Haaga-Helia
ammattikorkeakoulu Oy

Sisäisen valvonnan kehittäminen Yritys X:n materiaali- ja tarvikevarastossa

Emilia Muhonen

Opinnäytetyö
Liiketalouden koulutusohjelma
2019

Haaga-Helia
ammattikorkeakoulu Oy

Tekijä
Emilia Muhonen

Koulutusohjelma
Liiketalouden koulutusohjelma

Raportin/Opinnäytetyön nimi
Sisäisen valvonnan kehittäminen Yritys X:n materiaali- ja tarvikevarastossa

Sivu- ja liitesivumäärä
56+5

Tiivistelmä

Viime vuosituhannen aikana laajamittaisesti otsikoissa olleet väärinkäytökset ja kasvaneet vaatimukset yrityksen liiketoiminnan sekä talouden läpinäkyvyyden suhteen ovat lisääntyneet. Yrityksillä on tarvetta panostaa yhä enemmän sisäisen valvonnan eri osa-alueisiin ja raportointiin. Sisäinen valvonta on yhtiön tärkeä ja kokonaisvaltainen hallinnointimalli, jossa vastuu sisäisen valvonnan järjestämisestä on yhtiön ylimmällä johdolla, mutta mallin käytännön toteutus ja siihen liittyvät kontrollitoimenpiteet ovat koko organisaation vastuulla.

Tämän opinnäytetyön toimeksiantaja on suuri suomalainen teollisuus- ja markkinointiyritys, jolla on tuotantolaitoksia sekä Suomessa että ulkomailla ja toimintaa useissa maissa ympäri maailmaa. Pääasiallinen tavoite on selvittää, miten toimeksiantajayrityksen sisäiseen valvontaan liittyvät osa-alueet on tällä hetkellä hoidettu hankintaprosessiin kuuluvan materiaali- ja tarvikevaraston toimintojen osalta ja tulisiko niitä kehittää. Kohdeyritys noudattaa COSO 2013 viitekehystä ja siksi materiaali- ja tarvikevaraston riskiarvioinneissa ja kontrollitoimenpiteiden tehokkuuden määrittelyssä tulee noudattaa kyseisen viitekehyksen suosituksia ja periaatteita.

Opinnäytetyö toteutettiin tapaustutkimuksena eli Case-tutkimuksena, joka on osa kvalitatiivista eli laadullista tutkimusperinnettä. Tiedonkeruumenetelminä käytettiin havainnointia kyseisessä työympäristössä ja suunnitelman mukaisia ryhmäkeskusteluja, joissa ongelmanratkaisumalleista ja toteutuksesta keskusteltiin asianomaisten prosessiasiantuntijoiden kanssa. Havainnointi tapahtui toimeksiantajayrityksessä tehdyn määräaikaisen työsuhteen aikana.

Opinnäytetyön toimeksiannosta sovittiin lokakuussa 2017, teoriaan perehtyminen ja suunnitelmaehdotuksen tekeminen tehtiin vuoden 2017 loppuun mennessä. Riskianalyysi ja kontrollien läpikäynti sekä uuden viitekehysmallin suunnittelu tapahtui vuoden 2018 aikana ja itse lopputyödokumentaation viimeistely tehtiin vuonna 2019, kun opinnäytetyöntekijä palasi äitiyslomalta.

Tutkimuksessa saatiin selville, että kohdeyritys oli lähivuosien aikana systemaattisesti kehittänyt yhtiön sisäistä valvontaa ja noudatti laajasti COSO 2013 periaatteita sekä oli implementoinut hyvän hallinnointimallin mukaisen kolmen puolustuslinjan periaatteen. Tästä huolimatta sekä yritys että opinnäytetyöntekijä olivat havainneet puutteita ja kehitystarpeita niin prosessi- ja kontrollikuvausten kuin työohjeiden osalta. Materiaali- ja tarvikevaraston osalta tehtiin riskikartoituksen perusteella ehdotus uudeksi kontrollikatalogiksi sekä laadittiin korjaavien toimenpiteiden lista toteutettavaksi kohdeyrityksen toimesta kyseisten prosessien osalta.

Asiasanat

Sisäinen valvonta, COSO, kontrollitoimenpide, tarvikevarasto

Sisällys

1 Johdanto

1.1 Toimeksiannon taustaa

Laajamittaiset otsikoissa edellisvuosituhannen aikana olleet väärinkäytökset ja kasvaneet vaatimukset yrityksen liiketoiminnan ja talouden läpinäkyvyyden suhteen ovat lisänneet yritysten tarvetta panostaa yhä enemmän sisäisen valvonnan eri osa-alueisiin ja raportointiin. Vastuu sisäiseen valvontaan liittyvien asioiden ymmärtämisestä on koko yrityksellä, eikä vain kirjanpitäjillä ja sisäisellä tarkistuksella. Kaikilla yrityksen eri tasoilla ja osa-alueilla on vastuu yrityksen sisäisestä valvonnasta, erityisesti ylimmällä johdolla. Muita sisäistä valvontaa toteuttavia tahoja ovat esimiehet, taloushallinto, eri prosessien vastuuhenkilöt, lakiosasto, henkilöstöhallinto, hankinta- ja myyntiosasto. (Ratsula 2016, 10.)

Sisäinen valvonta on tärkeä ja kriittinen osa yritysten johtamis- ja hallintotapaa, joka hyvin järjestettynä auttaa johtamaan organisaatiota pääsemään kohti asetettuja tavoitteitaan, ehkäisemään riskejä, turvaamaan julkisuuskuvaa ja näin saavuttamaan itselleen pysyvän kilpailuedun. (Ratsula 2016, 10.)

Englanninkielinen termi Internal Control tarkoittaa sisäistä valvontaa ja sen avulla yrityksen johto ohjaa henkilöstöä tahtotilansa mukaiseen suuntaan. Sisäisen valvonnan perustan luo siis niin sanottu tone from the top – ylimmän johdon asettamat suuntaviivat, eli ohjeet ja käytännön tavoitteet sille miten yrityksen sisällä tulee toimia. Koska sisäisen valvonnan merkitys yritykselle on korostunut, on siihen palkattu yhä enemmän sisäisen valvonnan ammattilaisia, joiden tehtävänä on auttaa rakentamaan juuri kutakin yritystä parhaiten tukeva ja toimiva sisäisen valvonnan järjestelmä. (Ratsula 2016, 10-13.)

Tärkeitä painopisteitä sisäisen valvonnan kehittämisellä on sisäisen valvonnan määritelmät ja viitekehykset, johdon, esimiesten ja yksittäisen työntekijän vastuut, yleisesti tunnetun sisäisen valvonnan COSO 2013:n mukaiset tärkeimmät periaatteet. Sisäisen valvonnan on oltava osa jokapäiväistä politiikkaa organisaation eri toiminnoissa ja prosesseissa kuten esimerkiksi hankinta- ja varastoprosesseissa. Sisäinen valvonta valvoo myös väärinkäytöksiä ja auttaa niiden havaitsemisessa. (Ratsula 2016, 11-13.)

1.2 Kohdeyrityksen esittely

Opinnäytetyön toimeksiantaja on suuri suomalainen teollisuus- ja markkinointiyritys, julkinen osakeyhtiö, jolla on tuotantolaitoksia Suomessa ja ulkomailla sekä toimintaa useissa maissa ympäri maailmaa. Työntekijöiden määrä on noin 5.500 henkeä eri puolella maail-

maa. Vaikka mikään erillinen lainsäädäntö ei suoraan määrää yrityksen sisäisen valvonnan järjestämistä, julkisen osakeyhtiön ollessa kyseessä osakeyhtiölaki ja esimerkiksi Finanssivalvonta ja Suomen listayhtiöiden hallinnointikoodi ovat antaneet kohdeyritykselle ohjeistuksia sisäisen valvonnan järjestämisestä. (Yritys X 2019.)

Toimeksiantajayritys on listattu Nasdaq Helsinki Oy:ssä (Helsingin pörssi) ja kuuluu täten listattuihin pörssiyhtiöihin. Tämän vuoksi yrityksen tulee ja se myös noudattaa Corporate Governancea – arvopaperimarkkinayhdistyksen antamaa hallinnointikoodia, jonka tavoitteena on saada suomalaiset listayhtiöt noudattamaan korkeatasoista kansainvälistä hallinnointitapaa. (Yritys X 2019.)

Yrityksen eettiset säännöt asettavat maailmanlaajuiset raamit sen koko liiketoiminnalle. Yritys noudattaa myös yleisesti tunnetun sisäisen valvonnan COSO 2013:n periaatteita ja sisäisen valvonnan ohjausmallina käytetään ns. kolmen puolustuslinjan (Three Lines of Defence) mallia, jossa vastuu riskienhallinnan valvonnasta on viime kädessä yrityksen hallituksella, jonka tehtäviin kuuluu esimerkiksi konsernin riskinottohalukkuuden vahvistaminen ja riskienhallintapolitiikan hyväksyminen. Käytännössä roolit ja vastuut jakautuvat seuraavasti:

Ensimmäinen puolustuslinja vastaa tavoitteiden määrityksestä, päivittäisen suorituksen johtamisesta ja tehokkaiden riskienhallinnan toimenpiteiden jalkauttamisesta tavoitteiden saavuttamiseksi. Tähän puolustuslinjaan kuuluvat liiketoiminta-alueet sekä yhteiset toiminnot silloin kun ne toteuttavat tähän puolustuslinjaan kuuluvia tehtäviä. Osana ensimmäistä puolustuslinjaa yrityksen toimitusjohtajalla ja johtoryhmällä on kokonaisvastuu asianmukaisen riskienhallinnan järjestämisestä. Käytännössä riskien valvonta ja riskiraportointi tapahtuu nimettyjen riskiasiantuntijoiden verkoston avulla. (Yritys X 2019.)

Toisen puolustuslinjan toimijoiden roolina on riskienhallinnan toteutuksen tukeminen sekä riskienhallinnan prosessien ja työvälineiden kehittäminen. Toisen puolustuslinjan pitää pystyä haastamaan ensimmäisen puolustuslinjan toimijoita päivittäisen suorituksen johtamisen osalta ja päätöksenteon riskitietoisuuden lisäämisessä. Yritys X:ssä toiseen puolustuslinjaan kuuluvat toisen puolustuslinjan roolia toteuttavat yhteiset toiminnot ja riskienhallintaan keskittyvät asiantuntijatiimit (yhtiön riskienhallinta, compliance eli sisäinen valvonta ja kontrollien kehitys) sekä erillinen Ethics and Compliance -toimikunta, joka pyrkii varmistamaan asianmukaisen valvonnan ja edistämään prosessien tehokkuutta ulkoisten ja sisäisten vaatimusten mukaisesti, sekä eettisiin toimintatapoihin liittyvissä kysymyk-

sissä. Yhtiön riskienhallintatiimi vastaa kokonaisuutena riskienhallinnan viitekehyksen ylläpidosta. Riskienhallinnan toimintatapojen täytyy olla johdonmukaista läpi organisaation ja kaikissa riskiluokissa. Yhtiön riskienhallinta kehittää myös jatkuvasti riskienhallinnan politiikkoja ja työkaluja. Tiimin tukena toimii riskiasiantuntijoista koostuva verkosto ja riskien koordinoinnin työryhmä, joka pyrkii varmistamaan yrityksen riskienhallintapolitiikkojen vaikuttavuuden sekä tehokkuuden. (Yritys X 2019.)

Kolmatta puolustuslinjaa edustaa sisäinen tarkastus – riippumaton elin, joka arvioi yhtiötasolla määritellyn riskienhallinnan viitekehyksen, roolien ja politiikkojen toimivuutta ja tehokkuutta sekä arvioi sisäisen valvonnan ja riskienhallinnan asianmukaisuutta yksityiskohtaisemmin tarkastuksen kohteena olevilla alueilla. Sisäinen tarkastus myös antaa kehityssuosituksia sisäisen valvonnan ja riskienhallinnan kehittämiseksi. (Yritys X 2019.)

Viime vuosien aikana yrityksen riskienhallinnan erityisanalyysit kohdistuivat merkittävimpiin investointeihin, järjestelmähankkeisiin ja liiketoimintamallien muutoksiin. Osana yhtiötason kehityshankkeita riskienhallinta osallistui johtamisjärjestelmän uudistamiseen ja kolmen puolustuslinjan mallin selkiyttämiseen. Näiden mainittujen painopistealueiden seurauksena Yritys X:ssä on ilmennyt tarve käydä läpi mm. hankinta- ja tarvikevaraston prosesseja ja päivittää globaalisti niihin liittyviä politiikkoja, ohjeita, puutteellisia prosessikuvauksia sekä riskianalyysin avulla varmistaa tunnistettujen riskien eliminointiin liittyvät tarvittavat sisäisen valvonnan toiminnot kyseisten prosessien osalta. (Yritys X 2019.)

1.3 Opinnäytetyön synty, tavoite, rajaus ja kysymykset

1.3.1 Opinnäytetyön synty

Opinnäyteyön aihe syntyi, kun Yritys X ilmaisi globaalin kehitys- ja harmonisointitarpeen materiaali- ja tarvikevaraston prosessikuvausten ja taloudellisen raportoinnin kontrollien osalta. Yritys halusi varmistaa, että COSO 2013 periaatteita ja valvontatoimia noudatetaan globaalisti koko yhtiössä. Samanaikaisesti opinnäytetyöntekijä huomasi erinäisiä puutteita ja epäselvyyksiä materiaali- ja tarvikevaraston toimintojen ja kontrollien osalta työskennellessään Yritys X:ssä.

Puutteellinen ohjeistus ja puuttuvat kontrollit, harmonisoimattomat työskentelytavat sekä epäselvyydet vastuissa aiheuttivat virheitä raportoinnissa. Kuunvaihteen katkossa jouduttiin käyttämään luvattoman paljon aikaa virheiden korjaukseen, joka aiheutti taas ylityötarvetta ja henkilöstön ylikuormitusta sekä myöhästymisiä kuunvaihteen raportointiaikatau-

lussa, joka uhkasi pahimmillaan viivästyttää koko yhtiön kauden raportoinnin valmistumista. Nämä epäkohdat herättivät opinnäytetyöntekijän mielenkiinnon jo aloitetun toimeksiannon parissa, kun opinnäytetyö oli saanut alkunsa ja kirjoittaja sai uuden tehtävän kuunvaihteen täsmäytysvastuun ostoreskontran osalta. Tämän vuoksi lopputyöntekijä kiinnostui tutkimaan ovatko sisäisen valvonnan osa-alueet kunnossa materiaali- ja tarvikevaraston osalta. Näin ollen, jos materiaali- ja tarvikevaraston prosesseissa löytyy kehitysehdotuksia, ne tulevat olemaan olennainen osa opinnäytetyötä.

1.3.2 Tavoite, rajaus ja kysymykset

Tämän opinnäytetyön pääasiallinen tavoite on selvittää, miten toimeksiantajayrityksen sisäiseen valvontaan liittyvät osa-alueet on tällä hetkellä hoidettu hankintaprosessiin kuuluvan **materiaali- ja tarvikevaraston toimintojen** osalta ja tulisiko niitä kehittää. Yhtenä tavoitteena on saada ajantasainen kuva siitä, ovatko sisäiseen valvontaan liittyvät toimenpiteet riittävät ja toimivatko ne tehokkaasti. Kohdeyritys noudattaa COSO 2013 viitekehystä ja siksi materiaali- ja tarvikevaraston riskiarvioinneissa ja kontrolliaktiviteettien tehokkuuden määrittelyssä tulee noudattaa kyseisen viitekehyksen suosituksia ja periaatteita.

Työ on rajattu koskemaan yrityksen Suomen toimintojen materiaali- ja tarvikevarastojen osa-alueita – osittain siksi, että työ vastaa ammattikorkeakoulun opinnäytetyön laajuutta ja toisaalta siksi, että kyseiset prosessit linkittyvät olennaisena osana opinnäytetyöntekijän toimenkuvaan yrityksessä opinnäytetyön suorittamisen ajankohtana. Lisäksi Suomen toimintojen opinnäytetyön tuloksena kehitetty sisäisen valvonnan malli (best practice), on tarkoitus valmistuessaan implementoida globaalisti yrityksen kaikkiin toimipisteisiin, jossa harjoitetaan vastaavaa materiaali- ja tarvikevarastotoimintaa.

Yhtiössä on meneillään projekti, jossa kaikkien end-to-end prosessien osalta prosessivastaavien on käytävä läpi COSO 2013 mukaisesti niihin liittyvät käytännöt ja ohjeistukset, eri tasoille määritellyt prosessikuvaukset, sisäisen valvonnan tavoitteet, niitä uhkaavat riskit sekä sisäiset kontrollit ehkäisemään riskiarvioinnissa esille tulleita riskejä ja väärinkäytöksiä.

Projekti toteutetaan pääosin ryhmätyöskentelynä ja palavereihin osallistuvat kyseisen prosessin omistajat ja muut prosessiasiantuntijat, kyseisen prosessin kontrollivastaavat sekä yhtiön Compliance Manager. Lopputyöntekijä toimii koordinaattorina kyseisissä ryhmätöissä tavoitteena havainnoida, tunnistaa ja dokumentoida puutteet Yritys X:n materiaali- ja tarvikevarastojen prosessien osalta, määritellä tarvittavat kontrollit ja lopuksi luovuttaa työ eteenpäin mahdollisia jatkotoimenpiteitä varten.

Tämä määrittelee opinnäytetyön tutkimuskysymykset:

1. Ovatko materiaali- ja tarvikevaraston prosessikuvaukset ajantasaiset, mitä ongelmia prosesseihin liittyy, mikä on Yritys X:n toiminnanohjausjärjestelmän käyttäjäoikeuksien sekä varaston työohjeiden nykytila?
2. Millaisia riskejä materiaalivaraston prosesseista löytyy ja millaiset kontrollit kattavat havaitut riskit?

1.4 Toteutus- ja tiedonkeruumenetelmä

Opinnäytetyö toteutettiin tapaustutkimuksena eli Case-tutkimuksena, joka on osa kvalitatiivista eli laadullista tutkimusperinnettä. Kyseistä tutkimustapaa käytetään usein, kun halutaan tutkia yrityksien ja organisaatioiden käyttäytymistä. Tapauksia tutkitaan niiden omassa erityisessä ympäristössään ja aineistoa kootaan luonnollisissa, todellisissa tilanteissa, kuten erilaisissa vuorovaikutustilanteissa. Tutkija voi esimerkiksi olla osa työyhteisöä, jolloin tutkimuksen tiedonhankintatapa on kokonaisvaltainen. Tutkijan omat havainnot ja keskustelut ovat instrumenttina käytetympiä kuin muut välilliset tai erilaiset kvalitatiiviset mittaustavat. (Aaltio 1999.)

On tärkeää, että tutkimusasetelma linkittyy aikaisempaan teoriapohjaan, joka näin muodostaa kokonaisvaltaisen perustan, josta analyysit ja tulkinnat tehdään johtopäätelmissä. Tutkija ja tutkimuskohde ovat case-tutkimuksessa läheisessä vuorovaikutussuhteessa keskenään, ja luottamuksen saaminen ja säilyttäminen läpi koko tutkimuksen on tärkeä osa tutkimusprosessia. Tuloksissa pyritään pääsemään syvälle tutkittavaan tapaukseen sekä ymmärtämään ja tulkitsemaan syvällisesti yksittäisiä tapauksia niiden erityisessä kontekstissa – hakemalla tietoa dynamiikasta ja prosesseista. (Aaltio 1999.)

Kvalitatiivisia aineistoja voidaan kerätä paitsi teksteinä, myös kuvien tai osallistuvan havainnoinnin avulla. Ominaista Case-tutkimuksen osalta on, että tutkija saattaa kerätä aineistoa osallistumalla tiiviisti tutkimansa työyhteisön elämään viikkoja tai jopa vuosia. Näin toimimalla saadaan luotettavaa ja tapauksen yksityiskohtaisiin perusteisiin ulottuvaa tietoa, jonka avulla saadaan luotettavia vastauksia tutkimuskysymyksiin. (Aaltio 1999.)

Tiedonkeruumenetelminä käytettiin havainnointia kyseisessä työympäristössä ja projektisuunnitelman mukaisia ryhmäkeskusteluja, joissa ongelmasta keskusteltiin asianomaisten prosessiasiantuntijoiden kanssa. Havannointi tapahtui toimeksiantajayrityksessä tehdyssä määräaikaisessa työsuhteessa. Asiantuntijoiden mukaan tutkimuksen luotettavan lopputuloksen kannalta on tärkeää, että lopputyöntekijä voi työskennellä toimeksiantajayrityksessä ja saa näin päivittäin olla tekemisissä kyseisten kysymysten parissa, jolloin voidaan tarkkailla tutkittavaa ilmiötä läheltä. Ryhmätöissä ja

muissa keskusteluissa esiintuodut epäkohdat sekä työympäristössä päivittäin havaitut opinnäytetyön kysymyksiin liittyvät puutteet dokumentointiin opinnäytetyöntekijän toimesta ja ne käytiin myöhemmin läpi asianomistajien kanssa.

Ryhmätyömuotona kuvattiin prossessiin liittyvät riskit opinnäytetyöntekijän ohjauksessa. Näin todetut riskit, jotka toteutuessaan vaarantaisivat yhtiön taloudellisen raportoinnin tavoitteet tunnistettiin ja dokumentoitiin prosessikohtaisesti. Validi keino tämän tutkimuksen toteuttamiseen on ollut seurata yrityksen toimintatapoja, keskustella työntekijöiden kanssa päivittäin ja näin havainnoimalla oppia tunnistamaan prosessin eri osaalueisiin liittyviä ongelmakohtia. Toinen toimiva keino toteuttaa tätä tutkimusta ovat olleet ohjatut ryhmätyökeskustelupalaverit, koska näissä tilanteissa käydyn dialogin aikana opinnäytetyöntekijä on voinut tarvittaessa selvittää taustaa kysymyksilleen reaaliajassa ja näin ollen lisännyt myös organisaation tietoisuutta ongelmaa kohtaan.

Henkilöstön kanssa käydyissä vuoropuheluissa on ollut toisaalta mahdollista puolin ja toisin selkeyttää kysymyksiä sekä vastauksia. Tämä antaa paljon luotettavamman lähtökohdan nykytilanteen kuvaukselle, verrattuna että tutkimus olisi suoritettu esimerkiksi kyselylomaketta käyttäen. Kysymysten läpikäynti ryhmätyöskentelynä on jo itsessään kasvattanut yksilöiden tietoisuutta käsiteltävää ilmiötä kohtaan. Tästä syystä kohdeyleisö on voinut tuottaa luotettavaa informaatiota sekä nykytilan kuvauksen että mielestään olemassa olevien puutteiden ja jopa korjaavien toimenpide-ehdotusten suhteen.

1.5 Rakenne, prosessisuunnitelma ja sen toteutus

1.5.1 Tutkimuksen rakenne

Lopputyö alkaa johdannolla, jossa kerrotaan toimeksiannon taustoista ja kohdeyrityksestä sekä esitetään opinnäytetyöaiheen että toteuttamistavan valinnan kannalta olennaiset seikat. Alussa on esitelty opinnäytetyön syntyyn, tavoitteeseen, rajaukseen ja kysymyksiin liittyvät osa-alueet. Toteutukseen ja tiedonkeruuseen paneudutaan johdannossa, jossa esitellään myös prosessin toteutussuunnitelma ja kuvataan suunnitelman toteutumista.

Toinen ja kolmas luku avaavat toimeksiannon teoreettisen viitekehyksen yrityksen sisäisen valvontajärjestelmän osalta sekä kertovat miten hyvin järjestetty sisäinen valvonta parhaimmillaan toimii osana johdon valvontajärjestelmää turvaten tavoitteiden toteutumisen.

Neljännessä luvussa perehdytään tapaustutkimukseen, eli Case-Yritys X Oyj:n toimeksiantoon, jossa on esitetty havaintojen ja ryhmätyökeskustelujen pohjalta esiin nousseet tulokset ja niiden perusteella on määritelty korjaavat toimenpide-ehdotukset niin kontrollikatalogin kuin muiden sisäisen valvonnan osa-alueisiin liittyvien puutteiden ja dokumentoinnin osalta.

