Tomi Koistinen

TAPAUSTUTKIMUS KONTROLLIEN KEHITTÄMISESTÄ TALOUDEN PROSESSEISSA SOX:N VAATIMUSTEN POHJALTA TIETOJÄRJESTELMIEN NÄKÖKULMASTA

Tietojärjestelmätieteen pro gradu -tutkielma

2.9.2007

Jyväskylän yliopisto
Tietojenkäsittelytieteiden laitos
Jyväskylä

TIIVISTELMÄ

Koistinen, Tomi Ilmari
Tapaustutkimus kontrollien kehittämisestä talouden prosesseissa SOX:n vaatimusten pohjalta tietojärjestelmien näkökulmasta/ Tomi Koistinen
Jyväskylä: Jyväskylän yliopisto, 2007
134 s.
Tietojärjestelmätieteen pro gradu - tutkielma

Tässä tutkielmassa tarkastellaan kontrollien kehittämistä talouden prosesseissa Sarbanes-Oxley lain pohjalta syntyneiden käytäntöjen pohjalta. Kontrollien kehittämistä kohdeyrityksessä tarkasteltiin kirjallisuuskatsauksen perusteella määritellyn viitekehyksen avulla.

Tutkielman teoriaosuudessa perehdyttiin kontrollikäytäntöjen asettamiseen määrittelemällä tässä yhteydessä tarkoitettu oikea ja luotettava informaatio talouden raportoinnissa. Tätä tarkasteltiin vasten Sarbanes-Oxley -laissa määriteltyä sisäisen kontrollin määritelmää talouden raportoinnin oikeellisuuden ja luotettavuuden varmistamisessa.

Tutkielmassa havaittiin lain pohjalta syntyneiden kontrollikäytäntöjen hyödyntämisen olevan suomalaisen yrityksen toiminnassa erinomainen keino kehittää talouden prosessien kontrollikäytäntöjä. SOX-projekteissa käytettyjen viitekehysten pohjalta voitiin määritellä kontrollitavoitteita, joiden pohjalta kyettiin asettamaan selkeitä kehityskohteita nimenomaan suomalaisen yrityksen näkökulmasta.

AVAINSANAT: Sarbanes-Oxley, sisäinen kontrolli, oikea ja luotettava informaatio, prosessien kehittäminen, kontrolliprosessi

SISÄLLYSLUETTELO

1 JOHDANTO

Informaatio sekä sitä tukeva teknologia ovat useimmille yrityksille tärkein voimavara, vaikkakin hyvin huonosti ymmärretty. Menestyvät yritykset ymmärtävät informaation arvon liiketoiminnassa ja tämä tuottaa yrityksen omistajille lisäarvoa. Nämä yritykset myös tiedostavat ja hallitsevat niitä riskejä, joita liiketoimintaprosessien perustuminen ja riippuvuus IT:hen (informaatioteknologia) aiheuttaa. ISACA (2005b)

Kesäkuussa 2002 Yhdysvalloissa julkaistiin Sarbanes-Oxley -laki (SOX) useiden suurien julkisten yhtiöiden (kuten esimerkiksi Enron, WorldCom, Tyco & Xerox) konkurssiskandaalien jälkeen. Lain tavoitteena on ehkäistä vastaavien suurten skandaalien aiheutuminen. Lain päätarkoitus on lisätä yrityksen taloudellisen raportoinnin sekä informaation tuottamisen tarkkuutta sekä oikeellisuutta (Agrawal ym. 2006). Tavoitteena on korostaa yrityksen sisäisen tarkastuksen sekä – kontrollin asemaa ja korostaa johdon vastuuta asianmukaisen sisäisen kontrollin järjestämisestä. *Sisäisellä kontrollilla* tarkoitetaan tämän tutkielman yhteydessä niitä toimintoja sekä entiteettejä ,joiden avulla varmistetaan taloudellisen informaation oikeellisuus, tarkkuus sekä oikea-aikaisuus (Changchit ym. 1999).

Sarbanes-Oxley laki ei kuitenkaan tarjoa täysin riskitöntä liiketoimintaympäristöä, vaan sisäisen kontrollin rakentaminen lain pohjalta vasten hyväksyttyä viitekehystä tuottaa hyötyjä ja varmuutta liiketoiminnalle pitkällä aikavälillä (ISACA 2005a). Volonino:n ym. (2004) mukaan täyttääkseen lain tarkoituksen informaation laadun takaamiseksi yrityksen tulee lisätä informaationsa läpinäkyvyyttä, tarkkuutta, oikea-aikaisuutta ja luotettavuutta. Tämä nostaa esille yrityksissä tarpeen kehittää prosesseja, dataa sekä teknologia yksinkertaisemmaksi sekä standardoidummaksi (Volonino ym. 2004).

Tämän tutkimuksen teon motiivit perustuvatkin nimenomaan taloudellisen toiminnan kehittämiseen yrityksissä SOX:ssa määriteltyjen vaatimusten

pohjalta. ISACA:n (2005a) mukaan SOX:n vaatimuksiin vastaaminen tulisi nähdä ennemmin prosessina kehittää hallinnollisia rakenteita IT:n pohjalta. Tämän avulla voidaan saavuttaa kilpailullista etua suorituskykyisimmillä prosesseilla, lisätä IT:n ymmärrystä ja hallintaa sekä lisätä ymmärrystä käyttää hyväksi IT-pohjaisia ratkaisuja. Lisäksi prosessien optimointi ja integrointi turvallisuuden takaamiseksi ISACA:n (2005b) mukaan tuottaa paremmat edellytykset oikeille liiketoiminnallisille päätöksille perustuen oikeellisempaan sekä luotettavampaan informaatioon.

Haasteena SOX-projekteissa on ollut tarkkojen ohjeistusten puuttuminen lain noudattamiseksi ja tämän vuoksi suurten tilintarkastusyritysten (Ernst&Young, KPMG & PriceWaterhouseCoopers) toiminta on vaikuttanut suuresti periaatteiden ja toimintamallien kehittämiseen lain noudattamiseksi. Tässä tutkielmassa päälähdeaineistona käytetään edellä mainittujen tilintarkastusyritysten tuottamia julkaisuja sekä ITGI:n kaltaisten organisaatioiden tutkimusten tuloksia. Nämä toimivat pohjana prosessien kehittämiselle suomalaisissa organisaatioissa.

Yleisimmin käytetyt viitekehykset SOX-projekteissa THEIIA:n (2005) mukaan ovat olleet COBIT (Control Objectives for Information and related Technolgy) sekä COSO (The Committee of Sponsoring Organizations of the Treadway Commissions). COBIT tarjoaa viitekehyksen IT:n hallinnointiin sekä kontrollien määrittämiseen liiketoiminnan ja teknologian välillä. COBIT:n tavoitteena on tunnistaa liiketoimintaprosessien ja IT:n riippuvuudet. COBIT:n avulla kehitetään liiketoiminnan ja IT:n yhteistoimintaa vastamaan lisääntyviä vaatimuksia (kuten SOX). Lisäksi kehittämisellä pyritään parantamaan riskien- sekä kokonaisuuden hallintaa. COSO puolestaan määrittelee sisäisen kontrollin, joka on prosessi johon vaikuttavat organisaatio ja sen ihmiset ja joka, tarjoaa loogisen - muttei absoluuttista - varmuuden oikeellisen toiminnan todentamiseksi. COSO:n määritelmä nojaa suorituskykyiseen sekä tehokkaisiin operaatioihin, taloudellisen raportoinnin oikeellisuuteen ja lakien sekä määräysten noudattamiseen (compliance). ITG (2006b)

Tutkielman tarkoituksena on tutkia kuinka SOX:n pohjalta syntyneitä kontrollikäytäntöjä sekä kokemuksia voidaan hyödyntää suomalaisessa liiketoiminnassa. Tutkimuksen tavoitteena on löytää SOX:n pohjalta syntyneiden ratkaisujen sekä toimintamallien joukosta ne, joista voidaan hyötyä nimenomaan suomalaisen yrityksen liiketoiminnan kehittämisessä. Tutkimuksen tutkimusongelma on seuraava: Millaisin kontrollein voidaan dokumentoidusti varmentaa, että talouden prosessien tuottama informaatio on luotettavaa, oikeellista ja läpinäkyvää? Tutkimusongelma voidaan jaotella edelleen seuraaviin alakysymyksiin: 1) Millainen on talouden prosessi, 2) Millaisia ovat kontrollit, 3) Millaista on oikeellinen ja läpinäkyvä taloudellinen informaatio sekä 4) Millaisia riskejä talouden prosesseissa voi esiintyä sekä miten niitä voidaan kontrolloida? Tutkimuksen pohjalta luodaan näkökulma sekä tavoitteet kehittämissuunnitelman laatimiseen yrityksessä talouden prosessien kehittämiseksi. Tutkielma ei anna valmista ohjeistusta tai vaiheita kehittämissuunnitelman laatimiseen, vaan esittää nimenomaan sen laatimisen perusteet pohjautuen parhaisiin käytäntöihin (best practises) SOX-implementaatioprojekteista.

Tietojärjestelmäpohjaisten kontrollitoimintojen ja käytäntöjen kehittämistä tarkastellaan tässä tutkimuksessa sisäisen valvonnan näkökulmasta. Sisäisellä tarkastuksella tarkoitetaan tässä yhteydessä niitä riippumattomia sekä objektiivisia arviointi-, varmennus- sekä konsultointitoimintoja, joilla tuotetaan lisäarvoa organisaatiolle ja sen toiminnalle (THEIIA 2005). Kontrollitoimintojen ja käytäntöjen kehittämisellä pyritään luotettavaan, läpinäkyvään ja oikeelliseen raportointiin yrityksen tuloksesta ja taloudellisesta asemasta.

SOX:n myötä yritykset ovat kuitenkin löytäneet monia hyötyjä lain edellyttämien vaatimusten perusteella. Useat merkittävät hyödyt koskevat kontrollien tunnistamista, dokumentaatio- sekä testausprosessia. Evaluointiprosessi on johtanut peruskontrollien kohentumiseen päivittäisissä toiminnoissa, kuten tehtävien eriyttäminen (segregation of duties) ja yhteensovittaminen. Rittenberg & Miller (2005)

Informaatioteknologiset kontrollit koetaan usein yrityksissä kaikkein vaikeimmin hallittavaksi kokonaisuudeksi. Kontrolliympäristön kehittymisessä tärkeimmiksi osa-alueiksi koettiin kontrollien valvonta, hallituksen tietämyksen lisääminen sekä osallistuminen, sisäinen auditointi sekä yrityksen menettelyohjeen hyväksynnän parantuminen. Toisaalta suomalaisessa yritysmaailmassa IT-kontrollien tärkeys tunnistetaan yrityksissä, mutta niiden kehittämisen vastuu jää usein ainoastaan IT-organisaation vastuulle. IT-kontrollien osalta tärkeimmiksi kehityskohteiksi määriteltiin kehittyneempi tietojärjestelmien turvallisuus, tehtävien eriyttäminen järjestelmätasolla, pääsyn hallinnan kontrollointi ja valvonta, testausproseduurien parantuminen sekä ohjelmistomuutosten hallinnan kehittyminen ja prosessien määrittäminen koskien proseduurien sekä kontrollien dokumentointia. Erityisesti lisääntyvä IT-riippuvuus tunnistettiin organisaatioissa. Rittenberg & Miller (2005)

Tässä tutkimuksessa tarkastellaan talouden prosessien kehitykseen vaikuttavia tekijöitä organisaation näkökulmasta. Tämän tutkimuksen osalta näkökulmana on kehittää taloudellisen raportoinnin oikeellisuutta hyödyntäen SOX-projekteissa syntyneitä käytäntöjä sekä kontrollitoimintoja, ilman täysimittaista implementaatiota. SOX-laki nähdään suomalaisesta näkökulmasta jokseenkin byrokraattisena valvontamallina, joka ei välttämättä istu suoraan suomalaiseen yrityskulttuuriin, jossa lähtökohtaisesti ihmisten toiminta on eettisesti oikein. Opuscapita (2007)

Tärkein motiivi tämän tutkimuksen teolle muodostuu kokonaisvaltaisen ymmärryksen luomisesta ja taloudellisen raportoinnin kehittämisestä vasten uusia teknologioita, joita riippuvuus IT:stä edellyttää. Lisäksi SOX:n kaltaisen lain kehittyminen Suomessa tai suomalaisen yrityksen listautuminen SEC:iin nostaa esille tärkeyden ymmärtää järjestelmien ja taloudellisen raportoinnin kehittämistä laissa esitettyjen vaatimusten mukaisiksi. Tutkimuksen tärkeimpänä tavoitteena on tutkia, miten suomalainen yritys voi kehittyä ja hyödyntää SOX-projekteissa syntynyttä tietämystä kehittääkseen toimintaansa.

Luvussa 2 käsitellään oikean ja luotettavan informaation määritelmää sekä suomalaisen yrityksen näkökulmasta että SOX:n vaatimusten pohjalta. Luvussa 3 käsitellään talouden prosesseihin liittyviä riskejä ja kontrolleja, jotka vaarantavat oikean ja luotettavan informaation yrityksen toiminnassa. Luvussa 4 käsitellään talouden prosessien kehittämistä prosessien kehittämisen näkökulmasta ja SOX:n vaatimusten mukaisesti. Luvussa 5 perehdytään tarkemmin SOX-projektin vaiheisiin ja SOX-projekteissa opittuihin käytäntöihin. Luvussa 6 esitellään, kuinka empiirinen tutkimus toteutettiin. Luvussa 7 tutustutaan suoritettuun empiiriseen tutkimukseen ja vastataan tutkimuksessa kerätyn aineiston pohjalta tutkimuskysymyksiin. Luvussa 8 esitetään tutkimuksen pohdinta. Lopuksi luvussa 9 käsitellään tutkielman johtopäätökset.

2 OIKEELLINEN JA TODENNETTAVA INFORMAATIO

Luvussa selvitetään mitä oikea ja riittävä informaatio on suomalaisen yrityksen toiminnassa. Aluksi tutustutaan talouden informaation tuottamiseen ja pyritään hahmottelemaan informaation tuottamiseen liittyviä haasteita. Lopuksi määritellään sisäisen kontrollin olemus talouden raportoinnissa, kuvataan SOX:n vaatimusten vaikutusta talouden raportoinnin funktioon sekä määritellään miten informaatio todennetaan oikeaksi ja riittäväksi.

2.1 Oikea ja riittävä informaatio tilintarkastuksen mukaan

Oikea ja riittävä informaatio toimii yrityksen toiminnan perustana. Oikea ja riittävä informaatio varmennetaan vuotuisella tilintarkastuksella.

> *”Tilintarkastuksen tavoitteena on, että tilintarkastaja voi antaa lausunnon siitä, onko tilinpäätös kaikilta olennaisilta osin oikein laadittu voimassaolevien säännösten ja määräysten mukaisesti ja siitä, antaako se kirjanpitolaissa tarkoitetulla tavalla oikeat ja riittävät tiedot tarkastuskohteen toiminnan tuloksesta ja taloudellisesta asemasta”.* KHT-yhdistys (2004).

Tilinpäätösinformaatio toimii Leppiniemen (1999) mukaan lähtökohtana oikeille ja riittäville tiedoille kirjanpitovelvollisen toiminnan tuloksesta ja taloudellisesta asemasta. Kirjanpitolaissa (KPL) tilinpäätöksen sisällöksi määritellään:

1. Tuloslaskelma, joka kuvaa tuloksen muodostumista
2. Taloudellinen laskelma, eli tase, joka kuvaa tilinpäätöspäivän taloudellista asemaa
3. Liitetiedot, jotka ovat tuloslaskelman, taseen ja rahoituslaskelman liitteenä ilmoitettavat tiedot
4. Rahoituslaskelma, selvitys varojen hankinnasta ja niiden käytöstä

5. Kirjanpitovelvollisen tiedot toiminnan kehittymistä koskevista tärkeistä seikoista toimintakertomuksena

KHT-yhdistys (2003) määrittelee näkökulmia oikeista ja riittävistä tiedoista seuraavasti:

1. *Hyvä kirjanpitotapa on aina sisältänyt velvoitteen antaa oikeat ja riittävät tiedot tilikauden tuloksesta ja taloudellisesta asemasta tilikauden lopussa.*

2. *On aina ollut ja on edelleen hyvän kirjanpitotavan vastaista korostaa muotoa enemmän kuin asiaa.*

3. *"Oikeat tiedot" on melko ongelmaton käsitepari, kunhan pidetään mielessä olennaisuuden periaate ja muut hyvän kirjanpitotavan taustaolettamat.*

4. *"Riittävät tiedot" on vaikea käsitepari, koska ulkopuolisten tietojen mahdollisen hyväksikäyttäjän on taipumus arvioida tietojen riittävyyttä omista subjektiivisista lähtökohdistaan."*

5. *"Kuva" on myöskin hankala käsite; mikäli tilinpäätösinformaation hyväksikäyttäjä ei saa riittävistä tiedoista oikeaa kuvaa, voi syy olla informaation hyväksikäyttäjässä eikä itse annetun informaation sisällössä."*

6. *Tietoja annetaan ja kuva muodostetaan, ts. tietojen antaja ei koskaan muodosta kuvaa.*

Tilinpäätöksen laadinnassa ja tilinavausta tehtäessä noudatettavia periaatteita ovat oletus kirjanpitovelvollisen toiminnan jatkuvuudesta, johdonmukaisuus laatimisperiaatteiden ja –menetelmien soveltamisessa tilikaudesta toiseen, varovaisuus riippumatta tilikauden tuloksesta, edellisen tilikauden päättäneeseen taseeseen perustuva tilinavaus, maksupäivästä riippumaton tilikaudelle kuuluvien tuottojen ja kulujen huomioon ottaminen sekä erillisarvostus kunkin taseeseen merkittävän hyödykkeen ja muun tase-erän kohdalla. KTM (1997)

Näiden näkökulmien lisäksi tulee ymmärtää myös edellä esiintyneiden käsitteiden merkitys: *Hyvällä kirjanpito* tavalla tarkoitetaan yhtiön tai säätiön kirjanpidon laatimista voimassaolevien kirjanpitosäännösten mukaisesti. *Olennaisuuden periaate*, jonka mukaan tieto on olennaista, jos sen esittämättä jättäminen tai vääristäminen voi vaikuttaa tilinpäätösinformaation avulla tehtäviin taloudellisiin päätöksiin. *Tietojen hyväksikäyttäjä* voi tässä yhteydessä tarkoittaa esimerkiksi rahallisen pääoman yritykselle antanutta sijoittajaa. (KHT-yhdistys 2004)

2.2 Oikeellisen ja luotettavan informaation tuottaminen

Taloudellista informaatiota tuotettaessa puhutaan tässä yhteydessä yrityksen ulkopuolisille sidosryhmille tuotettavasta sekä sisäisen päätöksenteon tueksi tuotettavasta informaatiosta. Leppiniemen (1999) mukaan yrityksen taloutta koskeva informaatio taataan tilinpäätöstä koskevien säännösten avulla mihin tahansa käyttötarkoitukseen, johon julkistettavat tiedot antavat lakisääteisesti mahdollisuuden. Näin tilinpäätöksen tavoite ja laatimisnäkökulma liittyvät informaation antamiseen.

Yrityksen taloudellisesta toiminnasta ovat kiinnostuneita erityisesti osakkeenomistajat, yhteistyökumppanit sekä potentiaaliset sijoittajat, jotka vaativat, että yritykset noudattavat sekä *hyvää hallintotapaa (corporate governance)* että säännöksiä ja ohjeistuksia. Tutkimusten mukaan hyvä johtamis- ja hallintojärjestelmä ovatkin tärkeä tekijä sijoituspäätöstä tehtäessä. (KPMG 2005)

Nykyisin liiketaloudellinen raportointi, ulkoinen – sekä sisäinen laskentatoimi eivät enää perustu ainoastaan tietokoneilla tehtävään toimintaan, vaan Debreceny:n (2006) mukaan taloudellinen raportointi perustuu useisiin järjestelmiin, joiden tiedoista muodostuvat syötteet luovat laskentatoimen järjestelmän (*financial accounting system*).

Tietojärjestelmien käytön lisääntyminen yrityksissä ja viimeaikainen lainsäädännön kehitys, kuten Sarbanes-Oxley -laki (SOX), ovat lisänneet

tietojärjestelmien merkityksen tärkeyttä lakisääteisissä toiminnoissa (attest services) (O'Donnell & Rechtman 2005). Liiketoiminnan perustuminen informaatioteknologisiin sovelluksiin nostaa esiin ISACA:n (2005a) mukaan informaatioteknologian kriittisen hallinnan, joka pohjautuu seuraaviin tekijöihin:

- lisääntynyt riippuvuus informaatioon ja informaatiota tuottaviin tietojärjestelmiin
- lisääntyneet uhat; informaatioteknologiset haavoittuvuudet
- Tulevaisuudessa sitoutunut pääoma tulee lisääntymään informaatioteknologisissa investoinneissa
- Uusien teknologioiden luomat uudenlaisen liiketoiminnan mahdollisuudet

Bailey, Duke, ym. (1985) ja Changchit, Holsapple, ym. (1999) mukaan liiketoimintaa harjoittava yritys ei voi selviytyä kilpailullisessa ympäristössä ilman, että taloudellisen informaation luotettavuus ja tarkkuus voidaan varmentaa.

2.3 Sisäinen valvonta

TheIIA (2005) määrittelee sisäisen valvonnan johdon suunnittelemaksi ja asettamaksi prosessiksi, jonka tavoitteena on lieventää riskejä ja edesauttaa tavoitteiden saavuttamista. Sisäinen kontrolli yrityksissä perustuu yleisesti tunnettuihin ja hyväksyttyihin viitekehyksiin - mm. COBIT ja COSO -, jota myös Sarbanes-Oxley laki edellyttää Agrawal & Johnson & ym. (2006), ISACA (2005a), etc.

KHT-yhdistyksen (2004) mukaan sisäisellä kontrollijärjestelmällä tarkoitetaan johdon käyttöönottamia toimintaperiaatteita ja menettelytapoja, joiden tarkoituksena on auttaa, jos käytännössä mahdollista, varmistamaan, että

johdon tavoitteet saavutetaan asianmukaisesti ja tehokkaasti. On tärkeää huomata, että *sisäinen tarkastus* ei kuitenkaan tarkoita samaa kuin sisäinen valvonta. Sisäisen tarkastuksen tehtävä ja tavoite on varmistua sisäisen valvonnan toimivuudesta (Nuuttila 1997). Valvonta on toimintaa, jolla varmistetaan tavoitteiden, tehtävän tai prosessien onnistuminen. Yrityksen toiminnassa valvonta tarkoittaa yrityksen eri toimintojen oikeellisuudesta varmistumista ja tavoitteiden täyttymisen seuraamista. Suuressa yrityksessä valvonnan toteutuminen edellyttää sen luotettavuutta ja tehokkuutta. Luotettavuudesta ja tehokkuudesta voidaan varmistua sisäisellä tarkastuksella, jonka keskeisenä tehtävänä on tutkia ja arvioida edellä mainittuja valvonnan tekijöitä (Sisäiset tarkastajat r. y. 1988).

Kuten johdannossa todettiin tietojärjestelmien kasvava merkitys taloudellisessa raportoinnissa, niin tietojärjestelmien tarkastus osana sisäistä valvontaa varmistaa, että organisaation tietojärjestelmillä saavutetaan niille asetetut päämäärät ja tavoitteet. Lisäksi niiden tulee synnyttää tietoa, varmistaa tietojen saatavuus sekä tiedon säilyminen ja eheys. Tietojärjestelmätarkastuksen tulee varmentaa, että organisaation tietojenkäsittely-ympäristö on valvottu, sekä osaltaan myös varmistaa, että organisaatio noudattaa lakeja ja määräyksiä tietojenkäsittelytoiminnassaan. Nuuttila (1997).

Sisäinen kontrollijärjestelmä rakentuu ISACA:n (2000a) mukaan seuraavista komponenteista:

1. Kontrolliympäristö *(control environment)*

   Tehokkaan sisäisen kontrollin perusta on kontrolliympäristö.

2. Riskien määrittelystä *(risk assesment)*

   Riskien määrittely luo perustan kontrollien määrittelylle, joka perustuu johdon näkemykseen liiketoiminnallisista riskeistä.

3. Kontrollitoiminnoista (control activities)

Kontrollit ovat käytäntöjä ja menettelytapoja, joilla toiminta saavuttaa tavoitteensa.

