404.

Committee of Sponsoring Organizations of the Treadway Commission 1992. *Internal Control - Integrated Framework.*

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

Doyle, J., Ge, W. & McVay, S. 2007. Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting and Economics*, 44, 193–223.

Eisenhardt, K. 1989. Agency Theory: An Assessment and Review. *The Academy of Management Review*, 14, 57–74.

Fama E., 1970. Efficient Capital Markets: A Review of Theory and Empirical Work. *The Journal of Finance,* 25, 383–417.

Fama, E. 1980. Agency Problems and the Theory of the Firm. *The Journal of Political Economy*, 88 (April), 288–307.

Ge, W., & McVay, S. 2005. The Disclosure of Material Weaknesses in Internal Control after the Sarbanes-Oxley Act. *Accounting Horizons*, 19, 137–158.

Hammersley, J., Myers, L., & Shakespeare, C. 2008. Market reactions to the disclosure of internal control weaknesses and to the characteristics of those weaknesses under Section 302 of the Sarbanes Oxley Act of 2002. *Review of Accounting Studies,* 13, 141–165.

Hemraj, M. 2004. Preventing corporate scandals. *Journal of Financial Crime*, 11, 268–276.

Hermanson, D., Smith, J., & Stephens, N. 2012. How Effective are Organizations' Internal Controls? Insights into Specific Internal Control Elements. *American Accounting Association,* 6, A31–A50.

Hightower, R. 2008. *Internal Controls Policies and Procedures*. Hoboken, NJ: Wiley.

Jain, P., Kim, J-C. & Rezaee, Z. 2008. The Sarbanes Oxley act of 2002 and Market Liquidity. *The Financial Review,* 43, 361–382.

Jensen, M. & Meckling, W. 1979. Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. *Journal of Financial Economics (JFE)*, 3, 305–360.

Kaplan, S. & Garrick, J. 1981. On The Quantitative Definition of Risk. *Risk Analysis*, I, 1–28.

Kim, Y. & Park, M. 2009. Market uncertainty and disclosure of internal control deficiencies under the Sarbanes–Oxley Act. *J. Account. Public Policy,* 28, 419–445.

KPMG 1999. The KPMG Review. Internal control: A Practical guide. <http://www.ecgi.org/codes/documents/kpmg_internal_control_practical_guide.pdf>

KPMG 2012. Continuous auditing and continuous monitoring: The current status and the road ahead. <http://www.kpmg.com/PT/pt/IssuesAndInsights/Documents/cacm2012.pdf>, 10.12.2013.

Lee, M. & Colbert, J. 1997. Analytical procedures: management tools for monitoring controls. *Management Decision*, 35, 682 – 688.

Leitch, M. 2008. *Intelligent Internal Control and Risk Management.* Hampshire, England: Gower Publishing Limited.

Lumijärvi, O-P. 1987. *Agenttiteoria ja sen eräitä sovellutuksia*. Turun kauppakorkeakoulun julkaisuja – keskustelua ja raportteja.

Neilimo, K. & Näsi, J. 1980. *Nomoteettinen tutkimusote ja suomalaisen yrityksen taloustiede.* Tampereen yliopisto, yrityksen taloustieteen ja yksityisoikeuden laitoksen julkaisuja, sarja A2.

Niiranen, E. 2005. *Identification of key controls when implementing section 404 fo the Sarbanes-Oxley act of 2002 – Case UPM-Kymmene Oyj*. Tampereen yliopisto. Taloustieteen laitos. Pro gradu -tutkielma.

OECD 2004. OECD Principles of Corporate Governance. <www.oecd.org>, 20.02.2012.

PWC 2003. Key Elements of Antifraud Programs and Controls. <www.verityintel.com>, 01.02.2012.

Ramos, M. 2004. Evaluate the control environment. *Journal of Accountancy*, 197 (May), 75–78.