Viidennessä luvussa esitellään opinnäytetyöhön liittyvät johtopäätökset ja yhteenveto kehitysehdotuksista sisäisen valvonnan eri osa-alueisiin liittyen Yritys X:ssä. Lopuksi pohditaan tutkimuksen onnistumista sen kulkuun, luotettavuuden ja opinnäytetyöntekijän oman oppimisen kannalta.

1.5.2 Suunnitelma ja sen toteutuminen

Tietoisuus materiaali- ja tarvikevarastoon liittyvien raportointiongelmien osalta kasvoi Yritys X:ssä kevään ja kesän 2017 aikana opinnäytetyöntekijän työskennellessä kohdeyrityksessä määräaikaisissa taloushallinnon tehtävissä. Itse opinnäytetyön suunnitteluprosessi alkoi syksyllä 2017 aiheen valinnalla. Toimeksiannosta sovittiin kohdeyrityksen edustajan kanssa lokakuussa 2017 (liite 1). Tämän jälkeen tehtiin opinnäytesuunnitelma (liite 2), jonka välitavoite sisälsi hyväksytyn tutkimussuunnitelman lisäksi Yritys X:lle tuotetun raportin, jossa kerrottiin alustavista havainnoista liittyen toimeksiannon materiaali- ja tarvikevarastoihin. Välitavoite toteutui alkuperäisen suunnitelman mukaisesti 12/2017 palaverien muodossa.

Lopullinen tavoite oli havaintojen ja riskikartoitusryhmätöiden avulla tehdä kevään 2018 aikana ehdotus Yritys X:n prosesseihin liittyvistä riskeistä sekä kontrolleista ja valmistella yritykselle kontrollikatalogi. Lisäksi tuli kiinnittää huomiota prosesseissa havaittuihin ongelmiin ja dokumentoida tulokset. Toteutussuunnitelmaa jouduttiin päivittämään osittain opinnäytetyöntekijän siirryttyä uuteen työtehtävään keväällä 2018. Tehtävä priorisoitiin tärkeys- ja vaikeusasteensa sekä osittain resurssipulan takia prosessityöskentelyn yläpuolelle, joka aiheutti kontrollityön viivästymisen. Ehdotuksen uusi takaraja oli vuoden 2018 loppuun mennessä, joka oli myös määräaikaisen työsuhteen päättymisajankohta. Päivitetty suunnitelma toteutui 10/2018. Samalla sovittiin, että opinnäytetyöntekijä kirjoittaa lopputyön valmiiksi omalla rajauksella ja aikataululla.

Yritys X:n opinnäytetyöohjaajan kanssa pidettiin kahdenkeskisiä etenemispalavereja säännöllisesti vuoden 2018 aikana. Palavereissa käytiin läpi toimeksiannon etenemistä ja sovittiin yhdessä seuraavista toimenpiteistä. Itse opinnäytetyön oli alun perin tarkoitus valmistua vuoden 2018 loppuun mennessä, mutta aiemmin mainittu uusi työtehtävä sekä

opinnäytetyötekijän 11/2018 alkanut äitiysloma aiheuttivat tarpeen opinnäytetyönsuunnitelman päivitykseen. Työtä jatkettiin huhtikuussa 2019 ja oppilaitoksen opinnäytetyöohjaajan kanssa sovittiin, että aikaa lopputyön valmistumiselle olisi vuoden 2019 loppuun saakka. Lopputyö valmistui ja lähetettiin arvioitavaksi annetun aikarajan puitteissa.

Suunnitelmana oli laadullista tapaustutkimusteoriaa käyttäen selvittää ja dokumentoida sisäisen valvonnan puutteet sekä tarvittavat avainkontrollit Yritys X:n materiaali- ja tarvikevaraston osalta. Tutkimuksen kannalta oleellinen tieto koottiin riskienarviointityöryhmän palavereissa ja muuten havainnoimalla. Voidakseen poimia aiheeseen liittyvät relevantit asiat, opinnäytetyöntekijä tutustui ensin yrityksen sisäisen valvonnan käsitteisiin. Yritys X:n Compliance Manager johdatti opinnäytetyöntekijää ymmärtämään yrityksen riskejä ja kontrolleja. Tämän jälkeen opinnäytetyöntekijä tutustui aiheen teoriaan, kuten kohdeyrityksessä noudatettuun COSO 2013-viitekehykseen sekä Yritys X:n olemassa olevaan sisäisen valvonnan viitekehykseen ja johdon organisaatiolle asettamiin tavoitteisiin, peilaten näitä saamaansa lopputyöaiheeseen. Lopputyöntekijä keskusteli yrityksen riskeistä ja kontrolleista yhdessä Compliance Managerin, kyseisten prosessin asiantuntijoiden sekä yrityksen Controllerin kanssa. ICT-asiantuntijoiden kanssa käytiin läpi Yritys X:n toiminnanohjausjärjestelmään liittyviä kysymyksiä.

Ryhmätyöpalaverit, joihin osallistui materiaali- ja tarvikevaraston prosessien tuntijoita, ICT:n asiantuntija, Compliance Manager ja Controller, sijoittuivat vuoden 2018 alkuvuosipuoliskolle kun taas prosessiin liittyvä havaintoja on käyty läpi asiantuntijaorganisaation kanssa vuoden 2017 lopun sekä koko vuoden 2018 aikana. Ryhmätyön pääasiallisilla kysymyksillä haluttiin selvittää mitkä olivat taloudellisen raportoinnin sisäiset kontrollit materiaali- ja tarvikevaraston osalta sillä hetkellä ja mitkä ovat ne taloudellisen raportoinnin kontrollit, jotka ehkäisevät todennettujen riskien toteutumisen materiaali- ja tarvikevaraston toimintojen osalta. Opinnäytetyöntekijä toimi ryhmätöiden koordinaattorina ja dokumentoi todettujen riskien lisäksi määriteltyjen asiantuntijoiden niin palavereissa kuin muissa keskusteluissa esille tuomat kommentit ja kehitysideat.

2 Yrityksen sisäinen valvontajärjestelmä

Sisäinen valvonta on osa yrityksen johtamis- ja hallintojärjestelmää, ja sen tavoitteena on tukea organisaatiota saavuttamaan johdon asettamat päämäärät. Käytännön tasolla sisäinen valvonta koostuu useista osa-alueista organisaation eri tasoilla, kuten esimerkiksi työtehtävien eriyttämisestä, hyväksymisvaltuuksista sekä laskenta- ja toiminnanohjausjärjestelmien sisältämistä kontrolleista. Osa kontrolleista liittyy siis järjestelmiin ja ohjeistuksiin mutta ennen kaikkea kyse sisäisessä valvonnassa on ihmisistä ja heidän toiminnastaan käytännön tasolla. (Ratsula 2018.)

2.1 Sisäisen valvonnan konsepti

Sisäisen valvonnan voi kuvata myös prosessina, jonka avulla pyritään varmistamaan tavoitteiden saavuttaminen. Tavoitteet voidaan jakaa neljään eri kategoriaan: 1) **strategiset** eli korkean tason tavoitteet – ovatko tavoitteet organisaation mission mukaisia ja sitä tukevia, 2) **toiminnalliset** eli käytetäänkö organisaation voimavaroja taloudellisesti ja tehokkaasti, 3) **raportointia koskevat** eli onko raportointi luotettavaa, 4) **vaatimustenmukaisuutta koskevat** eli noudattavatko tavoitteet sovellettavia lakeja ja määräyksiä. (Sisäiset tarkastajat ry 2019.)

Yrityksessä hyvin järjestetty sisäinen valvonta on tärkeä apuväline organisaatiolle. Tämä ohjaa yrityksen toimintaa kohti tavoitteita, vähentää liiketoiminnan riskejä, suojaa julkista yrityskuvaa ja täten ylläpitää kilpailuetua. Johdolla ja esimiehillä on tärkeä rooli hyvän ohjauskulttuurin luonnissa, koska usein käyttäytymiskulttuuri ja kirjoittamattomat säännöt voivat olla voimakkaampia kuin kirjoitetut ohjeistukset tai yrityksen käytännöt. Organisaation muutostila, esimerkiksi voimakas kasvu tai omistuspohjan muutokset vaikuttavat myös merkittävästi sisäisen valvonnan vaatimustasoon. Tärkeintä ei kuitenkaan ole se miten sisäinen valvonta on järjestetty, vaan se että valvonta toimii tehokkaasti. Sisäinen valvonta on aina järjestetty eri tavoin organisaatiosta riippuen ja valvonnan tarpeeseen vaikuttavat muun muassa yrityksen omistussuhde, koko, rakenne sekä toimiala ja toimintojen luonne. (Ratsula 2018.)

2.2 Sisäiseen valvontaan liittyvä lainsäädäntö ja ohjeistus

Mikään erillinen lainsäädäntö ei suoraan määrää yrityksen sisäisen valvonnan järjestämistä, mutta asiaa voidaan tarkastella osakeyhtiölain vaatimusten näkökulmasta. Myös esimerkiksi Finanssivalvonta ja Suomen listayhtiöiden hallinnointikoodi antavat ohjeistuksia sisäisen valvonnan järjestämisestä. (Ratsula 2016, 31.)

2.2.1 Osakeyhtiölaki ja finanssivalvonnan standardi

Osakeyhtiölaissa on säädetty, että yrityksen hallituksen on huolehdittava kirjanpidon ja varainhoidon lainmukaisesta ja luotettavalla tavalla järjestetystä hoidosta. Sisäisen valvonnan järjestämisestä päättää pitkälti yrityksen johto. Osakeyhtiölaki (21.7.2006/624) määrää hallituksen ja toimitusjohtajan vastuusta kirjanpidon ja varainhoidon valvonnasta. Hallitus on siis vastuussa yrityksen asianmukaisen sisäisen valvonnan järjestämisestä. (Ratsula 2016, 32.)

Finanssivalvonta (Fiva) on rahoitus- ja vakuutusvalvontaviranomainen, joka toimii Suomen Pankin yhteydessä, mutta on päätöksenteossaan itsenäinen ja valvottavia ovat muuan muassa pörssi, pankit, vakuutus- ja eläkeyhtiöt sekä muut vakuutusalalla toimivat, sijoituspalveluyritykset ja rahastoyhtiöt. Fiva antaa valvottavilleen ohjeistuksen sisäisen valvonnan järjestämisestä. Fivan mukaan yhtiön hallitus vastaa riittävästä ja toimivasta sisäisen valvonnan järjestämisestä. Standardin mukaan sisäisen valvonnan merkittävimmät osa-alueet ovat johtamistapa ja valvontakulttuuri, riskienhallinta, päivittäinen valvonta ja tehtävien eriyttäminen, raportointi ja tiedonvälitys, sisäisen valvonnan toimivuuden seuranta sekä järjestelmät ja turvallisuus. (Ratsula 2016, 33-34.)

2.2.2 Hyvä hallinnointimalli eli Corporate Governance ja hallinointikoodi

Hyvällä hallinnointimallilla, Corporate Governancella (CG) tarkoitetaan yhtiön hallinnointi- ja ohjausjärjestelmää, joka määrittelee yritysjohdon roolit, velvollisuudet ja suhteen osakkeenomistajiin. CG on järjestelmä, jonka avulla yritystoimintaa ohjataan ja valvotaan sekä sen suosituksilla on tarkoitus täydentää lakisääteisiä menettelytapoja. Tätä kutsutaan suomessa elinkeinoelämän itsesääntelyksi. (Arvopaperimarkkinayhdistys ry 2015a.)

Arvopaperimarkkinayhdistyksen antaman hallinnointikoodin tavoitteena on saada suomalaiset listayhtiöt noudattamaan korkeatasoista kansainvälistä hallinnointitapaa. Koodi yhtenäistää listayhtiöiden osakkeenomistajille ja muille sijoittajille annettavaa tietoa sekä lisää näkyvyyttä hallintoelimistä, johdon palkkioista ja palkitsemisjärjestelmistä. Koodi luo kokonaiskuvan suomalaisten listayhtiöiden hallinnointijärjestelmän keskeisistä periaatteista ja edistää suomalaisten listayhtiöiden menestystä. Pörssissä listattujen yhtiöiden tulee noudattaa koodia, elleivät yhtiön kotipaikan pakottavat säännökset ole ristiriidassa tämän kanssa. (Arvopaperimarkkinayhdistys ry 2015a.)

Hyvä hallinnointitapa tukee suomalaisten pörssiyhtiöiden arvonmuodostusta ja kiinnostavuutta sijoituskohteena ja sen tarkoitus on yhtenäistää pörssiyhtiöiden toimintatapoja.

Kaikkien Helsingin pörssiin (Nasdaq Helsinki Oy) listattujen pörssiyhtiöiden tulee noudattaa hallinnointikoodia. (Arvopaperimarkkinayhdistys ry 2015b.)

2.2.3 Sarbanes- Oxley laki

Yhdysvalloissa vuonna 2002 säädetyn Sarbanes-Oxley Act -lain (SOX) tavoitteena on parantaa yrityksen julkistamien tietojen oikeellisuutta ja luotettavuutta. Laki vaatii yrityksen johtamis- ja hallintojärjestelmiltä tehokkaampaa toimintaa ja johdon varmistusta yrityksestä raportoitavan tiedon oikeellisuudesta ja asianmukaisuudesta. SOX koskee kaikkia yhtiöitä, joiden osakkeet ovat kaupan Yhdysvaltojen arvopaperimarkkinoita valvovan viranomaisen SEC:n (Securities and Exchange Commission) alaisissa pörsseissä eli yhdysvaltalaisissa pörsseissä. (Protiviti 2007.)

Nimensä SOX-laki on saanut perustajansa senaattori Paul Sarbanesin ja edustajainhuoneen jäsenen Mike Oxleyn mukaan. Lain tarpeellisuus ymmärrettiin 2000-luvun alun merkittävien kirjanpitoskandaalien, kuten Enronin, Tyco Internationalin ja WorldComin takia. (Protiviti 2007.)

SOX vahvisti ulkoisten tilintarkastajien riippumattomuutta sekä sisäisen tarkastusvaliokunnan roolia. Listayhtiöillä pitää olla tarkastusvaliokunta, joka koostuu ainoastaan itsenäisistä jäsenistä, ja heistä vähintään yhden on oltava talouden asiantuntija (audit committee financial expert). Uuden lain myötä myös listayhtiöiden tilintarkastajia valvomaan perustettiin uusi elin, PCAOB (the Public Company Accounting Oversight Board), joka on velvollinen valvomaan SEC:n alaisissa pörsseissä listattujen yhtiöiden tilintarkastusta, rekisteröidä auktorisoituja tilintarkastusyhteisöjä sekä luoda ja ottaa käyttöön standardeja liittyen tilintarkastukseen, sisäiseen laadunvalvontaan, etiikkaan, riippumattomuuteen ja muihin seikkoihin, jotka liittyvä tilintarkastusraporttien laatimiseen. Tilintarkastusyhteisöjen ohjeistus kuuluu valvonnan lisäksi tärkeänä osana PCAOBn rooliin. (PCAOB 2007; Ratsula 2016, 46.)

SOX 404-pykälä on yksi vaativimmista SOX velvoitteista, jonka mukaan yrityksen vuosikertomuksessa on oltava maininta yritysjohdon vastuusta riittävän sisäisen valvonnan järjestämisestä, ylläpitämisestä ja sisäisen valvonnan raportoinnin tehokkuudesta päättyneen tilivuoden lopulla. Käytännössä tämä tarkoittaa sitä, että yritys joutuu dokumentoimaan taloudelliset prosessinsa ja tunnistamaan avainkontrollinsa sekä vuosittain arvioimaan sisäisen valvonnan tilaa testaamalla sisäisiä kontrollejaan. Tämä dokumentointi- ja arviointiprosessi vaatii yritykseltä uusia resursseja ja vie paljon aikaa. (Protiviti 2007.)

Dokumentointi voi tarkoittaa käytännössä esimerkiksi kaavioiden ja ohjeistuksen laatimista yrityksen taloudellisten prosessien osalta ja niihin liittyvien avainkontrollien listaamista kontrollikatalogiin. SOX velvoittaa yrityksen johtoa allekirjoittamaan vuosittain raportin, jossa todetaan, että he ovat vastuussa sisäisen valvonnan toiminnoista. Toimintojen ja menettelytapojen tehokkuutta tulee arvioida omaan sisäisen valvonnan järjestelmään sopivan viitekehyksen avulla. Yleisesti käytetyin viitekehys on luvussa 2.4 esitelty COSO-viitekehys. Tilintarkastajien tulee myös ottaa kantaa johdon arviointiprosessiin ja sisäisten valvontajärjestelmien tehokkuuteen ja toimivuuteen. (Protiviti 2007.)

Johdon on saatava tarpeeksi kattava kuva sisäisen valvonnan tehokkuudesta ja toimivuudesta organisaatiossa laatiakseen SOX:n vaatiman raportin. Sisäisen valvonnan kontrollien toimivuutta kuvataan kontrollitodisteaineistolla ja tällä kontrollievidenssillä voidaan varmistaa yrityksen raportoimien lukujen oikea-aikaisuus, varmistua raportoinnin oikeasta sisällöstä ja selvittää onko kirjaukset tehty yrityksen oikealle yksikölle. Yritys joutuu ensin dokumentoimaan vaadittavat avainkontrollit, jalkauttamaan ne organisaation eri tasoille ja lopuksi kontrollitestausta suorittamalla arvioimaan toimivatko kyseiset kontrollit. Esimerkkinä testauksesta voidaan ottaa tavaran vastaanotto. Kontrollikuvaus on, että valtuutetun henkilön tulee hyväksyä jokaisen varastoon saapuvan erän sisältö. Tarvittava otos valitaan esimerkiksi viimeisen puolen vuoden aikana saapuneista vastaanotoista ja tarkastetaan että jokainen vastaanotto vastaa hyväksyttyä tilausta ja on asianmukaisesti kirjattu varastokirjanpitoon. Suorittamattomat tai väärin suoritetut kontrollit raportoidaan kontrollipuutteena. Kohteena olevan organisaation on tehtävä korjaavat toimenpiteet kontrollipuutteiden osalta ja yrityksen on testattava kyseinen kontrolli uudelleen. (Ratsula 2016, 51-53.)

Muita sisäisen valvonnan malleja ja viitekehyksiä ovat tunnetuin COSO-malli, josta on kehittynyt ja myös käytössä oleva kokonaisvaltaisempi COSO-ERM-malli. COBIT (Control Objectives of Information and related Technology) on viitekehys, jota käytetään IT-kontrollien kehittämisessä sekä arvioinnissa ja joka yhdistää liiketoiminnan tavoitteita. (Ratsula 2016, 54, 65.)

2.3 COSO viitekehys ja johdon tilinpäätösväittämät

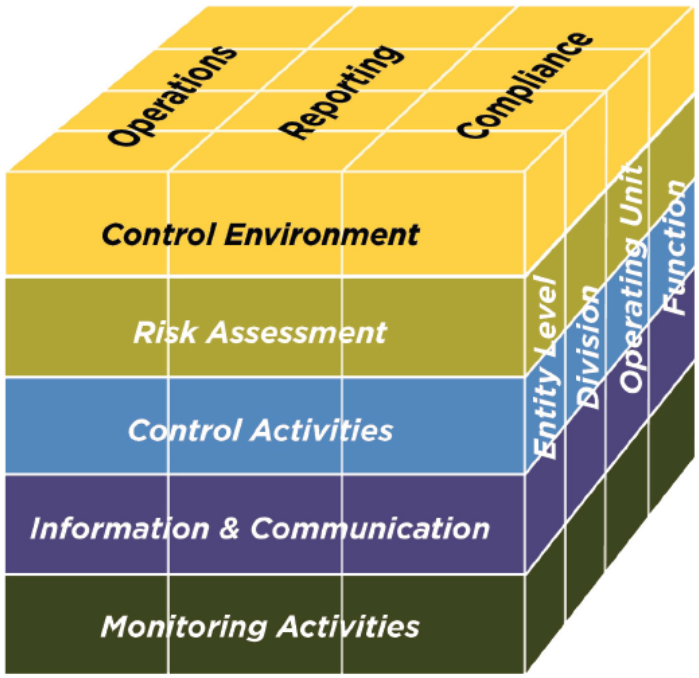
COSO-malli (Committee of Sponsoring Organisations of the Treadway Commission) on vuonna 1992 julkaistu malli, jota on päivitetty vuoden 2013 aikana. Uudistettu COSO 2013 raportti määrittelee tarkemmin sisäisen valvonnan osatekijöitä tukevia periaatteita ja laajentaa talousraportoinnin tavoitteet käsittämään myös sisäisen ja ulkoisen toiminnallisen

raportoinnin sekä keskittyy toiminto-, compliance- ja raportointitavoitteisiin. Yleisesti tunnettu ja käytetty sisäisen valvonnan viitekehysmalli COSO on yhtiön hallituksen, johdon ja muun henkilökunnan toteuttama prosessi, jonka tarkoitus on tuottaa kohtuullinen varmuus siitä, että yhtiön kolme tärkeää tavoitetta toteutuu:

- Toimintojen tehokkuus ja tarkoituksenmukaisuus
- Taloudellisen ja ei-taloudellisen raportoinnin luotettavuus
- Lakien ja säädösten noudattaminen (Protiviti 2014.)

COSO-mallin mukaan sisäisen valvonnan johtamisprosessiin kuuluu viisi eri osatekijää, organisaation ohjausympäristö, riskien arviointi, valvontatoimenpiteet, informaatio ja viestintä sekä seuranta ja valvonta (COSO 2013) ja näillä johdetaan ja valvotaan organisaation käyttäytymistä. (Ratsula 2016, 17.)

Tärkeä parannus vuoden 2013 COSO muutoksessa on viiden komponentin formalisointi 17 periaatteeseen, joiden tavoitteena on selkeyttää sisäisen valvonnan suunnittelua ja implementointia ja auttaa paremmin ymmärtämään sisäisen valvonnan vaatimuksia. Sisäinen valvonta on siis monisuuntainen prosessi, jossa osatekijät vaikuttavat toisiinsa ja joka koskettaa koko organisaatiota. Kuvassa 1 esitellään COSO-mallin osatekijöiden yhteys organisaation toiminnallisiin tavoitteisiin, taloudelliseen raportointiin, lakien ja säännösten noudattamiseen sekä organisaation yksikkö- ja toimintotahoihin. Organisaation tai sen yksikön tavoitteiden, sisäisen valvonnan osatekijöiden ja rakenteen välillä vallitsee suora yhteys. (Ratsula 2016, 57, 59-62.)



Kuva 1. COSO 2013 viitekehysmalli (COSO 2013)

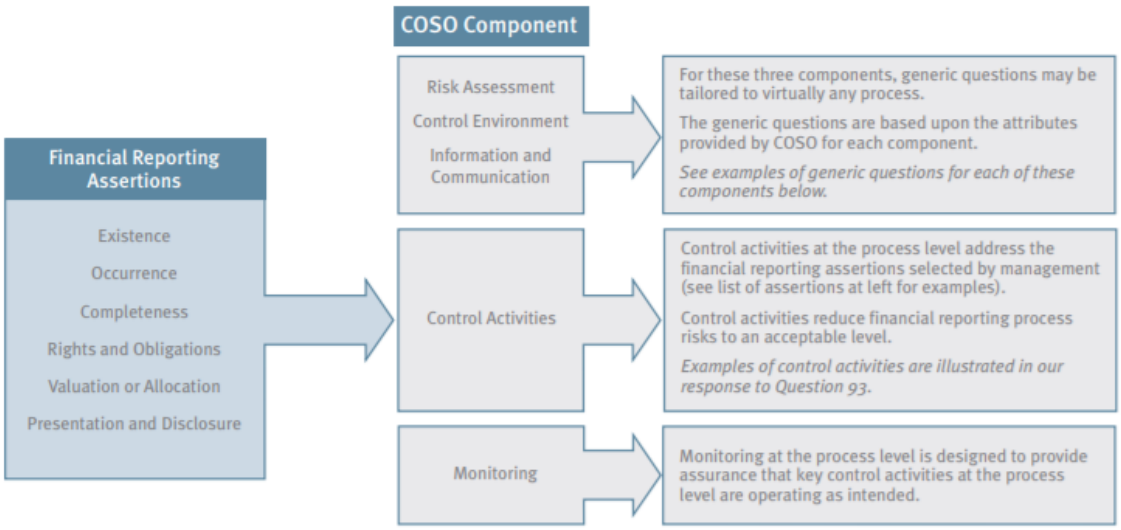
2.3.1 Johdon tilinpäätösasiakirjat (Management Assertions)

COSOn taloudellisen raportin väitteet (Financial Reporting Assertions) luovat perustaa johdon väitteille (management assertions, jotka tunnetaan myös nimellä tilinpäätösasiakirjat) ja viittaavat tilinpäätöksen laatimisesta vastuussa olevan henkilön, yleensä johdon väitteisiin. Johdon väitteet sisältävät tilinpäätöksen taloudellisten tietojen tunnistamisen, mittaamisen, esittämisen ja julkistamisen. (Protiviti 2014.)