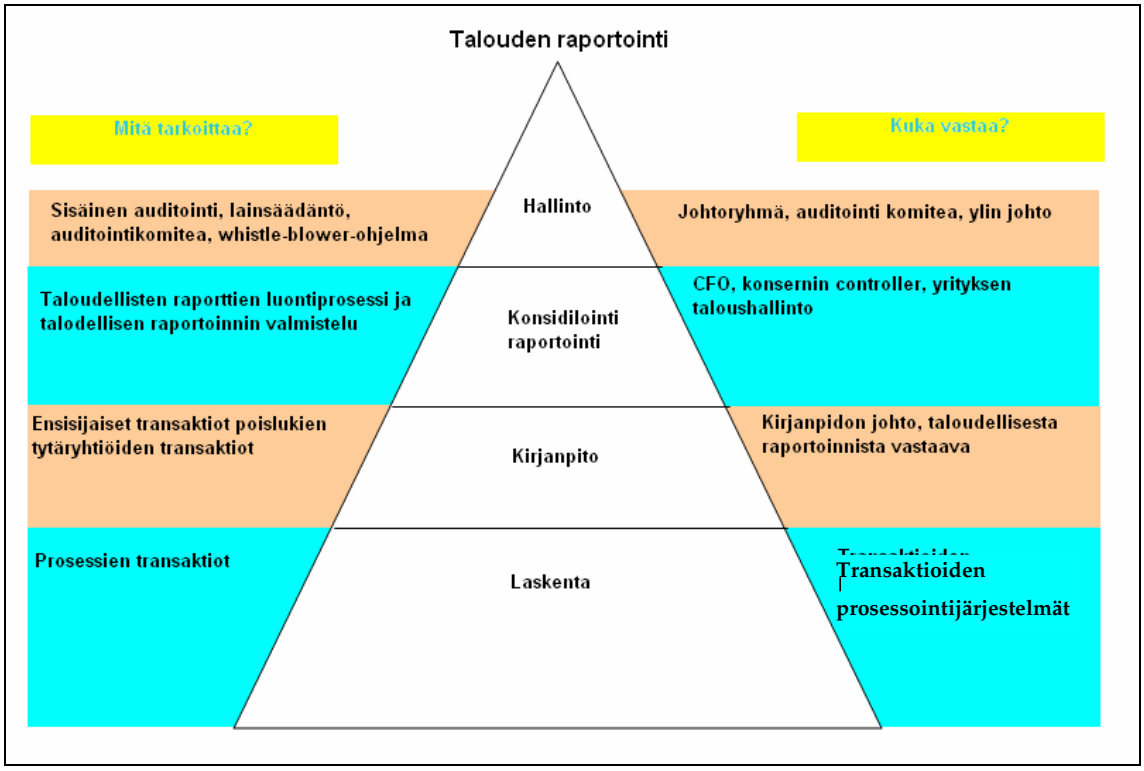
4. Informaatiosta ja viestinnästä *(information and communication)*

Informaatiota tarvitaan organisaation kaikilla tasoilla liiketoiminnan tavoitteiden saavuttamisessa. Informaation vaihtaminen, so. viestintä mahdollistaa ihmisten ja toimintojen toteutumisen. Tämä informaatio ja sen välittyminen muodostuu yhä etenevässä määrin tietojärjestelmien avulla.

5. Valvonnasta (monitoring)

Valvonnalla tarkoitetaan varmistumista sisäisen kontrollin toimivuudesta. Valvontaa on kahdenlaista: 1) jatkuvaa sekä 2) erillisiä arviointeja.

PCAOB (2004) määrittelee *sisäisen kontrollin taloudellisessa raportoinnissa* (internal control over financial reporting) olevan prosessi, jonka suunnittelee tai joka suunnitellaan johdon alaisuudessa. Sisäisen kontrollin tavoitteena on tuottaa riittävä varmuus taloudellisen raportoinnin luotettavuuteen sekä tilinpäätöksen laadintaan ulkoisia käyttötarkoituksia varten. Sisäisen kontrollin tulee olla linjassa yleisesti hyväksyttyjen kirjanpitokäytäntöjen kanssa. Sisäinen kontrolli sisältää menettelytavat ja proseduurit, jotka: 1) liittyvät asiakirjoihin, jotka kuvaavat riittävällä tarkkuudella ja oikeellisesti transaktiot ja sijainnin yrityksen varoista, 2) tuottavat riittävän varmuuden siitä, että liiketapahtumat ovat rekisteröity oikein ja kattavasti tuottaa tilinpäätös ja että tulojen sekä menojen käsittely on johdon hyväksymää ja 3) tuottavat riittävän varmuuden siitä, että taloudellisia väärinkäytöksiä, joilla voi olla oleellista vaikutusta yrityksen tilinpäätökseen, voidaan ehkäistä ja torjua. Kuvassa 1. havainnollistetaan niitä syötteitä, aktiviteettejä, raportointiprosesseja sekä raportteja, joita SOX asettaa taloudelliselle raportoinnille.



Kuva 1. Talouden raportoinnin yleiskuva SOX:n vaatimusten pohjalta. Volonino 2004

Lisäksi PCAOB (2004) määrittelee sisäisen kontrolloinnin osalta seuraavat käsitteet, joita käytetään suunnittelun periaatteina tässä tutkimuksessa:

1. *Kontrollipuute, joka ilmenee silloin, kun johto tai työntekijät eivät pysty havaitsemaan tai estämään väärinkäytöksiä riittävän aikaisin.*

    a. *puute suunnittelussa ilmenee, kun (i) riittävä kontrolli puuttuu tai (ii) käytössä oleva kontrolli on puutteellinen.*

    b. *puute toiminnossa ilmenee, kun oikeellinen kontrolli ei toimi, kuten suunniteltua tai kun henkilö ei suorita riittäviä toimenpiteitä suorittaakseen kontrollia tehokkaasti.*

2. *Merkittävä puute, tarkoittaa kontrollipuutetta tai kontrollipuutteiden yhdistelmää mikä vaikuttaa haitallisesti yrityksen kykyyn tuottaa luotettavaa informaatiota hyvän kirjanpitotavan mukaisesti. Merkittävän puutteen*

olennainen piirre on se, että on olemassa mahdollisuus puutteelliseen informaatioon taloudellisessa raportoinnissa, jota ei kyetä ehkäisemään ajoissa.

   a. *Todennäköisyyden arvioidaan olevan (i) mahdollinen, tuleva tapahtuma on todennäköinen, (ii) melko todennäköinen, tulevan tapahtuman todennäköisyys on suurempi kuin vähäinen, (iii) vähäinen, tapahtuman todennäköisyys on pieni.*

3. *Olennainen haitta, tarkoittaa merkittävää haittaa, tai useiden merkittävien haittojen yhdistelmää. Molemmat johtavat melko todennäköisesti epäluotettavaan tilinpäätösaineistoon.*

4. *Taloudellisen raportoinnin kontrollit jaetaan estäviin – ja havaitseviin kontrolleihin.*

   a. *Estävien kontrollien tavoitteena on ehkäistä virheiden, joiden vuoksi taloudellinen informaatio voi korruptoitua, syntyminen.*

   b. *Havaitsevien kontrollien tavoitteena on löytää jo sattuneet virheet, jotka voivat synnyttää virheellistä taloudellista informaatiota*

2.4 Oikeellisuuden todentaminen

Oikeellisuuden todentamisen lähtökohtana tässä tutkimuksessa toimii Sarbanes-Oxley lain vaatimus tehokkaasta sisäisestä kontrollista taloudellisessa raportoinnissa. Laki painottaa sisäisen kontrollin tehokkuutta ja yrityksen johdon vastuuta sisäisen valvonnan järjestämisestä sekä järjestelmällisestä dokumentoinnista (KPMG 2004a). Lain vaatimus nähdään usein hyvin työlääksi, mutta hyvin useat yritykset näkevät lain tuovan myös seuraavanlaisia hyötyjä: 1) sisäisen kontrollin tehon ja tehokkuuden parantuminen, 2) parantunut informaatio sijoittajille ja 3) sijoittajien luottamuksen lisääntyminen (PriceWaterhouseCoopers 2004).

Varsinaisen sisäisen kontrollin auditoinnin (auditoinnilla tarkoitetaan tässä yhteydessä vuotuista tilintarkastusta) suorittaa yrityksen tarkastava tilintarkastaja. Taloudellisen raportoinnin sisäisen kontrollin auditoinnissa tarkastajan tulee kerätä riittävästi todisteita sen suunnittelusta ja toiminnallisesta tehokkuudesta. Todisteiden tulee kattaa kaikkien merkittävien taloudellisten aineistojen muodostuminen. Tarkastajan tulee kuitenkin määritellä tarkastuksen oleellisuus ja tämän osalta suunnitella riittävän laaja tarkastus, jolla varmennetaan johdon tuottama sisäinen kontrollointi taloudellisessa raportoinnissa. PCAOB (2004)

Erityisesti sisäisen kontrollin tarkastuksessa PCAOB:n (2004) mukaan tarkastajan tulee sisällyttää toimintaansa seuraavat kohdat:

a. Toimeksiannon suunnittelu

b. Johdon prosessin arviointi

c. Yrityksen sisäisen kontrollin toteutuksen ymmärtäminen

d. Testaus ja arviointi suunnittelun tehokkuudesta sisäisestä kontrollista taloudellisessa raportoinnissa

e. Testaus ja arviointi taloudellisen raportoinnin sisäisen kontrollin tehokkuudesta

f. Arvion muodostaminen sisäisen kontrollin toteutuksesta taloudellisessa raportoinnissa

Tiedon oikeellisuuden ja sen varmentamiseksi järjestettävän sisäisen kontrollin lähtökohtana toimii Sarbanes-Oxley lain pykälä 404. Pykälässä 404 keskeisimmiksi tekijöiksi määritellään 1) riskien ja kontrollien tunnistaminen, 2) johdon arviointi toiminnasta sekä 3) dokumentoinnin vaatimukset (Securities and exchange comission 2006). Lain keskeisimmän vaatimuksen – tehokas ja luotettava sisäinen kontrolli taloudellisessa raportoinnissa – tarkoitus on

tuottaa luotettavia taloudellisia lausuntoja sekä oikeellista taloudellista informaatiota (THEIIA 2005). Lisäksi THEIIA (2005) määrittelee, että taloudellisen informaation on oltava *oleellisilta osin* (*materially)* luotettavaa. Tämän vuoksi kontrollitoimenpiteiden suunnittelussa tulisi keskittyä nimenomaan liiketoiminnan kannalta niihin toimintoihin, jotka ovat oleellisia ja näin voivat johtaa liiketoimintaa vaarantavan informaation syntyyn. Johdon tuleekin huolehtia, että tavoite ja tarkoitus sisäisen kontrollin kehittämisellä talouden informaation tuottamisessa eivät niinkään pitäisi olla tehty itsessään prosessin vuoksi. Lisäksi THEIIA (2005) täsmentää, että sisäisen kontrollin arvioinnin tulee tapahtua vuosittain.

Vastuu sisäisen kontrollin järjestämisestä on johdolla sekä ulkoisella tilintarkastajalla, joka hyväksyy johdon määrittelemän varmuuden. Johdon ei tarvitse omaksua samaa metodologiaa kuin ulkoisen auditoijan. Johdon tehtävä sisäisen kontrollin varmistamisessa pitää sen sijaan perustua siihen näkökulmaan, että seuraavan kahdentoista kuukauden aikana annettavat taloudelliset päätökset ja – informaatio ovat oikeellisia ja luotettavia. THeIIA (2005)

Tilintarkastajan hyväksytty lausunto arvioitavasta kohteesta edellyttää johdolta seuraavia toimenpiteitä (PCAOB 2004):

1. Johto on hyväksynyt vastuun sisäisen kontrollin tehokkuudesta taloudellisessa raportoinnissa

2. Johdon on arvioitava sisäisen kontrollin tehokkuutta vasten hyväksyttyä kontrollikriteeristöä

3. Johto käyttää arvion tekemiseen riittäviä todisteita, jotka ovat dokumentoidut, sekä;

4. Johto varmentaa kirjallisesti sisäisen kontrollin asettamisen ja sen tehokkuuden taloudellisessa raportoinnissa kuluvalta tilikaudelta

Johdon toimintaa arvioidessa ulkoisen tilintarkastajan tulee kiinnittää huomiota, ovatko toiminnan kannalta olennaisimmat sisäiset kontrollit asetettu, ovatko ne tehokkaita sekä kattavatko ne keskeisimmät tili- ja informaatiotiedot. Keskeisimmät kontrollit liittyvät toimintoihin, jotka vaikuttavat taloudellisen informaation synnyttämiseen, muokkaamiseen, tallentamiseen, valtuuttamiseen sekä raportointiin. Lisäksi tarkastajan tulee huomioida yleiset tietojärjestelmä-, merkittävien ei-säännöllisten toimintojen-, yritystason –kontrollit sekä yleinen kontrolliympäristö tarkastuksessaan. Arvioinnissa tulee myös käydä lävitse kontrollien suunnittelu sekä sijoittelu, so. liiketoimintayksiköiden sijoittuminen ja vaikutus kokonaisuuteen. PCAOB (2004)

Johdon dokumentaation sisällölle on asetettu SOX:n pohjalta seuraavanlaisia vaatimuksia: 1) kontrollien suunnittelussa tulee huomioida sisäisen kontrollin kaikki komponentit (COSO:n tai vastaavan määritelmän mukaan, kts. luku 2.2.1), 2) selvitys merkittävimpien transaktioiden toteutuksesta, 3) selvitys kriittisistä kohdista, joissa todennäköisin virhe voi tapahtua 4) selvitys kontrolleista, joilla ehkäistään tai tunnistetaan virhe, 5) edellisten tilikausien raportoinnin kontrollit, 6) selvitys varojen turvallisuuskontrolleista sekä 7) selvitys johdon suorittamista testeistä ja arvioinneista. Dokumentaatio toimii todisteena johdon osallistumisesta ja sitoutumisesta sisäisen kontrollin tehokkuuden varmistamiseen ja kehittämiseen. Dokumentaation tarkoitus on lisäksi luoda edellytykset viestinnälle johdon ja ulkoisen tarkastajan välillä sekä toimia perustana kontrollien kehittämiselle ja vastuuttamiselle. PCAOB (2004)

2.5 Yhteenveto

Oikea ja riittävä informaatio toimii yrityksen päätöksenteon perustana. Sijoittajien ja omistajien näkökulmasta oikea ja riittävä informaatio tarkoittaa tilinpäätösinformaatioita. Yrityksen toiminnan kannalta keskeinen informaatio on päätöksenteon tukena käytettävä informaatio, joka muodostuu tämänpäiväisessä liike-elämässä yhä enemmässä määrin tietojärjestelmien pohjalta. Informaation muodostuminen ei-ihmislähtöisesti tekee informaatiosta

huonosti ymmärrettyä, se vähentää informaation läpinäkyvyyttä sekä lisää väärinkäytösten riskiä. Nämä tekijät vaarantavat myös lakisääteisen informaation – so. kirjanpidollisen informaation - ja tämän vuoksi myös valtiollisen toiminnan on kehityttävä, kuten Yhdysvalloissa säädetty Sarbanes-Oxley –laki osoittaa.

Sarbanes-Oxley:n myötä yritysten vastuu toiminnastaan korostuu. Johdon on kyettävä ymmärtämään toiminnan luonne ja siten varmistuttava tietojen oikeellisuudesta. Laissa määritellään johdon vastuusta sisäisestä kontrollista taloudellisessa raportoinnissa, joka tarkoittaa niitä johdon asettamia toimenpiteitä ja menettelytapoja, joilla informaation oikeellisuus varmennetaan.

Johdon toimintaa kontrollien asettamiseksi ja kehittämiseksi arvioidaan vuotuisessa tilintarkastuksessa, jonka suorittaa yrityksen ulkopuolinen tilintarkastaja. Tilintarkastaja arvioi johdon toimintaa sisäisen kontrolliprosessin kehittämisessä, yrityksen sisäisiä kontrollirakenteita ja niiden toimivuutta sekä testaa ja arvioi sisäisen kontrollin tehokkuutta taloudellisen informaation tuottamisessa.

3 RISKIT JA KONTROLLIT

Tässä luvussa kuvataan riskejä ja kontrolleja talouden prosesseissa käsiteltävässä informaatiossa.

3.1 Sovellettavat viitekehykset

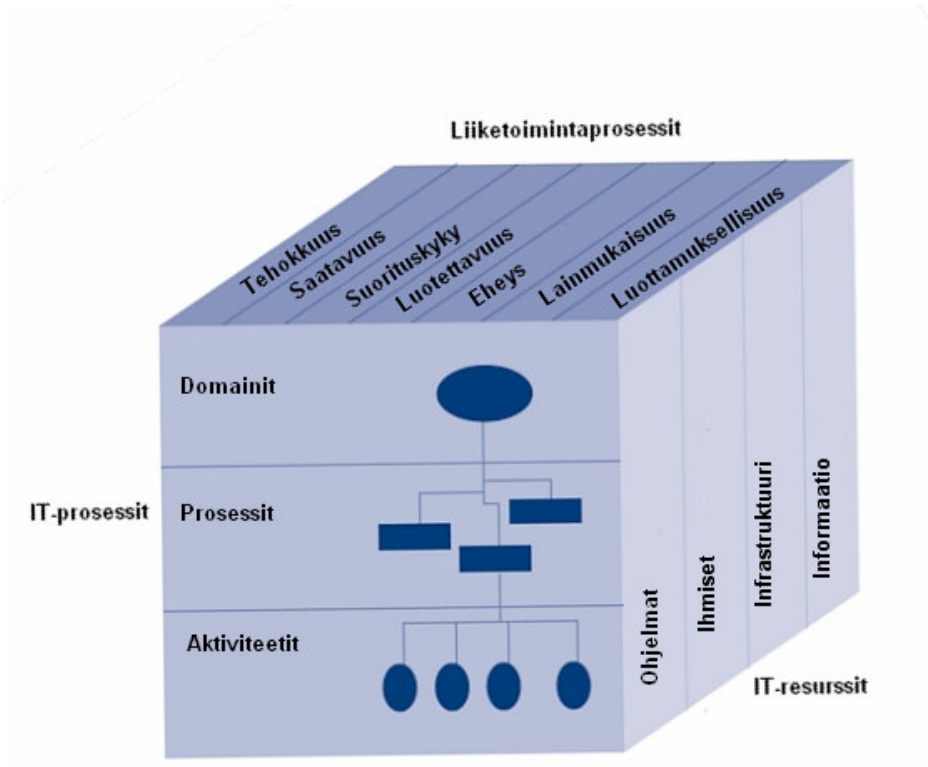
Tässä tutkimuksessa sovelletaan COBIT ja COSO viitekehyksiä sisäisen kontrollin tarkastelun tukena. COBIT sekä COSO ovat yleisimmät SOX-projekteissa käytetyt viitekehykset. ITGI (2006b)

COBIT-viitekehyksen ensimmäinen versio julkaistiin 1996 ja viimeisin, eli neljäs versio julkaistiin vuonna 2005. COBIT on liiketoimintalähtöinen viitekehys joka tarjoaa ylemmälle johdolle ja osakkeenomistajille mahdollisuuden ymmärtää paremmin IT prosesseja ja –palveluita sekä niiden liiketoimintalähtöisyyttä. COBIT:n tavoitteena onkin tutkia, kehittää, tehdä tunnetuksi sekä edistää kansainvälisesti tunnettuja informaatioteknologisia kontrollitoimintoja osaksi päivittäistä toimintaa johdolle, IT-ammattilaisille sekä muille liike-elämän ammattilaisille. ITGI (2006a).

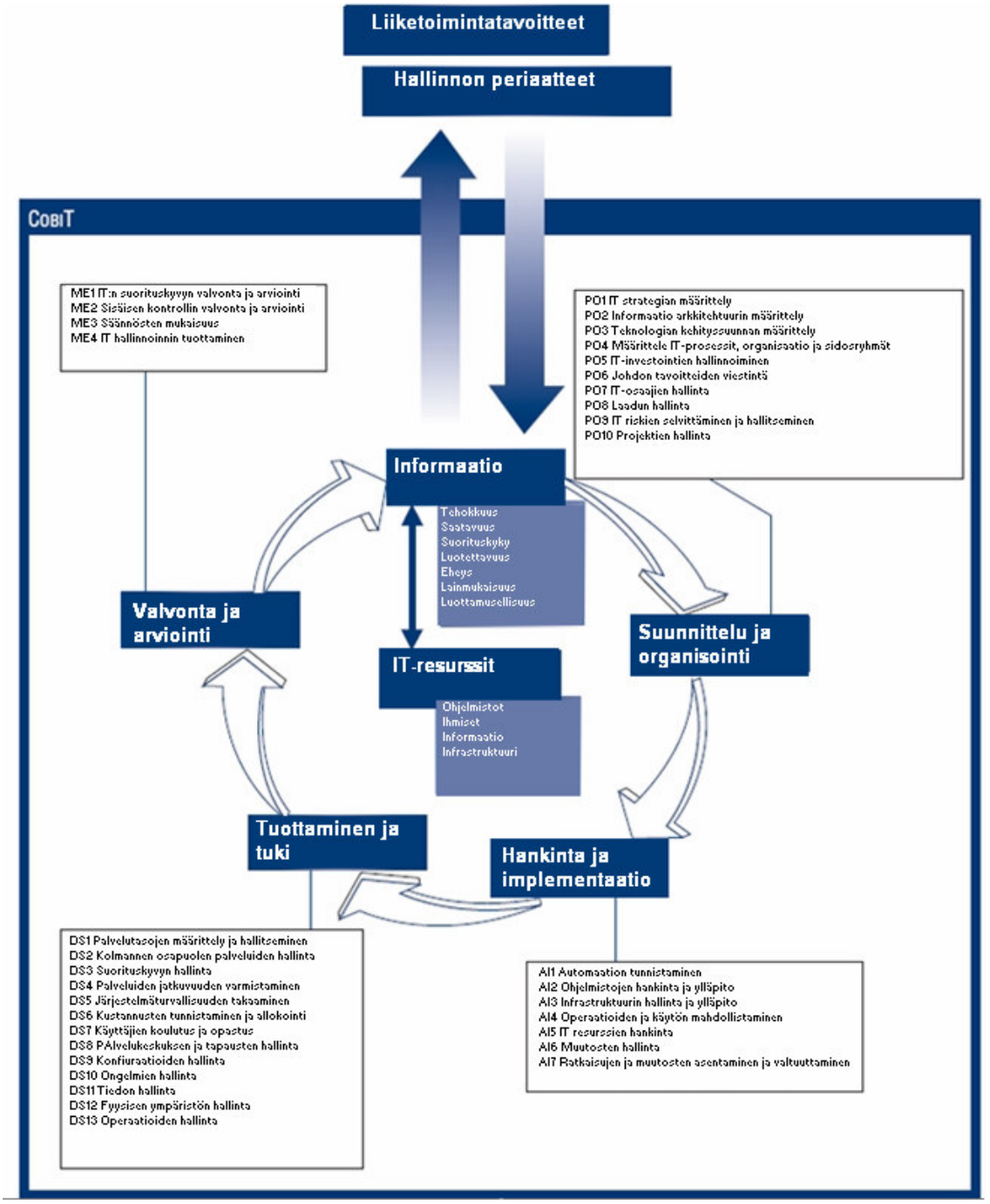
COBIT–viitekehyksen ja ohjeistuksen käyttämiselle on olemassa useita perusteita. ITGI (2006b) mukaan yritysten tulee hallita IT:tä kokonaisvaltaisesti, IT:lle asetettavien tavoitteiden tulee tukea liiketoiminnallisia tavoitteita, IT-prosessit tulee standardoida ja/tai automatisoida sekä kyetä noudattamaan ulkoisia vaatimuksia, kuten esimerkiksi Sarbanes-Oxley lakia.

Kuvassa 2 kuvataan COBIT–malli. COBIT–mallin ulottuvuudet ovat IT prosessit, IT resurssit sekä liiketoiminnalliset vaatimukset. IT–prosessit koostuvat neljästä päätoiminnosta (domains), joita ovat: 1) suunnittelu ja organisointi, 2) hankinta ja toteutus, 3) palvelutuotanto ja tuki sekä 4) valvonta ja arviointi. Päätoiminnot koostuvat prosesseista, jotka jakaantuvat edelleen 34 prosessiin, jotka sisältävät tietyt aktiviteetit. COBIT–prosesseja havainnollistetaan kuvassa 3. ITGI (2006d)

IT-resurssit jakaantuvat puolestaan ohjelmistoihin, informaatioon, infrastruktuuriin sekä ihmisiin. Ohjelmistoilla käsitetään automaattiset tai manuaaliset toiminnot, jotka käsittelevät informaatiota. Informaatio tarkoittaa kaikkea sitä informaatiota, jota liiketoimintaa käsittelee tai tuottaa. Infrastruktuuri puolestaan käsittää kaikki ne teknologiat ja fasiliteetit, jotka mahdollistavat informaation prosessoinnin (ITGI 2006b). Ihmiset ovat niitä fyysisiä henkilöitä, joita tarvitaan tiedon kokonaisvaltaiseen hyväksikäyttöön, prosessointiin sekä valvontaan. Liiketoiminnallisten vaatimusten täyttymiseen COBIT määrittää 7 informaatiolle asetettavaa kriteeriä jotka jakaantuvat kolmeen osa-alueeseen, joita ovat laatu, turvallisuus ja luottamuksellisuus. Vaatimukset eritellään tarkemmin luvussa 4, kappaleessa 3.