Tackett, James A., Wolf, F., & Claypool, Gregory A. 2006. Internal control under Sarbanes-Oxley: a critical examination. *Managerial Auditing Journal*, Vol. 21 Iss: 3 pp. 317 - 323

Wright, P., Mukherji, A. & Kroll, M. 2001. A reexamination of agency theory assumptions: extensions and extrapolations. *Journal of Socio-Economics*, 30, 413–429.

Muut lähteet:

Committee of Sponsoring Organizations of the Treadway Commission. Frequently asked questions. <http://www.coso.org/erm-faqs.htm>, 6.1.2014.

Cotton, D. 2002. Fixing CPA Ethics can be an Inside Job. Washington Post Company. <www.cottoncpa.com> 21.02.2012.

Sarbanes-Oxley Act of 2002. <http://www.sec.gov/about/laws.shtml> 13.3.2014

Sisäiset tarkastajat ry, www.theiia.fi/ (viitattu 16.3.2014)

UPM Oyj 2012. Vuosikertomus 2011.

UPM Oyj 2013. Vuosikertomus 2012.

Henkilölähteet:

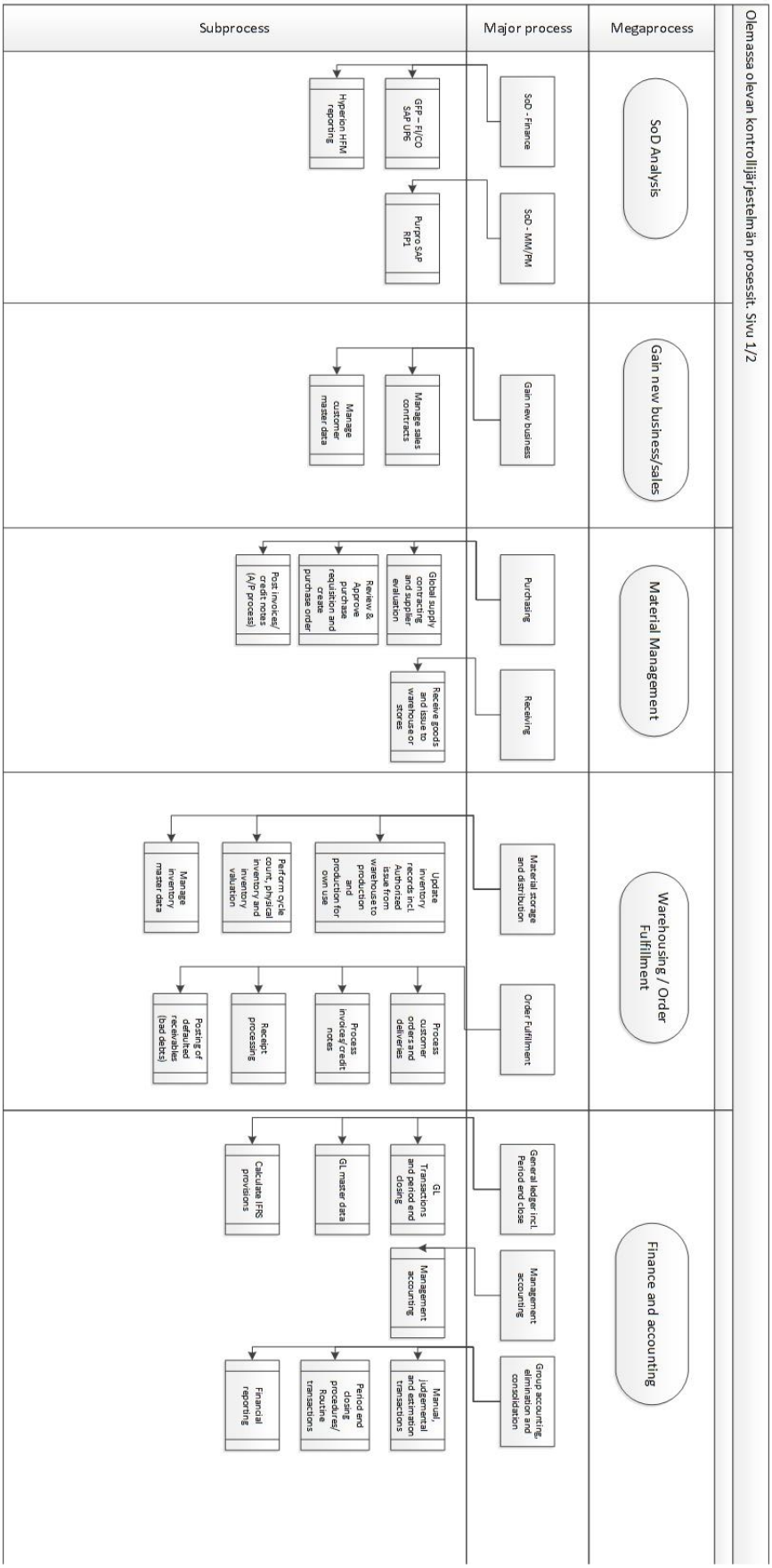
Hankkio, Mika. Process owner, GFPR, UPM-Kymmene Oyj.
Haastattelu 19.3.2013, kesto 1 h 23 min.