Useimmat johdon väitteet kuuluvat seuraaviin kolmeen luokitukseen:

- **Transaktiotason väitteet**, jossa kaikkien yhtiön liiketoimien, yritystapahtumien ja niiden johdosta syntyneiden tapahtumien osalta kaikki kirjanpidon viennit on kirjattu pääkirjaan tarkasti ilman virheitä, oikean raportointikauden aikana sekä kirjaukset on kohdistettu oikealle yksikölle.
- **Tilin saldon väitteet**, jossa kaikki tilin saldot on kirjattu omaisuuseriin, velkoihin ja omaan pääomaan asianmukaisesti arvostettuina, raportoitu täysin virheettömästi ja oikean raportointikauden aikana. Yhteisöllä on oltava oikeudet omistamiinsa varoihin ja se on velvoitettu raportoimaan velkansa asianmukaisesti.
- **Esitys- ja julkistamisväitteet**, jossa kaikki julkistetut tiedot ovat oikean määräisiä, heijastavat niiden asianmukaisia arvoja, on esitetty asianmukaisesti ja on ymmärrettäviä. Myös kaikki julkistettavat tapahtumat on julkistettu, tapahtuneet ja raportoivaan yhteisöön liittyvät oikeudet ja velvollisuudet on julkistettu.

Alla olevassa kuvassa 2 voidaan nähdä miten yllä mainitut johdon tilinpäätösasiakirjat, eli tilinpäätösväittämät (management assertions) ovat yhtenevät kuvan COSOn talousraportoinnin väitteiden kanssa ja näin tukevat yritysjohdon tavoiteasetantaa ja niitä käytetään pohjana riskiarvioinneissa, joiden pohjalta määritellään sisäiset kontrollitoimenpiteet. (Protiviti 2014.)



Kuva 2. Taloudellisen raportoinnin väittämät tavoiteasetannan perustana (mukaillen Protiviti 2014)

2.3.2 Ohjausympäristö

Ohjausympäristö, jota kutsutaan myös valvontaympäristöksi muodostaa perustan yrityksen muille sisäisen valvonnan osa-alueille ja on näin luomassa ilmapiiriä, joka vaikuttaa koko henkilökunnan asenteisiin sekä on olennainen osa yrityksen valvontakulttuuria. Ohjausympäristö tuo kurinalaisuutta ja järjestystä sekä toimii välineenä, jolla lisätä organisaation tietoisuutta sisäiseen valvontaan liittyvien toimintojen osalta. Ohjausympäristö sisältää viisi ensimmäistä COSOn periaatetta. Ensimmäinen tärkeistä ohjausympäristön periaatteesta on se, että organisaatio on sitoutunut integriteettiin ja eettisiin arvoihin. Toisen periaatteen mukaisesti hallituksen on osoitettava riippumattomuutta toimivasta johdosta ja valvottava sisäisen valvonnan toimivuutta. (Ratsula 2016, 96-97, 100-102.)

Periaatteessa kolme toimivan johdon on luotava hallituksen alaisena rakenteet, raportointilinjat ja toimivaltuudet tukemaan tavoitteiden saavuttamista. Valvontakulttuuri koostuu johdon ja henkilöstön asenteista sekä johdon asettamista toimintaperiaatteista ja toiminnasta sisäistä valvontaa kohtaan. Hyvän kulttuurin luomisessa avainasemassa on yrityksen ylin johto, joka viestii muulle henkilöstölle omalla esimerkillään, miten tärkeänä sisäistä valvontaa pidetään organisaatiossa. Kulttuuri on tärkeä valvontaympäristön osa, johon vaikuttavat muut sisäisen valvonnan elementit, kuten missio, arvot, liiketapaperiaatteet (Code of Conduct), toimintaohjeet ja ohjeistukset, tiedonkulku sekä asenteet kuten tapa, jolla virheisiin, kontrollipuutteisiin ja väärinkäytöksiin puututaan. Rehellisyyden ja eettisten arvojen tulee olla osa organisaation jokapäiväistä toimintaa ja keskustelua. Periaatteen neljä mukaisesti organisaation on sitouduttava tavoitteisiin, osaavan henkilöstön rekrytointiin, kehittämiseen ja säilyttämiseen. Organisaation oikea tapa toimia tulee määräytyä ylimmältä johdolta. Kuitenkin viime kädessä viidennen periaatteet mukaisesti tärkeää on, että organisaatio huolehtii, että sisäisen valvonnan tavoitteet toteutuvat. Tämä tarkoittaa, että esimiehillä on tärkeä vastuu viestiä alaisilleen sisäisen valvonnan periaatteista ja yrityksen johdon määrittämistä toimintatavoista. Virheiden, väärinkäytösten ja tehottomuuden riskit kasvavat, mikäli tätä vastuuta laiminlyödään. (Ratsula 2016, 103-105.)

2.3.3 Riskien arviointi

Yritysten riskienhallinnan lähtökohta on se, että jokaisen organisaation tarkoituksena on tuottaa sidosryhmilleen arvoa. Tehokkaan riskienhallinnan avulla yhtiön johto voi hallita epävarmuustekijöitä ja siihen liittyviä ulkoisia ja sisäisiä riskejä sekä mahdollisuuksia, jolloin myös yrityksen arvoa voidaan kasvattaa turvallisemmin ja tehokkaammin. Riskienhallinta auttaa myös varmistamaan luotettavan raportoinnin sekä lakien ja määräysten noudattamisen. COSO-mallissa riskien arvioinnilla pyritään tunnistamaan ja analysoimaan

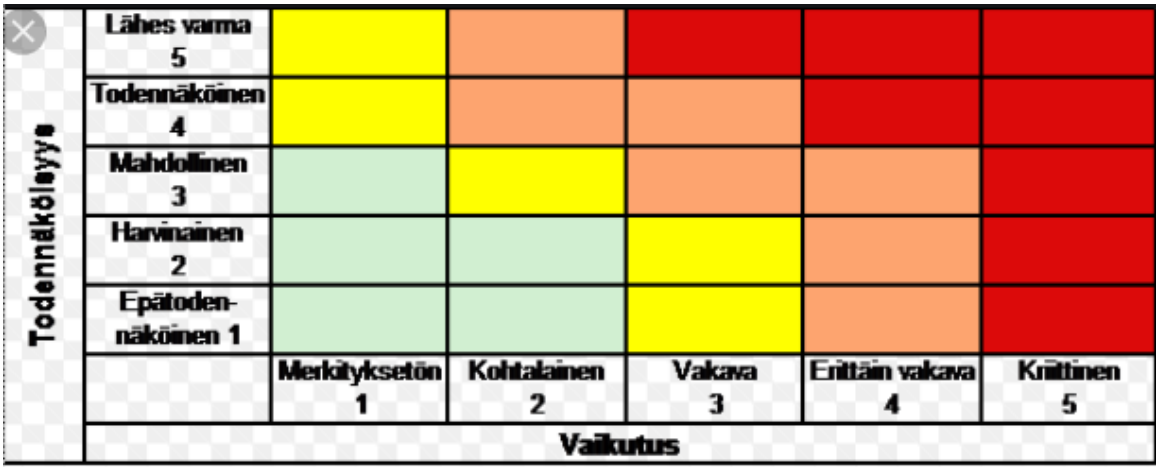
sellaiset riskit, jotka voivat toteutuessaan uhata yrityksen tavoitteisiin pääsyä tai pahimmillaan vaarantaa sen koko toiminnan. (COSO 2004.)

Organisaation riskienhallinta osana riskien tunnistamista ja analysointia on sen hallituksen, johdon ja muun henkilökunnan toteuttama jatkuva, kertautuva prosessi, jota sovelletaan strategian laadinnassa ja koko organisaatiossa. Riskienhallinnan tarkoituksena on tunnistaa organisaatioon vaikuttavia potentiaalisia tapahtumia ja pitää riskit riskinottohalukkuuden rajoissa, jotta voidaan varmistaa organisaation tavoitteiden toteutuminen. Sisäinen valvonta on organisaation riskienhallinnan olennainen osa, mutta jokainen työntekijä on oman roolinsa ja määriteltyjen vastuiden osalta vastuussa organisaation riskienhallinnan toteutumisesta. Hallitus valvoo riskienhallintaa, sekä tietää ja hyväksyy organisaation riskinottohalukkuuden. (COSO 2004.)

COSOn periaatteen kuusi mukaisesti riskikartoituksen aluksi on asetettava haluttu tavoite, jonka jälkeen pystytään tunnistamaan tavoitteita uhkaavat riskit ja mahdolliset vaaran paikat, jotka voivat olla tavoitteiden esteenä. COSO-mallin mukaan tavoitteet täytyy asettaa yrityksen eri tasoille sekä tämän lisäksi myös jokaiselle toiminnan tasolle, jolloin sillä voidaan kattaa yrityksen kaikki tasot (Kuva 3). Tällöin pystytään tunnistamaan periaatteen seitsemän mukaisesti juuri ne avaintekijät, jotka ovat kriittisiä kunkin tavoitteen kohdalla. Periaatteen kahdeksan mukaisesti organisaation on huomioitava riskinarvioinnissa väärinkäytösten mahdollisuus ja periaatteen yhdeksän mukaisesti tunnistettava ja arvioitava muutoksia, joilla voi olla merkittävä vaikutus sisäiseen valvontajärjestelmään. (Ratsula 2016, 107-117.)

Kuva 3. Riskien tunnistus ja arviointiprosessi riskitason ja tavoitteiden määrityksen jälkeen (mukaillen Ratsula 2016, 110)

Yritykset käyttävät riskien arvioinnin tukena erilaisia riskimatriiseja, joissa yhtenä elementtinä tarkastellaan riskin toteutumisen todennäköisyyttä ja toisaalta sitä, miten suuri vaikutus riskillä toteutuessaan olisi yrityksen raportoinnille. Alla olevan kuvan 4 riskimatriisin mukaan ainakin punaiselle nousseet riskit tulisi kattaa avainkontrolleja käyttäen. Myös oranssin statuksen osa-alueiden osalta on syytä tarkasti miettiä kontrollien implementointia. Alla olevassa taulukossa oranssin ja vihreiden kohtien osalta riskien toteutuminen on alhaisempaa ja toteutuessaan riskin vaikutus ei ole todennäköisesti erittäin vakava. (Turun kaupunki 2015.)



Kuva 4. Riskinarviointimatriisi (Turun kaupunki 2015)

2.3.4 Valvontatoiminnot

COSOn mukaan valvontatoiminnot ovat yrityksen vakiintuneita politiikkoja, prosesseja ja menettelytapoja, joiden avulla varmistetaan, että yritys toimii johdon asettamien tavoitteiden mukaisesti ja varmistaa, että tarvittaviin toimiin on ryhdytty riskien tunnistamiseksi ja niiden toteutumisen estämiseksi. (COSO 2013.)

Toimintaperiaatteet antavat suuntaviivat sille, mitä pitäisi tehdä, toimintatavat taas ovat osa käytännön toimenpiteitä ja kontrolleja, joiden avulla toimintaperiaatteiden toteutumien määritellään. Periaatteen kymmenen mukaisesti organisaation toimintojen ja prosessien eri kohtiin sekä teknologiseen ympäristöön sijoitetaan näitä valvontatoimenpiteitä, joiden tavoitteena on vastata toimintoihin, prosesseihin ja teknologiaan kohdistuviin riskeihin. (Ratsula 2016, 119-120.)

Valvontatoimenpiteet voivat olla ehkäiseviä, paljastavia, automaattisia, manuaalisia tai johtamiskontrolleja ja ne voidaan jakaa myös erilaisten valvontatavoitteiden perusteella. Eri tasoilla toteutettavat kontrollit kohdistuvat usein eri tyyppisiin asioihin. Kontrollit, jotka

toteutetaan ylimmällä tasolla sisältävät monesti analyyttisia tarkasteluita, joissa tietyn ajanjakson suoritusta verrataan budjetteihin, kilpailijoihin, ennusteisiin sekä historiatietoihin. Tällöin ylätasolla pyritään selvittämään, missä laajuudessa tavoitteet on saavutettu ja löytämään merkittäville poikkeamille selityksiä. Alemman tason kontrollit kohdistuvat yksittäisiin liiketapahtumiin, joiden avulla pyritään tarkistamaan liiketoimien paikkansapitävyyttä, loppuunsaattaminen ja toimintavaltuuksia. (Ratsula 2016, 122-125.)

Organisaatio valitsee ja kehittää yleisiin tieto- ja muihin teknologioihin kohdistuvia valvontatoimenpiteitä, jotka tukevat tavoitteiden saavuttamista periaatteen yksitoista mukaisesti. Johdolla on oltava ymmärrys siitä, mitä riippuvuussuhde prosessikontrollien, automaattikontrollien sekä IT-kontrollien välillä tarkoittaa ja kehitettävä IT-infrastruktuuriin liittyviä kontrolleja. Johto valitsee ja kehittää tietojärjestelmien käyttäjäoikeuksien rajaamiseen liittyviä kontrolleja sekä valitsee ja kehittää IT-järjestelmien hankkimiseen, kehittämiseen ja ylläpitämiseen tarvittavia kontrolleja. (Ratsula 2016, 126.) Alla oleva kuva 5 esittää riskien arviointiprosessia riskitason ja tavoitteiden määrityksen jälkeen.

Kuva 5. Riskien arviointiprosessi (mukaillen Ratsula 2016, 122-127)

Periaatteen **kaksitoista** mukaan yhtiön politiikkojen ja ohjeistusten tulee olla kirjallisia, ajantasaisia, helposti saatavilla ja ymmärrettäviä. Näistä muodostuu yhteiset pelisäännöt, jotka viestittävät työntekijöille mikä on sallittua ja mikä ei. Valvontatoimenpiteiden dokumentointi riippuu organisaation koosta, rakenteesta ja johdon asettamista periaatteista. Yleiset toimintaperiaatteet, kuten hyväksymiskäytännöt, yleiset laskentaperiaatteet, hinnoittelukäytännöt ja matkustusohjesäännöt, ovat useimmiten olemassa kirjallisina dokumentteina. Kirjallinen dokumentointi ei kuitenkaan takaa, että toimintaperiaatteita aina noudatetaan, mutta myös kirjoittamaton vakiintunut käytäntö voi toimia organisaatiossa, jossa se on juurtunut toimivaksi ja henkilöstön sisäistämäksi käytännöksi. Tärkeintä on,

että olemassa olevista valvontatoimenpiteistä ja niiden kehittämistarpeista ollaan tietoisia siellä missä kuuluukin. (Ratsula 2016, 126-128.)

2.3.5 Informaatio ja kommunikaatio

Yrityksessä työskentelevillä henkilöillä pitää olla tarvittava ja olennainen tieto käytettävissä ja se on voitava omaksua, kyetäkseen huolehtia työtehtävistä ja omasta roolista tärkeänä osana sisäistä valvontajärjestelmää. Johto käyttää sekä sisäisistä että ulkoisista lähteistä tulevaa oikeaa ja laadukasta informaatiota, joka tukee sisäisen valvonnan seurantaa. Tietojärjestelmät tuottavat raportteja, joiden sisältämän tiedon avulla ohjataan liiketoimintaa. Ne käsittelevät tietoa myös ulkoisista tapahtumista, toiminnasta ja olosuhteista sisäisesti luodun tiedon lisäksi. (Ratsula 2016, 130.)

COSOn kolmannentoista periaatteen mukaisesti organisaatio hankkii tai tuottaa ja käyttää relevanttia, laadukasta informaatiota, joka tukee sisäisen valvonnan toimintaa. Fokusalueet, jotka kuvaavat kyseisen periaatteen sisältöä ovat informaatiovaatimusten tunnistaminen, eli tietyn prosessin mukaisesti tunnistetaan tarvittava tieto, joka tukee muiden sisäisen valvonnan osa-alueiden toimintaa tavoitteiden saavuttamisessa. Tietoa on lisäksi voitava tallentaa sisäisistä sekä ulkoisista lähteistä sekä tietojärjestelmien tuottavan datan muuntaminen käyttökelpoiseksi informaatioksi on varmistettava. Tärkeää on tietojärjestelmien tuottaman tiedon laadun säilyttäminen läpi tiedonkeruuprosessin, jonka kustannukset ja hyödyt on huomioitava suhteessa tavoitteiden saavuttamiseen. Sisäisen kommunikaation avulla tietoa levitetään organisaation joka tasolle ja tällä on tarkoitus johtaa ja ohjata toimintaa kohti asetettuja tavoitteita. Kommunikaatiossa henkilöstö saa ylimmältä johdolta selkeän viestin sisäisen valvonnan tärkeydestä ja johto taas asetettujen tavoitteiden toteutumisesta. Kommunikaatiota käytetään erilaisten taloudellisten ja ei-taloudellisten raporttien koostamiseen, operatiiviseen ja strategiseen päätöksentekoon sekä toiminnan seuraamiseen. Informaatiota saadaan useissa eri muodoissa useista eri lähteistä. Sisäisiä tietolähteitä ovat esimerkiksi sähköpostiviestintä, kokousten pöytäkirjat ja muistiot, asiakaskyselyt, henkilöstökyselyt ja eettinen ilmoituskanava. Ulkoisia tietolähteitä ovat esimerkiksi toimialakohtaiset tutkimusraportit, sosiaalinen media ja messut. (Ratsula 2016, 131-132.)

COSOn periaatteen neljätoista mukaan organisaation on viestittävä sisäisesti tietoa kuten sisäisen valvonnan tavoitteet ja vastuut, tämä varmistaa sisäisen valvonnan toiminnan tehokkuuden. Organisaation viestintäprosessin tavoite on taata, että koko organisaatio saa tietoa, jonka avulla ymmärretään sisäisen valvonnan vastuu vaatimusten suhteen sekä toimitaan ohjeistuksen mukaisesti. Johto sekä hallitus keskustelevat, jotta kummallakin on

käytettävissä kaikki asiaan liittyvä tarpeellinen tieto. Erilaiset kommunikointiväylät, kuten esimerkiksi eettiset kommunikaatioväylät varmistavat, että henkilöstö voi tuoda esiin epäkohtia ja huoliaan vaikkapa anonyymisti. Miettiessä mitä kommunikaatiovälineitä ja metodia käytetään, tulee ottaa huomioon kohdeyleisö, ajoitus ja kyseisen tiedon luonne. Läpi koko henkilöstön annetun tiedon tulisi kattaa yhtiön politiikat ja toimenpiteet, organisaation tavoitteet eri tasoilla, tietoa viestinnän tärkeydestä ja hyödyistä. Kommunikaation on myös katettava kontrollien toteuttamisvastuut, henkilöstön velvollisuuden kommunikoida yhtiötasolla ylös, alas ja poikittain kaikista valvonnan puutteista ja toimintaperiaatteita vastaan tehdystä toiminnasta. (Ratsula 2016, 133-135.)

Organisaatio viestii periaatteen viisitoista mukaan ulkoisten sidosryhmien kanssa asioista, joilla on vaikutusta sisäisen valvonnan toimivuuteen. Näihin ryhmiin kuuluvat konsultit, tilintarkastukset ja tarkastusraportit, asiakaspalaute koskien palvelun laatua ja virheellisiä tositteita, uudet lait ja asetukset ja niiden muutokset, viranomaisten organisaatiota koskevat tiedot, toimittajien palaute esim. maksamattomista laskuista sekä sosiaalisen median kautta tulleet yhteydenotot ja kirjoitukset. (Ratsula 2016, 138-139.)

2.3.6 Seuranta ja valvonta

Seuranta eli prosessi, jonka avulla arvioidaan sisäisen valvontajärjestelmän toimivuutta ja laatua, on olennainen osa sisäistä valvontaa. Seurantaa toteutetaan jatkuvilla seurantatoimenpiteillä ja erillisillä arvioinneilla sekä niiden molempien yhdistelmillä. Jatkuva seuranta toteutuu osana jokapäiväistä esimiesten sekä johdon ohjausta ja valvontarutiineja. Erilliset, kausittain toteutettavat arvioinnit vaihtelevat laajuudeltaan ja esiintymistiheydeltään riippuen riskiarvioinnista, jatkuvan seurannan tehokkuudesta sekä muun johdon harkintaan vaikuttavista tekijöistä. Seurannan tarkoituksena on arvioida kuinka organisaatiossa toteutunut toiminta vastaa lainsäädännöllisiin tai organisaation itse laatimiin periaatteisiin, kuten politiikkoihin ja toimintaohjeisiin. Johdolle sekä tarvittaessa hallitukselle esitetään seurannan tuloksena tuotetut havainnot. (Ratsula 2016, 140.)

COSOn periaatteen kuusitoista mukaisesti organisaation prosessien sisään tulee rakentaa jatkuvia seurantatoimenpiteitä, joiden ollessa riittävän laajoja ja tehokkaita, tarvitaan erillisiä arviointeja vähemmän. Sisäisen valvonnan nykytila on seurannan lähtökohta, mutta muutokset liiketoiminnassa ja organisaation prosesseissa on huomioitava seurantakeinoja päivitettäessä ja valittaessa. Riskiarvio on oltava perustana arviointien laajuutta ja toteuttamisfrekvenssiä päätettäessä. (Ratsula 2016, 141.)

Jatkuvaan seurantaan kuuluu säännönmukaiset johtamis- ja ohjaustoimet, vertailut, täsmäytykset ja muut rutiinitehtävät. Sisäisen valvonnan tehokkuuden todisteita saadaan esimerkiksi poikkeamien analysoinnin ja talousraportoinnin tuloksena. Esimiesten tekemä päivittäinen ohjaus on myös tärkeä osa jatkuvaa seurantaa, sillä esimiehen tulee tietää missä mennään. Jatkuvat valvontatoimenpiteet toimivat reaaliaikaisesti, reagoivat muuttuviin olosuhteisiin ja ovat osa yritystä, kun ne on rakennettu yrityksen normaaleihin, toistuviin toimintarutiineihin. (Ratsula 2016, 141.)

Erillisiä arviointeja tehdään tärkeisiin kohteisiin, jotka ovat ennalta valittuja. Mikäli toimintaympäristössä on tapahtunut muutoksia tai kohteeseen kohdistuu korkeampi riski verrattuna muihin kohteisiin, voidaan se ottaa arvioitavaksi. Erilliset arvioinnit voidaan suunnata yksittäisiin valvontatoimiin tai koko valvontajärjestelmään. Koko valvontajärjestelmään suunnattu arviointi on tarpeen silloin, kun yrityksessä on meneillään merkittävä johtamismuutos, uusi suuri hankinta tai käyttöönotto tai merkittäviä muutosvaatimuksia taloudellisen informaation tuottamisessa. Yksittäisten valvontatoimien arvioinnissa keskitytään yksittäisten kontrollien tai prosessien tai niiden osien arviointiin. Erillistä arviointia voidaan toteuttaa esimerkiksi sisäisen tarkastuksen- ja sisäisen valvontaosaston sekä vertaisarvioinnin keinoin. Arvioinnissa voidaan käyttää benchmarking-vertailua, jossa verrataan yrityksen valvontatoimia muiden yritysten vastaaviin toimiin tai itsearviointia, joka on kuitenkin aina muita menetelmiä subjektiivisempaa. (Ratsula 2016, 142-143.)