Kuva 2. COBIT prosessit. ITGI (2006b)



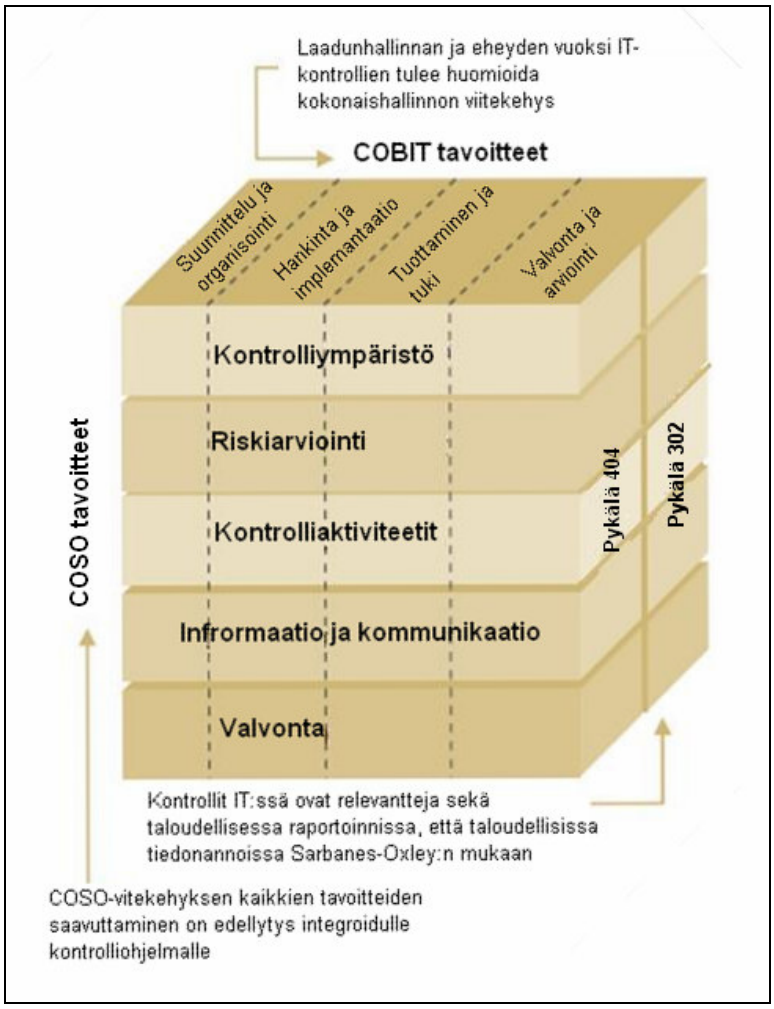
Kuva 3. COBIT-prosessit. ISACA (2005a).

COBIT:n määritelmän mukaan IT:n ja IT prosessien hallinnointi on jatkuvaa sekä säännöllistä poikkeamien mittaamista sekä arviointia vasten määriteltyjä standardeja hyödyntäen implementoituja mittareita. COBIT:n liiketoimintalähtöisyys IT:n auditoinnissa sekä useat COBIT–malliin liitetyt elementit, kuten CMM-kypsyystasomalli (Capability Maturity Model) tarjoavat

johdolle ja muille mahdollisuuden arvioida erityisten prosessien riskejä, strategialähtöisyyttä sekä prosessin operatiivista vaikutusta (Debreceny 2006). ISACA (2005b)

COSO on sisäisen kontrollin viitekehys, joka on tarkoitettu parantamaan talouden prosessien tuottaman informaation laatua sekä varmistamaan tehokkaan sisäisen kontrollin kehittäminen organisaatioissa. Viitekehyksen implementaation perusteita ovat tarve järjestelmälliselle lähestymistavalle kehitettäessä kontrolliympäristöä. Lisäksi tarve sisäisten kontrollien tehokkuuden parantamiselle, kontrollien asettamisen ja arvioinnin tukeminen sekä ohjeistus saavuttaa ulkoiset säädökset, kuten esimerkiksi Sarbanes-Oxley laki ovat tärkeitä perusteita viitekehyksen käytölle. FERF (2003)

COSO-viitekehyksessä sisäisen kontrollin määritellään koostuvan viidestä komponentista (kts. kappale 2.2.1), joita sovelletaan vasten COBIT:n prosesseja (ITGI 2006a). Kuvassa 4 havainnollistetaan COBIT:n IT-prosessien suhdetta COSO:n komponentteihin.



Kuva 4. COSO:n yhteys COBIT:iin. ISACA (2005a)

3.2 Riskit

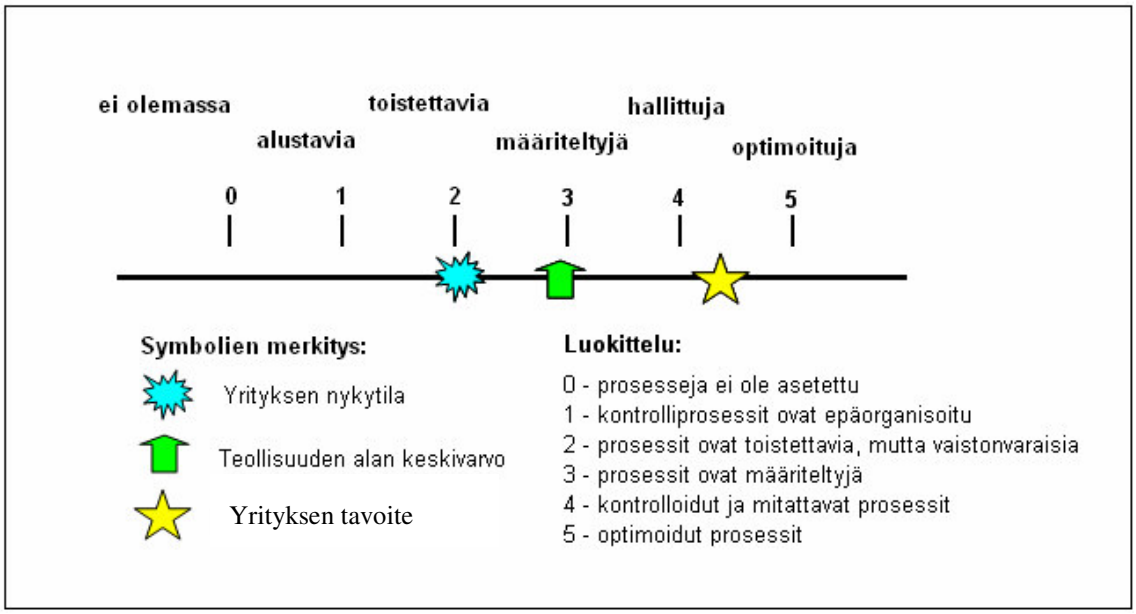
Informaatioteknologia muuttaa yritysten toiminnan luonnetta ja laajuutta muuttamalla liiketoimintaprosesseja, tarjoamalla globaalin viestinnän sekä häivyttämällä siten perinteiset liiketoiminnan organisatoriset rajat. IT voidaan nähdä vaikuttajana, kuin myös mahdollistajana prosessien ja strategioiden johtamisessa. Tärkeäksi nousee kyky ymmärtää informatiivisten järjestelmien suuri kyky kerätä, luoda ja prosessoida päätöksen teon tueksi luotavaa ja olemassa olevaa informaatiota riskeistä ja kontrolleista hallittaessa organisaatioiden toimintaa. Ramamoorti & Weidenmier (2004)

IT:n vaikutuksia yrityksen toimintaan ja organisaatioon tarkastellaan sekä vaikuttavana että mahdollistavana funktiona. IT:n tarkastelu vaikuttavana toimintona luo tarpeen entistä kehittyneemmälle hyvälle hallintotavalle (corporate governance). Liiketoimintaprosessien rakentuminen ja toimintamallien perustuminen yhä kasvavassa määrin IT:hen luo riippuvuuden tietoverkkojen, tietokonejärjestelmien ja järjestelmien toimivuudelle. Uudet ratkaisut eivät siis ainoastaan muuta liiketoimintaa, vaan lisäävät riskejä ja vaadittavia käytäntöjä kokonaisvaltaiselle kontrollien kehittämiselle. Lisääntynyt riski muodostuu 1) organisaation kyvyttömyydestä jatkaa liiketoimintaa, jos liiketoiminnan järjestelmät eivät toimi oikein, ja 2) IT:n hyödyntämisestä globaalisti ulkopuolisten entiteettien kanssa. Globaalissa toiminnassa erityisesti sisäiset kontrollit järjestelmien ja verkkojen luotettavuuden ja palautettavuuden kannalta ovat kriittisiä. IT on kiinteä osa yrityksen hallinnan kokonaisuutta, koska se on ensisijainen toiminto organisaatiolle täyttää sen tavoitteet ja samanaikaisesti toiminto, jonka vuoksi riskit ja tarvittavat kontrollit lisääntyvät. Kuitenkin IT on vähiten ymmärretty komponentti yritysten hallinnassa. Tämä näkyy myös sijoittajien toimissa, sillä sijoittajien huoli IT:n aiheuttamista riippuvuuksista ja riskeistä lisääntyy. Epävarmuuden lisääntyminen näkyy myös lainsäädännön kehittymisessä, kun se pyrkii vähentämään riippuvuutta ja riskejä IT:n lisääntymisen myötä. Ramamoorti & Weidenmier (2004)

ITGI:n (2006c) mukaan organisaatiot ovat muutosten keskellä koskien informaation hallintaa. Tavoitteet kasvavat koskien lisäarvon tuottamista organisaatiolle ja sijoittajille. Tässä yhteydessä korostuvat myös yhä lisääntyvä globalisaatio, yksityisyyden turvaaminen, lain ja säädöksenmukaisuuden vaatimukset sekä potentiaalinen haitallisten toimintojen kohdistuminen organisaatioon. Tämän myötä on entistä tärkeämpää yritysten hallinnon sekä johdon kiinnittää huomiota informaation turvallisuuden ja oikeellisuuden takaamiseen.

Riskien kartoittamiseksi tässä tutkimuksessa käytetään nimenomaan SOX-pohjaista lähestymistapaa, jonka vaikutukset järjestelmiin ja prosesseihin ovat Kaarst-Brown & Kellyn (2005) mukaan moninaiset. Nämä vaikutukset liittyvät raportoinnin sisältöön, oikea-aikaisuuteen, yksityiskohtaiseen dokumentointiin sekä informaation tuottamiseen ja yhdistämiseen sekä automaattisista että manuaalisista toiminnoista.

Informaation vaarantavia riskejä (liitteessä 1 havainnollistetaan esimerkein IT:n ominaisuuksien perusteella syntyviä riskejä) tulee ITGI:n (2006c) mukaan pyrkiä arvioimaan yrityksessä ja asettaa tavoitteita hyväksyttävän tason sekä tulevan kehityksen takaamiseksi. Kun organisaatiossa on tunnistettu keskeisimmät IT-lähtöiset riskit, niiden arviointiin tulisi käyttää informaation arvioimiseksi soveltuvaa mallia. Tähän tarkoitukseen COBIT määrittelee kypsyystasomallin, jonka avulla voidaan määritellä yrityksen prosessien nykytila ja asettaa tavoitetila. Kuvassa 5 havainnollistetaan COBIT:n kypsyystasomallin käyttöä. Mallin avulla voidaan määritellä organisaation nykytaso suhteessa ko. toimialan keskiarvoon ja luoda perusta kehittämissuunnitelman laadinnalle. Mallin avulla arvioidaan nykyisen tason perusteella suurimmat puutteet ja näin fokusoidaan projektin tavoitteet oikein. ITGI (2006c)



Kuva 5. Kypsyystasomallin käyttö kehittämissuunnitelman perustana. ITGI (2006c)

Mallin eri tasoja voidaan ISACA:n (2005a) mukaan tulkita seuraavasti:

- 0-taso, kontrollointiprosesseja ei ole asetettu

  Organisaatio ei tunnista liiketoimintariskejä, jotka liittyvät informaation haavoittavuuteen. Tarvetta riskien hallinnalle ei tunnisteta, velvollisuuksia sekä vastuita ei ole asetettu informaation oikeellisuuden takaamiseksi.

- 1-taso, kontrolliprosessit ovat epäorganisoituja ja ad-hoc –tasolla

  Organisaatiossa tunnistetaan tarve riskien hallinnalle, mutta riskien hallinta perustuu yksittäisiin suoritteisiin (esimerkiksi prosessin kontrollointi on yhden ihmisen varassa). Toiminta on reaktiivista.

- 2-taso, prosessit ovat toistettavia, mutta vaistonvaraisia

  Organisaatiossa tunnistetaan tarve riskien hallinnalle IT–toiminnoissa, mutta riskienhallinnan prosessi on vielä epäkypsää sekä vaistomaista. Yrityksessä on tietoa informaation vaarantavista riskeistä, mutta se on analysoimatonta.

- 3-taso, prosessit ovat määriteltyjä

  Organisaation laajuinen riskienhallinta määrittelee, miten ja milloin informaation oikeellisuus ja turvallisuus voivat vaarantua. Informaation turvallisuusvaatimukset on asetettu ja ne on sovitettu organisaation toimintoihin. Informaation oikeellisuuden todentaminen on IT-orientoitunutta liiketoimintalähtöisyyden sijaan.

- 4-taso, kontrolloidut ja mitattavat prosessit

Riskienhallinta on määriteltyä ja sitä vasten on asetettu toimintamalli organisaatiossa ylemmän johdon taholta. Ylempi johto sekä IT–johto ovat selvillä organisaation keskeisimmistä riskeistä liittyen informaation oikeellisuuteen sekä turvallisuuteen ja organisaatiossa vallitsee tietämys siedettävistä riskeistä. Organisaatiossa on myös määritellyt mittaristot riskien vaikutusten arvioimiseksi. Vastuut informaation oikeellisuuden takaamiseksi ovat selvästi määritellyt, johdetut sekä resursoidut.

- 5-taso, optimoidut prosessit

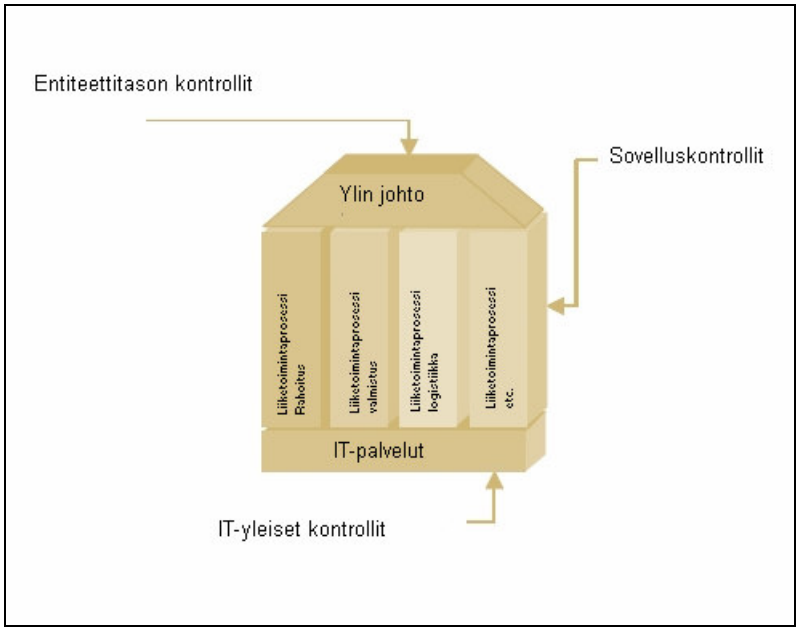
Riskienhallinta on määritelty organisaation laajuiseksi prosessiksi, jota johdetaan ja hallitaan osana päivittäistä toimintaa. Informaation oikeellisuus ja turvallisuus on integroitu kokonaisuus yhdessä yrityksen liiketoiminnallisten tavoitteiden kanssa. Riskienhallinnan tavoitteet ovat selkeästi määritellyt, optimoidut sekä arvioidut. Raportointi riskienhallinnan pohjalta mahdollistaa aikaisen varautumisen virheisiin kriittisissä järjestelmissä.

3.3 Kontrolliprosessit

Kokonaisvaltainen kontrollien tarkastelu SOX:n vaatimusten pohjalta käsittää ISACA:n (2005a) mukaan entiteettitason -, yleiset IT - tason - sekä sovellustason kontrollit (kts. luku 4.4). Sarbanes-Oxley määrittelee johdon vastuulliseksi sisäisen kontrollin asettamisesta, arvioinnista ja valvonnasta. Useimmissa organisaatioissa IT:n rooli tässä toiminnossa on keskeinen; oli kyseessä yrityskohtainen toiminnanohjausjärjestelmä tai kokoelma taloushallinnon ohjelmistoja, IT on keskeisin tekijä asetettaessa sisäisen kontrollin vaatimuksia. ISACA (2005a)

Kuvassa 6 entiteettitason kontrollit määritellään kuuluvaksi johtotason kontrolleihin. Johto määrittelee yrityksen liiketoiminnalliset tavoitteet sekä liiketoimintastrategian. Yrityksessä tämä tarkoittaa operatiivisten tavoitteiden asettamista sekä päätöksentekoa. IT:n näkökulmasta yrityksen toimintamallit ja

– proseduurit viestitään tällä tasolla. Täten entiteettitason kontrollit käsittävät 1) strategian, 2) käytännöt sekä proseduurit, 3) riskien hallinnan vaatimukset, 4) laadun varmistuksen sekä 5) sisäiset auditoinnit. ISACA (2005a)



Kuva 6. Kontrollit suhteessa yrityksen tasoihin. ISACA (2005a)

Yleisen tason IT-kontrollit määritellään kuuluvan yrityksen elementeistä IT-palveluihin. IT-kontrolliympäristö sisältää IT:n hallinnointiprosessin, valvonnan ja raportoinnin. IT-hallinnointiprosessi sisältää IT-strategian, IT-riskienhallintaprosessin, säädösten noudattamisen määrittelyn ja hallinnan sekä IT–toimintomallit, -proseduurit sekä –standardit. Valvonnan ja raportoinnin osalta vaaditaan niiden vastaamista liiketoiminnan tavoitteisiin sekä –strategiaan. ISACA (2005a)

IT-palvelut muodostavat perustan operatiiviselle toiminnalle organisaatiossa. Ne sisältävät tietoliikenne-, tietokanta- ja operatiivisten järjestelmien, tiedon varastoinnin sekä turvallisuuden johtamisen. Yleisen tason IT-kontrollit sisältävät ohjelmistokehityksen, ohjelmisto muutokset, käyttäjien hallinnan sekä infrastruktuurin toiminnot. ISACA (2005a)

Sovellustason kontrollit sisältyvät organisaatiotasolla liiketoimintaprosesseihin. Liiketoimintaprosessit käsitetään tässä yhteydessä niiksi toiminnoiksi, joista organisaatio saa lisäarvoa pääomalle. IT:n myötä liiketoimintaprosessit automatisoituvat sekä koostuvat yhä kompleksisimmista järjestelmistä. Liiketoimintaprosesseihin sisältyvät kontrollit tukevat suoraan taloudellisen kontrollin tavoitteita. Sovellustason kontrollivaatimukset käsittävät täydellisyyden, tarkkuuden, luvanvaraisuuden sekä esitystason kontrollivaatimukset. ISACA (2005a)

3.4 Yhteenveto

Sarbanes-Oxley laissa määritellään, että yritysten tulee käyttää yleisesti hyväksyttyä viitekehystä kontrollien määrittämisessä taloudellisissa toiminnoissaan. Tässä tutkimuksessa sovelletaan COBIT- sekä COSO–viitekehyksiä, jotka molemmat ovat hyväksyttyjä käytettäväksi SOX-projekteissa ja joita sovelletaan yleisesti SEC:iin listautuneissa yrityksissä.

COBIT on liiketoimintalähtöinen viitekehys, jossa kontrollitoimintoja arvioidaan vasten 34:ää määriteltyä prosessia. COSO puolestaan määrittelee sisäisen kontrollin ja on myös pohjana COBIT:n prosesseissa kontrollien määrittämisessä.

Informaatioteknologia muuttaa yritysten tapoja toimia ja riippuvuus IT:n mahdollistavista uusista toimintatavoista järjestelmien ja ohjelmistojen myötä kasvattaa riippuvuutta IT:stä. Uusien järjestelmien myötä syntyneet käytännöt luovat entistä monimutkaisempia kokonaisuuksia, joiden tuottaman informaation todentaminen oikeaksi on merkittävästi vaikeutunut, vaikka informaation käyttö ja määrä päätöksenteon tukena on lisääntynyt.

COBIT sisältää kypsyystasomallin sekä informaation arvioimiseksi määritellyt kriteerit, joiden avulla organisaatioissa voidaan lain edellyttämien vaatimusten mukaisesti määritellä merkittävimmät riskit ja arvioida informaation oikeellisuus ja luotettavuus.

Määriteltyjä riskejä vasten asetetaan kontrollitoimintoja, joilla pyritään ennakoimaan, ehkäisemään ja toipumaan riskeistä. Kontrollit voidaan edelleen luokitella entiteettitason -, aktiviteettitason – ja yleisiksi IT-tason kontrolleiksi. Entiteettitason kontrolleilla tarkoitetaan johtotason kontrolleja, joiden taustalla on liiketoimintastrategia ja tavoitteet. Aktiviteettitason kontrolleilla tarkoitetaan niitä kontrolleja, joilla varmennetaan operatiivisen tason, kuten liiketoimintaprosessien tuottaman informaation oikeellisuus. Yleiset IT-tason kontrollit tarkoittavat niitä kontrollitoimenpiteitä, joiden avulla informaatioteknologisia toimintoja kontrolloidaan sekä arvioidaan.

4 TALOUDEN PROSESSIEN KEHITTÄMINEN

Tässä luvussa perehdytään talouden prosessien kehittämisen periaatteisiin sekä talouden prosessien kehittämiseen SOX:n vaatimusten mukaisesti.

4.1 Prosessiajattelu

Tämän tutkimuksen yhteydessä sanalla prosessi viitataan merkitykseen liiketoimintaprosessi. Laamanen (2002) määrittelee liiketoimintaprosessin olevan joukko toistuvia toimintoja, jotka liittyvät toisiinsa. Prosessi sisältää resursseja, jotka tarvitaan syötteiden muuntamiseen tuotteiksi sekä toimintoprosessin, joka koostuu toisiinsa loogisesti liittyvistä toimintojen joukosta ja resursseista, joilla aikaan saadaan toiminnan tulokset. Prosessi koostuu Laamasen (2002) mukaan siis toiminnasta tai toiminnoista, resursseista ja tuotoksista.

Tässä tutkimuksessa organisaatiota tarkastellaan prosessiajattelun näkökulmasta. Laamanen (2002) esittää organisaation koostuvan kolmesta tekijästä:

1. Toimintajärjestelmä

   Prosessit, työmenetelmät, tietojärjestelmät, tilat, tuotteet ja palvelut

2. Osaaminen

   Kokemus ja hiljainen tieto, ydinosaaminen, teknologia, tiedot ja taidot sekä tietämys

3. Ihmissuhteet

   Vuorovaikutus, kulttuuri ja arvot, tiimit, verkostot ja motivaatio

Tässä yhteydessä prosessien tehtävänä on kuvata organisaation toiminnan logiikka. Prosessit kuvaavat sarjan toimintoja, joiden avulla organisaatio

saavuttaa tuloksensa. Prosessikuvausten avulla puolestaan pyritään kriittisesti ymmärtämään ja kuvaamaan keskeisten tavoitteiden saavuttaminen. Laamanen (2002)

4.2 Liiketoimintaprosessien kuvaaminen

Yamamoto ym. (2006) ovat kehittäneet liiketoimintaprosessien mallintamismetodologian sekä liiketoimintaprosessien jakamiseen tarkoitetun työvälineen. Heidän keskeisimpinä periaatteina metodologian kehittämisessä ovat tieto-taidon (know-how) ja parhaiden käytäntöjen (best practices) jakaminen. Tällä saavutetaan huomattavaa ajansäästöä liiketoimintajärjestelmien kehittämisessä sekä parempaa prosessikuvausten uudelleenkäytettävyyttä, joka mahdollistaa liiketoimintaprosessien kuvaamisen tarkemmin ja paremmin liiketoimintayksikkökohtaisesti.

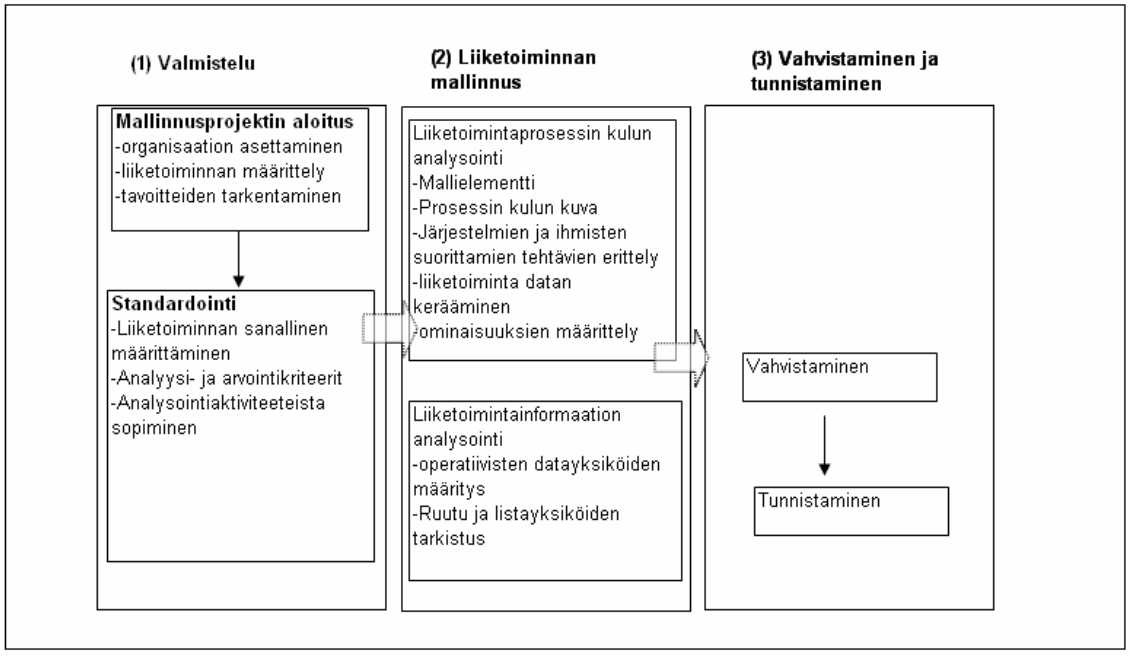
Yamamoto ym. (2006) tavoitteena on lyhentää aikaa kehittää ratkaisuja liiketoiminnassa, järjestelmien suunnittelussa sekä uudelleenkehityksessä. Nämä tekijät ovat tärkeitä liiketoimintaprosessien kehittämisessä, koska Sarbanes-Oxley-lain vaatimusten mukaan sisäisen kontrollin varmentaminen ja uudelleen arviointi tulee tehdä vuotuisesti (PCAOB 2004).