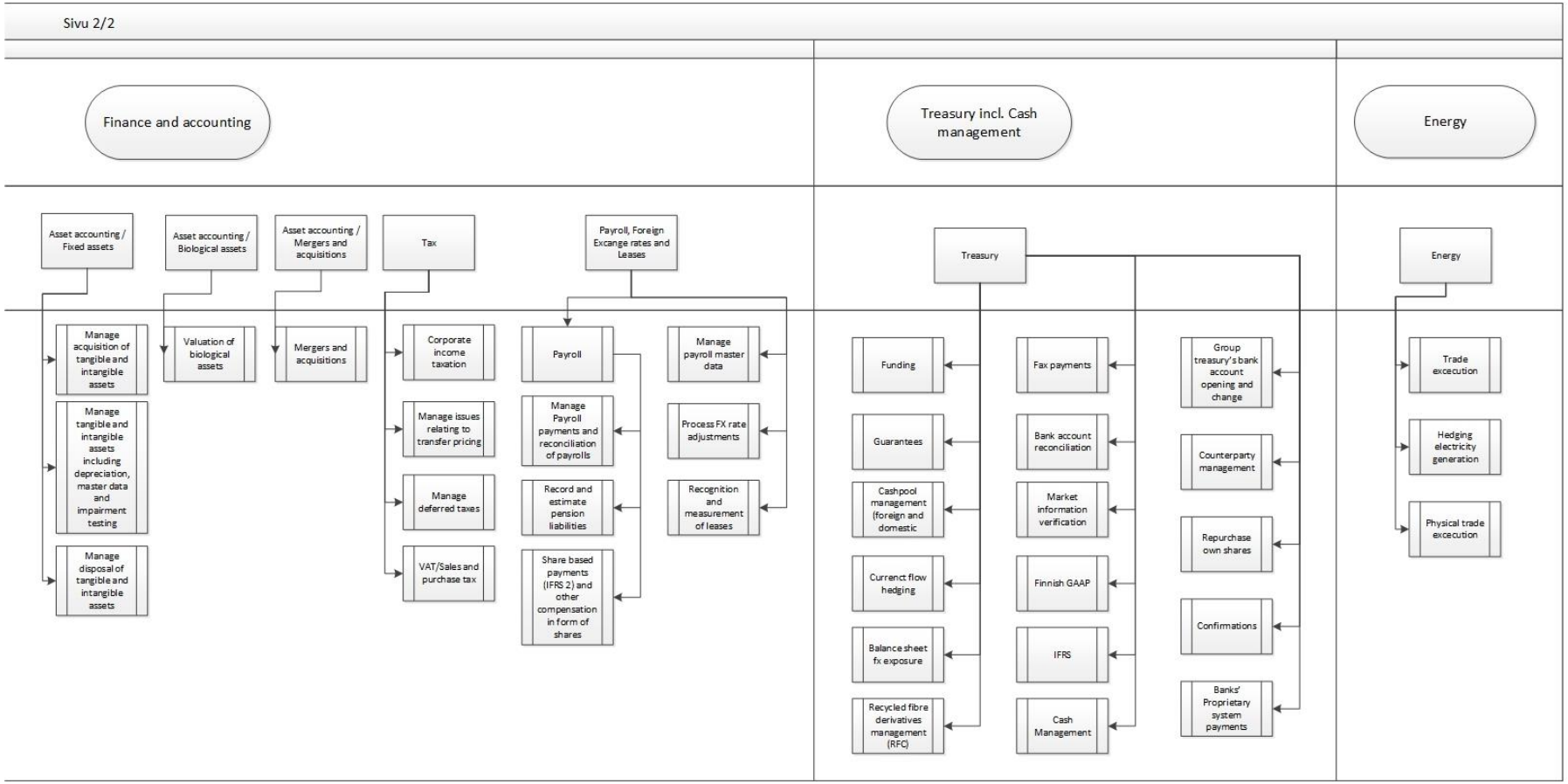
Kaski, Kristiina. Expert, Financial Accounting Compliance and Development, UPM-Kymmene Oyj.
Haastattelu 8.4.2013, kesto 1 h 7 min.