COSOn periaate seitsemäntoista velvoittaa organisaatiota arvioimaan sisäisen valvonnan puutteita ja kommunikoimaan ne oikeille tahoille, jotka ovat vastuussa korjaavista toimenpiteistä ja tarpeen vaatiessa myös ylimmälle johdolle ja hallitukselle. Sisäisen valvonnan arvioinnin tavoitteena on tuottaa tietoa organisaation sisäisen valvonnan tilasta ja kehittämismahdollisuuksista. Arvioinnin onnistumisen mittarina toimii se, kuinka hyvin saadaan positiivista muutosta aikaan. Kehitystoimenpide voi olla esimerkiksi yhden työtehtävän muokkaaminen, mutta toisinaan se voi olla koko prosessin kehittäminen ja muuttaminen. Kontrollipuutteet ja kehitysehdotukset tulee esittää selkokielellä ja niiden on oltava tarpeeksi konkreettisia, jotta ymmärretään saavutettavat hyödyt ja ne nähdään toteuttamiskelpoisina. Muutostoimenpiteille nimetään vastuuhenkilö ja aikataulu, jonka toteutumista seurataan aktiivisesti. On erittäin tärkeätä seurata, että sovittuja korjaavia toimenpiteitä todella tehdään ja mikäli näin ei ole, on puutteista raportoitava ylöspäin esimiehelle. Hallitukselle ja tarkastusvaliokunnalle raportoidaan merkittävimmistä puutteista, joiden korjaamisesta laaditaan suunnitelma, jota seurataan ja jonka toteutuminen on varmistettava. (Ratsula 2016, 144-145.)

2.4 COSO-ERM 2017 uusi strategiaan perustuva riskienhallintamalli

COSO-ERM (ERM=Enterprise Risk Management) -viitekehys julkaistiin alun perin 2004, versiossa korostui riskienhallinnan sekä sisäisen valvonnan välinen suhde, riskienhallinta nähtiin vahvasti compliance-työkaluna. Aiemmin riskien hallinta oli compliance- ja sisäisen valvonnan työkalu. Päivitetyn mallin merkittävin muutos on, että riskienhallinta kuvataan liiketoimintaa tukevana toimintana. Tämä auttaa ja ohjaa strategian laadinnassa sekä toteutuksessa. (Noukka 18.10.2017.)

Päivitetyn COSO-ERM:in periaatteena on käyttää riskienhallintaa tukemaan strategian määritystä. Keskusteluun on tullut viitekehyksen myötä kaksi uutta näkökulmaa:

1. Onko strategia linjassa organisaation vision ja mission kanssa?
2. Kykeneekö yhtiö kantamaan määriteltyjen riskiprofiilien mahdolliset seuraukset?

COSO-ERM:in mukaan riskienhallinnan tulisi olla mukana strategiaprosessia jo hyvin varhaisessa vaiheessa, jotta voidaan ymmärtää, sopiiko yrityksen riskiprofiili sen omaan riskinottohalukkuuteen. Strategian määrityksen jälkeen riskienhallinta tunnistaa asioita jotka voivat haitata strategian toteuttamista. (Noukka 18.10.2017.) Kuva 6 kuvaa päivitettyä strategian ja riskienhallinnan yhteyttä:

Kuva 6. COSO-ERM ja strategia (COSO 2017, 5)

Vanha COSO malli on kuvattu kuutiona, joka on nyt korvattu graafisella ilmeellä. Uutta kuvaa on helpompi tulkita kuin kuutiomallia joka on esitetty aiemmin kuvassa 1. COSO-ERM mallissa on viisi osa-aluetta jotka jakautuvat 20 periaatteeseen. (Noukka 18.10.2017.) Uusi malli esitetään kuvassa 7.

Kuva 7. Uudistettu COSO-ERM viitekehys (COSO 2017, 6)

Päivitetty COSO-ERM antaa yhtiön riskienhallinta-, compliance- ja tarkastustyöntekijöille parannellun työkalun viestiä yhtiössä, miksi riskienhallinta on tärkeä osa strategista suunnittelua ja miksi yhtiön riskienhallintaa tulisi uudistaa. Tämän lisäksi COSO-ERM painottaa riskien määrittelyssä kvantitatiivisia (määrällisiä) menetelmiä. COSO-ERM:ssä puhutaan esimerkiksi riskiprofiileista ja -käyristä. Viitekehyksen uudistukset ovat pieniä, joten yhtiöllä ei kuitenkaan ole välitöntä tarvetta uudistaa riskienhallintaprosessia ja tähän liittyvää dokumentointia. Päivitetty COSO-ERM kuitenkin auttaa parantamaan yhtiön riskienhallintaa ja antaa sille hyvän perustan. (Noukka 18.10.2017.)

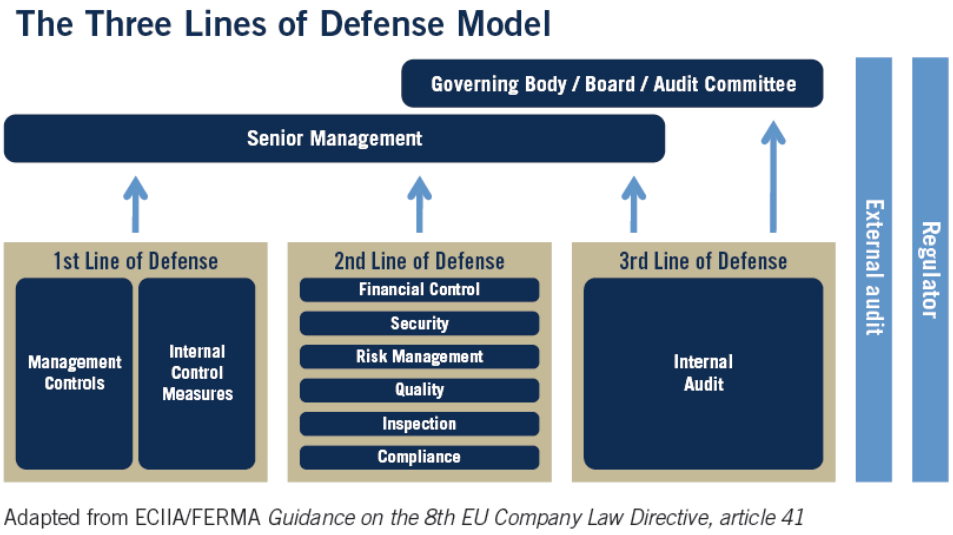
3 Sisäinen valvonta osana johdon hallintojärjestelmää

3.1 Sisäisen valvonnan hallinnointimalli

Sisäisen valvonnan hallinnointimallista käytetään lähteestä riippuen nimitystä ohjaus- tai hallintomalli joista kummallakin tarkoitetaan samaa asiaa. Hallinnointikoodi määrittää mitä hallinnointimallin tulee sisältää. Sisäisen valvonnan hallinnointimalli koostuu sisäisestä valvonnasta (internal control) ja sisäisestä tarkastuksesta (internal audit). Sisäinen tarkastus on riippumaton elin, joka tukee yhtiön hallitusta ja ylintä johtoa. Sisäisen tarkastuksen tehtävänä on olla johdon tukena organisaation kehittämisessä ja asetettujen tavoitteiden saavuttamisessa. Kansainvälinen ohjeistus ohjaa sisäistä tarkastusta ja sen työ kohdistuu yhtiön sisäiseen valvontaan, riskienhallintaan sekä johtamis- että hallinnointiprosessiin. Ulkoinen valvonta taas pitää sisällään tilintarkastajat ja -tarkastuksen. Kolme puolustuslinjaa on hyvän hallinnointimallin kulmakivi. (Ratsula 2018.)

3.1.1 Kolme puolustuslinjaa

Toimivaksi sisäisen valvonnan ohjausmalliksi on laajasti havaittu ns. kolmen puolustuslinjan (Three Lines of Defense, kuva 8) malli, jossa ensimmäisenä elimenä toimii yhtiön hallitus, joka vastaa siitä, että riskienhallinnan valvonta toteutuu yrityksessä suunnitelman mukaisesti. Toista puolustuslinjaa edustaa riskienhallintaan erikoistunut asiantuntijaorganisaatio, joka toteuttaa ja valvoo käytännössä johdon asettamia tavoitteita. Kolmantena osapuolena toimii yrityksen sisäisen tarkastus, joka on riippumaton elin ja valvoo sisäisen laskennan toimivuutta yrityksessä. (The Institute of Internal Auditors 2013.)



Kuva 8. Three Line of Defense, Kolmen puolustuslinjan malli (The Institute of Internal Auditors 2013, 2)

Yhtiön operatiivinen johto edustaa **ensimmäistä puolustuslinjaa** ja on vastuussa tavoitteiden määrittelystä ja riskienhallinnan kokonaisvaltaisesta järjestämisestä. Käytännössä johdon nimeämä yleensä operatiivinen riskiasiantuntijaorganisaatio vastaa riskien arvioinnista, valvonnasta, riskien minimoinnista ja määriteltyjen kontrollien jalkauttamisesta sekä kontrolliaktiviteettien tehokkaasta suorittamisesta. (The Institute of Internal Auditors 2013.)

Toisena puolustuslinjana toimii riskienhallintaan erikoistunut asiantuntijaorganisaatio, joka johtaa ja valvoo operatiivisen johdon riskienhallintapolitiikkojen toimeenpanoa sekä kontrollien suorittamista, koordinoi riskien määrittelyprosessia sekä vastaa johdon raportoinnista, esimerkkinä asiantuntijaorganisaatiosta voidaan mainita sisäinen valvonta ja riskienhallinta tiimit. Toisen puolustuslinjan tehtäviin kuuluu sisäisessä valvonnassa käytettävien työkalujen kehitys ja hallinnointi. Toisen puolustuslinjan rakenne vaihtelee organisaatiokohtaisesti. (The Institute of Internal Auditors 2013.)

Kolmas puolustuslinja on sisäinen tarkastus, joka on riippumaton funktio ja raportoi suoraan yhtiön ylimmälle johdolle ja omaa raportointikanavan myös yhtiön hallitukselle. Sisäisen tarkastuksen rooli on arvioida sisäisen valvonnan ja riskienhallinnan toimivuutta ja sitä kuinka ensimmäinen ja toinen puolustuslinja toimivat. ECIIA 2013 (European Confederation of Institutes of Internal Auditing), sisäisen tarkastuksen kansainvälisen kattojärjestön mukaan sisäisen tarkastuksen riippumattomuus ja objektiivisuus erottavat sen muista puolustuslinjoista. (The Institute of Internal Auditors 2013.)

3.2 Sisäisen valvonnan elementtien tunnistaminen, kehittäminen ja dokumentointi

Sisäinen valvonta on tärkeä osa yhtiön johtamisjärjestelmää. Mikäli yritys listautuu pörssiin, tarve kehittää ja arvioida sisäistä valvontaa voi olla lakisääteistä tai suositusten sanelemaa. Tarve kehittää sisäisen valvonnan prosessia voi johtua siitä, että toiminnassa on havaittu vakavia puutteita, rikkomuksia tai väärinkäytöksiä. Kun yrityksen käytännön toimet osoittavat, että sisäisen valvonnan rutiinit on implementoitu osaksi jokapäiväistä työtä, on tällä positiivinen vaikutus yrityskuvaan, brändiin ja muihin yhteistyökumppaneihin. Tämä viestittää sijoittajille, toimittajille, asiakkaille, työntekijöille ja -hakijoille sekä muille sidosryhmille sekä yhteistyökumppaneille, kyseisen yhtiön sisäinen valvonta toimivuudesta luoden luottamusta yhteistyön pohjalle. (Ratsula 2016, 146.)

3.2.1 Sisäisen valvonnan kehittämishankkeet

Lisääntynyt tarve kehittää sisäistä valvontaa on käynnistänyt monissa yrityksissä sisäisen valvonnan kehittämishankkeita, joiden kautta nähdään tarve parantaa myös yrityksen ydinprosesseja ja niihin liittyvää kontrollointia. Kyseisien kehittämisprojektien tavoitteena

on yrityksen kulttuurin, toimintatapojen, prosessien ja kontrollien läpikäynti uudelleenarviointi riskianalyysin näkökulmasta, selkeyttämien ja tehostaminen. Yrityksillä on tarve saada suurempi varmuus, että asioita tehdään oikein, tehokkaasti ja yritysten tavoitteiden ja lainsäädännön velvoitteiden mukaisesti. Lisäksi raportoitavan tiedon on oltava oikeansisältöistä ja luotettavaa. Sisäinen valvonta on osa yhtiön governance -mallia vaikkakin se on erilainen eri yrityksissä. Projektin alkuvaiheessa on hyvä konkretisoida mitä kaikkea haluttu sisäinen valvonta kattaa ja tässä työssä voidaan käyttää esimerkiksi COSO-viitekehystä, jonka avulla sisäinen valvonta ja sen eri osa-alueet voidaan ymmärrettävästi kuvata auki. Dokumentointivaiheessa on hyvä kuvata ensin olemassa oleva tilanne AsIs ja sen jälkeen arvioida mitä komponentteja tulee vahvistaa ja luoda uusi ToBe -malli. (Ratsula 2016, 146-147.)

Lähtökohtana kehitysprojektille voi olla, mitä projektilla halutaan saavuttaa. Halutaanko kattaa vain lakisääteiset minimivaatimukset, jolloin kuitenkin vaarana voi olla valvonnan jääminen pintapuoliseksi, vai ajatellaanko alusta asti kehitysprojektia liiketoiminnan ja sisäisten prosessien kehittämisen näkökulmasta, jolloin sisäinen valvonta olisi osana koko yhtiön johtamisjärjestelmää. Tämän kaltainen ajattelu on osa kokonaisvaltaista riskienhallintaa ja mitä paremmin prosessit on tunnistettu, sitä varmemmin tiedetään miten ne toimivat. Läpinäkyvyys eri prosessien ja osastojen välillä lisääntyy, kun riskiymmärrys kasvaa. Kehityshankkeessa on tärkeää huomioida, että kehityskustannukset korreloivat saatua hyötyä. Kuva 9 havainnollistaa kehityshankkeen kulkua. (Ratsula 2016, 146-147.)

Kuva 9. Sisäisen valvonnan kehitysprojektin vaiheet (mukaillen Ratsula 2016, 148)

3.2.2 Yritystason kontrollit

Ohjausympäristö muodostaa perustan sisäiselle valvontajärjestelmälle ja tämä on olennainen osa yritystason kontrolleja. Näitä kontrolleja on jokaisella, mutta kaikki eivät ole tunnistaneet niitä kontrolleiksi eikä niitä ole kuvattu. Kuva 10 havainnollistaa kontrollin kuvausta. Tällaisia organisaation hallintopolitiikkoja ja toimintomalleja ovat esimerkiksi yhtiön hallitus, johtoryhmä, tarkastusvaliokunta, palkitsemisvaliokunta sekä yrityksen liiketapaperiaatteet (Code of Conduct, joissa määritellään yrityksen yleiset linjaukset koskien odotuksiin henkilöstön ja liikekumppaneiden käyttäytymisen osalta). (Ratsula 2016, 149-150.)

Kuva 10. Esimerkki yritystason kontrollin dokumentaatiosta (mukaillen Ratsula 2016, 150)

Yhtiötasolla olevia kontrolleja kutsutaan myös nimellä yksikkötason kontrollit eli Entity Level Controls (ELC) jotka ovat koko organisaatiota koskevia kontrolleja. Yhtiötason kontrollit eivät edusta itsessään tehokasta valvontajärjestelmää, mutta ne muodostavat kontrolliympäristön, jossa prosessikontrollit voivat toimia tehokkaasti. Yhtiötason kontrollit liittyvät tyypillisesti kontrolliympäristön tärkeimpään “Tone at the Top” osa-alueeseen, joka tarkoittaa ja määrittelee yrityksen johtajuuden ja johdon sitoutumisen avoimuuteen, rehellisyyteen, lahjomattomuuteen ja eettiseen käyttäytymiseen. ”Tone at the top” määritelmän arvoja on noudatettava yhtiön jokaisella organisaationtasolla. Yhtiötason kontrolleja ovat tyypillisesti johdon organisaatiolle määrittämät roolit ja valtuutukset, jotka on määritetty ti-

linkäyttöoikeuksien ja hyväksymisrajojen kautta (Delegation of Authority). Muita yhtiötasolla olevia kontrolleja ovat politiikat, ohjeet sekä yhtiökohtaiset ohjelmat kuten esimerkiksi menettelyohjeet (Code of Conduct). (Edelkoort Smethurst Schein 2010.)

Code of Conduct eli eettinen ohjeisto tarkoittaa organisaation omia hyvän liiketavan periaatteita tai eettisiä pelisääntöjä. Se on organisaation itseään varten laatima itsenäinen dokumentti, joka ohjaa organisaation johdon sekä työntekijöiden nykyistä ja tulevaa toimintaa kohti asetettuja tavoitteita. Eettinen ohjeisto tai eettiset periaatteet auttavat organisaatiota toimimaan vakuuttavasti sekä turvallisesti verkottuneessa ja kansainvälisessä ympäristössä. Muita yksikkötason kontrolleilla katettuja osa-alueita ovat johdon riskienhallintaprosessit, keskitettyjen ja harmonisoitujen prosessien ja kontrollien kehittäminen ja noudattaminen. Nämä kontrollit voidaan luokitella ehkäiseviin ja paljastaviin kontrolleihin toiminnallisuutensa perusteella. (Edelkoort Smethurst Schein 2010.)

3.2.3 Avainprosessit ja prosessikontrollit

Yritystason kontrollien kuvausten jälkeen on tunnistettava avainprosessit ja määriteltävä riskikartoituksen avulla tarpeelliset prosessikontrollit. Tyypillisiä avainprosesseja ovat esimerkiksi osto-, valmistus-, varasto-, tuotekehitys- ja myyntiprosessi. Tärkeitä kontrolleja liittyy myös kirjanpitoon, raportointiin ja henkilöstöhallintaan kuten myös IT-prosessiin liittyviä kontrolleja. (Ratsula 2016, 152-153.)

Tärkeää prosessien tunnistamisessa on ymmärtää koko prosessiketjua eli puhutaan end-to-end prosessin tunnistamisesta, joka voi koostua useasta osaprosessista. Kuvaamalla prosesseja kokonaisvaltaisesti syntyy parempi kuva kokonaisuudesta. Ymmärretään paremmin mahdollisia puutteita ja helpotetaan prosessien harmonisointia, jonka mukaan koko yhtiön tulisi toimia. Prosessikuvauksella voidaan välttyä päällekkäiseltä työltä, tahallisilta tai tahattomilta virheiltä ja ongelmatapauksien selvitys helpottuu, kun ymmärretään missä prosessinvaiheessa ongelma ilmenee. Prosessikontrolleja käytetään ennalta ehkäisemään, todentamaan ja havaintojen perusteella kehittämään riskeihin liittyviä prosesseja ja kontrolleja ja näin ollen vähentämään yhtiön prosesseihin ja transaktioihin liittyviä kontrollipuutteita. (Ratsula 2016, 152-153.)

Tyypillisiä prosessikontrolleja ovat tuloksen tarkastelu, esimerkiksi controllerin tai johdon käydessä lukuja läpi säännöllisesti vertaillen budjettiin, aikaisempien kausien toteumaan. Fyysiset kontrollit, esimerkiksi pääsyn estäminen johonkin tilaan tai vaihto-omaisuuden inventointi. (Honkaranta 23.8.2017.)

Tase-eriin liittyviä järjestelmiä, prosesseja ja niihin liittyviä tyypillisiä kontrolleja jotka tulee dokumentoida ovat kirjanpidon täsmäytykset, joissa tulee säilyttää kirjausketju (audit trail). Dokumentaatioon liittyy myös täsmäytyslaskelmien tekeminen. Kontrollit jotka liittyvät fyysiseen olomuotoon kuten että tuotantokoneiden käyttöön on sallittu vain ennalta määrätylle henkilölle tai yhtiön tuotantotilat sekä järjestelmät on lukittu ulkopuolisilta. Hyödykkeet on merkitty tunnisteilla jotka löytyvät yrityksen toiminnanohjausjärjestelmästä. Vaihto omaisuuteen liittyviä avainkontrolleja ovat varastolistojen täsmäyttäminen kirjanpidossa ja inventaariolla varmistetaan varaston ajantasaisuus ja todenmukaisuus. (Honkaranta 23.8.2017.)

Yhtiön kontrolleihin kuuluvat myös käytännöt, esimerkiksi on sovittu etukäteen millä perusteella laina myönnetään, kenen toimesta tämä tapahtuu ja kenelle voidaan myöntää lainaa. Tähän kuuluu oleellisena osana dokumentaation tallentaminen kuten tässä tapauksessa lainasopimukset. Siirtosaamisiin ja siirtovelkoihin kuuluvat jaksotukset perustuvat usein arvioihin ja laskelmiin, joita varten tarvitaan riittävä taustadokumentaatio. Laskelmat tulee käydä läpi toisen henkilön toimesta ja näille on hyvä olla olemassa ennalta määrätty hyväksymiskäytäntö. (Honkaranta 23.8.2017.)

Kontrollit jotka liittyvät rahaan ja pankkisaamisiin ovat tärkeitä, tästä syystä yrityksen on tärkeä määrittää, kenellä on pääsy pankkijärjestelmään tai tilinkäyttöoikeudet. Nämä oikeudet tulee rajata ja käydä läpi riittävän usein. Tähän liittyy myös olennaisena osana maksuliikenteen seuraaminen ja kontrolloiminen asiattomaan rahankäyttöön liittyen. Osakirjanpidolla seurataan ostovelkoja ja niihin liittyen on usein eriytetty tehtävät niin että sama henkilö ei tarkista ja maksa laskua. Riskien kontrolloimiseksi on tarpeen myös määritellä hyväksymisrajat. Myös prosessikontrollit kuten yksikkötason kontrollit voidaan luokitella ehkäiseviin ja paljastaviin kontrolleihin. (Honkaranta 23.8.2017.)

3.2.4 Avainkontrollien tavoitteet, tunnistaminen, dokumentointi ja omistajuus

Tärkeimpien prosessien tunnistamisen sekä kuvauksen jälkeen on mietittävä mitkä ovat prosessin eri osa-alueiden tärkeimmät tavoitteet, mitkä riskit voivat vaikeuttaa tavoitteiden toteutumista ja suunnitella millä valvontatoimilla eli kontrolleilla voitaisiin estää kyseisten riskien toteutuminen. Yrityksen valvontatoimintojen kontrollit eivät ole samanarvoisia vaan osa niistä koetaan tärkeämmäksi kuin toiset. Tämä luokittelu tehdään yleensä riskimatriisin avulla, jolla pyritään luokittelemaan riskit eri tasoihin. Korkean tason riskien kattamiseen määritellään avainkontrollit, joiden tarkoituksena on tuottaa luotettavaa tietoa yrityksen sisäisen valvonnan sen hetken tilanteesta ja tehokkuudesta. Valittujen kontrollien tu-

lisi antaa kattava kuva valvontajärjestelmästä ja kattaa kaikki merkittäviin kirjanpidon tileihin liittyvät riskit, joiden toteutuminen voisi olennaisesti vääristää yhtiön taloudellista raportointia. Vaarana on liian monen avainkontrollin valinta, jolloin se voi heikentää valvonnan tehokasta tarkastelua. (Ratsula 2016, 155-157.)

Kontrollien dokumentointi tuo arvokasta tietoa yrityksen prosesseista ja niihin liittyvistä kontrolleista. Yhtiön politiikkojen, vuokaavioiden, riski- ja kontrollimatriisien avulla henkilöstö ymmärtää paremmin työnkuvansa, roolinsa ja vastuunsa sekä linkityksen muiden työhön. Prosessi- ja kontrollikuvaukset voivat toimia tarkistuslistoina, että kaikki omaan työhön mukaan luetut kontrollit on suoritettu. Tarkat prosessi- ja kontrollikuvaukset auttavat henkilöä suoriutumaan työstään ohjeiden mukaisesti ja ovat korvaamaton tuki esimerkiksi poissaolotilanteessa, jolloin tuuraaja pääse paremmin selville kyseisen työn vaatimuksista. Dokumentoinnin avulla on myös helpompi seurata kontrollien toimivuutta. (Ratsula 2016, 156-158.)