Liiketoimintaprosessin kuvaamisessa pitää noudattaa seuraavia vaatimuksia erityisesti silloin, kun kyse on liiketoiminnan kehittämisprojektista: 1) objektiivisuus, kuvauksen tulkinta tulee pysyä samana riippumatta tulkitsijasta, 2) johdonmukaisuus, mallinnustekniikan pitää olla määritelty, 3) ylläpidettävyys, jatkuva ylläpidettävyyden kontrollointi tulee olla helppoa, 4) saatavuus, prosessin tulostetta voidaan käyttää analyysissä ja 5) yksityiskohtaisuus, yksityiskohtaisuus on käytettävällä tasolla. Yamamoto ym. (2006)

Kehitetyn metodologian tavoitteena on kuvata liiketoimintaprosessin jokainen tehtävä systemaattisesti ja selventää ko. tehtävän tarkoitus. Lisäksi heidän kehittämän metamallin tavoitteena on kuvata sekä selittää systemaattisesti

erityyppisen informaation tarkoitus. Metamalli mahdollistaa liiketoimintaprosessimallin uudelleenkäytettävyyden tietojen jakamisen näkökulmasta. Tämä varmistaa objektiivisuuden sekä ylläpidettävyyden. Yamamoto et al. (2006)

Liiketoimintaprosessien mallintaminen on olennainen osa talouden prosessien kehittämistä tässä tutkimuksessa. Yamamoto ym. 2006 tarjoavat selkeät periaatteet metodologiansa sekä mallinsa puitteissa. Näitä periaatteita käytetään tässä tutkimuksessa soveltuvin osin kehittämisen tukena. Heidän metodologian kulku on havainnollistettu kuvassa 7, jossa määritellään prosessien kehittämisprojektin vaiheet, joita ovat 1) valmistelu, 2) liiketoiminnan mallinnus ja 3) hyväksyminen ja tunnistaminen. Vaatimukset prosessien mallintamisesta, jakamisesta ja uudelleenkäytettävyydestä palvelevat talouden prosessien kehittämistä yrityksessä, jossa organisaatio on suuri ja liiketoimintaprosessit monimutkaiset. Tällöin tärkeiksi tekijöiksi nousevat juuri uudelleenkäytettävyys sekä objektiivisuus, so. kuvausten merkitys on sama tulkitsijasta riippumatta.



Kuva 7. Liiketoimintaprosessin mallintamismetodologian aktiviteettikaavio. Yamamoto ym. 2006.

4.3 Prosessin laatutekijät ja läpinäkyvyys

Tärkeänä osana talouden prosessien mallintamista tulee ISACA:n (2005b) mukaan huomioida, mitä pitää määritellä, kuinka tarkasti, mitä pitää mitata ja arvioida, mitä voidaan ja tulee automatisoida, mikä on paras käytäntö sekä voidaanko nämä tekijät sertifioida. Tässä kappaleessa määritellään ne laatutekijät, joiden perusteella prosessin synnyttämää informaatiota voidaan arvioida.

Talouden prosessien tuottaman informaation arvioimiseksi COSO-viitekehys määrittelee IT:n tuoman laajemman näkökulman informaation arvioimiseksi. COSO:n määritelmän mukaan informaation arvioimisen lisäksi tulee arvioida myös viestintä, joka on keskeinen osa informaation tuottamista ja välittämistä. COSO:n mukaan informaation laatu koostuu tiedon oikeellisuudesta vastaanottajalle, tiedon ajallisuudesta, eli onko tieto saatavilla tarvittaessa sekä onko tieto raportoitu oikea-aikaisesti, versionhallinnasta, eli onko tiedon viimeisin muoto saatavilla, tarkkuudesta sekä saavutettavuudesta, eli onko tieto saatavilla vain henkilöille, joille se on tarkoitettu. Nämä tekijät ja toiminnot muodostavatkin kasvavan haasteen tunnistaa, hallita ja viestiä relevantti informaatio organisaatioissa. ISACA (2005a)

ISACA:n (2005a) mukaan entitettitasolla informaation oikeellisuuden perusta määrittyy yhtiön käytäntöjen kehityksestä ja niiden viestinnästä. Raportoinnin määräaikojen kehittäminen, niiden viestintä ja taloudellisen informaation konsolidointi ovat myös tärkeitä entiteettitason viestinnässä. Aktiviteettitasolla oikeellisuuden perusta tarkoittaa standardien laatimista yhtiön käytännöissä, oikea-aikaisuuden ja väärinkäytösten tunnistamista informaation tuottamisessa sekä säännöllistä raportointianiiden toiminnan oikeellisuudessa.

COBIT-viitekehyksessä ISACA:n (2005a) mukaan ydinprosessien tuottaman taloudellisen informaation laadun arvioinnin perustaksi on asetettu seitsemän kriteeriä, jotka ovat:

1. Tehokkuus, informaation relevanttius ja saatavuus suhteessa kyseessä olevaan talouden prosessiin

2. Suorituskyky, tiedon tuottamista hyödyntäen optimaalisesti tiedon tuottamiseen osallistuvia resursseja

3. Luottamuksellisuus, luottamuksellisen informaation suojaaminen

4. Eheys, informaation tarkkuus sekä täydellisyys sekä informaation tarkoituksenmukaisuus suhteessa ko. talouden prosessiin

5. Saatavuus, informaatio on suhteessa talouden prosessiin satavilla oikea-aikaisesti tarvittaessa, myös tulevaisuudessa

6. Lain- ja säädöstenmukaisuus, informaation sisällön oikeellisuus suhteessa lakeihin, säädöksiin sekä organisaation politiikkaan

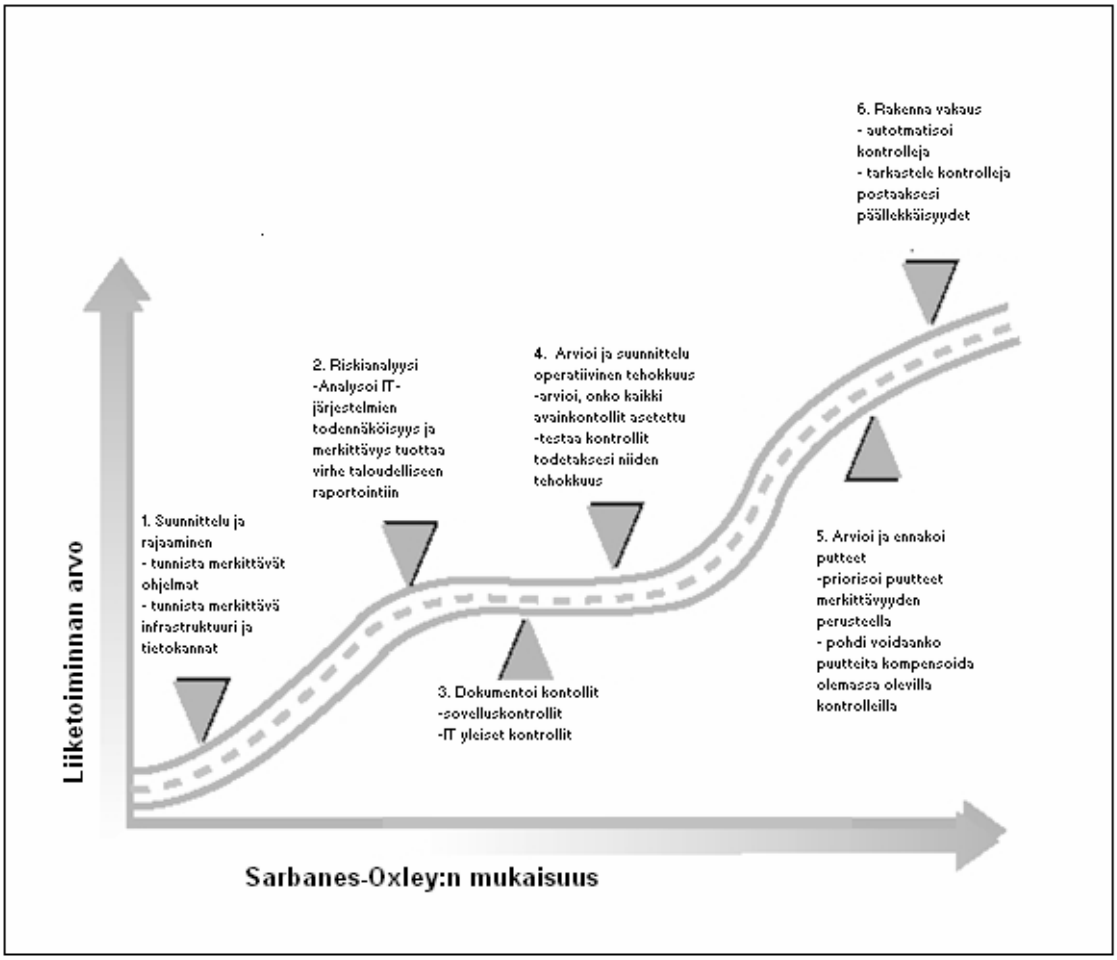
7. Luotettavuus, päätöksenteon tukena käytettävän informaation tarkoituksenmukaisuus sekä oikeellisuus suhteessa liiketoiminnalliseen kokonaisuuteen

4.4 Kehittämisprojektin määrittely SOX:n pohjalta

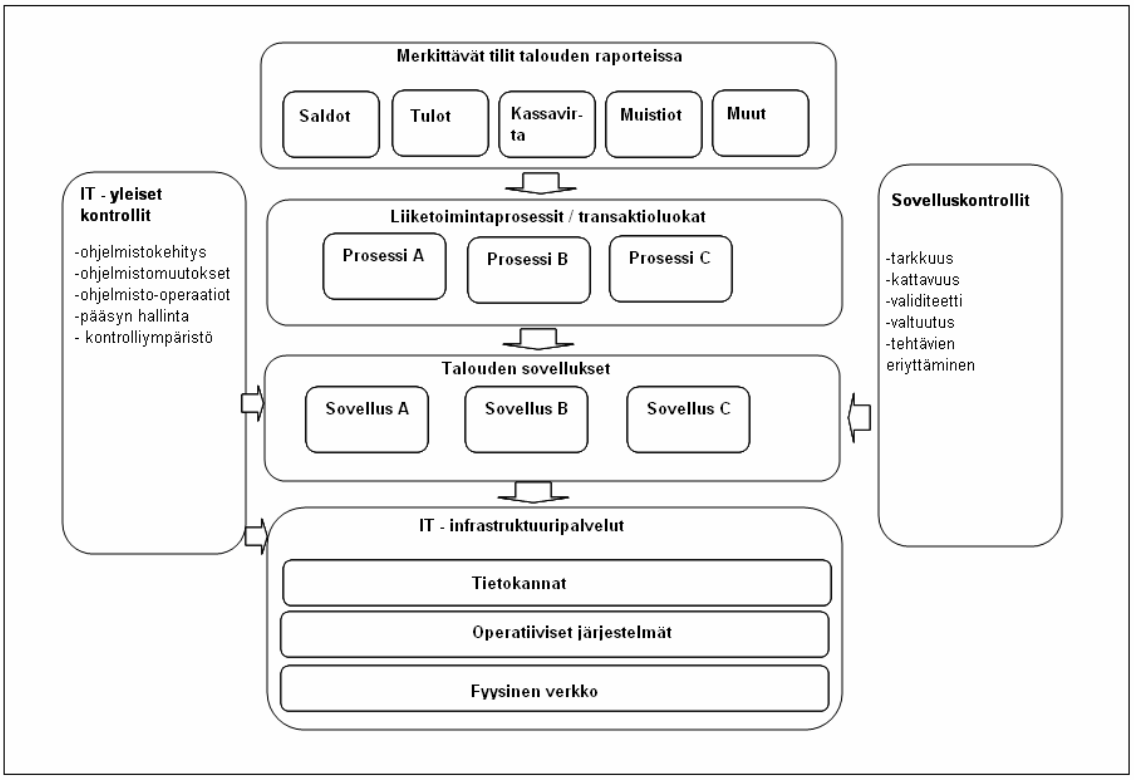
Sisäisen kontrollin sekä raportoinnin kehittyminen perustuvat SOX-lain pykälän 404 vaatimuksiin, jossa määritellään KPMG:n (2004a) mukaan johtoa luomaan ja ylläpitämään riittävä sisäinen valvontajärjestelmä. Lisäksi johdolta vaaditaan vuosittain raportti valvontamenettelyistä ja valvonnan tehokkuudesta. Raportin tulee sisältää toteamus, että riittävät menettelyt talouden raportoinnin osalta on luotu ja ylläpidetty, johdon arvio talouden raportoinnin sisäisen valvonnan tehokkuudesta sekä toteamus siitä, että yhtiön tilintarkastajat ovat vahvistaneet johdon raportin sisäisestä valvonnasta.

Kuvassa 8. esitellään SOX-projektin keskeisimmät vaiheet. Ensimmäisessä vaiheessa tunnistetaan liiketoiminta-alueen tai yksikön keskeisimmät taloudellisesti merkittävimmät assosiaatiot. Näiden liityntöjen osalta

määritellään niihin kuuluvat prosessit, ohjelmistot sekä infrastruktuuri, joita havainnollistetaan kuvassa 9. Laajuuden määrittelyn jälkeen määritellään riskit, niiden taloudellinen merkittävyys sekä todennäköisyys. ISACA (2005a) mukaan laajuuden määrittely ja ymmärtäminen ovat tärkeimpiä projektin vaiheita, sillä niissä luodaan ymmärrys projektin laajuudesta sekä määritellään resurssien käyttö.



Kuva 8. SOX-projektin vaiheet IT:n näkökulmasta. ISACA (2005a)



Kuva 9. SOX-projektin osa-alueet. ISACA(a) 2005

Seuraavassa projektin vaiheessa edellä kuvatun vaiheen tulokset dokumentoidaan. Dokumentoinnin perusteella johto voi arvioida riskien liittyvyyttä liiketoimintaprosesseihin. Tämä luo johdolle edellytykset sekä päätöksentekoon, että arviointiin esitutkimusvaiheen ulkopuolelle jäävistä riskeistä ja liitynnöistä. ISACA(a) 2005

Projektin neljännessä vaiheessa määritellään ja arvioidaan olemassa oleva kontrolliympäristö. Tämän vaiheen tavoitteena on painostaa johtoa arvioimaan kriittisesti kontrolliympäristön ominaisuuksia täyttää riittävä kontrollin taso ja varmuus oikeellisen ja luotettavan informaation takaamiseksi. Tarkemmin tämä tarkoittaa estävien-, havaitsevien-, automaattisten sekä manuaalisten kontrollitoimenpiteiden riittävyyden sekä tehokkuuden arviointia vasten määriteltyä tasoa. Tässä yhteydessä kypsyystasomalli tarjoaa työvälineen edistämään ja tukemaan prosessia ISACA(a) 2005.

Projektin viidennessä vaiheessa luodaan kohteen kehittämissuunnitelma. Kehittämissuunnitelmassa asetetaan ja priorisoidaan laadittavat kontrollitoimenpiteet.

Viimeisessä vaiheessa määritellään kehitettyjen toimenpiteiden yleistettävyys ja luodaan kontrollien kehittämiselle organisaation laajuinen kehityshanke, jonka tavoitteena on sisällyttää kontrollien riittävyyden arviointi osaksi vuotuista toimintaa (kts. luku 2.3). ISACA(a) 2005

4.5 Yhteenveto

Prosessi on joukko toimintoja, jotka muodostavat syötteistä tulosteita. Prosessi sisältää resursseja sekä loogisia toimintoja, joilla aikaansaadaan toiminnan tulokset. Prosessit organisaatiossa kuuluvat toimintojärjestelmään, jonka muita osia ovat työmenetelmät, tuotteet, tilat ja palvelut. Toimintojärjestelmän lisäksi organisaatioon voidaan esittää kuuluvan osaaminen sekä ihmissuhteet.

Liiketoiminnan näkökulmasta organisaatioiden toimintaa tarkastellaan liiketoimintaprosessien muodossa. Liiketoimintaprosessit tuottavat yritykselle lisäarvoa, mutta niiden hallinta ovat kasvava haaste IT:n lisääntymisen myötä.

Tässä kappaleessa liiketoimintaprosessien kehittäminen esitettiin koko organisaation näkökulmasta. Tästä näkökulmasta erityisesti liiketoimintaprosessien mallintamisessa käytetyille tekniikoille on tärkeää tieto-taidon sekä parhaiden käytäntöjen jakaminen. Tämän lisäksi prosessikuvausten tulkintojen objektiivisuus sekä uudelleenkäytettävyys ovat merkittäviä vaatimuksia liiketoimintaprosessien kehittämisessä. Näillä tavoitellaan liiketoiminnan kehittämiseen suunnattujen ratkaisujen lyhyempää vasteaikaa ja reaktiivisempaa toimintaa. Nämä tavoitteet tukevat myös Sarbanes-Oxley:n vaatimusta prosessien arvioinnin sisällyttämisestä osaksi vuotuista toimintaa ja auditointia.

SOX-projektien keskeisimmät vaiheet ovat projektin suunnittelu ja rajaaminen, riskianalyysi, kontrollien dokumentointi, kontrollien tehokkuuden tarkastelu, mahdollisten puutteiden arviointia ja vakauden perustaminen. Projektin keskeisimmistä osa-alueista on prosessien kehittämisen viitekehys.

Prosessien kuvaamiseen on kehitetty standardiin perustuvia viitekehyksiä, jotka perustuvat informaation oikeellisuuteen sekä Sarbanes-Oxley:n vaatimuksiin. Nämä viitekehykset tarjoavat kokonaisvaltaisen työvälineen organisaation prosessien kehittämiseen ja informaation tulkintaan, arviointiin, ja valvontaan. Viitekehyksillä tavoitellaan mitattavia sekä optimoitavia prosesseja, jotka integroituvat liiketoiminnallisten tavoitteiden ja – strategian kanssa ja täten tuottavat yritykselle lisäarvoa vähentämällä riskiä informaation korruptoitumisesta.

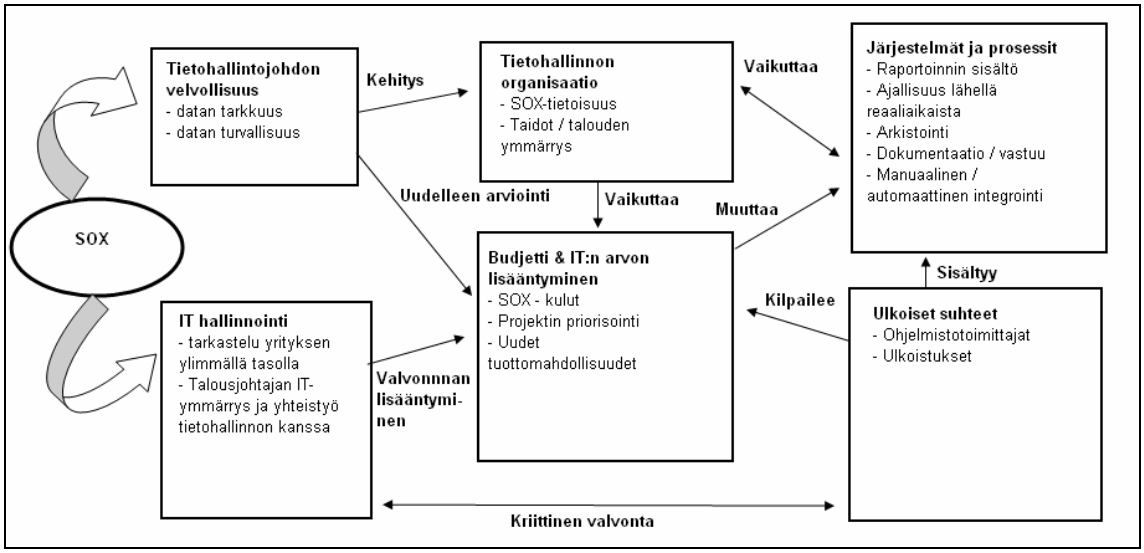
5 KEHITTÄMISSUUNNITELMAN LAATIMINEN SOX:N POHJALTA

Tässä luvussa käsitellään SOX-implementaatioprojektin vaiheita sekä koko projektin näkökulmasta, että yksittäisen prosessin näkökulmasta. Lisäksi luvussa käsitellään kontrollitoimenpiteiden asettamista ja arviointia SOX-projekteissa muodostuneisiin käytäntöihin pohjautuen.

5.1 SOX-implementaatioprojektin vaiheet

SOX-projektin ensimmäinen vaiheessa projektille määritellään projektin johto sekä varmistetaan ylimmän johdon tuki. Ylimmän johdon tuen puuttuminen voi johtaa projektin epäonnistumiseen, koska SOX-implementaatioprojekti kattaa koko organisaation päätoiminnot sekä osastot. Tästä syystä projektin läpiviemiseksi tarvitaan huomattavia resursseja ja riittävästi aikaa. PWC (2004)

Kaarst-Brown ym. (2005) mukaan SOX vaikuttaa yrityksissä kuuteen osa-alueeseen, joita esitellään kuvassa 10. Nämä osa-alueet ovat Kaarst-Brown ym. (2005) mukaan ohjenuoria IT-johdolle SOX:n vaatimusten täyttämiseksi.

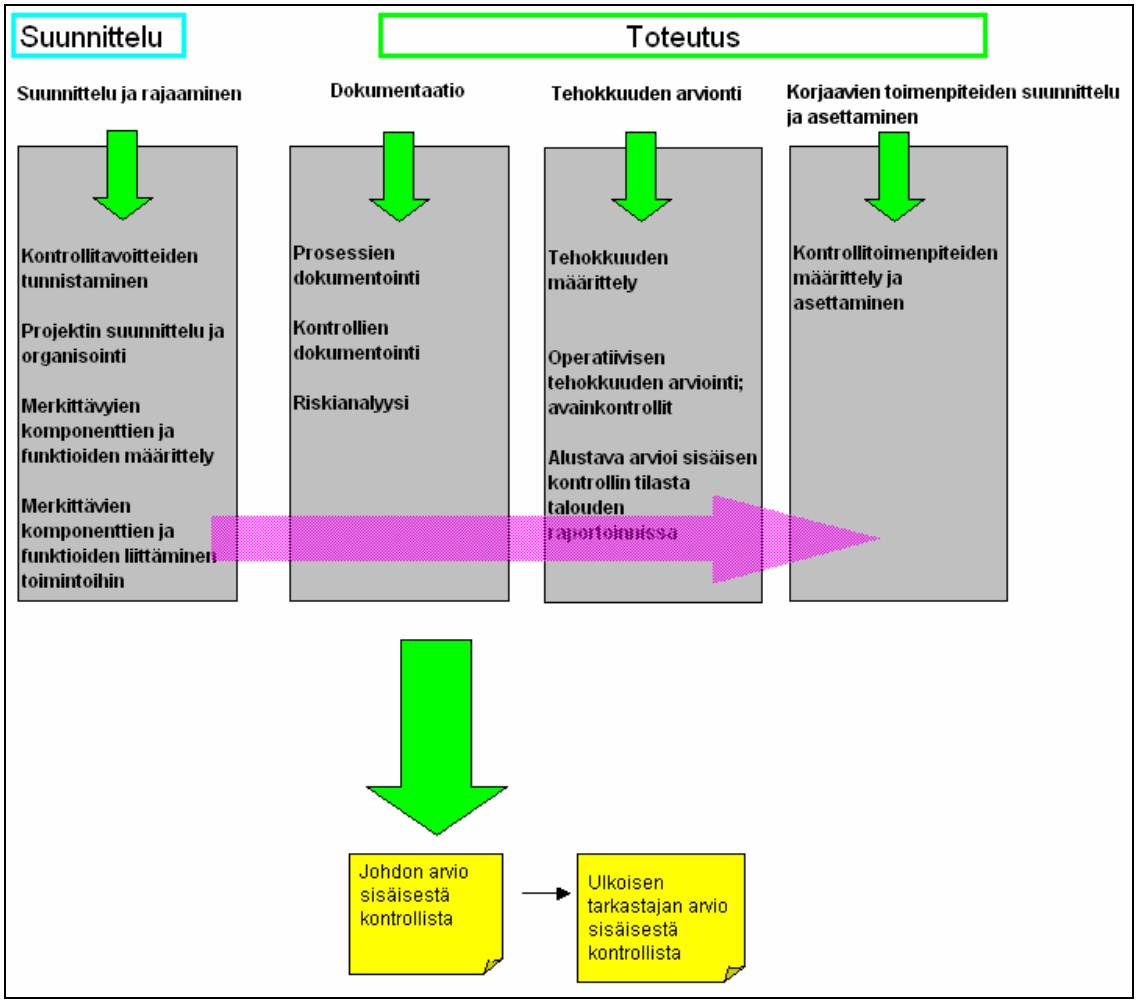


Kuva 10. SOX:n vaikutus tietohallinnon näkökulmasta. Kaarst-Brown ym. (2005)

Kuvassa 10 Kaarst-Brown ym. (2005) esittävät lain vaikuttavan tietohallinnon näkökulmasta tietohallinnon velvollisuuksiin, IT:n hallinnointiin, tietohallinnon organisaatioon, budjetointiin ja IT:n arvon lisääntymiseen, järjestelmiin ja prosesseihin sekä ulkoisiin suhteisiin. Lain vaatimusten saavuttamiseksi tietohallinnon näkökulmasta Kaarst-Brown ym. (2005) havainnollistavat vaiheita seuraavassa esitellyllä yksinkertaistetulla mallilla:

1. Prosessien dokumentointi tietohallinnon näkökulmasta
2. Kontrollipisteiden tunnistaminen prosessista
3. Kontrollien testaaminen tehokkuuden toteamiseksi
4. Puutteiden arviointi
5. Kontrollien kehittämissuunnitelma puutteiden korjaamiseksi
6. Viitekehyksen asettaminen sisäisen IT-kontrollin luomiseksi

Kuvassa 11. esitellään SOX-projekti yleisellä tasolla. Projekti alkaa huolellisella suunnittelulla ja rajaamisella. Projektin rajaamisella tarkoitetaan sitä, että ainoastaan merkittävimmät taloudelliset funktiot ja komponentit kuten prosessit ja taloudelliset ilmoitukset sisällytetään projektiin. Toteutusvaiheessa edellisen vaiheen perusteella määritellyt prosessit ja niiden kontrollit dokumentoidaan. Lisäksi suoritetaan riskianalyysi. Tämän jälkeen määritellään prosessien kontrollien tehokkuus ja tehdään alustava arvio sisäisen kontrollin tilasta. Lopuksi määritellään tarvittavat kontrollitoimenpiteet. PWC(2004)



Kuva 11. SOX-implementaatioprojektin yleiskuva. Ernst & Young 2004

THEIIA:n (2005) mukaan SOX-projekti sisältää seuraavat vaiheet:

1. Riskianalyysi

   Projektin rajaamisen tarkastelussa suositellaan riskipohjaista ylhäältä – alas lähestymistapaa taloudellisen merkittävyyden arviointiin.