Piikkilä, Jaana. Expert Human Resources Development, UPM-Kymmene Oyj.
Haastattelu 12.3.2014, kesto 1 h 5 min.

Rainamaa, Maarit. Manager, Internal Controls, UPM-Kymmene Oyj. Business process and risk based controls -projektin päällikkö.
Haastattelu 29.1.2013, kesto 1 h 55 min.
Haastattelu 20.3.2013, kesto 55 min.
Haastattelu 30.9.2013, kesto 1 h 9 min.
Sähköpostiviesti, 16.7.2014.

LIITE 1. NYKEHETKEN PROSESSIT




Finance and accounting
Treasury incl. Cash management
Energy
Asset accounting / Fixed assets
Asset accounting / Biological assets
Asset accounting / Mergers and acquisitions
Tax
Payroll, Foreign Excange rates and Leases
Manage acquisition of tangible and intangible assets
Manage tangible and intangible assets including depreciation, master data and impairment testing
Manage disposal of tangible and intangible assets
Valuation of biological assets
Mergers and acquisitions
Corporate income taxation
Manage issues relating to transfer pricing
Manage deferred taxes
VAT/Sales and purchase tax
Payroll
Manage Payroll payments and reconciliation of payrolls
Record and estimate pension liabilities
Share based payments (IFRS 2) and other compensation in form of shares
Manage payroll master data
Process FX rate adjustments
Recognition and measurement of leases
Treasury
Funding
Guarantees
Cashpool management (foreign and domestic
Currenct flow hedging
Balance sheet fx exposure
Recycled fibre derivatives management (RFC)
Fax payments
Bank account reconciliation
Market information verification
Finnish GAAP
IFRS
Cash Management
Group treasury's bank account opening and change
Counterparty management
Repurchase own shares
Confirmations
Banks' Proprietary system payments
Energy
Trade excecution
Hedging electricity generation
Physical trade excecution