Kontrollijärjestelmä voi toimia tehokkaasti COSOn mukaan, vaikkei kontrolleja olisikaan dokumentoitu, mutta dokumentaatiosta on havaittu olevan paljon etuja. Kontrollien omistajuus ja omistajien vastuut on selkeästi määriteltävä jo kontrollien tunnistamisen ja dokumentoinnin yhteydessä. Omistaja tulisi olla taho, jolla on kokonaisvaltainen vastuu kontrollien implementoinnista. Kontrollien omistajat ovat tärkeitä kumppaneita sisäisen valvonnan osastolle sekä sisäiselle tarkastukselle kontrollitestauksien yhteydessä. Kontrollin omistajalla on vastuu tunnistaa eri sidosryhmät, joiden on osallistuttava kontrollikoulutuksiin, vastuu kouluttamisesta ja vastuu esimiehenä ymmärtää ja jalkauttaa kaikki yhtiön tärkeät politiikat ja ohjeet omille alaisilleen. (Ratsula 2016, 158-159.)

3.2.5 Sisäisen valvonnan arviointi

Sisäisen valvontajärjestelmän toimivuutta ja laatua tulee seurata ja arvioida jotta tiedetään miten toteutunut toiminta vastaa lainsäädännön tai organisaation politiikkojen ja toimintaohjeiden asettamia vaatimuksia. Tulosten pohjalta ryhdytään tarpeen vaatiessa korjaaviin toimenpiteisiin. Tilintarkastajat ja sisäinen tarkastus arvioivat sisäistä valvontaa ja ne voidaan toteuttaa myös itsearviointina, vertaisarviointina tai jatkuvalla poikkeumien raportoinnilla. Ulkoinen tarkastus hoitaa valvonnan osana tilintarkastusta, jossa arvioidaan, voidaanko sisäisen valvonnan olevan riittävä tuottamaan kohtuullinen varmuus tilinpäätöksen oikeellisuudesta. Tilintarkastajat tarkastelevat asiaa myös kansanvälisten tilinpäätös standardien näkökulmasta. (Ratsula 2016, 161.)

Sisäinen tarkastaja valvoo asiaa osana sisäistä tarkastusta ja heidän työtään voidaan pitää riippumattomana ja objektiivisena. Sisäinen tarkastus tekee yhteistyötä esimerkiksi kontrollerien, lakiosaston ja eri osastojen asiantuntijoiden kanssa ja heidän tarkastuksensa on suunnitelmallista ja strukturoitua toimintaa. (Ratsula 2016, 161.)

Arviointitapana voidaan käyttää myös vertaisarviointia, jossa asiantuntijat kiertävät arvioimassa toistensa suoriutumista tai kontrolleja eri osastojen tai yksikköjen välillä. Tämä menetelmä on hieman ulkoista ja sisäistä tarkastusta joustavampi. Etuna on mielekäs työssäoppiminen sekä parhaan toimintavan omaksuminen ja jakaminen muualle organisaatioon. (Ratsula 2016, 162.)

Itsearvioinnissa yksiköt/organisaatiot arvioivat sisäistä valvontaa joko kyselylomakkeen tai workshopin muodossa. Kuka tahansa organisaation jäsen voi käyttää menetelmänä jatkuvan poikkeaman raportointia, jossa havaitut kontrollipoikkeamat raportoidaan eteenpäin organisaatiossa määriteltyjen vastuiden mukaisesti. Onnistunut itsearviointi vahvistaa omistajuutta ja ihmiset oppivat paremmin ymmärtämään kontrollien merkityksen ja tärkeyden omalle työlleen. (Ratsula 2016, 160-163.)

Edellä kuvattujen suunnitelmallisten menetelmien lisäksi käytössä on poikkeamien raportointi, jossa kuka tahansa voi ja pitää ilmoittaa havaituista poikkeamista raportoinnissa. Kirjanpitäjä voi esimerkiksi huomata jaksotusvirheen, kontrolleri huomaa laskun puuttuvan, esimies huomaa matkasuunnitelman puuttuvan tai yritys on ostanut tavaraa toimittajalta, jota ei ole kilpailutettu. (Ratsula 2016, 169-170.)

3.2.6 Prosessien ja kontrollien jatkuva kehittäminen

Toimivan valvontajärjestelmän tavoite on tuottaa luotettavaa tietoa kontrollien toimivuudesta, jotta havaitut kontrollipuutteet voidaan korjata. Toimivuutta arvioidessa voidaan esimerkiksi todeta, että kontrolli ei ole alkuperinkään kattanut tiettyä riskiä, kontrollia ei ole noudatettu tai se ei ole toiminut tarkoitetulla tavalla. Kontrolli ei estä tiettyjä prosessiriskejä tai sitä ei ole suunniteltu kunnolla. Saattaa olla, että kontrolli on tehty, mutta siihen liittyvää dokumentaatiota tai evidenssiä ei ole säilötty asianmukaisesti tai että kontrollia ei ole implementoitu täysin koskaan. (Ratsula 2016, 170-171.)

Prosessien muuttuessa tai kun uusia kontrolleja otetaan käyttöön, on oltava huolellisia niiden kommunikoinnissa ja kontrollien on tuotettava enemmän lisäarvoa kuin mitä niihin käytetään resursseja. Haasteita voi olla uusien kontrollien juurruttamisessa osaksi yrityksen toimintatapoja. Nimettyjen henkilöiden tulee kommunikoida uusista ja muutetuista

kontrolleista ja on tärkeää, että ihmiset ymmärtävät kontrollin merkityksen ja omat kontrollivastuunsa, jolloin on todennäköisempää, että he ovat motivoituneita toimimaan kontrollivaatimuksen mukaisesti. Pelkkä kontrollin orjallinen suorittaminen ei hyödytä ketään vaan kontrollitavoitteet toteutuvat vasta silloin kun ihmiset ymmärtävät kontrollin merkityksen ja syyt siihen, miksi on syytä toimia prosessi- ja kontrolliohjeiden mukaisesti ja miten ne tukevat yhtiön ja yksilön tavoitteita. Sitoutumisessa on onnistuttu hyvin, kun henkilöstö aidosti haluaa toimia tavoitteiden mukaisesti ja erityisesti myös ylin johto ja oma esimies näyttävät hyvää esimerkkiä. (Ratsula 2016, 171-172.)

4 Case: Yritys X:n kontrollitoimenpiteet ja tulokset

Toimeksiannon tehtävänä oli Yritys X:n materiaali- ja tarvikevaraston prosessiriskien tunnistaminen (määritys ja dokumentointi), kontrollien määrittäminen tunnettujen riskien minimoimiseksi, varastoon liittyvän ohjeistuksen kommentointi sekä käyttövaltuuksien ja vastuiden läpikäynti varastossa käytettävän toiminnanohjausjärjestelmän osalta. Yritys X siirtyi käyttämään uutta toiminnanohjausjärjestelmää materiaali- ja tarvikevarastoja hallitsevan järjestelmän rinnalle. Tämän seurauksena osa prosesseista täytyi päivittää ja siirtymän vaikutukset kuvata. Yritys X:ssä huomattiin, ettei dokumentaatio ole ajantasaista, joten yrityksessä ei ollut kokonaisvaltaista käsitystä siitä, miten prosessi etenee ja asioita tehdään käytännön tasolla. Asiat olivat pitkälti muutamien ihmisten omien työohjeiden sekä muistin varassa ja tästä syystä yritykselle arvokas tieto täytyi dokumentoida. Kuvatut prosessit ovat itsessään kontrolli ja kontrollitarve määräytyy Yritys X:ssä riskiperusteisesti.

4.1 Hankinta- ja tarvikevarastoprosesseihin liittyvät yleiset kontrollointisuositukset materiaali- ja tarvikevaraston näkökulmasta

Johdon tilinpäätösväittämät perustuvat osittain ulkoisten tilintarkastajien (PCAOB) standardiin, jonka mukaan yhtiön on turvattava omaisuutensa (Safequard of Assets) sekä sisäisiä että ulkoisia virheitä ja väärinkäytöksiä vastaan. Kunnossapidon koneet ja kalusto sekä varastomateriaalit on pidettävä hyvässä kunnossa ja tarvikkeiden kunto sekä olemassaolo on tarkistettava suunnitelman mukaisesti. Kunnossapidon ja varaston tarvikkeet on määritelty ”easy to steal” omaisuusryhmään, joka tarkoittaa, että niitä on haluttaessa helppo varastaa tai materiaalin vastaanottoa on mahdollista manipuloida. Tästä syystä kontrollit on mahdollisten tahattomien virheiden lisäksi suunniteltava laajasti kattamaan myös sisäisen ja ulkoisen petoksen mahdollisuus.

Seuraavissa luvuissa kerrotaan yleistä liittyen hankinta- ja tarvikevarastoprosesseihin, jotka liittyvät toimeksiannossa mainittuun Yritys X:n materiaali- ja tarvikevarastoon. Yritys X:n varastosta voidaan käyttää myös yleisempää nimitystä kunnossapito- ja varaosavarasto.

4.1.1 Hankinta- ja tarvikevarastoprosessit

Yrityksen hankinnat jaetaan tyypillisesti välittömien raaka-aineiden, puolivalmisteiden ja tarvikkeiden ostoon sekä välillisiin ostoihin, kuten esimerkiksi alihankintaan ja toimistotarvikkeisiin. Jotta sisäisessä valvonnassa onnistutaan, on seurattava koko hankintaprosessia eli end-to-end prosessia kokonaisuutena ja sen jälkeen tunnistettava sekä määritel-

tävä jokaisen prosessistepin osalta relevantit kontrollit, joilla voidaan ehkäistä riskejä. Tämän jälkeen on tunnistettava organisaation osat, järjestelmät ja ihmiset, jotka liittyvät kyseisiin kontrolleihin. (Ratsula 2016, 173).

Yritys X:n toimeksiannon mukaisesti tässä lopputyössä keskitytään hankintaprosessin (Kuva 11) materiaali- ja tarvikevaraston osaprosessien kuvaamiseen, niihin liittyvien prosessiriskien arviointiin ja riskimatriisin perusteella määriteltyjen kontrollien implementointiin riskien eliminoinniksi kyseisen aihealueen osalta.

Kyseiseen end-to-end hankintaprosessiin liittyen lopputyössä tarkastellaan alla olevan matriisin osalta pääasiassa tavaran ja palvelun vastaanottoa materiaali- ja tarvikevarastoon. Tähän kuuluu lähinnä ostotilaus-, ostolaskujen vastaanotto ja täsmäyttäminen vastaanotettuun tavaran ja palveluun sekä laskun hyväksyntä. Toki analyyttinen tarkastelu on myös osana tätä työtä kuten varaston arvostukseen ja fyysiseen inventointiin liittyvät toimenpiteet.

Kuva 11. Esimerkki tyypillisestä hankintaprosessista (mukaillen Ratsula 2016, 176)

4.1.2 Riskienarviointi pohjana tehokkaiden sisäisten kontrollien määrittelyssä

Sisäisen valvontajärjestelmän toimivuuteen voi liittyä erilaisia riskitilanteita; esimerkiksi varastoon on ostettu liian suuria määriä tuotteita, joille ei ole käyttöä ja tavara pilaantuu tai ettei hankintaohjeistusta ole noudatettu, jonka takia ostolla ei ole asiaankuuluva hyväksyntä tai toimittajien kanssa tehtyä sopimusta ei ole kilpailutettu. Kiellettyä on myös käyttää toimittajia, johon kohdistuu eturistiriita tai on huono maine. Sitoudutaan kuluihin ilman vaadittavaa hankintojen etukäteishyväksyntää. Samoja ostolaskuja maksetaan useampaan kertaan, yhtiön varoja käytetään väärin, tavoitteiden vastaisesti tai niillä katetaan

henkilökohtaisia kuluja. Hankintaprosessin kontrollien tavoitteena on varmistaa, että yrityksen maksut ja menot koskevat vain yrityksen vastaanottamia sekä hyväksymiä tavaroita tai palveluja, jotka on hankittu yrityksen tarpeisiin. (Ratsula 2016, 174-175.)

4.1.3 Hankinta- ja tarvikevarastoon liittyviä kontrolleja

Hankintasopimuksen lisäksi käytetään usein ostoehdotusta, jonka hyväksynnän jälkeen luodaan ostotilaus, joka lähetetään toimittajalle. Ostotilaukseen liittyvien kontrollien tulisi varmistaa, että politiikat, ohjeet ja rajat hankintojen hyväksymisille on olemassa ja niitä noudatetaan. Tilaus on tehtävä olemassa olevan hyväksytyn hankintapäätöksen mukaisesti. Tilaajalla on oltava valtuuden tilauksen tekemiseen. Hankintaehdotuksen tekijä ja hyväksyjä ei saa olla sama henkilö eikä hankintaehdotuksen ja ostotilauksen tekijä saa olla sama henkilö. (Ratsula 2016, 184.)

Tilattu tavara tai palvelu on vastaanotettava ennen kuin loppulaskun voi maksaa. Ennen laskun maksua on tärkeää varmistaa, että laskun erittely ja tilaus vastaavat toisiaan. Ilman tätä varmistusta yritys saattaa maksaa tavarasta liikaa, jos toimitettu määrä on pienempi kuin tilattu. Vastaanotot tulisi kirjata järjestelmään viipymättä. Vastaanottajan tulee osata arvioida, vastaako toimitettu tavara tai palvelu tilausta niin toimituksen laadun, määrän, toimitusajan, hinnan ja muiden sopimusehtojen suhteen. Ostotilauksen tekijän ei tulisi toimia tilauksen vastaanottajana. (Ratsula 2016, 187.)

Ostolaskujen vastaanottoon, hyväksymiseen ja täsmäyttämiseen liittyvien kontrollien tulisi varmistaa, että kaikki laskut ja niihin liittyvät liitteet päätyvät samaan paikkaan. Laskut tallennetaan ja säilytetään mahdollisten epäselvyyksien varalta ja ne lähetetään asiantarkastajille ja/tai hyväksyjille, joilla on riittävät hyväksymisvaltuudet. Ostolaskut tarkastetaan toimituksen määrän sekä hinnan osalta vastaamaan tilausta. Mahdolliset määrä ja hintaerot sekä muut täsmäytyserot monitoroidaan ja selvitetään. Laskun hyväksyy hyväksymispolitiikan mukaisesti siihen valtuutettu henkilö, hyväksymispolitiikan ja -limitin mukaisesti. (Ratsula 2016, 189.)

Varastohallinnan puutteellisesta tai tehottomasta sisäisestä valvonnasta saattaa olla kyse, mikäli esimerkiksi varaston inventointiarvon ja kirjanpidon arvon välillä on merkittäviä ja toistuvia täsmäytyseroja. Varasto on yli- tai aliarvostettu taseessa tai alaskirjaukset on tehty toimintaohjeiden vastaisesti. Virheelliset varaston arvot voivat johtaa tarvikkeen loppumiseen kriittisessä vaiheessa. Tuotekustannukset eivät perustu oikeisiin kuluihin tai varastossa on epäkuranttia tavaraa, jonka arvo alenee ja se joudutaan hävittämään. Varaston hävikkikustannukset ovat korkeat ja perustuvat epätarkkoihin ja virheellisiin laskelmiin.

Varastonhallinnan kontrollien keskeiset tavoitteet ovat, että varaston arvo on oikein kirjanpidossa sekä arvostuksen että määrän osalta. Arvonalennuskirjaukset ovat realistisia ja kohtuullisia sekä noudattavat yrityksen toimintaohjeita. Taseen näkökulmasta varastoerät ovat fyysisesti olemassa ja varastoerien kirjanpidon kirjaukset ovat oikeellisia. Tuotekustannuslaskenta perustuu oikein määriteltyihin arvoihin. Myytyihin varaosiin kohdistuvia kuluja ei kirjata menoiksi ennen kuin tuotteet on fyysisesti toimitettu ja myytyihin tuotteisiin liittyvät menot on kirjattu oikein kirjanpitoon. (Ratsula 2016, 234-235.)

4.2 Materiaali- ja tarvikevaraston prosessikuvaus

Välitavoite eli tutkiva vaihe oli selvittää minkälaisia prosesseja ja toimintatapoja Yritys X: n varastossa noudatetaan tavaran vastaanoton ja tilauksen osalta ja mihin kuun vaihteen tehtäviin varastoprosessi liittyy. Tarkoitus oli havainnoida ongelmakohtia ja raportoida näistä yritykselle. Prosessikuvausten aikana opinnäytetyöntekijä toimi tarkkailijana, mutta häntä pyydettiin jatkamaan prosessin ongelmakohtien päivitystä samalla kun riski- ja kontrollityötä käytiin läpi.

Materiaali- ja tarvikevarastolle kuvattiin yhteensä 11 osaprosessia, joihin tuli määrittää riskit ja kontrollit. Kuvatut prosessit esitellään kuvassa 12 ja ne ovat: Manage external material needs, Manage internal material needs, Manage material returns, Manage reclamation, Manage internal inventory transfers, Manage inventory location transfers, Manage repaired material, Manage part corrections, Manage scrapping materials, Manage counting ja Manage period closing tasks.

Kuva 12. Yritys X:n varastoprosessit (Yritys X 2018)

Havainnointivaiheessa opinnäytetyöntekijä seurasi prosessikuvausten siirtoa prosessinkuvausjärjestelmään, johon kuvataan myös Yritys X:n riskit ja kontrollit. Prosessipiirtämisen yhteydessä oli havaittu useita **epäselviä rajapintoja,** näitä olivat osittain keskeneräiset prosessikuvaukset varastoon liittyvissä prosesseissa (varaston input ja output). Myös varastoon palautettavan materiaalin käytännön prosessi oli epäselvä ja tähän kaivattiin päivitystä. Tällaisessa tapauksessa oli jo voinut tapahtua järjestelmän käyttäjän virhe, eikä materiaalia pystytty palauttamaan varastoon oikeaoppisesti, joka johti korjaavien toimenpiteiden tekoon kirjanpidossa.

Yritys X:n varastoon kirjattava materiaali saapuu joko suoraan varastolle tai vaihtoehtoisesti kentälle, jolloin se ei koskaan käy fyysisesti materiaali- ja tarvikevarastolla. Materiaali vastaanotetaan järjestelmään aina dokumentaation perusteella ja toisinaan kentälle saapuneen materiaalin dokumentaation toimittamisessa varastolle saattaa kestää kohtuuttoman kauan. Varastokirjanpitäjän siis täytyy odottaa dokumentaatiota ennen kuin hän voi kirjata materiaalin järjestelmään. Tämä saattaa aiheuttaa materiaalin kirjauksen väärälle raportointikaudelle tai kustannusten kohdentumisen väärälle kohteelle.

Puuttuva dokumentaatio, joka liittyy materiaalin palautukseen varastolle saattaa aiheuttaa varastokirjanpitoon virheitä kuten materiaalin kirjauksen virheelliselle nimikkeelle, kaudelle, virheelliselle yksikköhinnalle tai kustannuksia väärälle osastolle. Jos näitä ei voida ottaa vastaan prosessin mukaan oikealla tavalla aiheutuu varastokirjanpidolle huomattava määrä manuaalista työtä, tarkastusten ja mahdollisten korjauksien muodossa. Vaikka ongelmaan on jo kiinnitetty huomiota Yritys X:n materiaali- ja tarvikevaraston prosessin parantamiseksi, epäselvät palautukset aiheuttavat paljon manuaalista työtä varastokirjanpidossa. Kustannuksia ei voida kohdentaa oikein, jos ei ole riittävää dataa. Varastoon palautettavalle materiaalille olisi hyvä laatia lomake, jonka materiaalia palauttava osapuoli täyttää ennen palautusta. Yrityksellä ei ole käytössä valmista mallia dokumentaatiosta, joka sopisi näihin tarpeisiin ja sen vuoksi tarvittavat tiedot on mietittävä etukäteen valmiiksi varastokirjanpidon ja sidosryhmien kesken. Lomakkeella täytyy ilmetä minimitiedot, joita tarvitaan materiaalin vastaanottoon varastolla esimerkiksi materiaalin tunnistenumero, työtilausnumero tai nimikkeettömän materiaalin palautuksessa hyväksyntä, järjestelmän ostotilausnumero sekä muu mahdollinen järjestelmän tieto, joka kertoo miltä järjestelmän tapahtumalta/kohteelta materiaali palautetaan.

Varastoprosessin kuvaamista Yritys X:ssä vaikeuttaa osaltaan se, ettei kaikkea materiaalia vastaanoteta varastohenkilöstön toimesta. Osa tilauksista liittyy suoraan johonkin tiettyyn projektiin. Projektitilausten vastaanottokäytäntö eroaa varaston prosesseista, eivätkä nämä kuulu varastoprosessiin. Yritys X:ssä projekteille tilattavat ylijäämämateriaalit on

mahdollista palauttaa varastoon niiltä osin, kun ne ovat relevanttia materiaali- ja tarvikevaraston kannalta. Projektien materiaalien tai hyödykkeiden vastaanotto järjestelmään tapahtuu ostajan toimesta, joka on saanut hyväksynnän tähän projektivastaavalta. Tämä käytäntö on vastoin toimintojen eriyttämisvaatimuksia, eikä suoranaisesti liity materiaalivaraston prosesseihin, mutta on asia, joka hankaloittaa huomattavasti sidosryhmien työskentelyä tilausten käsittelyssä ja johon on kiinnitettävä erityistä huomiota prosessin selkiyttämiseksi.

Ongelmia esiintyi myös prosesseissa, joissa varaston kautta käsitellään materiaalin korjausta. Tyypillisesti näissä tapauksissa materiaali viedään korjattavaksi varaston kautta, jotta materiaalille voidaan kohdistaa korjauksesta syntyvät kustannukset. Jos tätä ei ole kirjattu oikein järjestelmään materiaalin hinta muuttuu. Järjestelmä mahdollistaa virhekirjaukset ja on erittäin herkkä käyttäjävirheille, joista saattaa aiheutua väärin kohdennettuja kustannuksia kirjanpitoon. Tässä huomattiin erityisesti, että eri osastot toimivat epäselvissä tapauksissa erilaisen käytännön mukaan. Oikeaa tapaa kirjata asioita ei ole sisäistetty ja ohjeistus on erittäin puutteellinen. Tähän kuitenkin ollaan rakentamassa uutta ohjeistusta, joka on tarkoitus jalkauttaa ja kouluttaa kaikille asianomaisille.

Yksi tärkeä havaituista prosessikuvauksiin liittyvistä osa-alueista on inventointiin liittyvän ohjeistuksen tarkastus ja päivitys. Yrityksessä tehdään inventointia kuukausittain mutta toiset materiaalit inventoidaan todella harvoin, jopa 4 vuoden välein. Pitkät inventointivälit saattavat vääristää varaston arvoa. Varastossa saattaa esiintyä hävikkiä tai epäkuranttia materiaalia, joka on arvostettu virheellisesti täyteen arvoonsa.

Kaikki yllä mainitut ongelmat, jotka on huomattu prosesseja piirrettäessä kertovat, että yrityksellä on ollut jo pitkään tarvetta kuvata prosessit uudelleen ja tarkistaa näihin liittyvät rajapinnat. Samalla on tehtävä työohjeiden päivittäminen, toimintatapojen yhdenmukaistaminen ja parannettava informaation kulkua osastojen välillä, jotta yhteinen oikea toimintatapa löytyy.

4.3 Materiaali- ja tarvikevaraston riskit ja kontrollit

Riskien tunnistamisessa ja priorisoinnissa sekä kontrollien määrittelyssä havaittujen riskien osalta käytetään COSOn mukaista riskientunnistusmetodia, jossa tunnistetut riskit priorisoidaan todennäköisyyden ja vaikuttavuuden mukaan. Kun riskit oli analysoitu yrityksen johdon asettamien tavoitteiden (tilinpäätösväittämät) mukaisesti kuva 13 määriteltiin tarvittavat kontrollit kattamaan havaittuja riskejä.