2. Prosessien ja kontrollien dokumentointi

   Tässä vaiheessa dokumentoidaan avainprosessit ja –kontrollit. Tarkastelun kohteena ovat taloudellisesti merkittävimmät assosiaatiot.

3. Avainkontrollit

Avainkontrollien kriittinen määrittely. Määrittelyssä tulee arvioida varovaisesti, mitkä ovat avainkontrolleja, sillä liian monen kontrollin määrittely avainkontrolliksi heikentää kontrollien tehokkuuden tarkastelua. Toisaalta avainkontrollien kattamattomuus voi vaarantaa merkittävyyden tarkastelun.

4. IT-kontrollien tunnistaminen

IT-kontrollien tunnistaminen on yksi projektin tärkeimmistä osa-alueista. IT-kontrollien dokumentointi, arviointi ja asettaminen vaikuttavat merkittävästi projektin onnistumiseen.

5. IT-yleiset kontrollit

Jokaisen projektiin sisältyvän ohjelmiston osalta tulee määritellä joukko kontrollitavoitteita. Näiden kontrollitavoitteiden tulee koskea uusien ohjelmistojen kehityksen, olemassa olevien ohjelmistojen ylläpidon, käyttäjähallinnan, tietojärjestelmä operaatioiden, tietoliikenteen sekä IT-organisaation johtamisen osa-alueita.

6. Automaattisten kontrollien testaaminen

Jokainen automaattinen kontrolli, mukaan lukien avainraportit, tulee testata yksilöllisesti. Testaaminen sisältää testidatan käytön, ohjelmistojen parametroinnin tarkastelun, auditointiohjelmistojen käytön ja automaattisen kontrollin manuaalisen testauksen.

7. Tehtävien eriyttäminen ja rajoitetut käyttöoikeudet

Tehtävien eriyttäminen ja käyttöoikeuksien rajoitukset tulee tunnistaa, dokumentoida sekä asettaa.

8. Taulukkolaskentasovellukset ja muut loppukäyttäjäraportit

Merkittävimpien taulukkolaskentasovellusten ja loppukäyttäjien tekemien raporttien osalta tulee suorittaa läpikäynti (walkthrough) niiden oikeellisuuden toteamiseksi.

9. Kolmannen osapuolen kontrollit

Kolmannen osapuolten palveluiden osalta tulee varmistua, että prosessi on oikeellinen myös tuotettavan tai käsiteltävän informaation osalta.

10. Väärinkäytösten mahdollisuuden arvioiminen

Väärinkäytösten osalta tulee määritellä ne osa-alueet, joissa väärinkäytökset ovat mahdollisia (esimerkiksi varastoinventaari) ja määritellä kontrollit niiden osalta.

5.2 Kehittämisprojektin tavoite ja vaiheet prosessien näkökulmasta

Suomalaisen yrityksen näkökulmasta kehittämisprojektin tavoitteena on tunnistaa prosessin keskeisimmät ja merkittävimmät riskit taloudellisen informaation tuottamisessa. Tämän perusteella luodaan kontrollien kehittämissuunnitelma, jolla prosessia kehitetään SOX:n vaatimusten nojalla luotettavammaksi. Damianides:n (2005) mukaan järjestelmien kehittämistä SOX:n mukaiseksi edesauttaa COBIT:n implementointi, joka auttaa IT-hallinnon luomisessa, riskien hallinnassa sekä tietojärjestelmien auditoinnissa. Tämän vuoksi tämä kappale perustuu ISACA:n (2005a) artikkeliin IT kontrollien kehittämisestä SOX:n vaatimusten mukaisesti, koska artikkelissa kootaan sekä COBIT-, että COSO-mallin kontrollikäytännöt ja määritellään niiden pohjalta kontrollitavoitteet talouden prosessien kehittämiseksi SOX:n vaatimusten mukaisiksi.

Fox ja Zonneweld (2003) esittävät Damianides:n (2005) mukaan vahvan sisäisen kontrollin kehittämisen IT:n avulla edesauttavan kohentamaan yleistä IT:n hallintaa, luomaan ymmärrystä IT-asioista ylemmän johdon tasolla, parantamaan päätöksenteon laatua, kehittämään lisäarvoa tehostuneiden

operaatioiden kautta sekä parantamaan riskien hallintaa. Edelleen prosessin kehittämiseksi projekti käsittää samat vaiheet kuin luvussa 3.4 esitettiin. Seuraavassa käydään ko. vaiheet lävitse yksittäisen prosessin näkökulmasta.

Suunnittelu ja rajaaminen

Tässä vaiheessa luodaan ymmärrys, mitkä järjestelmät ja ohjelmistot sisällytetään projektiin, ja mitkä järjestelmät ja ohjelmistot voidaan sulkea sen ulkopuolelle. Yksittäistä prosessia kehitettäessä arvioidaan, mitkä järjestelmät ja ohjelmistot sekä niiden alijärjestelmät ja –ohjelmistot liittyvät prosessin perusteella syntyvään taloudelliseen informaation tuottamiseen. Tässä yhteydessä tulee arvioida myös rajaamista taloudellisen merkittävyyden näkökulmasta. Kehittämissuunnitelman laadintaan valitaan ainoastaan ne järjestelmät ja ohjelmistot, jotka ovat relevantteja liiketoiminnan sekä sitä tukevan raportoinnin tukemisessa. Tämä vaihe luo perustan projektin aikataulu sekä resurssisuunnittelulle.

Organisaation prosessit sisältävät useita toimintoja, järjestelmiä, ohjelmistoja sekä kontrolleja. SOX-projekteissa rajaamisen kannalta on oleellista määritellä juuri ne toiminnot, jotka tukevat taloudellista raportointia. Kontrollien tunnistamiseksi on kaksi lähestymistapaa: 1) IT-kontrollit ja taloudelliset kontrollit kehitetään erikseen ja tämän jälkeen määritellään liitynnät tai 2) IT-kontrolli sekä taloudelliset kontrollit kehitetään yhteistyössä IT:n sekä talouden näkökulmasta. Lähestymistavan valinnalla ei ole merkitystä, kunhan IT-riippuvaiset kontrollit tunnistetaan kokonaisvaltaisesti ja täydellisesti. Suunnitteluvaiheen rajaamisen jälkeen on tärkeää keskustella ja yhteisesti hyväksyä projektin kattavuus sekä rajaaminen yhdessä IT:n että talouden toimintojen kesken. Tässä yhteydessä myös määritellään prosessin omistajat ja suunnitellaan vastuualueet. Projektin rajaamisessa ei kuitenkaan tule sulkea pois kolmannen osapuolen palveluita, koska yrityksissä on paljon ulkoistettuja toimintoja, jotka tulee myös määritellä projektiin kuuluviksi tai kuulumattomaksi. Kolmannen osapuolen kontrollien kehittämisessä tulee

arvioida sisäisen kontrollin kattavuutta ko. toiminnon suhteen dokumentoidusti.

IT-riskianalyysi

Tässä vaiheessa projektia suoritetaan riskianalyysi niiden IT-toimintojen pohjalta, jotka kuuluvat projektiin (scope applications and systems). Keskeisin SOX-projektien oppi on, että projektin tulee olla riskilähtöinen, koska kaikki IT-toiminnot eivät aiheuta merkittävää taloudellista riskiä. Tämän vuoksi resurssien kohdentaminen oleellisiin toimintoihin on tärkeää.

Riskien arviointi tietojärjestelmissä ja ohjelmistoissa, kuten tietokannoissa, operatiivisissa systeemeissä, verkoissa sekä fyysisissä ympäristöissä on tärkeää riittävien kontrollien arvioimiseksi. Tärkeää on myös ymmärtää kontrollien toimivuuden sekä tehokkuuden testaaminen kyseisiltä osin. Keskeisten riskitekijöiden määrittelyn tarkoitus on tuottaa organisaatiolle relevanttia informaatiota riittävän riskianalyysin tekoa varten (esimerkiksi ilman pääsyn kontrollointia on olemassa riski, että järjestelmään voidaan syöttää vääriä transaktioita ilman, että tiedetään niiden alkuperää). Ilman kontrollointia vastaavanlaisten toimintojen toteuttaminen on mahdollista ja täten taloudellisen riskin toteutuminen hyvin todennäköistä. Tuloksena riski todetaan merkittäväksi ja oleellista on kontrollin suunnittelu riskin ehkäisemiseksi. Taulukossa 1 on esimerkki organisaatiotason kontrollitoimenpiteistä.

Sisäisen kontrollin ja uhkien ehkäisyohjelien komponentit	Ihmisresurssit	Yritystason riskienhallinta	Auditointikomitea	Sisäinen auditointi	Ilmiantokanava	Tapa toimia (code of conduct)	IT - ympäristö ja - organisaatio	Itsearviointi	Jaetut palvelut	Tiedonantokomitea	Valvonta(muu kuin auditointi komitea)	Käytäntöjen ja yrityspolitiikan manuaalit	Kauden lopun raportointi	Liiketoiminnan suorituskyvyn arvioinnit
Uhkien ehkäisyohjelma	x	x	x	x	x						x		x	
Kontolliympäristö	x		x		x	x	x					x	x	
Riskien arviointi	x	x	x	x	x			x		x	x			
Kontrollitoiminnot									x				x	x
Informaatio ja kommunikaatio	x	x	x	x	x	x	x		x	x	x	x	x	
Valvonta			x	x	x			x		x	x	x		

Taulukko 1. Riskitekijät riskiarvioinnissa. PWC(2004)

Riskianalyysin tuloksena voidaan arvioida tarvittavien kontrollien määrä ja niiden testaaminen. Liitteessä 2 määritellään ISACA:n (2005a) pohjalta keskeisimmät yleiset IT-kontrollit, jotka tulee huomioida kehityksessä ja niiden testaamisen arvioinnin perusteet. Lisäksi liitteessä sidotaan kontrollit osaksi COBIT-viitekehyksen prosesseja.

Kontrollien dokumentointi

Kontrollien dokumentoinnilla pyritään esittämään keskeisimmät riskit, jotka liittyvät taloudellisen informaation perusteella tehtävään päätöksentekoon. Esimerkiksi, jos taloudellisesti merkittävä päätös perustuu raskaisiin laskelmiin ja kompleksisiin järjestelmiin, niin laskelmassa tai järjestelmässä tapahtuva hallitsematon muutos voi johtaa liiketoiminnallisesti merkittävän riskin laukeamiseen. Tämän vuoksi on kriittistä tunnistaa ja dokumentoida kontrollit, jotka estävät edeltävän kaltaisen riskin toteutumisen.

SOX:n alaisuudessa toimivien yritysten tulee dokumentoida taloudellisen raportoinnin kontrollit sekä arvioida niiden tehokkuutta ja suunnittelua vuotuisesti. Dokumentaatio voi käsittää useita eri muotoja, jotka voivat sisältää dokumentaation yrityksen toimintojen politiikan käsikirjan, IT käytännöt ja proseduurit, käyttäjäkertomuksia, tietomalleja, vuokaavioita sekä kysymyslistoja etc. Kuitenkin useimmilla yrityksillä kontrollien tulee sisältää tietyt dokumentaatiot, kuten taulukossa 2 esitetään.

Kontrollitaso	**Dokumentaatio**
Entiteettitaso	Entiteettitason kontrollien kuvaus sekä johdon arvio niistä.
Aktiviteettitaso	Prosessien ja alaprosessien kuvaukset, prosesseihin liittyvien riskien kuvaukset sekä arvio taloudellisesta merkittävyydestä. Arvio kontrollien riittävyydestä ja liitännästä yleisesti hyväksyttyyn viitekehykseen.

Taulukko 2. Kontrollitason edellyttämä dokumentaatio. ISACA (2005a)

Kontrollitoimintojen suunnittelun ja toteutuksen tehokkuuden arviointi

IT kontrollien suunnittelu osana kokonaisvaltaista kontrollien suunnittelua ja testausta on tärkeä osa sisäisen kontrollin kokonaisuutta. PCAOB:n (2004) mukaan sisäisen kontrollin tehokkuus riippuu kaikkien eri kontrolliympäristöjen tehokkuudesta, kuten esimerkiksi IT-kontrolliympäristöstä. Kypsyystasomallia voidaan hyödyntää osana koko kontrolliympäristön arvioinnissa (katso luku 4.2).

Dokumentaatio kontrollitoiminnon tehokkuudesta sisältää kehityksen selvityksen luonteen, ajoituksen ja tehdyt kehitysaskeleet -, testauksen tulokset, testin suorittajan nimi ja päivämäärän. Tämän lisäksi ajankohta jona testi

suoritettiin, otannan koko ja testin populaatio ovat osa dokumentaatiota. Toimintaa tukevan materiaalin dokumentoinnin, johtopäätöksen kontrollin tehokkuudesta sekä poikkeusten tunnistamisen ja varautumissuunnittelun näiden varalle tulee myös olla dokumentaatiota.

Dokumentaation osana olevan evidenssin luonteesta on säädetty PCAOB:n standardissa 2 PCAOB:n (2004) mukaan seuraavaa: i) tiedustelua on tehtävä asianomaisilta henkilöiltä, ii) relevantin dokumentaation osalta on tehtävä tarkastuksia, iii) yritysten toiminnasta on tehtävä tarkkailua sekä iv) tutkia uudelleentestattavuutta. Evidenssin tulee sisältää edellä mainittuja standardin muotoja.

Kehityskohteiden priorisointi ja ennaltamistaminen

Käytännössä yritysten pitää määritellä kahdenalaisia kehityskohteita: 1) suunnittelun puutteellisuudet sekä 2) operatiiviset puutteellisuudet. Suunnittelun puutteellisuudet tarkoittavat puuttuvia kontrolleja tai puutteellisia kontrolleja, jotka eivät vastaa määriteltyyn riskiin. Operatiiviset puutteellisuudet viittaavat niihin kontrollitoimintoihin, jotka ovat olemassa, mutta eivät toimi täydellisesti arviointijakson aikana (kontrollien kehittäminen on osa vuotuista toimintaa, joten arviointijakso käsittää yhden yrityksen tapauksessa yhden tilikauden).

Ennaltamistaminen (remediate) tarkoittaa määrätyn kontrollin tarpeen ratkaisemista lyhytaikaisella toimenpiteellä pitkäaikaisen ratkaisun sijaan. Esimerkiksi pääsyn hallinnan kontrolloimiseksi valitaan henkilö suorittamaan manuaalinen hallinnointi vastaavan ohjelmiston ominaisuuden sijaan, joka maksaisi enemmän ja vaatii enemmän aikaa toteutukseen. Tässä yhteydessä pitkän aikavälin suunnittelulla voidaan säästää merkittävästi ja suunnittelun pitäisikin olla kauaskantoista.

Kehitysohjelman laajentaminen osaksi yrityskulttuuria

Talouden raportoinnissa kontrollien kehittämisen viimeisin tavoite on luoda kehitysprojektista prosessi osaksi vuotuista toimintaa. Tämä tarkoittaa talouden sekä IT:n toimintojen yhtenäistä kehittämistä vasten yrityksessä määriteltyjä liiketoiminnallisia tavoitteita.

5.3 SOX:n pohjalta opittuja käytäntöjä

Sarbanes-Oxley lain voimaantulosta tulee tämän tutkielman teon yhteydessä kuluneeksi viisi vuotta. Tänä aikana SOX:n vaatimusten aiheuttamien projektien osalta on opittu useita käytäntöjä - kuten mm. ISACA:n ja ITGI:n tuottamat julkaisut, jotka edesauttavat projektin läpiviemiseksi. Seuraavassa käydään lävitse näitä käytäntöjä ISACA:n (2005a) pohjalta.

Vastuu IT-kontrolleista

Hyvin usein vastuu IT-kontrolleista on yrityksissä epäselvä. Yleisimmät epäselvyydet koskivat liiketoimintaprosessien omistajuutta, ohjelmistojen kontrolloinnin vastuullistamista sekä taulukkolaskentasovellusten kontrollointia.

IT-kontrollien osalta on opittu, että vastuiden tulee olla selvästi määritellyt liiketoimintaprosessien omistajien osalta. Edelleen ohjelmisto- ja loppukäyttäjätason sovellusten osalta kontrollit ja vastuu niistä tulee kuvata ja hyväksyttää.

Viestintäsuunnitelman puutteellisuus tai puuttuminen

Uusien kontrollien osalta viestintä niiden merkityksestä on oleellinen osa kontrollin tehokasta asettamista. Useissa yrityksissä ei kuitenkaan projektin vaiheissa ollut huomioitu viestinnän järjestämistä. Esimerkiksi, kun uusi kontrolli asetetaan, niin pitää suunnitella, miten siitä tiedotetaan eri sidosryhmille.

Keskitettyjen kontrollien asettamisen vaikeus

Mahdollisuuksia keskitettyjen ja/tai standardoitujen kontrollien osalta ei oltu riittävästi arvioitu yrityksissä. Tämä voi johtaa tehottomaan sisäiseen kontrolliin tai sisäisen kontrollin testaamiseen kuluvan ajan lisääntymiseen.

Organisaatioiden tulisi arvioida keskitettyjen ja/tai standardoitujen kontrollien mahdollisuuksia riittävästi osana sisäistä kontrollia. Näin saavutetaan suurempi tehokkuus ja vähennetään testaukseen kuluvaa aikaa.

Huono IT- ja talousorganisaation välinen viestintä

Useissa yrityksissä SOX-projekteissa IT ja taloushallinnon projektiryhmät työskentelivät erillään samojen kontrollitavoitteiden parissa. Tästä johtuen automaattisten kontrollien kehittäminen ja IT:n tehokkaampi hyödyntäminen osana taloudellista raportointia ei toteutunut tehokkaimmalla mahdollisella tavalla.

Ertyisesti IT:n ja taloushallinnon organisaatioiden tulisi työskennellä yhdessä yrityksen taloushallinnon prosessien kehittämisessä SOX:n mukaisiksi. Tällä tavoin kontrollien integroiminen ja automatisointi sekä IT:n syvällisempi huomiointi osana kehitystä varmistaa sisäisen kontrollin tehokkuuden.

Prosessien dokumentoinnin puutteellisuus

Prosessien dokumentoinnissa oli usein keskitytty enemmän prosessin tavoitteeseen, kuin avainkontrollien tunnistamiseen. Tämä johti epätäydelliseen kontrollien tunnistamiseen prosesseissa.

Prosessien dokumentointi ei ole tavoite, vaan keino löytää prosessin kehityskohteet. Osana dokumentointia yritysten tulisi löytää prosessin keskeisimmät riskit ja asettaa niitä vastaavat kontrollit ja huomioida nämä dokumentoinnissa.

Kaikkien kontrollien tunnistaminen avainkontrolleiksi

Joissakin tapauksissa kaikki kontrollit oli tunnistettu avainkontrolleiksi. Tämä johtaa tarpeettomaan testaukseen. Saavuttaakseen tarkoituksenmukaisen tason testauksessa ja dokumentoinnissa organisaatioiden tulisikin kriittisesti arvioida, mitkä ovat merkittäviä kontrolleja.

Jälkiarviointien puuttuminen

Yrityksissä ei ollut sovittu SOX-projektin jälkeen, miten prosesseja voitaisiin edelleen kehittää. Yritysten tulisikin määritellä vuotuisesti, miten SOX-projektin tuloksia voitaisiin edelleen kehittää. Kehitystavoitteita tulisi lisäksi käydä lävitse myös osakkeenomistajien kesken parhaan mahdollisen tason saavuttamiseksi.

Toisaalta SOX-projekteissa opittujen käytäntöjen lisäksi SOX:n pohjalta syntyy erinäisiä hyötyjä. Erityisesti COBIT:n implementointi osana auditointiprosessia on merkittävästi parantanut riskien hallintaa ja luonut varmuuden siitä, että käytettävä auditointitekniikka noudattelee alan parhaita käytäntöjä sekä kontrollitoimintoja. Muina hyötyinä kohdeorganisaatiossa ovat olleet asiakkaiden aktiivisuuden lisääntyminen osana auditointiohjelmaa sekä positiiviset vaikutukset asiakassuhteisiin. Mukana olleet osapuolet uskovatkin sisäisen auditoinnin olevan tehokasta toimintaa ja tuottavan lisäarvoa osakkeenomistajille. Damianides (2005)

5.4 Yhteenveto

Tämän tutkimuksen näkökulman ja tavoitteen mukaisesti kontrollien kehittämisessä tulee huomioida se, että toimintoja ja prosesseja kehitetään luotettavammaksi. Kehityksessä tulee hyödyntää SOX-projektien pohjalta syntyneitä käytäntöjä.

Prosessien kehittäminen, jonka lopullisena tavoitteena on kehittää kontrollien kriittinen arviointi prosessiksi, tulee sisällyttää osaksi vuotuista liiketoimintaa ja käytäntöjä. SOX:n voimaantulon jälkeen on toteutettu useita projekteja

vaatimusten pohjalta ja näistä on kyetty määrittelemään useita puutteita ja hyviä käytäntöjä, miten SOX:n vaatimuksiin voidaan parhaiten vastata.

Tämän tutkimuksen tavoitteena olevan kehittämissuunnitelman laatimisessa noudatetaan kyseisiä vaiheita soveltuvin osin ja lopputuloksena syntyvän kehittämissuunnitelman yhtenä tärkeänä ominaisuutena on yleistävyys myös muiden organisaation prosessien kehittämisen tueksi.

6 TAPAUSTUTKIMUS

6.1 Tutkimusmenetelmät

Hirsijärvi ym. (2001) mukaan tutkimuksella on olemassa tarkoitus, joka ohjaa tutkimusstrategisia valintoja. Yin (2001) jaottelee eri tutkimusstrategioiden olevan kokeet, katselmukset, arkistoanalyysit, historiikit ja tapaustutkimukset. Tämä pro gradu – tutkielma on tapaustutkimus, joka käsittelee kontrollien kehittämistä talouden prosesseissa Sarbanes-Oxley lain vaatimusten pohjalta.

Syrjälä ym. 1994 mukaan tapaustutkimus on luonteva lähestymistapa, kun kyseessä on käytännön ongelmien kokonaisvaltainen tarkastelu ja kuvaus. Tapaustutkimuksen valintaan tutkimusstrategiaksi Yin:n (2001) mukaan vaikuttavat kolme ehtoa, joita ovat tutkimuskysymyksen muoto, tutkijan tarve kontrolloida ja mahdollisuus vaikuttaa tutkittavien todelliseen käyttäytymiseen sekä keskittyykö tutkimus menneisiin tapahtumiin, vai nykyhetkeen.

Tutkimuskysymyksen muotoa tarkastellessa Yin:n (2001) mukaan tutkimuskysymyksen tulisi vastata kysymyksiin ”Miten?” ja ”Miksi?”, mutta myös kysymys ”Millaisia?” voidaan tulkita soveltuvan tapaustutkimukseen. Tämän tutkimuksen tutkimuskysymys on: Millaisin kontrollein voidaan dokumentoidusti varmentaa, että talouden prosessien tuottama informaation on luotettavaa, oikeellista ja läpinäkyvää?