LIITE 2. RISKIT JA KONTROLLITAVOITTEET SEKÄ RISKIEN ANALYSOINTI

Record to Report								
General Ledger Accounting and Controlling (incl. GL and CO Master Data Maintenance, Period-End-Closing)								
Risks	Type	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
		Incomplete / inaccurate Interfaces	Insufficient Quality of Data received via Interfaces	Incorrect GL and CO Master Data and Parameters in SAP	Incomplete / inaccurate / non-existent / unpunctual accrual calculations or other manual journals	Incomplete / insufficient / unpunctual period end closing activities	Incorrect interpretation of complex IFRS accounting policies	Uncontrolled differences between group and statutory accounts
Business Risk								
Financial Statement Risk								
Fraudulent Reporting (financial, non-financial, misappropriation of assets, illegal acts)		x	x	x	x	x	x	x
Safeguarding of Assets (theft, money laundering)					x			
Corruption (bribery)								x
Major Accounts		All except equity, provisions, some loans and finance charges/income, some accruals, defined benefit plans, income taxes	All except equity, provisions, some loans and finance charges/income, some accruals, defined benefit plans, income taxes	All	Equity, provisions, some loans and finance charges/income, some accruals, defined benefit plans, income taxes	All	P&L, BS	P&L, BS
Control Objective 1		Consistent data between the preceeding legacy systems, GL and Hyperion	Identification of significant misstatements and inconsistences in the data received	Harmonised and uniform GL and CO master data for all entities	All significant transactions, assets and liabilities are recognised and in the correct period	Relevant closing activities in SAP are performed and in correct sequence	Accounting policies are correctly applied to each derivative and hedged item.	Differences between IFRS and local accounting principles or possible adjustments outside accounting system are identified and systematically documented.
Control Objective 2		No unexpected changes in accounting information (data content and accuracy) from legacy systems.	Correct and complete parameters (e.g. foreign currency exchange rates, VAT codes)	All significant transactions, assets and liabilities are recognised at the correct amount	Relevant information is available within the given time schedules.	Accounting policies are correctly applied to each lease.		
Control Objective 3		Correct and complete CO allocations rules	All significant transactions, assets and liabilities that are recognised exist and are justified	No accounting postings to old periods	Information on leases available in compact format, e.g. lease register.			
Control Objective 4		Significant assumptions applied in financial calculations are internally consistent and based on best possible information available minimizing risk of future material adjustments.			Finance lease related balances reported are accurate.			
Control Objective 5					Obligations given rise to provisions are properly identified.			
Control Objective 6					Amount recognized as provision is based on the best estimate on the obligation.			
Control Objective 7					Changes to existing provisions are justified, complete and correctly disclosed.			
Control Objective 8					Accounting policies are correctly applied to post-employment benefit plans and other long-term employee benefit plans.			
Control Objective 9					Emission rights received are registered at correct price and quantity.			

LIITE 3. KONTROLLITAVOITE JA KONTROLLITOIMENPITEET

Process: Record to Report
Sub-process: General Ledger Accounting and Controlling (incl. GL and CO Master Data Maintenance, Period-End-Closing)

Risk 1
Incomplete / inaccurate Interfaces

Control id (code to identify the control)	Control point (name)	Key control (yes / no)	Control Objectives	Control Activities	Related instructions (work instructions to be written in this column)	Responsibility organisation / role	Control frequency Please select one: Each transaction (ET) Daily (D) Weekly (W) Monthly (M) Quarterly (Q) Half yearly (HY) Annually (A)	Control Rating Type Please select for each control activity step: Analysis (AN) Reconciliation (R) Management Review (M) Authorization (AU) Standard, policy, procedure (P)	Preventative / Detective Please select for each control activity step: Preventative Detective Automatic
RR012	Consistent data between the preceeding legacy systems, GL and Hyperion	Key	**Consistent data between the preceeding legacy systems, GL and Hyperion**	1. ALE interfaces monitoring (inbound)	1.	1. Global transactions	1.	1. R	1. Detective
				2. Batch interfaces reconciliation (inbound)	2.	2. Reporting department, Global transactions	2.	2. R	2. Detective
				3. Sub-ledger reconciliations (inbound)	3.	3. Reporting department	3.	3. R	3. Detective
				4. Data upload from SAP to Hyperion is done via interface and related mapping tables are systematically maintained and complete	4.	4. Reporting department, Finance opearating platform	4.	4. P (proocedure)	4. Preventative
				5. Reconciliation of GL with CO	5.	5. Reporting department	5.	5. R	5. Detective, partly Automatic (errors to be checked)
				6. SAP – Hyperion reconciliation (outbound)	6.	6. Reporting department	6.	6. R	6. Detective