Kyseiseen tapaukseen tyypillisesti liittyvät väittämät, jotka on katettava, ovat transaktiotason väitteet, joissa kaikki kirjanpidon viennit on kirjattu pääkirjaan tarkasti ilman virheitä, oikean raportointikauden aikana sekä kirjaukset on kohdistettu oikealle yksikölle. Tilin saldon väitteiden mukaan kaikki tilin saldot on kirjattu omaisuuseriin, velkoihin ja omaan pääomaan asianmukaisesti arvostettuina, raportoitu virheettömästi ja oikean kauden aikana. Esitys- ja julkistamisväitteet vaativat, että kaikki julkistetut tiedot ovat oikean määräisiä, heijastavat niiden asianmukaisia arvoja, on esitetty asianmukaisesti ja ymmärrettävästi.

Balance Sheet	Profit and Loss Statement
Existence An asset or liability exists at a given date.	**Occurrence** A transaction occurred during the period.
Valuation An asset or liability is booked to the correct amount and according to laws and policies.	**Measurement** A transaction is booked to the right amount and an income or loss is to right period.
Rights and obligations An asset or liability belongs to the right entity.	
Completeness There are no assets, liabilities or transactions that are not booked.	
Presentation and disclosure Financial statement is reliable and are presented correctly.	

Kuva 13. Johdon tilinpäätösväittämät (mukaillen COSO 2013)

4.3.1 Prosessiriskien tunnistaminen

Riskikartoitus ja -analyysi tehtiin riskiworkshopeissa prosessiomistajien, varaston asiantuntijoiden ja kontrollivastuuhenkilöiden kanssa opinnäytetyöntekijän vetämänä. End-to-end prosessin määrittelyn jälkeen kyseisen prosessin eri osa-alueet kuvattiin ja dokumentointiin. Kontrollikatalogiin viedyt riskit ja kontrollit on kasattu ryhmätyönä vaihe vaiheelta prosessikaaviota läpikäyden.

Kontrollityövaiheessa riskejä ei ole priorisoitu Yritys X:n materiaali- ja tarvikevarastojen osalta mutta teorian mukaan nämä olisi hyvä priorisoida vähintään asteikolla High, Medium ja Low. Priorisoinnin perusteella Yritys X:lle pystyttäisiin määrittelemään avainkontrollit niiden riskien osalta, joiden toteutuminen on joko todennäköinen tai lähes varma ja joiden vaikutus on toteutuessaan vakava, erittäin vakava tai jopa kriittinen. Riskien priorisointi tulisi tehdä yhdessä prosessinomistajan kanssa ja arvioida kuinka suuri todennäköisyys kullakin riskillä on toteutua ja toisaalta kuinka suuri vaikutus raportointiin on, mikäli kyseinen riski jostain syystä toteutuisi.

Yleisesti käytetty arviointi tehdään käyttämällä asteikkoa 1-5, jossa 1-tasolle nousseet riskit olivat epätodennäköisiä ja toteutuessaan merkityksettömiä. 5-tasolle arvioitujen riskien

todennäköisyys oli lähes varma ja vaikutus kriittinen. Kyseisen arvion perusteella riskit luokitellaan yleisesti kriittisyyden mukaisesti High, Medium ja Low.

4.3.2 Kontrollien määrittäminen

Kontrollit määräytyvät yritys X:ssä riskiperusteisesti, joten oli luonnollista käydä prosesseja läpi kohta kohdalta, kunnes tunnistettiin riski, johon määriteltiin kontrolli. Kontrollit käytiin läpi yhdessä kontrollivastaavien kanssa ja arvioitiin niiden toimivuutta ja kattavuutta tunnistettujen riskien ehkäisemiseksi. Päivitettyjen prosessikuvausten perusteella jo olemassa olevia hyviksi havaittuja kontrollikuvauksia ja evidenssivaatimuksia päivitettiin ajan tasalle. Uusien prosessiosa-alueiden sekä vielä kattamattomien riskien osalta määriteltiin uudet kontrollit yhdessä prosessi- ja kontrollivastaavien kanssa.

Kun kontrollit ja kontrollievidenssivaade oli tunnistettu ja kuvattu, ne käytiin läpi ja analysoitiin jotta voitiin olla varmoja siitä, että kaikkien väittämien osalta riskit oli katettu. Joko siis ei ollut havaittu korkeaa riskitasoa ja tavoite täyttyi hyvien ohjeiden ja selkeän prosessikuvauksen ja työohjeiden avulla tai niissä tapauksissa, jossa riski oli todennäköinen ja vaikutus toteutuessaan olisi ollut ilmeinen, määriteltiin kontrollit kattamaan kyseisiä riskejä. Toki havaitut puutteet ohjeistuksissa sekä työohjeissa kuvattiin opinnäytetyöntekijän toimesta korjaavina toimenpiteitä.

4.4 Dokumentointi

Yritys X:n varastoprosessin kuvaus aloitettiin 5/2017 määrittämällä olemassa olevia varastoprosesseja. Opinnäytetyöntekijä on ollut seuraamassa prosessien kuvaamista ja tehnyt jo tässä vaiheessa omia havaintoja materiaali- ja tarvikevaraston näkökulmasta sekä tutustunut varaston prosesseihin. Kuvausten yhteydessä tehtyjä havaintoja on avattu luvussa 4.2 Materiaali- ja tarvikevaraston prosessikuvaus. Työryhmä teki workshopeissa prosessikuvaukset taulukkolaskentaohjelma Exceliin, jonka jälkeen ne vietiin prosessikuvaussovellukseen. Lopulliset prosessikuvaukset valmistuivat alkuvuodesta 2018.

Riskejä ja kontrolleja määrittäessä prosessikuvauksissa huomattiin puutteita, jotka käytiin läpi yrityksen vastuuhenkilön kanssa, jotta ne voidaan tarkistaa ja päivittää tarvittaessa. Prosessikontrollien määritys varastoprosessien perusteella tehtiin 2-5/2018 opinnäytetyöntekijän ohjaamana yhdessä työryhmän asiantuntijoiden kanssa. Opinnäytetyöntekijän tehtäviin kuului suunnitella työryhmän palaverien koolle kutsuminen, työskentelyn ohjaus ja havaintojen dokumentointi. Riskien ja kontrollien määrittämisen jälkeen toimeksiannon perusteella opinnäytetyöntekijä täydensi kontrollikatalogin riskien ja kontrollien osalta.

Kontrollikatalogia täydennettäessä opinnäytetyöntekijä huomasi puutteita, kuten että osa kontrollievidensseistä tai niiden tallennuspaikoista on epäselviä.

Yritys X:n kontrollikatalogiin lisättiin myös kontrolleja, jotka havaittiin varastoprosesseihin liittyvissä prosesseissa. Työryhmä katsoi tärkeäksi kirjata nämä ylös ja tiedottaa niistä asiankuuluville tahoille jatkotoimia varten. Riskit ja kontrollit esimerkiksi Master Data ja kunnossapitoprosessien osalta kirjattiin ylös ja luovutettiin vastuuhenkilön tarkastettavaksi. Toimeksiannossa mainittu riskien ja kontrollien vieminen prosessikuvaussovellukseen jäi kuvaamatta ja tämä sovittiin tehtäväksi yhtä aikaa prosessikuvausten päivittämisen yhteydessä.

Dokumentaationa yritys X:lle on luovutettu riski- ja kontrollityöryhmien materiaali havaintoineen, täydennetty materiaalivaraston kontrollikatalogi ja loppuraportti esityksen muodossa, johon on kerätty tärkeimmät huomioitavat asiat, jatkotoimenpiteet (seuraava steppi kontrollityössä) ja korjaavien toimenpiteiden ehdotukset. Työ on luovutettu eteenpäin ja ohjeistettu yrityksen osoittamalle vastuuhenkilölle.

4.4.1 Yhtiötason ohjeistus

Yhtiötason kontrollit eli Entity Level Controls (ELC) ovat kontrolleja, jotka koskevat koko organisaatiota ja luovat näin perustan prosessitason kontrolleille. Yrityksen tulee varmistaa, että kaikki ohjeistukset on asianmukaisesti kommunikoitu ja jalkautettu organisaatioon. Tyypillinen ja tärkeä yhtiötason kontrolli on yhtiön politiikkojen, eri funktioiden sekä yhtiökohtaisten ohjeiden ja ohjelmien kuten esimerkiksi menettelyohjeiden (Code of Conduct) ajantasainen päivittäminen ja jalkauttaminen organisaatioon.

Hankintaprosessiin liittyvät yhtiötason käytännöt ovat tyypillisesti ohjeita, joissa johto määrittää organisaation **roolit, -valtuutukset sekä käyttäjäoikeusrajat**. Toimittajiin kohdistuva **Code of Conduct** menettelyohje sekä sisäisen valvonnan määrittelyt ja ohjeet **kontrollien monitoroinnin osalta** antavat ohjeistusta miten kyseiset asiat tulee hoitaa. Riskihallintaprosessissa tulee määritellä **ohjeistus yhtiön hankintakäytännön ja -prosessiin liittyvien yhtiötasoisten** ohjeiden osalta. (COSO 2013).

Opinnäytetyön aikana tehtyjen havaintojen perusteella voimme todeta että, Yritys X:n ohjeistus on osittain puutteellinen materiaali- ja tarvikevaraston ja siihen liittyvien prosessien osalta. Olemassa olevaa ohjeistusta ei ole reaaliaikaisesti päivitetty eikä kommunikoitu asianmukaisesti sidosryhmille. Yhtiötasolla on huomattu, että työohjeita säilytetään use-

assa eri paikassa ja niitä on hankala löytää. Toimintatavat saattavat vaihdella maa- ja toimipistekohtaisesti, joka ei vastaa Yritys X:n käytäntöä, koska tarkoitus on yhdenmukaistaa toimintatapoja, prosesseja ja ohjeistusta globaalilla tasolla.

Yritys X:ssä on meneillään organisaatiomuutos, jonka tarkoituksena on selkeyttää olemassa olevia rooleja ja vastuita. Tämä tarkoittaa myös, että prosessit on kuvattu, riskit ja kontrollit on määritetty, työohjeistus on olemassa ja tallennettu yhtiön tavoitteiden mukaisesti. Organisaatiomuutokseen liittyy olennaisena osana myös roolien ja käyttäjäoikeuksien sekä vaarallisten työyhdistelmien tarkennus sekä määrittely, joka on olennainen osa yhtiötason kontrolleja.

4.4.2 Prosessikontrollit

Ryhmätöiden ja työssä tehtyjen havaintojen perusteella materiaali- ja tarvikevarastoon liittyviä mahdollisia riskejä voidaan ehkäistä tehokkaiden prosessikontrollien avulla. Esimerkkinä avainkontrolleista toimeksiannon osalta ovat fyysiseen olomuotoon liittyvät kontrollit kuten, että yhtiön IT-palvelimet ja **varastotilat ovat lukittujen ovien takana ja vain valtuutetuilla henkilöillä on pääsy varastoon,** toiminnanohjausjärjestelmässä on jokaiselle nimikkeelle (materiaali tai varaosa) **oma tunnistenumero** ja itse hyödykkeessä **sitä vastaava hyllypaikkamerkintä**.

Vaihto-omaisuuden tyypillisiä avainkontrolleja ovat, että **varastolistat tulisi täsmäyttää pääkirjanpidon kanssa** riittävän usein**, varastolistojen ajantasaisuus ja todenmukaisuus tulisi varmentaa inventaariolla.** Vastaanotettavan **materiaalin tulee vastata tilausta** ja vastaanotto on **syötettävä järjestelmään oikea-aikaisesti.**

Varastoon palautettavien tavaroiden osalta on suuri vaara, että varastokirjanpitoon tehdään virheellisiä kirjauksia puutteellisen ohjeistuksen takia ja siksi on erittäin tärkeää, että varastoon ei saa vastaanottaa tavaroita, mikäli dokumentaatiota ei ole asianmukaisesti tehty.

4.4.3 Kontrollikatalogi

Kesän 2018 aikana opinnäytetyöntekijä valmisteli opinnäytetyön tavoitteen mukaisesti sisäisen valvonnan dokumentaation käyttäen MS Excel -ohjelmaa. Prosessi- ja riskikuvaus, kontrollin nimi ja kontrollin kuvaus sekä evidenssi ja muut prosessiin liittyvät määritykset kuvattiin kontrollikatalogiin niiltä osin, kun se oli mahdollista. Evidenssien sijaintipaikan osalta huomattiin kehitystarve, koska tällä hetkellä aineisto on tallennettuna esimerkiksi

henkilökohtaisissa sähköposteissa tai kansioissa (näitä ei saada luotettavasti vietyä kontrollikatalogiin). Evidenssiä ei ole aina mahdollista tallentaa suoraan Yritys X:n varastoa koskevaan toiminnanohjausjärjestelmään, joten evidenssien tallennuspaikkoja on tarkennettava sekä työohjeistusta selkeytettävä.

Toimeksiannon oheismateriaali, sisältäen raportoinnin, havainnot, kontrollikatalogin on tallennettu opiskelijan luomaan kansioon, joka sijaitsee yrityksen määrittämässä tallennustilassa ja on luovutettu yrityksen käyttöön. Samalla Yritys X:n vastuuhenkilölle on ohjeistettu jatkotoimenpiteet, jotka ovat nousseet esille toimeksiannon aikana. Toimenpide-ehdotuksena on määritellä Yritys X:lle yhtenäinen tallennustila tai SharePoint kansio, jonne evidenssit tallennetaan ja niitä ylläpidetään. Tätä varten voidaan myös implementoida tarkoitukseen sopiva sisäisen valvonnan työkalu, jonne aineisto taltioidaan. Haluttaessa tämä mahdollistaa keskitetyn kontrollimonitoroinnin suorittamisen ja edesauttaa mm sisäisen- ja ulkoisen tarkastuksen sujuvuutta.

4.4.4 Käyttäjäoikeuksien hallinta

Käyttäjäoikeuksien hallintaprosessin tarkoitus on rajoittaa pääsy ainoastaan järjestelmiin ja dataan, johon henkilö on oikeutettu sekä käyttäjät tunnistetaan yksilöllisellä tunnisteella ja heidät todennetaan ennen pääsyä järjestelmään. (Ratsula 2016, 242.)

Käyttäjäoikeudet määrittää yrityksen johto **yritystasolla olevan kontrollien** (Entity Level Controls, ELC) mukaisesti eli **käyttäjäroolien ja -valtuutuksien määrittelyllä** (Delegation of Authority). Esimerkkinä tästä yritystason kontrollista on, että johto määrittää ja ohjeistaa selkeästi ymmärrettävällä tasolla kuka saa tarkistaa ja hyväksyä ostolaskuja tietyn yksikön ja kustannuskohteen osalta ja mitkä ovat sallitut hyväksymisrajat. Teoriaosuudessa 3.2.2 Yritystason kontrollit kerrotaan tästä lisää.

Prosessikontrolliksi luetaan puolestaan **ennaltaehkäisevä käyttäjäoikeuksien hyväksyntäkontrolli,** jossa tyypillisesti esimies, joka tietää mitä oikeuksia henkilö työssään tarvitsee, hyväksyy pyynnön ennen kuin oikeudet voidaan luoda järjestelmään. Esimerkkinä valtuutettu henkilö, yleensä esimies hyväksyy alaisensa ostolaskun hyväksymisoikeudet ja -rajat ennen kuin ne voidaan luoda ja ottaa käyttöön.

Myös **todentava olemassa olevien oikeuksien monitorointikontrolli** on ns. prosessikontrolli, jonka tarkoituksena on varmistaa, että vain organisaatiossa työskentelevillä ja valtuutetuilla henkilöillä on olemassa valtuutettuja käyttöoikeuksia tarkastettaviin järjestel-

miin. Esimerkkinä esimies ajaa ostolaskujärjestelmästä raportin, josta näkyy kaikki ne tasot (yksikkö, kustannuskohde jne.) joille henkilöllä on hyväksymisoikeudet ja vastaavat hyväksymisrajat. Mikäli raportilla on tarpeettomia henkilöitä siksi, etteivät he enää työskentele yrityksessä tai tarpeettomia rooleja koska henkilöstöä on esimerkiksi siirtynyt toiselle osastolle, on kyseiset henkilöt/käyttöoikeudet välittömästi pyydettävä poistamaan järjestelmistä ja mahdolliset muut virheet on pyydettävä korjaamaan. (Ratsula 2016, 242-243.)

Toimintojen eriyttämiskontrollissa (Segregation of Duties, SoD) tarkastellaan, onko henkilöllä ns. **kriittisiksi määriteltyjä kombinaatioita eli vaarallisia työyhdistelmiä.** Tämä tehdään tyypillisesti, kun ylimääräiset käyttäjäoikeudet on poistettu. Tällä kontrollilla varmistetaan, ettei samalla henkilöllä ole valtuuksia muodostaa ns. riskikirjastossa määriteltyjä kriittisiä kombinaatioita, esimerkiksi sama henkilö ei voi tarkastaa ja hyväksyä samaa ostolaskua. Mikäli esimerkiksi matalan organisaation takia eriyttäminen ei ole mahdollista, voidaan käyttää ns. **kompensoivia kontrolleja,** joilla varmistetaan, ettei väärinkäytöksiä ole tapahtunut. (Ratsula 2016, 192, 239.)

IT:n järjestelmäkontrolleiksi kutsutaan ns. sovelluskontrolleja, joilla ennaltaehkäistään väärinkäytöksiä ja virheitä, jolla varmistetaan, että tieto on täydellistä, tarkkaa vain valtuutettujen tuottamaa ja yhtenäistä. Esimerkkinä ostolaskujärjestelmään on rakennettu sovelluskontrolli, joka estää samaa henkilöä tarkastamasta, että hyväksymästä samaa laskua. (Ratsula 2016, 245).

Yhtiön johdon tehtävä on huomioida kaikki organisaatiorakenteet, laatia hyväksymisohjeet sekä määritellä henkilöstön roolit ja vastuut näihin liittyen (Ratsula 2016, 242). Johto määrittää, nimittää ja rajoittaa käyttäjäoikeuksia ja vastuita saavuttaakseen tavoitteet käyttövaltuuksien osalta. Tämä edellyttää, että varastokontrolleihin liittyvä organisaatiorakenne on kuvattu sisältäen raportointilinjat ja vastuut. Käyttöoikeuksille on luotava hyväksyntäohjeet ja ne tulee ajantasaisesti päivittää.

Toimeksiannon alussa todettiin, ettei Yritys X:n toiminnanohjausjärjestelmän käyttöoikeusominaisuuksia ole hyödynnetty riittävästi. Alkutilanne käyttäjäoikeuksin osalta oli 3/2018 sekava. Opinnäytetyöntekijä kävi keskustelua käyttöoikeuksista järjestelmästä vastaavien henkilöiden kanssa, selvittääkseen nykytilaa (liite 4). Vastauksena kerrottiin, että Yritys X:n toiminnanohjausjärjestelmän käyttöoikeudet on rakennettu 10 vuotta sitten silloisten roolien ja tehtävien mukaan. Käyttöoikeuksia on mahdollisuus tarkistaa ja muuttaa tarpeen mukaan mutta tässä on lähdetty roolien uudelleen määrittämisen sijaan lisäämään henkilöille ja järjestelmässä oleville rooleille uusia oikeuksia. Käyttäjille on myös lisätty oikeuksia sitä mukaan, kun he ovat vaihtaneet osastoa tai positiota talon sisällä. Vanhoja

käyttöoikeuksia ei ole poistettu automaattisesti, joten käyttöoikeudet voivat olla näillä henkilöillä erittäin laajat. Vaikuttaa että samalla henkilöllä voi olla esimerkiksi oikeus tilata, vastaanottaa ja kirjata materiaaleja sisään varastoon. Järjestelmässä on olemassa katselu- ja muokkaus vaihtoehdot, sekä Super User oikeudet, joilla pystyy päivittämään käytännössä kaiken. Järjestelmä mahdollistaa paljon rajatummat käyttöoikeudet, mutta tähän ei ole kiinnitetty ajoissa huomiota eikä tätä ominaisuutta juurikaan hyödynnetä.

Yritys X:n toiminnanohjausjärjestelmässä on luotu vain muutamia rooleja eri osastoille. Nykytilassa käyttäjäoikeudet ja roolit on luotava uudelleen alusta asti koska käyttäjäkohtaisten oikeuksien selvitys on liian suuri työ. Järjestelmässä on tuhansia käyttäjiä ja satoja rooleja, joita on upotettu ristiin rastiin toisten roolien sisään. Oleellisinta on löytää oikeat henkilöt, jotka pystyvät kertomaan millaisia rooleja ja oikeuksia tulisi olla. Käyttöoikeusasiat ovat yksi ensimmäisistä osa-alueista, joita Yritys X:ssä on tarkoitus kehittää yhdessä pääkäyttäjien kanssa. Järjestelmän käyttäjäoikeusrooleihin on pitkään kaivattu päivitystä, mutta Yritys X:n resurssit eivät ole tässä vaiheessa olleet riittävät pureutumaan ongelmaan.

Liian laajat käyttäjäoikeudet mahdollistavat käyttäjävirheen, jonka seurauksena raportointi vääristyy tai mahdollisen petoksen riskin. Yritys X:ssä on myös määrittelemättä, kuinka usein toiminnanohjausjärjestelmän käyttäjäoikeudet tulee tarkastaa. Säännöllisillä tarkastuksilla pyritään poistamaan turhat käyttäjät järjestelmästä ja ehkäisemään liian kattavat käyttöoikeudet. Yritys X:n tulee tehdä vähintään vuosittainen käyttäjävaltuuksien verifiointi. Tämä tarkoittaa, että järjestelmästä ajetaan käyttäjäoikeuslista, joka käydään läpi vastuuhenkilön toimesta, joka poistaa tarpeettomat henkilöt järjestelmästä ja näin estetään pääsy ohjelmiin tai poistetaan oikeuksia henkilöltä, jolle ne eivät enää kuulu.

Paljon keskustelua herättäneen käyttövaltuuskartoituksen jälkeen Yritys X:n käyttäjäoikeuksia on alettu tarkistaa 8/2018. Tarkoituksena on tehdä käyttäjäoikeuksien siivous järjestelmässä. Käyttäjäoikeuksien siivoaminen on aloitettu poistamalla ylläpito ja järjestelmävalvoja oikeuksia turhilta henkilöiltä. Yritys X:ssä käydään käyttövaltuuksien läpikäynti eri osastojen pääkäyttäjien kanssa (Key User). Aluksi hahmottelemalla millaisia oikeuksia työntekijät tarvitsevat ja määrittelemällä roolit käyttäjille uudelleen.

4.4.5 Työohjeet

Yrityksen politiikat antavat perustan ja suuntaviivat yrityksen toiminnalle ja kertovat mitä pitää tehdä, mitä ei saa tehdä ja miten asiat on hoidettava. Politiikoissa mainitut ja erityi-

sesti muuttuneet seikat pitää jalkauttaa kaikkiin aiheeseen liittyviin yksikkötason sekä prosessitason ohjeistuksiin ulottuen tarkkoihin työohjeisiin saakka. Politiikat sekä muu ohjeistus on pidettävä ajan tasalla ja ne on kommunikoitava organisaatiossa tarvittaville henkilöille ymmärrettävällä tasolla, jotta myös kaikki työ- ja muut ohjeet ymmärretään päivittää. Ajan tasalla olevat yhtiön ylimpiin ohjeisiin linkitetyt työohjeet on oltava kuvattuna riittävän tarkalla tasolla, jotta henkilöt suoriutuvat työtehtävistään ja ne on kommunikoitava organisaatiolle ymmärrettävällä tasolla, jotta vältytään virheellisten tai puutteellisten ohjeistusten takia tapahtuvilta virheiltä tai väärinkäsityksiltä.

Esimerkiksi tapauksessa, jossa siirrytään uuteen toiminnanohjausjärjestelmään, joka on synkronoitava vanhan järjestelmän kanssa ja aiheuttaa täten muutostarpeita vanhan järjestelmän konfiguroinnin ja ohjeistuksen suhteen on erittäin tärkeää, että järjestelmän ohjeistuksen laativa henkilö tuntee kaikki asiaan liittyvät järjestelmät ja niiden toimintatavat sekä ymmärtää tarkalla tasolla toimintojen muutosten vaikutuksen raportoitaviin lukuihin.