Tutkijan tarvetta ja mahdollisuutta kontrolloida ja vaikuttaa tutkittavien todelliseen käyttäytymiseen Yin:n (2001) mukaan ei tapaustutkimusta käytettäessä tule olla. Tapaustutkimuksen vahvuus onkin useiden erityyppisten evidenssien – dokumentit, artefaktit, haastattelut sekä havainnointi - käytön mahdollisuus (Yin 2001). Tässä tutkimuksessa tarkastellaan nimenomaan syntyneiden käytäntöjen hyödyntämistä kohdeyrityksessä, joka tarkoittaa sitä, että tutkijalla ei ole minkäänlaista vaikutusta tapahtumien tai todellisen käyttäytymisen kulkuun.

Edelleen tapaustutkimuksen käyttöä tutkimusstrategiana tämän tutkimuksen yhteydessä puoltaa se, että tässä tutkimuksessa tarkastellaan nykyhetkeä. Yin:n (2001) mukaan tapaustutkimus keskittyy nykyhetkeen.

Tutkimuksen teon yhteydessä tulee huomioida myös tutkimuksen laatu. Hirsijärvi ym. (2001) mukaan tutkimuksessa pyritään välttämään virheitä, mutta siitä huolimatta tulosten luotettavuus ja pätevyys vaihtelevat. Tämän vuoksi kaikissa tutkimuksissa pyritään arvioimaan tehdyn tutkimuksen luotettavuutta (Hirsijärvi 2001). Tutkimuksen tulosten luotettavuutta ja yleistettävyyttä Syrjälän ym. (1994) mukaan voidaan tarkastella käsitteiden reliaabelius ja validius avulla. Reliaabelius Hirsijärvi ym. (2001) mukaan yksinkertaisesti tarkoittaa sitä, että mittaustuloksia voidaan pitää toistettavina. Validius puolestaan tarkoittaa Hirsijärvi ym. (2001) mukaan tutkimusmenetelmän kykyä mitata sitä, mitä sen oli tarkoituskin mitata. Yin (2001) puolestaan määrittelee tapaustutkimuksen laadulle reliabiliteetin lisäksi kolme erityyppistä validiteettia, joita ovat sisäinen validiteetti, ulkoinen validiteetti ja rakenteellinen validiteetti. Sisäisellä validiteetilla Yin (2001) tarkoittaa kausaalisen syy-yhteyden muodostamista, missä osoitetaan tiettyjen olosuhteiden liittymisen toisiin olosuhteisiin. Ulkoinen validiteetti puolestaan käsittää tutkimuksen yleistettävyyden ja rakenteellinen validiteetti tarkoittaa oikeiden operationaalisten mittareiden asettamista tutkittavalle kohteelle (Yin 2001).

Rakenteellisen validiteetin kannalta tässä tutkimuksessa on pyritty kuvaamaan aihetta sekä teoriaosuudessa, että empiriassa hyvin laajasti. Sisäisen validiteetin kannalta tutkimuksessa määritellään selkeästi ja johdonmukaisesti Yhdysvalloissa asetetun lain vaatimusten pohjalta syntyneiden kontrollikäytäntöjen hyödyntäminen suomalaisen yrityksen näkökulmasta, jota tarkastellaan edelleen empiriassa kyselytutkimuksella ja haastatteluilla. Ulkoisen validiteetin kannalta tutkimuksen aineisto kuvaa hyvin SOX:n pohjalta syntyneiden käytäntöjen hyödyntämistä suomalaisessa yritysmaailmassa. Reliabiliteetin kannalta puolestaan tutkimuksessa evidenssiä

on kerätty kirjallisuuden pohjalta, haastatteluin, kyselyin sekä kohdeyrityksen virallisten dokumenttien havainnoinnin pohjalta. Näistä on edelleen poimittu oleellisimmat havainnot ja johtopäätökset perustuvat kirjallisuudessa määriteltyyn aineistoon. Johtopäätösten tekoon vaikuttaa tällöin ainoastaan todelliset erot tutkittavassa kohteessa, eli esimerkiksi tämän tutkimuksen mukaisesti, eri yrityksissä asetettavat kontrollitavoitteet voivat vaihdella yrityksen kontrollitason mukaan. Tarkemmin tutkimuksen reliabiliteettia ja validiteettia arvioidaan pohdintaluvussa.

6.2 Talouden prosessien kehittämisprojekti kohdeyrityksessä

Kohdeyritys on yksi suurimmista elintarvikealan yrityksistä Suomen ja Baltian markkina-alueella. Kohdeyrityksen toiminta jakaantuu kaikkiaan Suomen lisäksi neljään muuhun maahan. Kohdeyrityksellä on useita tuotantoyksiköitä Suomessa sekä Ruotsin lisäksi myös Baltian alueella. Kohdeyrityksen palveluksessa on yli kolme tuhatta henkilöä ja liikevaihto on useita satoja miljoonia vuodessa.

Kohdeyritys elää voimakkaan kasvun aikaa ja keskittyy erityisesti liiketoiminnan toimintatapojen ja käytäntöjen uudistamiseen. Yhtenä osana kohdeyrityksen toimintatapojen uudistamista tutkitaan, miten sähköisiä järjestelmiä voidaan kehittää ja hyödyntää tehokkaammin tukemaan yrityksen toimintaa.

Kohdeyrityksessä käynnistettiin syksyllä 2006 projekti talouden prosessien kehittämiseksi. Projektin tavoitteena on kuvata ja määritellä taloushallinnon nykytila ja prosessit ensimmäisessä vaiheessa. Projektin toisessa vaiheessa arvioidaan ja määritellään kehityskohteet talouden prosessien osalta. Projektin keskeisenä tavoitteena on kriittisesti tarkastella talouden prosessien hallittavuutta sekä tarkoituksenmukaisuutta ja edelleen kehittää prosesseja vastaamaan yrityksen voimakkaan kasvun aiheuttamia vaatimuksia.

Projektiorganisaatio koostuu projektiryhmästä ja projektin ohjausryhmästä. Projektiryhmään kuuluu ensimmäisessä vaiheessa yrityksen omia työntekijöitä ja toisessa vaiheessa projektissa hyödynnetään lisäksi ulkoisia asiantuntijapalveluita.

Projektin edistymistä ja tuloksia seurataan säännöllisesti projektin ohjausryhmässä, johon kuuluu projektipäällikön lisäksi yrityksen ylintä johtoa.

Tämä tutkimus tehdään projektin yhtenä osa-alueena arvioimaan talouden prosessien tilaa tietojärjestelmien näkökulmasta. Tässä yhteydessä tutkimus käsittää nykytilan ja yksittäisen prosessin läpikäynnin, mutta tulevaisuudessa tämän tutkimuksen osalta nousseita kehityskohteita ja tavoitteita on tarkoitus hyödyntää myös yrityksen muissa talouden prosesseissa.

6.3 Tutkimuksen suorittaminen

Tutkimuksessa haluttiin arvioida, miten SOX:n pohjalta syntyneitä kontrollikäytäntöjä voidaan hyödyntää suomalaisen yrityksen toiminnassa luotettavamman taloudellisen informaation takaamiseksi.

Tutkimuskohteena on yksittäinen prosessi, jonka vuoksi tämän tutkimuksen tutkimusmenetelmänä on tapaustutkimus, joka tutkii mennyttä tai nykyistä todellisuutta, tapahtumaa tai toimivia ihmisiä todellisessa kontekstissa (Järvinen & Järvinen 2004). Tutkimusmenetelmää sovelletaan luomalla ymmärrys teorian perusteella sekä määritellään kontrollien kehittämiseksi keskeisimmät kontrollitasot, joiden avulla pyritään kuvaamaan kattava kontrolliympäristö. Tavoitteena on saada selkeitä havaintoja SOX-projekteissa syntyneiden käytäntöjen ja kehitettyjen kontrollien soveltamisesta suomalaisen yrityksen prosessien kuvaamiseksi ja kehittämisestä luotettavammaksi, läpinäkyvämmäksi sekä kattavammaksi.

Tässä tutkimuksessa tiedonkeruumenetelminä käytettiin havainnointia, kyselyitä, kirjalliseen materiaaliin perehtymistä kirjallisuuskatsauksessa sekä

haastatteluja. Havainnointi suoritettiin tutkijan toimesta talouden prosessien kehittämisprojektin yhteydessä, jossa tutkija itse oli osallisena. Pääosin havainnointi on perustunut projektin materiaaliin perehtymiseen sekä oman toiminnan rekisteröimiseen. Täten havainnointi on ollut osallistuvaa havainnointia, joka Järvisen & Järvisen (2004) mukaan antaa tutkijalle laajemman ja syvällisemmän kuvan tutkittavasta tapahtumasta tai ilmiöstä. Toisaalta havainnointi tiedonkeruumenetelmänä on riippuvaista tiedonkerääjästä, mutta tutkimustehtävä myös ohjaa havainnointia ja vaikuttaa kerättävään tutkimusmateriaaliin (Järvinen & Järvinen 2004).

Tutkimus aloitettiin maaliskuussa 2006 tutkimuksen suunnittelulla. Tässä vaiheessa määriteltiin tutkimusongelma ja tutkimuksen rajaukset. Tutkimussuunnitelmaa varten kerättiin laaja-alaisesti kirjallista aineistoa, jonka keräämistä jatkettiin koko tutkimuksen ajan. Tutkimusstrategiaksi valittiin tapaustutkimus. Tämän valinnan pohjalta tutkija perehtyi tapaustutkimukseen tutkimusstrategiana, kuinka tapaustutkimus tehdään ja mitkä ovat sen laadullisia tekijöitä. Tutkimusongelman tarkennuksen ja aiheen rajaamisen jälkeen syksyllä 2006 työtä jatkettiin kirjallisuuskatsauksen kirjoittamisella.

Tutkimuksen empiirisen osan valmistelu aloitettiin tammikuussa 2007. Teorian pohjalta määritellyn kontrolliympäristön ja SOX kehitysprojektien vaiheiden perusteella laadittiin tiedonkeruun ensimmäisessä vaiheessa käytettävät kysymykset organisaation eri tasoille. Kysymysten valmistelun lähtökohtana toimi teoriassa kuvatut kontrollin eri tasot yrityksessä, jonka perusteella määriteltiin organisaation kohderyhmät, joille kysymykset jaettiin. Ennen kysymystä kyselyyn osallistuville henkilöille selvitettiin lyhyesti tutkimuksen tarkoitus, ja kysymyksiin vastaaminen. Kysymykset toteutettiin sähköpostin välityksellä ja vastaajille lähetettiin kysymykset excel-lomakkeina. Kysymyksiin (liite 3) vastaaminen tapahtui arvioimalla kysymyksessä esitettyä väittämää numeraalisesti.

Kysymyksillä kartoitettiin yrityksen kontrolliympäristön puutteita, joiden pohjalta etsittiin selkeitä puutteita eri tasojen kontrollitoiminnoissa. Kysymykset jaettiin yrityksessä henkilöille heidän asemansa mukaisesti. Taulukossa 3. esitetään kysymyksiin vastanneiden lukumäärä eri tasoihin nähden.

Taulukko 3. Kysymyksiin vastanneiden lukumäärä.

Taso	Lukumäärä
Entiteetti	1
Aktiviteetti	5
Sovellus	4

Taulukossa 4. kuvataan vastanneiden henkilöiden asemaa yrityksessä. Entiteettitason kysymykset esitettiin yrityksen ylimmälle johdolle. Aktiviteettitason kysymykset esitettiin operatiiviselle tasolle, tällä tasolla eri työnimikkeitä olivat: IT-manager, tietohallintopäällikkö ja raportointiasiantuntija. Sovellustason kysymyksiin vastanneiden työnimikkeitä olivat kirjanpitäjä, palvelupäällikkö sekä kehitysinsinööri.

Taulukko 4. Kysymyksiin vastanneiden asema yrityksessä.

Asema	Lukumäärä
IT-manager	2
Johtaja	1
Kehitysinsinööri	1
Kirjanpitäjä	2
Palvelupäällikkö	1
Raportointiasiantuntija	2
Tietohallintopäällikkö	1

Nykytilan kartoittamiseksi kysymykset jaettiin edellä kuvattujen tasojen mukaisesti kolmeen ryhmään. Eniteetti- sekä aktiviteettitaso kuvaavat yleistä kontrolliympäristöä ja sovellustaso kuvaa ostolaskuprosessiin liittyvää kontrolliympäristöä. Eri ryhmien kokonaisuus jaoteltiin edelleen eri osa-alueisiin COBIT:n prosessien mukaisesti (kts. Kuva 3, s.24).

Ensimmäisessä vaiheessa kyselyllä mitattiin karkeasti edellä mainittujen osa-alueiden tilaa ja tärkeyttä. Vastaajat arvioivat esitetyn väitteen tärkeyttä seuraavan skaalan mukaisesti:

1) osa-aluetta ei ole tunnistettu yrityksessä tärkeäksi

2) osa-alue on tunnistettu, mutta sitä ei pidetä tärkeänä

3) osa-alue on tunnistettu, mutta toiminta on hajanaista ja rajoittuu yksittäisten ihmisten toimintoihin

4) osa-alue on tunnistettu ja koetaan tärkeäksi. Toiminta on säännöllistä ja määriteltyä

5) osa-alue on tunnistettu ja koetaan erittäin tärkeäksi. Toimintaa arvioidaan ja kehitetään jatkuvasti.

Kysymyksiin vastanneet eivät tienneet, mihin kontrolliosa-alueeseen kysymykset kuuluivat, vaan arvioivat pelkästään lomakkeella ollutta väittämää edellä kuvatun asteikon mukaisesti. Vastaajat sen sijaan määriteltiin kuuluviksi tietyn tason ryhmiin organisaation rakenteen ja toimintojen perusteella, ja vastaaja sai määritellyn tasonsa mukaiset kysymykset.

Tutkimuksen toisessa vaiheessa tiedonkeruuta laajennettiin edelleen haastatteluiden avulla. Haastatteluita suoritettiin yrityksen tietohallinnossa IT-managereille ja tietohallintopäällikölle sekä taloushallinnossa palvelupäällikölle ja pääkirjanpitäjälle. Haastattelut olivat vapaamuotoisia, mutta toisaalta haastattelun tavoitteena oli löytää kohdeyritykselle merkittävimmät tekijät tehdyistä havainnoista ja tuloksista. Tapaustutkimuksen yhtenä etuna on käyttää hyvinkin erilaista materiaalia samasta tutkimuskohteesta. (Järvinen & Järvinen). Laajempien tiedonkeruumenetelmien käyttö laajentaa näkökulmia ja parantaa täten tutkimuksen luotettavuutta (Hirsijärvi ym. 2001).

Aineistoa analysoitiin siten, että ensimmäisen vaiheen kysymykset liitettiin teoriaosuudessa määriteltyyn kontrollikontekstiin, jonka pohjalta asetettiin kussakin osa-alueessa kontrolliprosessi ja - tavoitteet. Tämän jälkeen kontrolliprosessit ja – tavoitteet käytiin lävitse yhdessä yrityksen tietohallinnon kanssa vapaamuotoisten haastatteluiden avulla. Läpikäynnin tavoitteena oli löytää havaituista puutteista ne osa-alueet, joiden osalta tarve arvioitiin suureksi. Lisäksi ko. osa-alueiden kohdalla COBIT:n kontrolliprosesseista ja – tavoitteista määriteltiin yrityksen toiminnan kannalta merkittävimmät. Se, että kaikkia COBIT:n prosesseja ei käsitelty on linjassa tutkielman näkökulman kanssa, missä määritellään SOX:n pohjalta syntyneiden kontrollien hyödyntämisen suomalaisen yrityksen toiminnassa.

Tarkemmin tutkimuksen viitekehys on seuraava:

Ensimmäinen vaihe

Valitaan ja kuvataan kohdeprosessi tai kohdeprosessit sekä kartoitetaan eri kontrollitasojen nykytila. Mallinnuksessa kuvataan prosessin konteksti, eli miten prosessi sijoittuu suhteessa organisaation muihin talousprosesseihin ja edelleen kuvataan valittu prosessi yksityiskohtaisesti. Nykytila kartoitetaan tämän tutkimuksen yhteydessä yrityksen henkilöstölle jaetuilla kysymyksillä.

Toinen vaihe

Toisessa vaiheessa nykytila sekä kohdeprosessi käydään lävitse yhdessä yrityksen tietohallinnon sekä prosessin omistajan kesken. Läpikäynnin tavoitteena on löytää kriittisimmät kehityskohteet ja arvioida niiden merkittävyyttä. Läpikäynnin perusteella määritellyt kehityskohteet liitetään edelleen COBIT:n prosesseihin.

Kolmas vaihe

Kolmannessa vaiheessa arvioidaan löydetyt puutteet. COBIT-prosessien perusteella määritellään kontrollitavoitteet, jotka lisäksi käydään lävitse

yhdessä kohdeyrityksen tietohallinnon kanssa. Näin löydetään ne käytännöt ja proseduurit, joilla nämä tavoitteet saavutetaan.

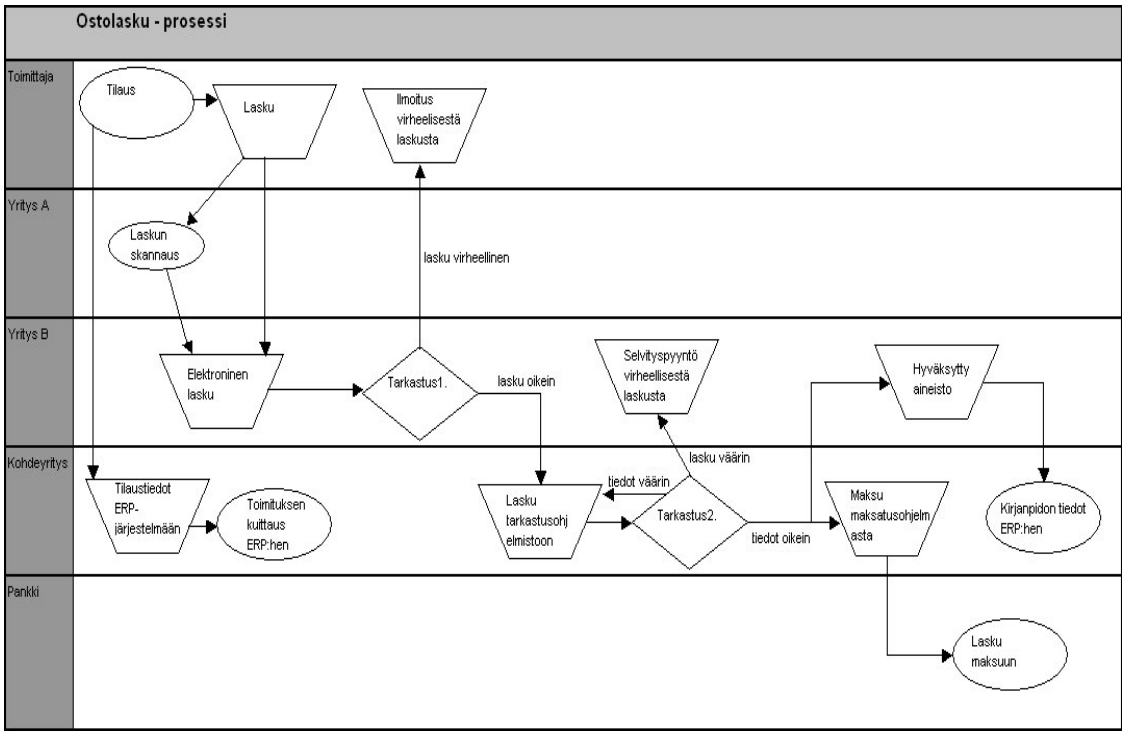
Rajaukset

Tämän tutkielman yhteydessä ei käsitellä kaikkia COBIT:ssa määriteltyjä kontrolliprosesseja ja – tavoitteita, vaan ainoastaan niitä, jotka yrityksen tietohallinnon ja prosessin omistajan kanssa ovat keskeisimmiksi määritellyt. Myös esille nousseista puutteista käsitellään ainoastaan ne, jotka ovat yhdessä kohdeyrityksen kanssa määritellyt merkittäviksi.

7 TUTKIMUSTULOKSET

7.1 Ensimmäinen vaihe: nykytilan kuvaaminen

Ostolaskuprosessi kuvattiin taloudenprosessien kehittämisprojektin ensimmäisen vaiheen aikana kuvaamalla ensin prosessin toimijat ja sitten haastattelemalla eri henkilöitä, jotka kuuluivat prosessiin. Kuvassa 12. on kuvattu ostolaskuprosessin nykytila. Kuviossa on esitetty vaakatasoille eri toimijat, joita ovat toimittaja, joka kuvastaa esimerkiksi tavarantoimittajaa, yritys A, joka vastaa yrityksen laskujen skannauksesta, yritys B, joka vastaa yrityksen taloushallinnon sähköisten palveluiden toteuttamisesta, itse kohdeyritys sekä pankki, joka vastaa varojen fyysisestä käsittelystä.

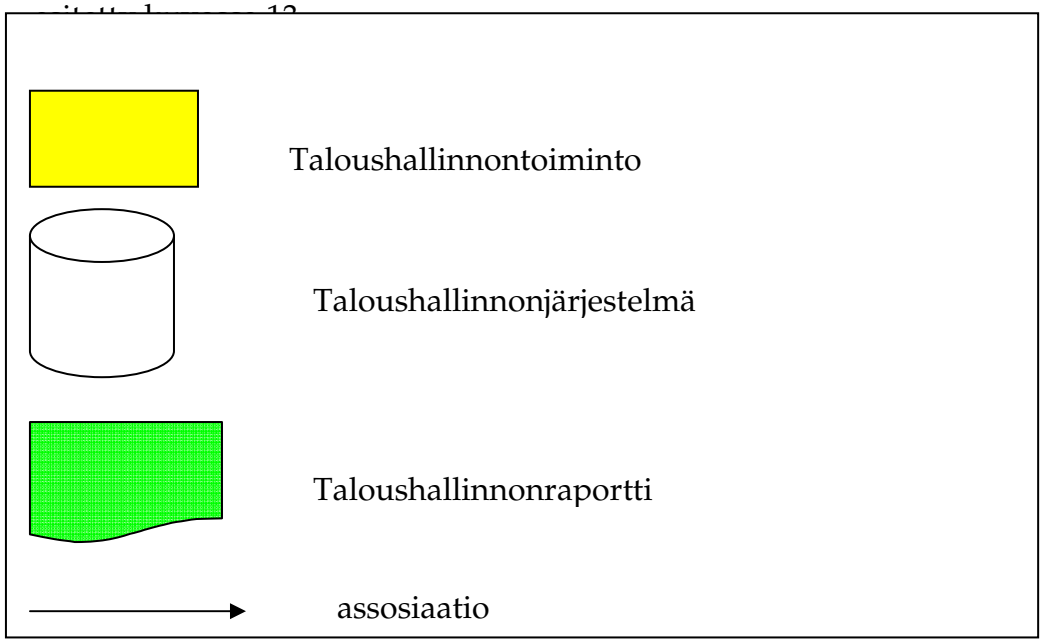


Kuva 12. Ostolasku – prosessin lähtötilanne.

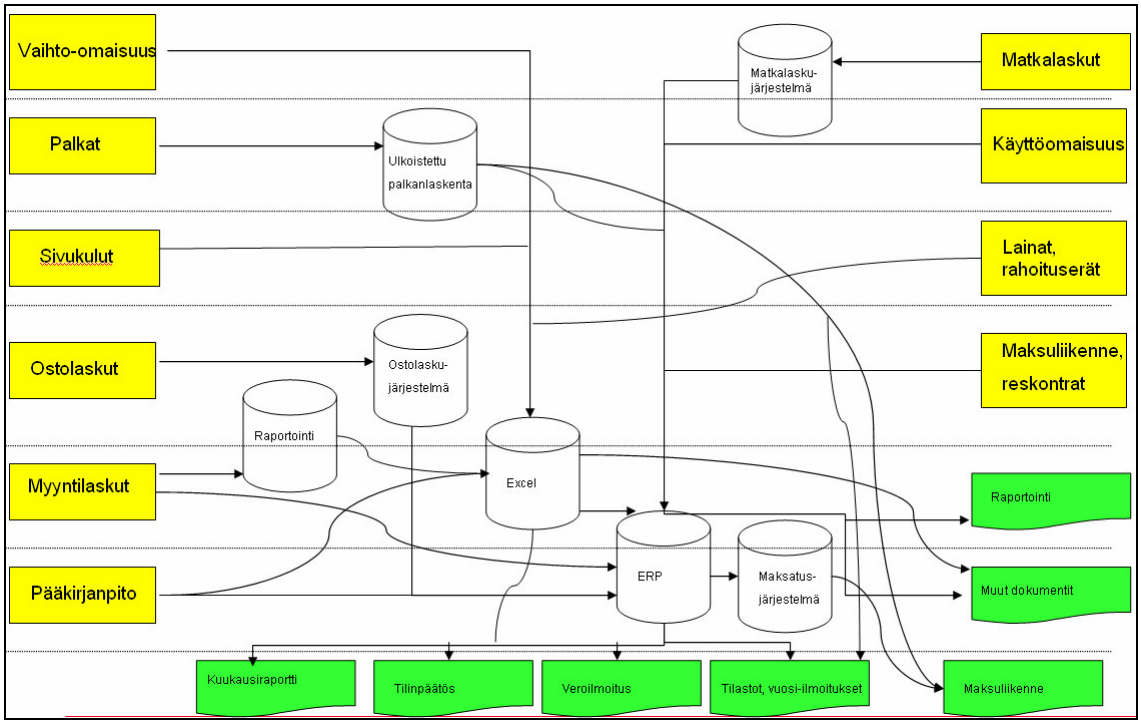
Ostolasku tulee toimittajalta joko EDI-sanomana suoraan yritys B:n järjestelmään elektroniseksi laskuksi tai paperisena laskuna ensin yritys A:lle, jossa lasku skannataan ja lähetetään elektronisena yritys B:n järjestelmään. Yritys B tarkastaa laskun teknisen toimivuuden ja toimittaa laskun

kohdeyrityksen ostolaskujen tarkastusjärjestelmään. Yritys B lähettää lisäksi ilmoituksen virheellisestä laskusta, jos laskun elektronisessa muodossa on virheitä. Kohdeyrityksessä lasku menee ensin henkilöille, jotka tarkastavat laskun tiedot ja tiliöivät laskun. Tämän jälkeen laskun hyväksyy määritelty henkilö, jolla on oikeus hyväksyä laskuja. Mikäli hyväksyjä havaitsee virheen, niin hän toimittaa laskun takaisin tarkastajalle. Mikäli lasku on tarkastajan ja/tai hyväksyjän mukaan virheellinen, laskusta lähetetään selvityspyyntö yritys B:lle. Laskun hyväksymisen jälkeen laskuaineisto siirtyy kohdeyrityksen maksatusohjelmistoon, josta pääkassan hoitaja maksaa sen edelleen pankkiin. Edelleen kun lasku on hyväksytty, niin se siirtyy yritys B:lle, joka siirtää hyväksytyn laskuaineiston kohdeyrityksen ERP-järjestelmässä oleviin kirjanpidon tietoihin.