Yritys X otti käyttöön uuden toiminnanohjausjärjestelmän, jonka seurauksena materiaalivaraston ja siihen liittyvien prosessien työohjeet tulee myös tarkistaa. Osittain työohjeita päivitetään myös koska ne ovat vanhentuneet tai puutteelliset. Yritys X:n työohjeiden päivitys aloitettiin paikallisen toimipisteen näkökulmasta 2017 samalla kun yrityksen materiaalivaraston prosessit kuvattiin uudelleen. Yritys X:n toimintatavat eroavat hiukan toisistaan koti- ja ulkomailla ja se käyttää kahta eri tavalla räätälöityä versiota toiminnanohjausjärjestelmästä. Työohjeet onkin tarkoitus yhtenäistää koko yritystä kattavaksi niin koti- kuin ulkomailla.

Suurin osa työohjeista on saatu valmiiksi ja nämä tulee vielä kääntää englanniksi. Päivitetyille työohjeille on luotu oma tallennustila ja työohjeet on tarkistettava niiden valmistuttua. Yritys X:ltä löytyi myös vanhoja työohjeita portaalista, jota ollaan lakkauttamassa. Tällä hetkellä on vielä epäselvää mihin tarkistetut työohjeet jatkossa tallennetaan, kun vanhat työtilat lakkautetaan.

Työohjeiden päivitys voi tuoda muutoksia myös toisen osaston toimintatapaan tai tapaan kirjata asioita järjestelmään. Tästä syystä työohjeiden valmistuttua Yritys X:n tulee pitää yhteinen läpikäynti varaston ja sidosryhmien välillä. Näissä palavereissa kerrotaan mahdollisista muutoksista ja sovitaan osastojen rajapinnassa tehtävistä toimista, samalla tulisi tarkastaa, että yhteiset roolit ja vastuut on kirjattu työohjeisiin.

5 Johtopäätökset ja pohdintaa

Tässä viimeisessä luvussa esitetään tutkimuksen johdosta syntyneitä johtopäätöksiä ja niiden pohjalta laaditut suositukset kehitystoimenpiteiksi. Lopuksi pohditaan vielä tutkimuksen kulkua ja luotettavuutta sekä opinnäytetyön vaikutuksia omaan oppimiseen.

5.1 Johtopäätökset

Tehdyn tutkimuksen perusteella voidaan todeta, että vaikka Yritys X on panostanut kovasti sisäisen valvonnan viitekehyksen luomiseen kokonaisuudessaan, eivät taloudelliseen raportointiin liittyvät kontrollitoimenpiteet olleet kattavat materiaali- ja tarvikevaraston osalta. Yrityksessä on paneuduttu ja määritelty hyvin johdon tavoitteet eli ns. tilinpäätösväittämät, joiden toteutumista uhkaavat riskit pitäisi minimoida sisäisten kontrollien avulla. Näitä toimenpiteitä ei kuitenkaan ole opinnäytetyön toimeksiantoa tehdessä vielä saatettu loppuun varastojen osalta, joten esimerkiksi riskikuvaukset ja niiden analysoinnin perusteella määritellyt kontrollit puuttuivat. Myöskään kontrollin suorittajia ei ollut nimetty ennen toimeksiantoa.

Niin yrityksen keskijohto kuin lähes kaikki ryhmätöihin osallistuneista henkilöistä tiedostivat jo entuudestaan puutteita prosessi- ja kontrollikuvausten suhteen. Samoin ongelmia oli tunnistettu roolien ja vastuiden määrittelyn osalta eikä ns. kolmen puolustuslinjan (Three Lines of Defense) mallia ollut vielä jalkautettu kattamaan materiaali- ja tarvikevaraston toimintoja.

Oltiin tietoisia, että käyttäjävaltuudet olivat liian laajoja eikä vaarallisten työyhdistelmien eriyttämistä (SoD) ollut tehty ja valvottu kyseisen osa-alueen osalta. Ymmärrettiin että ohjeistus oli osittain vanhentunut eikä järjestelmämuutosten vaikutuksista informoitu organisaatiotasolla riittävästi. Tämän takia opinnäytetyöntekijä otettiin positiivisesti vastaan ja hänen työtään tuettiin kiitettävällä tavalla osallistumalla laajasti sekä ryhmätöihin että henkilökohtaisiin keskusteluihin.

Tutkimustapa, jossa käytettiin ryhmätyöskentelymallia sekä havainnointia toimi hyvin ja antoi luotettavaa tietoa asiantilasta. Ryhmätyöpalavereissa pohdittiin yhdessä prosessin omistajien, prosessiasiantuntijoiden sekä compliance managerin kesken riskeihin ja tarvittaviin kontrolleihin liittyviä asioita. Pitkähkö määräaikainen työsuhde Yritys X:ssä takasi, että opinnäytetyöntekijä pystyi havainnoimaan asioita ja keskustelemaan laajasti asianosaisten kanssa, mikä tuotti luotettavaa taustatietoa kontrollien suunnittelun tueksi.

Toimeksiantajayritys halusi pysyä anonyymina, joka toi tiettyjä haasteita siihen, mitä yrityksestä voidaan kertoa ilman, ettei yritystä tunnisteta, eivätkä esimerkiksi kilpailijat voi käyttää hyväkseen tutkimuksessa esiin tullutta tietoa. Toimeksiantajayrityksen kanssa sovittiin jo ennen tutkimuksen aloittamista työn aihealueesta ja tavoitteista. Aihe oli kuitenkin tiedostettua laajempi ja aiheutti näin muutospaineita alkuperäiseen aikatauluun sekä suunnitelmaan.

Opinnäytetyön onnistumisen ja toimenpide-ehdotusten suhteen oli hyödyllistä, että opinnäytetyönkirjoittaja työskenteli jo ennen toimeksiantoa Yritys X:ssä. Kirjoittaja oli jo etukäteen oppinut tuntemaan opinnäytetyössä esitettyä hankinta- ja kunnossapitovaraston end-to-end prosessia, siihen liittyviä ongelmia ja tutustunut yrityksen työntekijöihin. Yrityksen ei tarvinnut kuormittaa selvitystyössä vakituisia resurssejaan aiheen osalta, mutta toki heiltä saatiin arvokasta tietoa kehitystä kaipaavista epäkohdista, joita ilman ei saada kokonaisvaltaista ymmärrystä kehitystarpeista.

Teoria-aineiston sekä yrityksen johdon määrittelemiä tavoitteita tutkimalla ja yhdistelemällä päästiin hyvään lopputulokseen tavoitetilan suhteen niin kontrollikatalogin kuin korjaavien toimenpide-ehdotusten osalta. Eri teoriatietolähteistä hankittujen tietojen ja opinnäytetyössä käytetyn aineiston osalta viitattiin tutkijoiden ja muiden tahojen julkaisuihin asianmukaisella tavalla.

Yrityksen johdon tuki ja kannustus asioiden kuntoon saattamiseksi loi tärkeän pohjan avoimen ilmapiirin luomiseksi ja näin henkilöt nostivat avoimesti esiin havaintojaan korjattavien toimenpiteiden osalta tuoden esiin myös omia ideoitaan. Todennäköisesti se, että työntekijät osallistuivat itse kyseisen prosessin ja korjaavien toimenpiteiden suunnitteluun luo hyvät edellytykset heille omaksua uuden kontrollikatalogin määrittelemät kontrolliaktiviteetit ja suhtautua positiivisesti esille nostettujen muiden toimenpide-ehdotusten jalkauttamiseen.

Opinnäytetyön aikana luodun kontrollikatalogin sisältämät kontrollit ja muut osa-alueet sekä ohjeistukseen ja käyttäjäoikeuksiin liittyvät parannusehdotukset on määritelty niin, että kyseisiä mallia voidaan hyödyntää globaalisti kyseisten prosessien osalta.

5.2 Yhteenveto kehitysehdotuksien osalta

Tässä luvussa esitetään vielä yhteenveto kehitysehdotuksista liittyen lukuun 4. Case: Yritys X:n kontrollitoimenpiteet ja tulokset esitettyihin havaintoihin sekä vastauksia aiemmin luvussa 1.3.2 Tavoite, rajaus ja kysymykset esitettyjen opinnäytetyön kysymyksiin:

1. Ovatko materiaali- ja tarvikevaraston prosessikuvaukset ajantasaiset, mitä ongelmia prosesseihin liittyy, mikä on Yritys X:n toiminnanohjausjärjestelmän käyttäjäoikeuksien sekä varaston työohjeiden nykytila?
2. Millaisia riskejä materiaalivaraston prosesseista löytyy ja millaiset kontrollit kattavat havaitut riskit?

Toimeksianto sisälsi monta eri tasoista ongelmakohtaa, johon opinnäytetyöntekijän täytyi kiinnittää huomiota. Materiaali- ja tarvikevarastoprojektin aikana löytyi monia erilaisia ongelmia, mutta suurin osa näistä ongelmista johtui siitä, että prosessien päivityksestä oli kulunut paljon aikaa, ja siksi prosessikuvaukset sekä siihen liittyvä ohjeistus ei ollut enää ajan tasalla.

5.2.1 Työohjeistus

Yhtiön eri politiikkojen ja ohjeistusten teko on myöskin osa yhtiötason kontrolleja (ELC) ja nämä yhtiön globaalit, usein yleisellä tasolla olevat ohjeistukset antavat suuntaviivat eri prosessien ohjeistuksille, joista johdetaan myös prosessitasoisia työ- ym. ohjeistuksia.

Työohjeiden päivittäminen oli kesken ja eri osastoilla oli omia totuttuja toimintamalleja, joita jatkettiin, kun päivitettyä ohjeistusta ei ollut saatavilla. Tästä syystä on erittäin tärkeää, että uudet prosessit koulutetaan Yritys X:ssä kunnolla ja näin päästään eroon vanhentuneista toimintamalleista. Myös toiminnanohjausjärjestelmän käyttöoikeudet sallivat käyttäjille mahdollisuuden tehdä asioita ohjeistuksen vastaisesti, mikä pahimmassa tapauksessa vääristi raportointia. Yritys X:ssä päivitettiin työohjeet kaikkien materiaali- ja tarvikevarastoprosessien osalta ja ne olivat käännöstyötä vaille valmiit opinnäytetyöntekijän luovuttaessa työnsä yritykselle.

Aina kun prosessi- tai muiden muutoksien takia työohjeet muuttuvat, tulee vastuuhenkilön pitää huolta asianmukaisesta päivityksestä ja huolehtia että asianomaisille annetaan riittävä koulutus työvaiheen suoritukseen. Työohjeet tulee pitää ajan tasalla ja ohjeisiin tulee merkitä myös kontrollit, jotka liittyvät kyseisen prosessin suorittamiseen, kontrollin suoritusväli, kontrollin evidenssivaade, evidenssin sijaintipaikka ja kontrollin suorittaja. Tämä selkeyttää yrityksen työtekijöiden rooleja, vastuita ja auttaa henkilöä toimimaan oikein.

5.2.2 Riskiarviot

Riskiperusteinen lähestyminen sisäisen valvonnan kehittämiseksi on myös osa yhtiötasolla olevia kontrolleja. Opinnäytetyön aikana prosessien päivityksen yhteydessä Yritys X:n vanhentuneet riskimääritelmät uusittiin, kontrollikatalogi päivitettiin ja luovutettiin lopuksi yrityksen määrittelemälle vastuuhenkilölle.

Riskiarvio on tehtävä jatkossa säännöllisesti tai vähintään aina kun prosessit muuttuvat. Riskit on priorisoitava ja sen pohjalta määritellyt avainkontrollit jalkautettava tarvittavalle tasolle. Ei riitä, että riskit ja kontrollit on määritelty, vaan niiden tarpeellisuus on perusteltava kontrollin suorittajan oman työprosessin riskien osalta. Tämä on työntekijän oikeussuojan kannalta ehdotonta, jotta hän varmistaa oman työnsä oikeellisuuden. Mikäli virheitä kontrolleista huolimatta kuitenkin syntyy ei työntekijää voida henkilökohtaisesti syyttää tapahtuneesta, vaan on tehtävä uusi arvio kyseisen kontrollin toimivuudesta.

5.2.3 Kontrollikatalogi

Opinnäytetyön aikana tehtyjen uusittujen riskimääritysten perusteella listattiin riskejä kattavat kontrollit, jotka dokumentoitiin yrityksen käytössä olevan kontrollikatalogin vaatimusten mukaisesti (Liite 3, otanta kontrollikatalogista). Kyseiset kontrollit kuuluvat prosessikontrollien ryhmään ja vaatimukset näille kontrolleille luo johdon määrittelemät tavoitteet, joita kutsutaan myös johdon tilinpäätösväittämiksi.

Opinnäytetyöntekijä täsmensi ryhmätöissä todennettujen kontrollien kuvauksia teoriasta oppimansa, sekä asiantuntijoiden kanssa käytyjen lisäkeskustelujen perusteella. Kun jokaiselle riskille oli määritelty kontrollit, koottiin ne Yritys X:n kontrollikatalogiin ja varmistettiin vielä, että kaikkiin riskeihin oli liitetty toimivat riskejä ehkäisevät kontrollit.

Kontrollikatalogin vaatimuksia on dokumentoida kyseinen prosessi, riski, kontrolli, kontrollikuvaus, suoritussykli, evidenssi ja sen kuvaus, evidenssin sijaintipaikka, tähän liittyvä ohjeistus, kontrollin koodimerkintä prosessikaaviossa, prosessin nimi ja numero prosessinkuvausjärjestelmässä, kontrollin linkitys johdon tavoitelistaukseen, kontrollin omistaja, kontrollin suorittajat sekä IT- järjestelmä johon kontrolli liittyy.

Kontrollityön aikana havaitut muihin kuin materiaali- ja tarvikevaraston prosesseihin liittyvät riskit sekä kontrollit kuvattiin myös Yritys X:n kontrollikatalogiin. Näihin muihin prosesseihin liittyvät kontrollit kuten käyttäjäoikeuskontrollien määrittely ei ollut osa kyseistä tehtävänantoa, vaan niiden kuvaus oli kyseisten prosessiomistajien vastuulla. Opinnäytetyöntekijä luovutti kontrollikatalogin yrityksen määrittelemälle vastuuhenkilölle, joka hyväksyi toimeksiannon mukaisen tehtävän suorituksen.

5.2.4 Prosessikuvaukset

Yhtiön vaatimus kuvata end-to-end prosessit liittyvät yhtiötason kontrollivaatimukseen (Entity Level Controls, ELC) joka luo pohjan sille, että prosessit voidaan kommunikoida

ymmärrettävästi organisaatiossa ja että sen perusteella pystytään määrittelemään tarvittavan ohjeistuksen sekä kontrollien taso.

Opinnäytetyön aikana laaditut prosessikuvaukset on jalkautettava organisaatioon asianmukaisella tavalla ja sovittava kuka vastaa siitä, että kuvaukset pysyvät ajan tasalla. Materiaali- ja tarvikevaraston prosessit on päivitettävä jatkossa säännöllisesti ja aina kun joko end-to-end prosessi tai jokin prosessi muuttuu. Mikäli toiminnanohjausjärjestelmässä tapahtuu muutoksia tai Yritys X:ssä otetaan käyttöön uusi toiminnanohjausjärjestelmä, täytyy prosessit tarkistaa sellaisten asiantuntijoiden kanssa, joilla on riittävä ymmärrys siitä, miten muutos vaikuttaa eri järjestelmiin ja raportointiin. Yrityksen on määriteltävä, kuinka usein prosessipäivitykset on tehtävä ja kuka vastaa näiden päivityksestä sekä muutosten koulutuksesta.

5.2.5 Käyttäjäoikeuskontrollit

Opinnäytetyön tekijän yhtenä tehtävänä oli havainnoida prosesseihin liittyviä ongelmia ja antaa näihin mahdollisia ratkaisuehdotuksia. Ennen Yritys X:n toimeksiannon alkua opinnäytetyöntekijä oli jo tietoinen että materiaali- ja tarvikevarastoprosesseihin liittyy paljon selvitettäviä sekä tarkennettavia työtapoja. Erilaisia ongelmia ilmeni erityisesti käyttäjäoikeuksiin ja eri prosessien väliseen yhteiseen toimintatapaan liittyen.

Johdon valtuutuksiin liittyvän dokumentoinnin ja kontrollien määrityksen osalta havaittiin puutteita. Ohjeistuksessa on kerrottava kuka saa suorittaa tiettyä yhtiön toimintoa ja mitkä ovat esimerkiksi työntekijälle määritellyt tilaus- tai laskunhyväksymisrajat. On toivottavaa, että tällaiset suuntaviivat kuvataan yhtiötason ohjeissa ja niistä johdetaan yksikkö- ja prosessitasolla olevat yksityiskohtaisemmat valtuutusohjeet.

Eri laitteiden ja järjestelmien osalta haetaan ja hyväksytään käyttäjäoikeuksia johdon valtuutuksen ja yrityksen määrittelemän käyttäjäoikeusprosessin mukaisesti. On suositeltavaa, että vastuuhenkilöt ajavat järjestelmäkohtaisesti käyttäjäoikeusraportit kahdesti vuodessa, **tarkistavat että vain valtuutetut henkilöt** löytyvät näiltä listoilta ja heillä on vain tarpeellinen määrä rooleja tai oikeuksia kyseiseen järjestelmään. Ylimääräiset oikeudet kuten myös ylimääräiset käyttäjät pyydetään poistamaan järjestelmistä.

Yrityksessä on vanhentuneita roolimäärityksiä ja sen vuoksi suositeltavaa on rakentaa **uudet käyttäjäoikeusroolit** erillisten toimenkuvien mukaisesti, jolloin vältytään liian laajojen käyttäjäoikeuksien takia virheiltä sekä vähennetään petoksen mahdollisuutta.

Yksi tärkeistä käyttäjäoikeuksiin liittyvistä kontrolleista on **vaarallisten työyhdistelmien eriyttämiskontrolli (Segregation of Duties, SoD)** jossa on tarkoitus tarkistaa, ettei henkilöllä ole ns. vaarallisia työyhdistelmiä. Yrityksen velvollisuus on listata kyseiset kielletyt yhdistelmät ja mikäli toimintoja ei voi jostain syystä eriyttää käyttäjäoikeuksien kautta, on implementoitava ns. **kompensoivat kontrollit,** joiden tarkoitus on tarkistaa, että väärinkäytöksiä ei ole tapahtunut.

5.2.6 Sovelluskontrollit (Application Controls)

Sovelluskontrollit määritellään järjestelmäkohtaisesti yhteistyössä prosessiomistajien ja IT:n kanssa. Nämä kontrollit estävät, ettei järjestelmässä tehdä kuin johdon valtuuttamia tai muita ohjeistettuja toimintoja ja näin vähennetään virheiden ja petoksen riskejä. Tällaisia kontrolleja voi olla, esimerkiksi että järjestelmä estää laskun tarkastajaa olemasta sama henkilö kuin hyväksyjä tai järjestelmässä on hyödynnetty pakollisia kenttiä, joita ei voida ohittaa ja täten ohjataan käyttäjää automaattisesti toimimaan oikein.

Koska käyttäjät jättivät toiminnanohjausjärjestelmässä usein pakollisia kenttiä täyttämättä tai käyttivät riittämätöntä tietoa, tarjottiin yritykselle ratkaisuksi räätälöityjä kenttiä, jotka ohjaavat käyttäjää toimimaan oikein. Yritys X lähti tutkimaan mahdollisuutta rajata kenttiä, mutta mahdollisuuksia muokata toiminnanohjausjärjestelmän tarjoamia rajoituksia pitäisi osata hyödyntää paremmin.

5.2.7 Valvonta ja monitorointi

Yrityksen noudattama sisäisen valvonnan viitekehys määrittelee, miten kontrollin suorittamista on valvottava. Kontrollin suoritus ja evidenssin oikeellisuus on monitoroitava yhtiötason kontrollivaatimuksen mukaisesti ja havaitut virheet on raportoitava hallinnointimallin mukaisesti. Päivitetyt prosessit tulee käydä läpi sidosryhmien kanssa ja tarvittaessa laatia ohjeet uusien tai epäselvien toimintatapojen työvaiheisiin. Varastohenkilökunnan ja muiden sidosryhmien osalta havaittiin epäselvyyksiä rooleissa sekä vastuissa ja nämä tulee määritellä uudelleen yhtiön hallintamallin määräämien roolien mukaisesti.

5.3 Pohdintaa

Opinnäytetyön tekeminen on antanut ymmärrystä mitä kaikkea sisäisen valvonnan viitekehyksellä tarkoitetaan, miten sen vaatimukset näyttäytyvät käytännön tasolla ja minkälaisia haasteita yritys saattaa kohdata riskiperusteisen kontrollikatalogin luomisessa ja se jalkauttamisessa organisaatioon. Toimeksiannon parissa työskennellessä opinnäytetyönte-

kijä huomasi kuinka tärkeää yhtenäisten toimintatapojen ja ohjeiden ylläpitäminen on yrityksen oikeanmukaisen raportoinnin kannalta. Tämä myös helpottaa yksittäisen työntekijän toimenkuvaa, selkeyttää työtehtäviä sekä vastuita ja vähentää inhimillisen virheen riskiä.

Yksityiskohtaiset kontrollien kuvaukset antavat ohjeistusta ja neuvoa miten organisaation tulee toimia saavuttaakseen johdon tavoitteet. Erityisen tärkeää on huolehtia siitä, että kontrollit jalkautetaan ymmärrettävällä tavalla organisaatioiden joka tasolle ja kontrollin suorittajat koulutetaan asianmukaisella tavalla niin, että sisäisten valvonnan tavoitteet ymmärretään yksilötasolla jokapäiväisinä tehtävinä oman työtehtävän näkökulmasta. Mikäli kuitenkaan rooleja ja vastuita ei ole selkeästi kommunikoitu työyhteisölle voi syntyä tilanteita, joissa sisäisen valvonnan toimenpiteitä pallotellaan edes takaisin ja selkeyden sijaan päädytään vain turhaa energiaa vievään väittelyyn.

Usein on, että työntekijät kokevat aluksi kontrollit vain ylimääräisenä työtehtävänä eivätkä heti ymmärrä niiden merkitystä oman työn tavoitteiden ja tätä kautta koko yhtiön tavoitteiden kannalta. Siksi johdon on tärkeää perustella kontrollivaatimuksensa perusteellisesti, jotta työntekijät ymmärtävät minkä takia kontrolleja tulee suorittaa ja mitä hyötyä kontrolleista on sekä yksilön, että yhtiön kannalta. Näin saavutetaan aito sitoutuminen sisäisen valvonnan toimenpiteiden osalta ja organisaation yhteiset tavoitteet saadaan toteutumaan.

5.3.1 Tutkimuksen kulku ja luotettavuus

Opinnäytetyön päätavoitteena oli selvittää ennalta määriteltyjen osaprosessien osalta havaitut puutteet sisäisen valvonnan eri osa-alueiden suhteen. Työ aloitettiin ”AsIs” tilanteen kartoituksella. Olemassa oli vanhentuneita prosessikaavioita, joita ei kuitenkaan enää pystytty hyödyntämään prosessien kuvauksessa ja tästä syystä päädyttiin kuvaamaan kaikki materiaali- ja tarvikevaraston prosessit uudelleen. Tästä syystä myös riskit ja kontrollit määriteltiin kokonaan uudelleen. Tämän jälkeen siirryttiin ”ToBe” vaiheeseen, jossa prosessit oli kuvattu, kontrollikatalogi päivitetty ja kontrollikuvaukset tehty. Seuraavana vuorossa on kontrollievidenssin määrittely niiltä osin, kun sitä ei vielä pystytty tekemään ja korjaavien toimenpiteiden ehdotuksen laadinta sekä työn esittely kohdeyrityksen organisaatiolle, jonka jälkeen raportti hyväksyttiin vastuullisen henkilön toimesta.