Ostolaskuprosessin sijoittumista suhteessa yrityksen muihin taloushallinnonprosesseihin kuvataan kuvassa 14. Kuviossa on eritelty taloushallinnontoiminnot, -järjestelmät sekä – raportit. Kuvion symbolit on



Kuva 13. Symboleiden selitys



Kuva 14. Ostolaskuprosessin sijoittuminen yrityksen muihin taloushallinnon prosesseihin.

7.2 Toinen vaihe: kontrollipuutteiden määrittely

Tässä kappaleessa määritellään esiin tulleet puutteet. Kontrollitavoitteet määritellään COBIT-viitekehyksen perusteella.

7.2.1 Kontrolliympäristön puutteiden määrittely

Kontrolliympäristö määriteltiin kolmella tasolla: i) entiteetti-, ii) aktiviteetti- ja iii) sovellustaso. Kaikille eri kontrolliympäristön tasoille määriteltiin empiirisen tutkimuksen ensimmäisessä vaiheessa kysymykset COBIT-mallin pohjalta. Eri kontrolliympäristön tuloksia kuvataan kaaviolla, jossa ensimmäisessä sarakkeessa on esitetty kontrolliosa-alue ja toisessa sarakkeessa on laskettu matemaattinen keskiarvo vastaajien antaman numeraalisen arvion perusteella kontrolliosa-alueen tilasta (tarkempi kuvaus numerojen merkitsevyydestä on esitetty luvussa 6.3).

Tulokset

Entiteettitason osa-alueiden vastausten tuloksia havainnollistetaan kaaviossa 2. Taulukosta 5 nähdään, että selkeimmin entiteettitasolla muita osa-alueita jäljessä on riskien hallinnan osa-alue. Riskien hallinnan osa-alue koostuu tietyistä kontrollitoiminnoista, jotka ovat kaavion perusteella riskien analysointi ja kontrollointi, laadun hallinta, suorituskyvyn mittaaminen ja arviointi sekä sisäisen kontrollin mittaaminen ja arviointi. Muita kontrollitoimintoja edellä on suorituskyvyn mittaaminen ja arviointi.

Taulukko 5. Entiteettitason kartoitus kysymysten perusteella.

Kontrolliympäristö	**3,95**
IT strateginen suunnittelu	**3,5**
IT prosessit, organisaatio ja sidosryhmät	**4,3**
IT henkilöstön johtaminen	**4**
Loppukäyttäjien opastus ja kouluttaminen	**4**
Informaatio ja viestintä	**3,7**
Johdon tavoitteiden ja visioiden viestintä	**3,7**
Riskien hallinta	**3,125**
Riskien analysointi ja kontrollointi	**3**
Laadun hallinta	**3**
Suorituskyvyn mittaaminen ja arviointi	**3,5**
Sisäisen kontrollin mittaaminen ja arviointi	**3**

Taulukossa 6 on esitelty aktiviteettitason kontrollitoimintojen taso tehdyn kyselyn perusteella. Taulukon tietojen perusteella on havaittavissa selkeät puutteet tietyissä kontrollitoiminnoissa. Selkeimmät puutteet kontrollitoiminnoissa taulukon 3 perusteella ovat toimintojen - , muutosten - , palvelutasojen hallinnassa sekä loppukäyttäjien kontrolloinnissa, järjestelmäturvallisuuden takaamisessa ja ongelmien hallinnassa. Näiden osalta toiminta on hajanaista ja se keskittyy yksittäisten ihmisten toimintoihin.

Taulukko 6. Aktiviteettitason kartoitus kyselyn perusteella.

Ohjelmistojen hankinta ja ylläpito	3,03
Hardwaren hankinta ja ylläpito	3
Toiminnnot	3,2
Ratkaisujen asentaminen ja muutokset; asennus ja valtuudet	3,07
Muutosten hallinta	2,75
Palvelutasojen määritys ja hallinta	2,8
Kolmannen osapuolen palvelujen hallinta	3,7
Järjestelmäturvallisuuden takaaminen	2,92
Konfiguraation hallinta	3,72
Ongelmien hallinta	2,93
Tiedon hallinta	3,07
Toimintojen hallinta	2,6
Loppukäyttäjät	2,9

7.2.2 Ostolaskuprosessin puutteiden määrittely

Kappaleessa 7.1 esitetty ostolaskuprosessi käytiin lävitse yhdessä taloushallinnon sekä IT-organisaation kanssa. Läpikäynti suoritettiin siten, että eri puutteista keskusteltiin; mitä eri puutteita ostolaskuprosessissa on, mikä on niiden merkittävyys prosessin kannalta ja kuinka oleellisia ne ovat yrityksen toiminnan kannalta. Prosessikuvauksen läpikäynnin lisäksi ostolaskuprosessia arvioitiin kyselyn avulla.

Prosessikuvauksen läpikäyminen nosti esille puutteita ostotilauksen kohdistamisessa laskulle, ostolaskujen hyväksymisen suuren työmäärän, vaarallisen työyhdistelmän syntymisen, puutteellisen dokumentoinnin maksuliikenteen osalta, riippuvuuden ohjelmistoihin, virheiden vaikean jäljitettävyyden sekä niiden havaitsemisen ylemmällä tasolla. Tämän lisäksi erittäin kriittisenä puutteena on laskun maksaminen; laskujen maksamisesta vastaa käytännössä yksi ihminen.

Taulukossa 7. on esitetty sovellustason kontrollien arvioinnin tuloksia ostolaskuprosessissa. Taulukon tietojen pohjalta voidaan todentaa edellä esitettyjen asioiden lisäksi seuraavia puutteita ostolaskuprosessissa:

- Toimittajarekisterin hallinta on puutteellista
- Toimittajarekisterin muutosten dokumentointi on puutteellista
- Muutoksien hallinta ei ole dokumentoitua

Taulukko 7. Sovellustason kysymysten tulokset

Ostoilaukset kohdistuvat ainoastaan hyväksytyille tilauksille	3,25
Ostotilaukset on syötetty oikein	2,75
Kaikki ostotilaukset syötetään ja prosessoidaan	3
Ostotileille (ostoreskontra) kirjatut summat esittävät ostettuja tuotteita ja palveluita	2,25
Ostotilien summat on laskettu ja kirjattu oikein	3
Kaikkien vastaanottettujen tuotteiden ja palveluiden määrät on syötetty ja prosessoitu	2,5
Kaikkien vastaanotettujen tuotteiden ja palveluiden summat on tallennettu oikealle ajanjaksolle	2,25
Ostoreskontran sisältöä on korjattu vain oikeasta ja perustellusta syystä	2,5
Hyvityslaskut ja muut muutokset on tarkasti kirjattu ja tallennettu	2,25
Kaikki hyvityslaskut ja muut muutokset syötetty ja prosessoitu	2,5
Kaikki hyvityslaskut ja muut muutokset on kirjattu oikealle ajanjaksolle	2,25
Maksusuoritukset tehdään vain vastaanotetuille tuotteille ja palveluille	3
Maksut suoritetaan oikeille toimittajille	3,25
Maksusuoritukset on laskettu ja kirjattu	2
Kaikki maksusuoritukset tallentuvat	3,5
Maksuoritukset kirjataan oikealle ajanjaksolle	3
Toimittajarekisteriin tehdään vain oikeat muutokset	3,25
Kaikki toimittajarekisterin muutokset prosessoidaan ja tallennetaan	2
Toimittajarekisterin muutokset ovat oikeellisia	3,25
Toimittajarekisterin muutokset prosessoidaan ajallisesti oikein	1,75
Toimittajarekisteri on ajantasalla	2,25

7.3 Kolmas vaihe: kehityskohteiden asettaminen

Tässä vaiheessa havaitut puutteet liitetään COBIT:ssa määriteltyihin kontrollitavoitteisiin. Kysymykset pohjautuivat COBIT:n viitekehykseen, jossa kukin osa-alue on liitetty COBIT:n prosessiin (kts. liite 2.). COBIT:n prosessille on määritelty keskeisimmät kontrollitavoitteet ja toimenpiteet tavoitteiden saavuttamiseksi. Kehitystoimenpiteet määriteltiin ja arvioitiin edelleen COBIT:n toimenpiteiden pohjalta yhdessä kohdeyrityksen IT-organisaation kanssa.

Entiteettitasolla heikoimmaksi osa-alueeksi määriteltiin kyselyn perusteella riskien hallinta. Riskien hallintaan on määritelty COBIT:ssa prosessi PO9, arvioi

ja hallitse riskejä ISACA (2005a). Riskien hallinnalle asetettavia kontrollitavoitteita COBIT:n mukaan havainnollistetaan liitteessä 4.

Aktiviteettitasolle kyselyn perusteella heikoimmiksi osa-alueiksi määriteltiin toimintojen hallinta, muutosten hallinta, palvelutasojen määritys ja hallinta, loppukäyttäjät, järjestelmäturvallisuuden takaaminen ja ongelmien hallinta. Näitä vastaavat COBIT:n kontrollitavoitteet on esitetty liitteessä 4.

7.3.1 Kehityskohteiden arviointi

Tässä kappaleessa kuvataan ainoastaan ne kehityskohteet, jotka kohdeyrityksessä arvioitiin merkittäviksi. Kehityskohteista määriteltiin yhdessä tietohallinnon kanssa COBIT:n pohjalta tärkeimmiksi koetut kontrolliprosessit ja – tavoitteet sekä toimenpiteet niiden parantamiseksi.

DS1 Palvelutasojen määrittely ja hallinta

COBIT:n kypsyystasomallissa ITGI:n (2006d) mukaan palvelutasojen määrittely ja hallinta – prosessi määritellään seuraavasti:

> *"Palvelutasojen määrittely ja hallinta – prosessi, joka täyttää asetettavat liiketoiminnalliset vaatimukset IT:lle takaamalla IT:n ydinpalveluiden linjautumisen liiketoimintastrategian kanssa, määritellään tasolle x, kun .."*

Edellä kuvatun määritelmän ja COBIT:n kypsyystasomalliin perustuvan arvioinnin perusteella yhdessä kohdeyrityksen tietohallinnon kanssa palvelutasojen määrittely ja hallinta – prosessin tilaksi määriteltiin 3 – määritelty prosessi. Tämä tarkoittaa ITGI:n (2006d) mukaan sitä, että yrityksessä on vastuut ovat hyvin määriteltyjä, mutta ne ovat epämuodollisia ja vähän tarkasteltuja. Palvelutasojen puutteet on määritelty, mutta puutteiden tarkempi käsittely puuttuu. On olemassa selkeä puute siinä, mitä palvelusta on sovittu ja mitä palvelulla käytännössä saavutetaan.

Palvelutasojen määrittelyn ja hallinnan - prosessin tärkeimmät tavoitteet ovat tietohallinnon kanssa tehdyn läpikäynnin perusteella IT-organisaation palveluiden määrittely ja kuvaaminen sekä sisäisesti että ulkoisesti, palvelutason määrittely sekä ulkoistettujen palveluiden sopimusten tarkoituksenmukaisuus ja palvelutasojen sekä sopimusten seuranta.

DS10 Ongelmien hallinta

COBIT:n kypsyystasomallissa ITGI:n (2006d) mukaan ongelmien hallinta – prosessi määritellään seuraavasti:

"Ongelmien hallinta prosessin hallinta joka täyttää IT:lle asetettavat liiketoiminnalliset vaatimukset, joita ovat käyttäjien tyytyväisyyden varmistaminen tarjotuissa palveluissa sekä ratkaisujen ja toimituspoikkeamien vähentäminen, määritellään tasolle x, kun .."

Edellä kuvatun määritelmän ja COBIT:n kypsyystasomalliin perustuvan arvioinnin perusteella yhdessä kohdeyrityksen tietohallinnon kanssa ongelmien hallintaprosessin tilaksi määriteltiin 2 – toistettava, mutta vaistonvarainen. Tämä tarkoittaa ITGI:n (2006d) mukaan sitä, että yrityksessä on laaja valveutuneisuus liiketoiminnallisen informaation ja tapahtumien IT-pohjaisten ongelmien hallinnan tarpeesta sekä eduista. Prosessissa vastuu on muutamilla avainhenkilöillä ja informaation jakaminen tässä yhteydessä on reaktiivista ja hajanaista.

Ongelmien hallinnan tärkeimmät tavoitteet ovat tietohallinnon kanssa tehdyn läpikäynnin perusteella ongelmien tunnistaminen ja luokittelu, ongelmien jäljittäminen ja laajuus, ongelmien käsittelyprosessi sekä muutosten - , konfiguraatio- sekä ongelmienhallinnan prosessin integroiminen.

DS13 Operaatioiden hallinta

COBIT:n kypsyystasomallissa ITGI:n (2006d) mukaan operaatioiden hallinta – prosessi määritellään seuraavasti:

> *"Operaatioiden hallinta – prosessi, joka täyttää asetettavat liiketoiminnalliset vaatimukset IT:lle vastustamalla ja palautumalla virheistä tiedon eheyden ja ylläpidettävyyden turvaamiseksi, määritellään tasolle x, kun .."*

Edellä kuvatun määritelmän ja COBIT:n kypsyystasomalliin perustuvan arvioinnin perusteella yhdessä kohdeyrityksen tietohallinnon kanssa operaatioiden hallinta – prosessin tilaksi määriteltiin 2 – toistettava, mutta vaistonvarainen. Tämä tarkoittaa ITGI:n (2006d) mukaan sitä, että organisaatiossa tunnistetaan IT:n merkitys liiketoiminnan tukemisessa. Operaatiot perustuvat kuitenkin hyvin pitkälle yksilöiden osaamiseen ja kykyihin. Ohjeistus siitä, mitä, milloin tehdään ja missä järjestyksessä ei ole säännöllisesti ylläpidettyä.

Operaatioiden hallinta - prosessin tärkeimmät tavoitteet ovat tietohallinnon kanssa tehdyn läpikäynnin perusteella tehtävien järjestely ja aikatauluttaminen, IT-infrastruktuurin valvonta ja informaation muodostumisen kontrollointi.

AI6 Muutosten hallinta

COBIT:n kypsyystasomallissa ITGI:n (2006d) mukaan muutosten hallinta – prosessi määritellään seuraavasti:

> *"Muutosten hallinta – prosessi, joka vastaa liiketoiminnallisiin vaatimusten ja strategian yhdenmukaisuudesta koskien IT:n palveluiden ja ratkaisujen tuottamista, määritellään tasolle x, kun .."*

Edellä kuvatun määritelmän ja COBIT:n kypsyystasomalliin perustuvan arvioinnin perusteella yhdessä kohdeyrityksen tietohallinnon kanssa muutosten hallinta – prosessin tilaksi määriteltiin 2 – toistettava, mutta vaistonvarainen. Tämä tarkoittaa ITGI:n (2006d) mukaan sitä, että organisaatiossa on olemassa epämuodollinen muutosten hallinnan prosessi, jota noudatetaan yleensä. Kuitenkaan se ei ole järjestelmällinen eikä anna täyttä

varmuutta virheiden estämiseen. Muutoksen hallintaa suunnitellaan ainoastaan rajallisesti ja välitön muutostarve johtaa välittömään muutokseen.

Muutosten hallinta - prosessin tärkeimmät tavoitteet ovat tietohallinnon kanssa tehdyn läpikäynnin perusteella olivat muutosten standardointi ja käytännöt, pikamuutosten hallinta sekä muutosten käsittelyn päättäminen ja dokumentointi.

AI7 Ratkaisujen asentaminen

COBIT:n kypsyystasomallissa ITGI:n (2006d) mukaan ratkaisujen asentaminen – prosessi määritellään seuraavasti:

> *"Ratkaisujen asentaminen – prosessi, joka tukee liiketoiminnallisia vaatimuksia varmistamalla uuden järjestelmän tai sovelluksen asentamisen ilman suurempia ongelmia, määritellään tasolle x, kun .."*

Edellä kuvatun määritelmän ja COBIT:n kypsyystasomalliin perustuvan arvioinnin perusteella yhdessä kohdeyrityksen tietohallinnon kanssa ratkaisujen asentaminen – prosessin tilaksi määriteltiin 2 – toistettava, mutta vaistonvarainen. Tämä tarkoittaa ITGI:n (2006d) mukaan sitä, että eri ratkaisujen asentamisen käytännöissä on yhdenmukaisuutta, mutta ne eivät perustu määriteltyyn yleiseen käytäntöön. Yleisesti kehityksestä vastaava ryhmä päättää testauksen ja asennuksen käytännöistä. Ratkaisujen hyväksyminen on epämuodollinen prosessi.

Ratkaisujen asentaminen - prosessin tärkeimmät tavoitteet ovat tietohallinnon kanssa tehdyn läpikäynnin perusteella henkilöstön kouluttaminen, testisuunnitelman laatiminen, muutosten testaus, hyväksymistestaus ja järjestelmän osien päivittäminen.

DS5 Järjestelmäturvallisuuden takaaminen

COBIT:n kypsyystasomallissa ITGI:n (2006d) mukaan järjestelmäturvallisuuden takaaminen – prosessi määritellään seuraavasti:

> *"Järjestelmäturvallisuuden takaaminen – prosessi, joka tukee liiketoiminnallisia vaatimuksia takaamalla tiedon käsittely-ympäristön eheyden ja vähentämällä riskien merkittävyyttä määritellään tasolle x, kun .."*

Edellä kuvatun määritelmän ja COBIT:n kypsyystasomalliin perustuvan arvioinnin perusteella yhdessä kohdeyrityksen tietohallinnon kanssa järjestelmäturvallisuuden takaaminen – prosessin tilaksi määriteltiin 2 – toistettava, mutta vaistonvarainen. Tämä tarkoittaa ITGI:n (2006d) mukaan sitä, että vastuunkuvat ovat määritelty IT-turvallisuuden takaamiseksi, mutta vastuiden kattavuus kaikilla organisaatioiden tasolla on rajallista. Tietämys turvallisuustekijöistä on hajanaista ja rajallista. Kolmannen osapuolen palvelut eivät välttämättä täytä yrityksen niille asetettamia tavoitteita.

Järjestelmäturvallisuuden takaaminen - prosessin tärkeimmät tavoitteet ovat tietohallinnon kanssa tehdyn läpikäynnin perusteella IT-turvallisuuden johtaminen, IT-turvallisuussuunnitelma, identiteetin hallinta, käyttäjätilien hallinta sekä turvallisuusuhkien tunnistaminen kattavasti organisaation eri tasoilla.

DS8 Käyttötuen ja käyttötapausten hallinta

COBIT:n kypsyystasomallissa ITGI:n (2006d) mukaan käyttötuen ja käyttötapausten hallinnan – prosessi määritellään seuraavasti:

> *"Käyttötuen ja käyttötapausten hallinta – prosessi, joka tukee liiketoiminnallisia vaatimuksia takaamalla käyttäjäpyyntöjen tehokkaan ja kattavan käsittelyn, määtirellään tasolle x, kun .."*

Edellä kuvatun määritelmän ja COBIT:n kypsyystasomalliin perustuvan arvioinnin perusteella yhdessä kohdeyrityksen tietohallinnon kanssa loppukäyttäjä – prosessin tilaksi määriteltiin 1 –alustavaa / Ad hoc. Tämä

tarkoittaa ITGI:n (2006d) mukaan sitä, että johto tunnistaa tarpeen prosessista käsitellä käyttäjäpyyntöjä. Toiminnassa ei kuitenkaan ole määritelty prosessia, vaan toiminta on reaktiivista, yksilöiden toimintaan perustuvaa.

Käyttötuen ja käyttötapausten hallinta - prosessin tärkeimmät tavoitteet ovat tietohallinnon kanssa tehdyn läpikäynnin perusteella selvityspyyntöjen rekisteröinti ja selvityspyyntöjen käsittely.

7.4 Kehityssuunnitelma

Tässä kappaleessa käydään kehityssuunnitelman eri osa-alueet lävitse.

7.4.1 Kontrolliympäristön kehitys

Tässä kappaleessa määritellään edellä käytyjen perusteella yhteenvetona kehittämissuunnitelma yrityksen talouden prosessien kehittämiseksi. Kehittämissuunnitelma sisältää COBIT:n pohjalta määritellyt kontrollitavoitteet sekä kuvauksen ostolaskuprosessin kehityskohteista ja tavoiteltavasta tilasta. Kehittämissuunnitelma perustuu tieto- ja taloushallinnon kanssa käytettyihin kehittämiskohteiden arviointiin sekä havainnointiin yrityksen toiminnoista.

Palvelutasojen määrittely ja hallinta

Tämän prosessin kehittämiseksi kohdeyrityksessä tulee määritellä IT – organisaation rajapinta. Rajapinnan avulla kuvataan niitä palveluita, joita IT tarjoaa liiketoiminnan tukemiseksi. Edelleen palvelut kuvataan ja määritellään niiden tukema liiketoiminnan osa-alue. Rajapinnan kuvaamisen ja palveluiden määrityksen jälkeen arvioidaan, onko olemassa liiketoiminnallisia tarpeita, joihin ei vielä täysin vastata IT – rajapinnassa.

Ulkoistettujen palveluiden, eli kolmannen osapuolen palveluiden osalta tulee määritellä prosessi ostetun palvelun arvioimiseksi. Prosessiin kuuluu sekä palvelun tarkoituksenmukaisuuden että palvelusopimuksen arviointi. Tällä

varmistetaan, että yrityksessä ostetaan tarkoituksenmukaista palvelua ja edelleen valvotaan sopimuksessa sovittujen palveluiden tuottamista.

Ongelmien hallinta

Ongelmien hallinta prosessin tueksi tulee muodostaa käytännöt koskien ongelmien tunnistamista ja raportointia. Käytännöissä tulee määritellä ongelmien luokitus, vaikutus, kiireellisyys ja prioriteetti suhteessa muihin ongelmiin. Tärkeä osa tätä prosessia on johdon sitouttaminen osaksi prosessia.

Operaatioiden hallinta

Operaatioiden hallinnan osalta tärkein kehityskohde on muodostaa tietämys IT operaatioiden käytännöistä suhteessa liiketoiminnallisiin vaatimuksiin. Tähän liittyen tulee edelleen määritellä mitkä ovat kriittisimmät operaatiot ja varmistaa näiden operaatioiden turvallisuus ja tarkoituksenmukaisuus. Keskeisintä on ymmärtää tietohallinnon töiden resursointi ja organisointi siten, että IT – organisaation tuottamat ja hallitsemat operaatiot kohtaavat liiketoiminnalliset tarpeet (esimerkiksi hankinnan ostojen tietyn osa-alueen hinnan kehityksen raportoinnin reaaliaikaisuus).

Muutosten hallinta

Muutosten hallinnassa tärkeimmäksi kehityskohteeksi määriteltiin dokumentoinnin kehittäminen ja muutosten rekisteröinti. Tässä yhteydessä tätä tarvetta vasten tulee suunnitella raportointijärjestelmä, jossa muutoksista pidetään yllä järjestelmäkohtaista muutoshistoriaa.

Ratkaisujen asentaminen

Ratkaisujen asentamisessa tärkein kehityskohde on ratkaisujen testauksen suunnittelu ja hyväksyntä. Tällä saavutetaan yhdenmukaisuus halutun ja saavutetun tavoitteen välillä.