Tuoretta ja luotettavaa suomenkielistä lähdeaineistoa kirjallisuuden muodossa oli melko vähän ja siksi teoriaosuudessa käytettiin laajasti Niina Ratsulan päivitettyä Yrityksen sisäinen valvonta 2016 kirjaa. Tämän lisäksi tutustuttiin kuitenkin laajasti kyseiseen aiheeseen

liittyviin sekä suomen- että englanninkielisiin lähdeaineistoihin, jotka täydensivät ja antoivat syvällisempää ymmärrystä siitä, mitä kaikkia eri osa-alueita sisäiseen valvontaan liittyy ja mitkä ovat ne lait ja säädökset, joita yrityksen tulee noudattaa sisäisen viitekehyksen määrittelyn suhteen.

Teoriaa aiheesta löytyi lopulta paljon, asia oli uutta ja tuntui mielenkiintoiselta, olikin vaikeaa säilyttää tasapaino siinä, miten paljon opinnäytetyöhön tulisi sisällyttää teoriaa ja millä tasolla itse opinnäytetyön tavoitteiden kuvaamiseen ja tutkimuskysymyksiin vastaamiseen tulisi käyttää aikaa. Oli mielenkiintoista havaita, että yrityksen sisäinen valvonta ja sisäinen tarkastus tulisi selkeästi erottaa toisistaan aivan erilaisten roolien ja vastuiden vuoksi. Yksi sisäisen valvonnan keskeisimmistä rooleista on toteuttaa ja varmistaa se, että johdon asettamat riskit on katettu kontrollien avulla ja että toteutumisesta on raportoitava johdolle. Sisäinen tarkastus on taas riippumaton elin, joka valvoo, että kontrollitoimenpiteet ovat riittävät suojaamaan yritystä virheiltä ja väärinkäytöksiltä ja näin voidaan vakuuttua raportoinnin oikeellisuudesta.

Laadullinen tutkimustapa toimi tässä tapauksessa erittäin hyvin. Tätä tuki olennaisesti se, että opinnäytetyöntekijä työskenteli kyseisten asioiden ja organisaation kanssa pitkään ja sai luotua luonnollisen ja luottamuksellisen dialogin organisaation kanssa joka näin ollen kertoi havaitsemistaan virheistä ja mahdollisista väärinkäytösmahdollisuuksista avoimesti. Myös työskentelyyn valittu ryhmätyötapa mahdollisti asiantuntijoiden kesken mahdollisuuden hyvään dialogiin. Tätä kautta perusteellisen ja luotettavan riskienhallintaprosessin kautta päästiin kattavaan kontrollikuvaukseen.

Kontrollit ja eritasoiset ohjeet selkeyttävät koko organisaation toimintatapoja ja näin ehkäisevät virheitä ja väärinkäytöksiä ja auttavat yritystä harmonisoimaan kuunvaihteen raportointiprosessia ja sitä kautta vältytään ylitöiltä ja henkilöstön hyvinvointi paranee samalla kun virheet sekä epäselvyydet vastuissa vähenevät. Selkeät työohjeet auttavat myös muita toimijoita ymmärtämään kyseistä prosessia paremmin ja yhteinen luottamus eri sidosryhmien välillä paranee. Nyt luotua ohjeistusta ja kontrollikatalogia on tarkoitus käyttää laajalti yhtiön niissä eri toimipisteissä, joissa on samankaltaista varastotoimintaa. Näin mahdollistetaan harmonisoitu toimintatapa, ohjeistus ja kontrollitoimenpiteet läpi koko yrityksen ja tämä antaa yrityksen johdolle kattavan ja luotettavan kuvan raportoinnin samanmuotoisuudesta ja oikeellisuudesta

5.3.2 Oma oppiminen

Työskentely kohdeyrityksessä on opettanut paljon uutta työelämään liittyvistä prosesseista, kommunikoinnin tärkeydestä, erilaisista haasteista sekä lopulta onnistumisen tunteesta silloin kun vaikea ongelma on saatu selvitettyä. Yrityksessä työskentely ja lopputyön tekeminen on kehittänyt opinnäytetyön kirjoittajan aikataulujen hallintaa, muutosvalmiutta sekä ihmissuhdetaitoja. Opinnäytetyötä tehtäessä keskustelujen sekä avoimuuden tärkeys korostui ja kärsivällisyys lisääntyi, kun opinnäytetyöntekijä joutui kohtaamaan suuren organisaation kohdistaman paineen sekä aikataulujen sovittamisen eri osa-alueiden asiantuntijoiden kanssa toimeksiannon loppuun saattamiseksi. Toisaalta kohdattaessa vaikeilta tuntuneita ongelmatilanteita toimeksiannon parissa, saavutti opinnäytetyöntekijä myös onnistumisen tunteen.

Opinnäytetyöntekijä ei alkuun käsittänyt kuinka laajasta kokonaisuudesta on kyse, kun hän otti vastaan Yritys X:n toimeksiannon. Työmäärä oli oletettua suurempi ja tämä osaltaan loi haasteita alkuperäisen aikataulun suhteen. Tästä syystä suunnitelmaan jouduttiin tekemään muutoksia, yksinkertaisesti aika ei riittänyt suorittamaan tehtävää opinnäytetyöntekijän halutulla vaatimustasolla, annetussa aikahaarukassa. Opinnäytetyö on ollut erittäin haastava prosessi koska yrityksen sisäisen valvonnan riski- ja kontrollitoimet eivät olleet opinnäytetyön kirjoittajalle entuudestaan tuttu kokonaisuus. Projekti oli kaiken kaikkiaan erittäin haastava, mutta samalla opettavainen.

Työryhmätyöskentelykoordinaattorina toimiminen toi esiin paljon projektin hallintaan liittyviä ongelmia. Ongelmien selvittäminen on kehittänyt opinnäytetyöntekijän ongelmanratkaisutaitoja. Projektin myötä yrityksen useampi osasto sai lisätietoa, miten heidän tulee toimia jatkossa, mitkä ovat heidän vastuitaan ja mitkä ovat niitä töitä, joista muut osastot huolehtivat. Ostolasku- ja varastojärjestelmien kontrollit esimerkiksi kuvataan erillisen Master Data -tiimin toimesta eikä osto- tai varastotiimien tarvitse näitä kontrolleja suorittaa.

Vaikka aikataulut oli alustavasti suunniteltu, tietoisuus tarkan suunnitelman tekemisen tärkeydestä korostui ja sitä kautta ymmärrys kasvoi siihen, että suunnitelmat harvoin todellisessa elämässä toteutuvat alkuperäisen aikataulun mukaisesti, varsinkin suuren yrityksen ollessa kyseessä. Kun aikataulussa ei jostain syystä pysytä, on erityisen tärkeää huolehtia suunnitelman reaaliaikaisesta päivityksestä heti kun havaitaan esteitä alkuperäisen suunnitelman toteutumisen suhteen.

Opinnäytetyöhön liittyvät muutostarpeet johtuivat sekä ulkopuolisista tekijöistä, että opinnäytetyöntekijään liittyneistä muuttuvista olosuhteista. Ulkopuolisia muutospaineita tuli sitä kautta, että kaikkia työryhmän jäseniä oli vaikea saada yhteiseen palaveriin tai tärkeille prosessien asiantuntijoille tuli esteitä ja palavereja jouduttiin siirtämään.

Opinnäytetyöntekijälle tarjoutui myös mahdollisuus pidempään määräaikaiseen työsuhteeseen ja uuden oppiminen sekä työn kireät aikataulut aiheuttivat muutospaineita, jolloin suunnitelmia ja toteutusaikatauluja jouduttiin päivittämään. Kun sitten toimeksiantajayrityksen tavoitteet opinnäytetyön osalta oli saavutettu syksyllä 2018, opinnäytetyöntekijän äitiysloma siirsi itse opinnäytetyön valmistumista vuodella eteenpäin.

Toisaalta aikataulutuksen kannalta oli vaikeaa sovittaa yhteen opinnäytetyön tekemisen aikana saatu uusi vaativa määräaikainen työ ja opinnäytetyön yhtäaikainen eteenpäin vieminen. Priorisointi näiden kahden tehtävän välillä oli erityisen haastavaa erityisesti johtuen siitä, että opinnäytetyön teettäjä oli eri henkilö kuin varsinainen oma esimies, jonka mielestä itse uusi määräaikainen työ tuli suorittaa ykkösprioriteetilla.

Lähteet

Aaltio, I. 1999. Case-tutkimus metodisena lähestymistapana. Luettavissa: https://metodix.fi/2014/05/19/aaltio-marjosola-casetutkimus/. Luettu 17.10.2019

Arvopaperimarkkinayhdistys ry 2015a. Corporate Governance, mitä se on? Luettavissa: https://cgfinland.fi/corporate-governancesta/corporate-governance-mita-se-on/. Luettu: 16.5.2019.

Arvopaperimarkkinayhdistys ry 2015b. Hallinnointikoodi 2015. Luettavissa: https://kauppakamari.fi/wp-content/uploads/2013/01/hallinnointikoodi-2015.pdf. Luettu: 16.05.2019.

COSO 2004. Kokonaisvaltainen ajatusmalli organisaation riskienhallintaan. Luettavissa: https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Finnish.pdf. Luettu: 19.5.2019

COSO 2013. The 2013 COSO Framework & SOX Compliance. Luettavissa: https://www.coso.org/documents/COSO%20McNallyTransition%20Article-Final%20COSO%20Version%20Proof_5-31-13.pdf. Luettu 15.6.2019.

COSO 2017. Enterprise Risk Management. Luettavissa: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf. Luettu 24.5.2019

Edelkoort Smethurst Schein 2010. Entity level controls. Luettavissa: https://escpas.com/sox/entity-level-controls-test-procedures. Luettu 30.5.2019.

Honkaranta, T. 23.8.2017. Tase-erien keskeiset kontrollit. Tilisanomat. Luettavissa: https://tilisanomat.fi/yritysjuridiikka/tase-erien-keskeiset-kontrollit. Luettu 2.6.2019.

Noukka, L. 18.10.2017. COSO ERM uudistui – eroon kuutioajattelusta. RISKI blogi. Luettavissa: https://riskiblogi.fi/?p=429. Luettu: 24.5.2019.

PCAOB 2007. Auditing Standard No. 5. Luettavissa: https://pcaobus.org/Standards/Archived/PreReorgStandards/Pages/Auditing_Standard_5.aspx. Luettu: 19.5.2019.

Protiviti 2007. Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements. Luettavissa: https://www.protiviti.com/sites/default/files/united_states/insights/protiviti_section_404_faq_guide.pdf. Luettu: 16.5.2019.

Protiviti 2014. The Updated COSO Internal Control Framework. Luettavissa: https://www.protiviti.com/sites/default/files/united_states/insights/updated-coso-internal-control-framework-faqs-third-edition-protiviti.pdf. Luettu: 15.5.2019.

Ratsula, N. 2016. Yrityksen sisäinen valvonta. Edita Publishing Oy. Helsinki.

Ratsula, N. 2018. Mitä on sisäinen valvonta? Luettavissa: http://www.codeofconduct.fi/2009/03/20/mita-on-sisainen-valvonta/. Luettu: 14.5.2019.

Sisäiset tarkastajat ry 2019. Sisäinen valvonta ja riskien hallinta. Luettavissa: https://theiia.fi/sisainen-tarkastus/sisainen-valvonta-ja-riskien-hallinta-2/. Luettu: 14.5.2019.

The Institute of Internal Auditors 2013. The Three Lines of Defense in effective Risk Management and control. Luettavissa: https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf. Luettu: 26.5.2019.

Turun kaupunki 2015. Riskienhallinnan ja sisäisen valvonnan ohje. Luettavissa: http://ah.turku.fi/kh/2015/0907021x/3282984.htm. Luettu:20.5.2019

Yritys X. 2018. Intranet.

Yritys X. 2019. Yritys X:n internetsivusto. Three Lines of Defence. luettu 19.5.2019.

Liitteet

Liite 1. Opinnäytetyön toimeksianto

LOPPUTYÖN LAATIMINEN JA SIIHEN LIITTYVÄT MUUT SOVITUT TEHTÄVÄT, Emilia Muhonen

1. Laadittavat dokumentit

a) Lopputyö Haaga-Helialle
Lopputyö laaditaan [redacted] varastohallinta-projektin sisäisistä kontrolleista. Lopputyöstä tehdään tutkimussuunnitelma, jonka hyväksyy osaltaan [redacted] lopputyön ohjaaja. Lopputyö koostuu teoria-osuudesta sekä case-esimerkistä. [redacted] nimeä ei julkaista. [redacted] lopputyön ohjaaja hyväksyy osaltaan lopputyön.

b) Raportti [redacted]
[redacted] sisäiseen käyttöön laaditaan kirjallinen, [redacted] lopputyön ohjaajan hyväksymä, raportti [redacted] k[redacted] varastohallinta-projektin etenemisestä sisäisten kontrollien näkökulmasta. Raportti sisältää havainnot ja suositukset kehitystoimenpiteiksi sisäisten kontrollien osalta. Raportti koostuu kohdassa 2. mainituista asioista.

2. Tehtävät liittyen yllämainittuihin dokumentteihin

a) Materiaalivaraston prosessikontrollit
- Materiaalivaraston prosessikuvauskokouksiin osallistuminen ja dokumentoijana toimiminen (dokumentointivastuu)
- Materiaalivaraston prosessiriskien tunnistaminen, kontrollien määrittäminen tunnistettujen riskien minimoimiseksi sekä näiden dokumentoinnista vastaaminen sekä [redacted] että kontrollikatalogiin (koordinointi- ja dokumentointivastuu)
- Materiaalivarastojen hallintaan liittyvän ohjeistuksen kommentointi ja kattavuuden arviointi sisäisten kontrollien näkökulmasta (kommentointivastuu)
- Käyttövaltuudet ja vastuut

b) Käyttövaltuudet ja vastuut
Materiaalivaraston hallinnan osalta roolien, vastuiden sekä [redacted] käyttövaltuuksien läpikäynti (selvitys- ja dokumentointivastuu).

3. Työhön käytettävä aika
Lopputyön laatimiseen voi käyttää [redacted], joka ei sisällä mm. projektipalavereja

4. Aikataulu dokumenttien valmistumiselle

a) Välitavoite
Välitavoitteena on hyväksytty tutkimussuunnitelma sekä luonnos [redacted] toimitettavasta raportista, joka sisältää alustavat havainnot sekä prosessikontrolleihin että käyttövaltuuksiin liittyen. Edellä mainitut tehtävät tulee olla valmiit 31.12.2017 mennessä.

b) Lopputyön valmistuminen ja raportti [redacted]
Yllämainittujen kohtien osalta sekä lopputyö että raportti [redacted] tulee valmistua 30.4.2018 mennessä.

ALLEKIRJOITUKSET

Liite 2. Opinnäytetyö suunnitelma ja toteutus

Opinnäytetyöprosessin suunnitelma		Toteuman status	Suunnitelma / Toteuma	Päivitetty Suunnitelma / Toteuma	Päivityksen syy
1. Prosessin alkusuunnittelu			**2017**		
1	Yritys X:n toimeksianto	100 %	10/2017	-	-
2	Prosessikuvauksiin osallistuminen	100 %	11/2017	-	-
3	Sisäiseen valvontaan tutustuminen	100 %	10/2017 alkaen	-	-
4	COSO kontrolliviitekehykseen tutustuminen	100 %	11-12/2017	-	-
5	Riskinarviomalleihin tutustuminen	100 %	11-12/2017	-	-
6	Suunnitelma, ehdotus Yritys X:lle	100 %	11/2017	-	-
2. Toimeksiannon välitavoite			**2018**		
1	Hyväksytty aiheanalyysi koululle	100 %	1/2018	-	-
2	Yritys X:n raportin alustavat havainnot:	100 %	12/2017	-	-
2.1.	alustavat havainnot prosessikaavioihin liittyen	100 %	12/2017	1/2018	Aikataulumuutos työryhmän ehdotuksen mukaisesti.
2.2.	alustavat havainnot käyttövaltuuksiin liittyen	100 %	12/2017	3/2018	Aikataulumuutos työryhmän ehdotuksen mukaisesti.
3	Yritys X:n toimeksiannon päivitys	100 %	2/2018	-	-
4	Prosessikuvaukset tarkistettu	100 %	12/2017	2/2018	Aikataulumuutos työryhmän ehdotuksen mukaisesti.
3. Riskien ja kontrollien läpikäyntiä (AsIs)			**2018**		
1	Ryhmätöiden ym. resurssien suunnittelu	100 %	1/2018	-	-
2	Prosessikuvausten koordinointi ja ryhmätyöt	100 %	1-3/2018	-	-
3	Riskinarviointimalli	100 %	3-/2018	-	-
4	Riskien läpikäynti ja päivitys	100 %	3-4/2018	2-5/2018	-
5	Riskien priorisointi	100 %	4/2018	2-5/2018	-
6	Olemassa olevan prosesikaavion läpikäynti ja luovutus sekä kontrolliviitekehyksen työstäminen	100 %	4/2018	5/2018	Prosessikuvaukset käyty läpi ja luovutettu prosessiasiantuntijalle.
4. Kontrolliviitekehyksen päivitys (ToBe)			**2018**		
1	Kontrollikatalogin päivitys riskiarvioon perustuen	100 %	4/2018	7-9/2018	Lopputyöntekijän uusi positio.
2	Johdon asettamien tavoitteiden tunnisteminen ja linkitys riskeihin	100 %	4/2018	7-9/2018	Lopputyöntekijän uusi positio.
3	Avainkontrollit ja kontrollikuvaukset	100 %	4/2018	7-9/2018	Lopputyöntekijän uusi positio.
4	Kontrollievidenssin määrittely ja evidenssin sijainti	100 %	4/2018	7-9/2018	Lopputyöntekijän uusi positio.
5	Korjaavien toimenpiteiden ehdotuksen teko ja esittely kohdeyrityksen organisaatiolla. Hyväksytyn raportin palautus.	100 %	4/2018	10/2018	Hyväksytty raportti palautettu 10/2018.
5. Lopputyön dokumentaation lopullinen tavoite ja toteutus			**2018**		
1	Sisällysluettelo viimeistely (contenct and scope)	100 %	4/2018	4/2019	Lopputyöntekijän äitiysloma.
2	Opinnäytetyöohjaaja kanssa sovittu opinnäytetyöprosessin jatkosta ja loppuun saattamisesta vuoden 2019 loppuun mennessä	100 %	-	5/2019	Lopputyöntekijän äitiysloma.
3	Lopputyöhön liitettävät kaaviot ja niiden linkit	80 %	4/2018	10/2019	Lopputyöntekijän äitiysloma.
4	Lopputyön Word-documentin palautus koululle	0 %	4/2018	10/2019	Lopputyöntekijän äitiysloma.
5	Lopputyön läpikäynti kohdeyrityksessä	0 %	4/2018	11/2019	Lopputyöntekijän äitiysloma.
6	Lopputyön läpikäynti oppilaitoksessa	0 %	12/2018	11/2019	Lopputyöntekijän äitiysloma.
7	Opinnäytetyön viimeistely ja palautus koululle	0 %	12/2018	11/2019	Lopputyöntekijän äitiysloma.
8	Hyväksytty opinnäytetyö	0 %	12/2018	12/2019	Lopputyöntekijän äitiysloma.

Liite 3. Ote Yritys X:n kontrollikatalogista

CONTROL CATALOG
Updated: **1.8.2018**

Process	Risk	Control Name	Control Description	Evidence of control	A / M	Evidence of control
1 Manage external material needs	1) Inventory level is not checked. 2) There is no permission for selling inventory part. There is a risk that inventory level gets too low.	Inventory level check and permission for selling granted	In case of external material request the inventory level is checked by material sender (techical). Permission for sale is approved by warehouse responsible person according to approval limits. Approval is documented (sales of external materials is an exception and needs to be concidered case by case).	Approval of the sales from the inventory including the documentation of invetory level check.	M	Approval of the sales from the inventory including the documentation of invetory level check.
2 Manage external material needs	Sales price of inventory part is incorrect. Selling with too low price increases production costs.	Material price check	Material price is checked before spare part is sold. Definition of the material sales price is calculated according to specific instructions.	Sales price calculation.	M	Sales price calculation.
3 Manage internal material needs	Inventory receipts are not recorded on a timely manner. Inventory receipts may not be recorded correctly and/or incorrect qualities and/or quantities are received and recorded.	Goods receipt verification (inventory parts)	Performer verifies that: a) the amount of goods received matches to the amount of goods ordered displayed in the purchase order in [redacted] b) the quality of goods received matches to the quality of the goods ordered displayed in the purchase order in [redacted] Performer then performs goods receipt in [redacted]	Received delivery note and corresponding goods receipt entry in system.	M	Received delivery note and corresponding goods receipt entry in [redacted]
4 Manage internal material needs	Outside inventory office time: 1. Unauthorized person is able to collect material from inventory with or without documenting the inventory collection. 2.Collection of inventory material is not documented at all leading to incorrect quantities in inventory.	Outside inventory office time: 1) Prevention of unauthorized collections 2) Documentation of inventory collection outside of office time.	Outside inventory office time: 1) Access to inventories prevented for unauthorized persons. 2) Documentation of inventory collection is performed according to specific instructions.	1) List of authorized persons having access to the warehouse. 2) Specific signed templates for collection of inventory materials outside the office time.	A/M	1) List of authorized persons having access to the warehouse. 2) Specific signed templates for collection of inventory materials
4 Manage internal material needs	Inside inventory office time: 1) Unauthorized person is able to collect material from inventory creating risk of fraud. 2) Waybills for materials not taken into physical inventory are not delivered to the technical receiver and the materials are not recorded into system in time or not at all leading incorrect inventory balances.	Inside inventory office time: 1) Prevention of unauthorized collections 2) Recording of material receipt	Inside inventory office time: 1) Access to inventories prevented for unauthorized persons. 2) Records of inventory receipts are done according to specific instruction. Physical inventory for material outside of physical inventory to be performed on regular bases.	1) List of authorized persons having access to the warehouse. 2) Follow up of open/undelivered items e.g. using the agreed delivery date information as support material.	A/M	1) List of authorized persons having access to the warehouse. 2) Follow up of open/undelivered items e.g. using the agreed delivery date information as support material.
5 Manage internal material needs	Mandatory documents are missing and material is not traceable.	Documentation of material receipt	All inventory receipts related documents e.g. way bills are stored according to instructions.	All inventory receipts related documents are store in Warehouse in a map/folder.	M	All inventory receipts related documents are store in Warehouse in a map/folder.
2 Manage material returns	Inventory items are incorrectly returned to inventory. Missitatement of inventory. Transfer of goods is not accurately documented and recorded in the inventory system. Goods can not be tracked, missiatement of inventory. Material is no longer usable.	Excess material is returned to inventory correctly and compliltely.	1) Performer performs a logical check for the goods by checking: - return is approved - where does the return come from - number of material requisition - work order number - non inventory part (approval, PO number and information of row from where the return is done)	Documentation of performed logical check.	M	Documentation of performed logical check.

Liite 4. Käyttäjävaltuuksiin liittyviä kysymyksiä

1. Millä perusteella uusi henkilö on lisätty tiettyyn käyttäjäryhmään?
   a) Positiokohtainen
   b) Osastokohtainen
   c) Toimipistekohtainen
   d) Jotain muuta

2. Onko kaikkien nykyisten käyttäjien ryhmämäärittelykriteerit samanlaiset?

3. Sisältääkö eri ryhmät eri rooleja ja transaktioita?

4. Onko käyttäjiä korvamerkattu niin että heidät voi tunnistaa osastokohtaisesti?

5. Onko käyttäjälistat ajettu ja lähetetty osastokohtaisesti tarkistettavaksi, jos/kun osastot ovat raportoineet muutoksista onko vastaavat muutokset viety järjestelmään?

6. Onko työsuhteen lopettaneet tai toiselle osastolle vaihtaneet käyttäjäoikeudet päivitetty/poistettu?

7. Miten on määritelty käyttäjäoikeuksien objektitaso, eli miten yhtiö/tehdas kohtaiset oikeudet on määritelty?