Järjestelmäturvallisuuden takaaminen

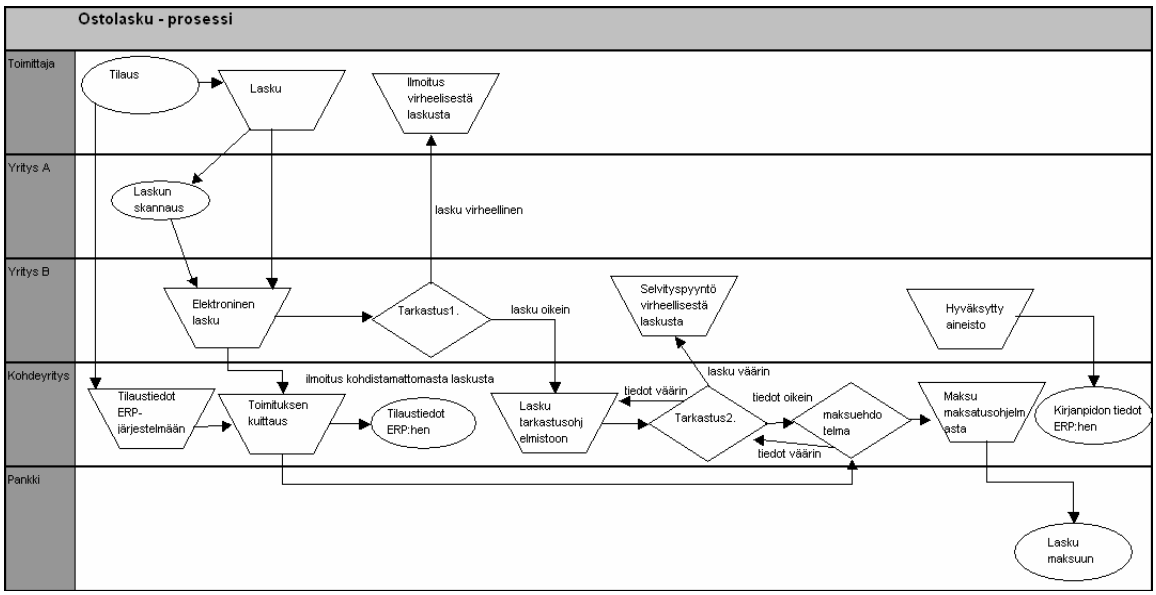
Järjestelmäturvallisuuden takaamiseksi tärkeimmäksi kehityskohteeksi määriteltiin riskiarvioinnin vuotuinen järjestäminen ja sen pohjalta tehty riskien taulukointi. Riskien taulukoinnin avulla voidaan edelleen arvioida kriittisimpiä riskejä sisäisessä kontrollissa talouden raportoinnissa ja –prosesseissa. Riskien kriittisyyden tulee perustua taloudelliseen merkittävyyteen.

Käyttötuen ja käyttötapausten hallinta

Käyttäjien virheilmoitusten ja käyttötukipyyntöjen tueksi kehityskohteeksi määriteltiin keskitetty, palvelukeskeisen prosessin kehittäminen. Prosessin tarkoitus on ohjata loppukäyttäjiä ottamaan yhteyttä järjestelmävastuussa olevaan henkilöön ja täten saamaan parempaa tukea sekä toisaalta vähentää organisaation päällekkäisen tuen aiheuttamaa henkilökuormitusta. Lisäksi tärkeänä prosessissa on käyttötapausten rekisteröinti, joka mahdollistaa ongelmien ja tukipyyntöjen luokittelun ja historiatietojen tallentamisen.

7.4.2 Ostolaskuprosessin kehitys

Ostolaskuprosessin osalta tärkeimmäksi kehityskohteeksi määriteltiin ostolaskujen kohdistaminen tilaukselle. Kuvassa 15. esitetään tavoitetila ostolaskuprosessille.



Kuva 15. Ostolaskuprosessin tavoitetila.

Laskun kohdistaminen muuttaa prosessia siten, että laskuntarkastusohjelmiston jälkeen laskut siirtyvät tarkastukseen maksuehdotelmalle. Maksatuksesta huolehtiva henkilö tarkistaa, että tilauksista muodostuneille laskuille löytyy toimituskuittaus.

Ostolaskuprosessin turvallisuuden kehittämiseksi prosessia tulee kehittää siten, että maksatuksen käytännöistä vastaavien ihmisten vastuita hajautetaan siten, että maksatuksesta ja ostoreskontrasta vastaavat eri ihmiset. Lisäksi maksatusprosessin läpiviemiseksi pitää kouluttaa varahenkilöstöä. Edelleen turvallisuuden kehittämiseksi toimittajarekisterin ylläpidosta määrätään vastuullinen henkilö ja luodaan dokumentointikäytännöt toimittajarekisterin ylläpidosta.

Lisäksi ostolaskuprosessille on määriteltävä varajärjestelmä tai käytännöt nykyisen prosessin toimimattomuuden varalle.

8 POHDINTA

Tämän tutkimuksen päätarkoituksena oli tutkia, miten Yhdysvalloissa asetetun Sarbanes-Oxley lain pohjalta syntyneitä kontrollikäytäntöjä voidaan hyödyntää suomalaisen yrityksen talousprosessien kehittämisessä. Tutkimuksessa keskityttiin tarkastelemaan lain pohjalta syntyneiden kontrollikäytäntöjen hyödyntämistä talouden prosesseissa informaation oikeellisuuden ja luotettavuuden lisäämiseksi.

SOX-käytäntöjen hyödyntäminen suomalaisissa yrityksissä

Tehdyn tutkimuksen perusteella voidaan todeta, että Sarbanes-Oxley lain pohjalta syntyneiden kontrollikäytäntöjen avulla voidaan kehittää ja tarkastella suomalaisen yrityksen talouden prosesseja. Tarkastelu suomalaisen ei SEC-listatun tai muun ei-SEC:n alaisen yrityksen kohdalla tärkeää on kuitenkin ensin pyrkiä määrittelemään liiketoiminnan kannalta oleellinen ja oikea informaatio. Tämä tarkoittaa, että määritellään yrityksen kontekstin perusteella yritystä velvoittavat säädökset ja lait sekä kuvataan yrityksen liiketoimintaympäristö, jotta ymmärretään kokonaisuuksien merkittävyys. Tätä määrittelyä voidaan pitää perustana yrityksen käyttämän informaation kuvaamisessa. SOX:n käytäntöjen pohjalta laadittujen kontrollitavoitteiden asettaminen ei suoranaisesti kuitenkaan aseta standardia oikealle ja luotettavalle informaatiolle. Vaan SOX pyrkii nimenomaan luomaan resurssit ja lähtökohdan sille, että informaatio on oikein tuotettu. Keskeinen informaatiota varmentava kontrollitoiminto kohdeorganisaation ostolaskuprosessissa oli toimittajarekisterin hallinnan kehittäminen (kts. luku 7.4.2). Toimittajarekisteri liittyy välillisesti ostolaskuprosessiin ja toimittajien hallinta on oma prosessinsa. Toisaalta toimittajien takana hallitaan toimittajien pankkiyhteystietoja ja nimenomaan pankkiyhteystiedoista koostuu ostolaskujen maksuliikenteen osoitteisto, so. minne rahat loppujen lopuksi maksetaan.

Käytetyt viitekehykset

Sarbanes-Oxley lain vaatimusten täyttämiseen on kehitetty useita viitekehyksiä. Yleisimmin käytetyt ovat olleet COBIT ja COSO, joita myös tässä tutkimuksessa hyödynnettiin. Toisaalta määriteltyjä viitekehyksiä on monia muitakin, mutta tässä yhteydessä on tärkeää huomata käytettävien viitekehysten teoreettinen perusta. Viitekehyksiä käytettiin tässä tutkimuksessa seuraavasti: empirian ensimmäisessä vaiheessa luotiin kysymykset nykytilan kartoittamiseksi COBIT:n kontrolliprosessien pohjalta. Kysymysten avulla kyettiin määrittelemään keskeisimmät puutteet yrityksen kontrollikäytännöissä talouden prosesseissa. Toisessa vaiheessa määritellyt puutteet liitettiin COBIT:n kontrolliprosesseihin, jolloin edelleen kolmannessa vaiheessa kontrolliprosessien avulla voitiin asettaa kehittämistoimenpiteitä. COBIT:n prosessien hyödyntäminen nykytilan kuvaamisessa edesauttoi määrittelemään ja jakamaan yrityksen toiminnan selkeisiin osa-alueisiin, kts. luku 7.2.1. Edelleen eri osa-alueiden sisältö oli selkeästi määriteltävissä COBIT:n prosessien perusteella.

Merkittävänä havaintona voidaankin pitää sitä, että COBIT-viitekehyksen avulla kyettiin määrittelemään myös suomalaisen ei-SEC-listatun yrityksen liiketoiminnan kontrollitoimintoja. Tässä yhteydessä tulee kuitenkin huomata, että SOX:ssa käytettyjen viitekehysten pohjalta tehdyt havainnot on syytä läpikäydä ja arvioida yhdessä kohdeorganisaation kanssa oikeiden ja käytännöllisten kontrollitavoitteiden asettamiseksi. Muussa tapauksessa viitekehyksen täysi noudattaminen voi johtaa tehottomaan ja turhan raskaaseen kontrolliympäristöön.

Yksittäisen prosessin kehitys

SOX:ssa määriteltyjen vaatimusten pohjalta voitiin tutkimuksessa nostaa suomalaisen liiketoimintainformaation kannalta oleellisia informaation laatua vaarantavia tekijöitä esiin yksittäisen prosessin kehityksessä. Ostolaskuprosessin erityisen kriittisiä havaintoja olivat ostotilauksen ja ko. laskun kohdistuminen, vaarallisen työyhdistelmän mahdollisuus sekä

riippuvuuden muodostuminen yhden ihmisen ja ohjelmiston varaan. Ostolaskun kohdistamattomuus tilaukselle heikensi informaation eheyttä, saatavuutta, luotettavuutta ja tehokkuutta. Eheys voi vaarantua, kun järjestelmästä menee ylimääräinen lasku hyväksytysti lävitse ja toisaalta saatavuus vaarantuu, kun ostolaskua ei voida tarkasti jäljentää. Toisaalta ostolaskujen käsittelyn keskittyminen yhdelle henkilölle heikentää informaation luotettavuutta ja synnyttää vaarallisen työyhdistelmän. Tällöin väärinkäytösten jäljittäminen ja ehkäiseminen vaikeutuvat. Myös informaation tehokkuuden kannalta ostolaskuprosessi oli puutteellinen ostolaskujen kohdistamattomuuden osalta.

Toisaalta tärkeä havainto tämän tutkimuksen perusteella oli myös se, että yksittäiseen prosessiin vaikuttaa myös prosessin konteksti hyvin voimakkaasti. Erityisesti talouden prosesseja ja – raportointia kehitettäessä yksittäiseen prosessin puutteet voivat olla riippuvaisia ylemmän tason kontrolleista. Tässä tutkimuksessa havaittiinkin ylemmän tason kontrolli- ja riskienhallintaympäristön puutteellisuuden vaikuttavan ostolaskuprosessiin. Esimerkiksi palvelutasojen määrityksellä ja hallinnalla voidaan kommunikoida edelleen eri osa-alueiden toimijoiden kesken raportoinnin kattavuudesta ja tarkoituksenmukaisuudesta.

Kehitys SOX:n pohjalta

COBIT-viitekehyksen käyttö kohdeyrityksen nykytilan kartoittamisessa edesauttoi selkeyttämään ja kuvamaan kontrolliympäristöä kokonaisvaltaisesti. Toisaalta tässä yhteydessä ei oteta kantaa COBIT-viitekehyksen paremmuudesta tai puutteellisuudesta suhteessa muihin vastaaviin viitekehyksiin. Tutkimuksen luonteen mukaisesti, COBIT:n perusteella määriteltyjä kontrolliprosesseja ja – tavoitteita arvioitiin edelleen kohdeyrityksen tietohallinnon kanssa. Läpikäynnin tarkoituksena oli löytää juuri suomalaiseen yrityskulttuuriin sopivimmat ja tärkeimmiksi koetut kehityskohteet. Tässä yhteydessä tuleekin huomata, että Sarbanes-Oxley lain

vaatimusten vaikutus ja niiden pohjalta syntyneiden kontrollikäytäntöjen hyödyntäminen suomalaisessa yritystoiminnassa ovat kaksi eri asiaa. Lain vaatimusten täysimääräinen noudattaminen voi johtaa suomalaisen yrityksen näkökulmasta toimimaattomiin ja byrokraattisiin käytäntöihin.

Tutkimuksen teon motiivit

Taustalla tämän tutkimuksen motiiveissa on lisäarvon tuottaminen yritykselle talousprosessien kehittämisen myötä. Tämä tarkoittaa sitä, että tässä tutkimuksessa esitettyjen kehittämiskohteiden luomiseksi kehitystyön tulisi lähteä siitä lähtökohdasta, että kontrollikäytäntöjen kehittäminen tukee yrityksen taloudellista toimintaa. Tästä syystä kontrollikäytäntöjen kehittämisen tuleekin perustua sen maan, missä yritys juridisesti sijaitsee, kirjanpidon ja tilintarkastuksen asettamiin vaatimuksiin. Kirjanpidon ja tilintarkastuksen vaatimusten pohjalta tulee edelleen kriittisesti arvioida asetettujen kontrollikäytäntöjen liiketoiminnallinen hyöty ja toimivuus.

Tutkimuksen reliabiliteetti ja validiteetti

Tutkimuksen reliabiliteetin ja validiteetin kannalta tässä tutkimuksessa keskityttiin määrittelemään ja löytämään niitä kontrollikäytäntöjä ja –tavoitteita, jotka ovat oleellisia suomalaisen lainsäädännön näkökulmasta ja merkityksellisiä suomalaisen yrityskulttuurin kannalta. Tutkimuksen reliabiliteetin kannalta tutkimuksen lopputuloksia varten kyselylomakkeista pyrittiin määrittelemään mahdollisimman yksinkertaisia ja yksiselitteisiä. Täten reliabiliteettia voidaan pitää kohtuullisena. Lisäksi tässä tutkimuksessa käsiteltiin oikeiden kontrollikäytäntöjen asettamista suomalaisessa yrityksessä, reliabiliteettia parantaa myös se, että havaittuja kontrollitoimintoja läpikäytiin yhdessä kohdeyrityksen kanssa oikeiden ja tarkoituksenmukaisten kontrollitavoitteiden asettamiseksi. Validiteetin kannalta rakenteellista validiteettia pyrittiin vahvistamaan määrittelemällä kontrollikäytännöt perustuen tutkimusten ja teorioiden hyödyntämiseen. Lisäksi rakenteellista validiteettia pyrittiin parantamaan tutustumalla aiempien vastaavien

kontrollikäytäntöjen asettamisessa sattuneisiin virheisiin ja pyrkimällä ohittamaan vastaavat tekijät tässä tutkimuksessa. Sisäisen validiteetin kannalta tutkimuksessa määriteltiin perusteellisesti oikea ja luotettava informaatio ja sen konteksti, eli talouden prosessit organisaatiossa. Ulkoisen validiteetin kannalta käytettyjen viitekehysten ja oikeellisen informaation perusteet määriteltiin huolellisesti. Tällä saavutettiin se, että tutkimusaineisto vastaa hyvin tutkimusongelmaa.

Tutkimuskysymys

Tutkimuksen tutkimuskysymys oli *"Millaisin kontrollein voidaan dokumentoidusti varmentaa, että talouden prosessien tuottama informaatio on luotettavaa, oikeellista ja läpinäkyvää?"*.

Talouden prosessien tuottaman informaation luotettavuuden, oikeellisuuden ja läpinäkyvyyden kannalta tämän tutkimuksen perusteella merkittäviä kontrolliparannuksia voidaan kehittää hyödyntämällä SOX-projekteissa käytettyjä ja hyväksyttyjä viitekehyksiä. Yksiselitteisesti ei voida määritellä tiettyjä kontrolleja, joiden avulla yritys voi kehittää talouden prosesseja, vaan kehitystyön perustuminen yleisesti hyväksyttyihin ja käytössä oleviin kontrolliviitekehyksiin tuottaa parhaan lopputuloksen. Kontrolliviitekehykset tarjoavat laajan ja kattavan kontrolliympäristön, joka perustuu SOX:n yhteydessä tarkoin määriteltyyn liiketoimintaympäristöön. Tutkimuksessa tulee ilmi myös se, että kontrollien kehittäminen on riippuvaista yritystä koskevista lainsäädännöistä ja määräyksistä. Tämän vuoksi nimenomaan oikeanlaisen kehityksen kannalta on oleellista tehdä yhteistyötä talouden ja IT:n eri funktioiden kesken. Ja, että SOX:n kaltaisen lain asettamien vaatimusten pohjalta määritellyt kontrollikäytännöt ovat yleisesti riittävän kattavia oikeellisuuden takaamiseksi.

Tämän tutkimuksen tulosten perusteella voidaan todeta, että tutkimus vastaa tutkimuskysymykseen selkeästi ja kattavasti esittämällä kontrolliviitekehyksiä kontrollien kehittämiseksi. Edelleen yleisimmin näiden kontrolliviitekehysten ja

SOX:n vaatimusten hyödyntäminen mahdollistavat kontrollien kehittämisen myös muissa yrityksissä riippumatta yritystä koskevasta lainsäädännöstä. Talouden prosessien kehittäminen viitekehysten perusteella antaa lisäksi mahdollisuuden asettaa yrityksen toiminnan kannalta keskeisimmät kontrollikäytännöt informaation laadun takaamiseksi. Lisäksi kontrollikäytännöt perustuvat tarkoin määriteltyyn lainsäädäntöön, mutta eivät ole lainsäädännöstä riippuvaisia.

Jatkotutkimus

Jatkossa olisi mielenkiintoista tutkia, millaisia kontrollitavoitteita ja – käytäntöjä suomalainen tai eurooppalainen yrityskulttuuri edellyttää vastaavanlaisen varmuuden takaamiseksi lain voimalla. Olisi myös mielenkiintoista tutkia, millainen vaikutus tällaisella lailla olisi suomalaisen yrityksen toimintaan ja aiheuttaisiko se liiketoiminnan kehittymistä, vai pystyttäisiinkö lain voimalla lisäämään yritysten taloudellista arvoa luottamuksen lisääntymisen myötä.

9 JOHTOPÄÄTÖKSET

Informaatiota käsittelevän teknologian hyödyntäminen yrityksissä on lisääntynyt eri liiketoiminnan funktioissa. Päätökset perustuvat yhä kasvavassa määrin tietojärjestelmien tuottamaan informaatioon ja tämän vuoksi tietojärjestelmien kriittinen ymmärtäminen on noussut keskeiseksi tekijäksi yrityksen toiminnoissa.

Oikea ja riittävä informaatio yrityksen toiminnassa on tärkeää yrityksen oman toiminnan lisäksi yrityksen eri sidosryhmille. Erityisesti kirjanpidon ja sitä tarkastelevan tilintarkastuksen mukaan informaation - ja sen tuottamiseksi syntyvien toimintojen - on tuotettava riittävää, luotettavaa ja oikeellista tietoa yrityksen taloudellisista toiminnoista.

Informaation vääristyminen tai tahallinen vääristäminen voi johtaa pahimmallaan maailmanluokan konkursseihin, kuten Yhdysvalloissa sattuneet suuren yritysskandaalit todistavat. Tämän vuoksi Yhdysvalloissa julkistettiin Sarbanes-Oxley laki, joka keskittää huomion yrityksen sisäiseen kontrolliin, sen valvontaan ja johdon vastuuseen sisäisen kontrollin asettamisesta.

Erityisesti Sarbanes-Oxley -lain pykälä 404 keskittyy sisäiseen kontrolliin. Pykälän tärkein tavoite on vaatia yrityksiä luomaan riittävä ja todennettavissa oleva sisäisen kontrollin järjestelmä talouden raportoinnin varmistamiseksi. Sisäisen kontrollin varmistamisesta on lain mukaan ensisijaisesti vastuussa yrityksen johto, joka toimillaan vastaa sisäisen kontrollin asettamisesta yrityksen toiminnoissa. Johdon tulee myös ulkoisen tarkastuksen lisänä varmentaa riittävin todistein sisäisen kontrollin olemassaolo.

Sarbanes-Oxley lain julkistamisesta on kulunut tämän tutkielman teon aikaan viisi vuotta. Tänä aikana lain vaatimuksia vasten on kehittynyt hyvin kapea erityisosaamisen haara. Erityisesti suurten tilintarkastusinstituutioiden toimet ovat luoneet käytäntöjä, joita sovelletaan hyvin yleisesti lain vaatimusten kohtaamiseksi. Tässä yhteydessä eri järjestöjen, kuten ISACA:n ja myöhemmin

ITGI:n kaltaisten organisaatioiden luomat viitekehykset ovat toimineet lain edellyttäminä standardoituina ohjeistuksina kehittää yrityksen taloushallintoa.

Tässä tutkielmassa hyödynnetään soveltuvin osin COBIT sekä COSO viitekehyksiä. COBIT on liiketoimintalähtöinen viitekehys, joka määrittelee informaatioteknologian hallinnoinnin kontrolliprosessien kautta. COSO puolestaan kuvaa ja määrittelee sisäisen kontrollin olemusta ja sisältöä. Viitekehyksiä käytetään limittäin tukemaan eri vaatimusten näkökulmia.

Tässä tutkielmassa tavoitteena oli määritellä SOX-projektien pohjalta syntyneiden käytäntöjen joukosta ne, joiden avulla voidaan kehittää suomalaisen yrityksen taloushallinnon toimintoja ja täten parantaa ja edelleen kehittää talouden prosesseja ja –raportointia. Tutkielman perusteella voidaankin todeta, että Sarbanes-Oxley lain pohjalta syntyneiden käytäntöjen avulla suomalaisessa yrityksessä voidaan kehittää taloushallintoa ja sen tuottamaa informaatioita luotettavammaksi, läpinäkyvämmäksi sekä oikeellisemmaksi.

Kohdeyrityksen nykytilaa kuvattiin kontrollitasoilla, jotka jaettiin kolmelle eri tasolle. Tasot käsittävät yrityksen ylimmän, strategisen tason, operatiivisen tason sekä edelleen kohdetason, joka oli tämän tutkielman yhteydessä prosessitaso. Teoriaosuudessa määriteltyjen vaiheiden pohjalta kohdeyrityksestä pystyttiin nostamaan esiin Sarbanes-Oxley lain vaatimusten nojalla lukuisia kehityskohteita. Niitä arvioitiin yhdessä talous- ja tietohallinnon kanssa sopivimpien, suomalaiseen yritysmaailmaan, sekä – kulttuuriin sopivien, käytäntöjen löytämiseksi.

Kehityskohteiksi kohdeyrityksessä määriteltiin kontrolliprosesseja ja –tavoitteita informaatioteknologian sekä edelleen prosessitason kehittämiseksi. Kehityskohteiksi määriteltyjä kontrollitavoitteita COBIT – viitekehyksen mukaan olivat mm. riskien hallinta yrityksen ylimmällä tasolla, järjestelmäturvallisuuden takaaminen, muutosten hallinta sekä operaatioiden

hallinta. Erityinen huomio kehityskohteiden määrittelyssä oli eri kontrollitoimintojen, prosessien kuvaamisen ja vastuiden vaillinaisuus. Kontrollitarpeet oli tunnistettu, mutta niiden kehittämiseksi ei oltu systemaattisesti määritelty konkreettisia toimenpiteitä. Tämä edelleen korostui sovellustasolla, jossa tehtyjen havaintojen perusteella oli perustavanlaatuisia puutteita, jotka pahimmillaan voivat vaarantaa yrityksen liiketoiminnan. Tässä yhteydessä kuitenkin korostuu suomalaisen ja yhdysvaltalaisen yrityskulttuurin merkitys. Suomalaisessa yritystoiminnassa lähtökohtaisesti oletetaan yksilöiden toimivan eettisten periaatteiden mukaan oikein ja siten luottamus suomalaiseen työntekijään on suuri. Vastoin kuin suomalaisessa yrityskulttuurissa, yhdysvaltalainen yrityskulttuuri ei luota yksilötason oikeellisuuteen ja tämän vuoksi myös Sarbanes-Oxley lain kaltainen pakote kehittää sisäistä tarkastusta ja kontrolleja voi olla liian byrokraattista suomalaisten yritysten toiminnan parantamiseksi.

LYHENTEET

Attest services	Lakisääteiset toiminnot yritystoiminnoissa
Best practises	Kokoelma parhaista käytännöistä
COBIT	The Control Objectives for Information and related Technology
Compliance	Lain noudattamista koskevien vaatimusten täyttyminen
Corporate Governance	Hyvä hallintotapa
COSO	Committee of the Sponsoring Organizations of the Treadway Comission
Financial accounting systems	Laskentatoimen muodostavat järjestelmät ja systeemit
Internal control over financial reporting	määritelmä sisäisen kontrollin prosessista taloudellisen informaation raportoinnissa
ISACA	Information Systems Audit and Control Association
IT	Informaatioteknologia
IT Governance	IT:n hyvä hallintotapa
Materiality	Taloudellisessa toiminnassa käytetty termi oleellisuudesta
PCAOB	Public company Acounting Oversight Board, yhdistys, joka valvoo julkisten yritysten tarkastajia

SEC	Securities and Exchange Comission, Yhdysvaltojen pörssin valvova elin
SOX	Sarbanes-Oxley laki
THEIIA	The Institute of Internal Auditors

LIITE 1. RISKITAULUKKO

Taulukko 8. IT:n aiheuttamia riskejä. Ramamoorti ym. 2004

IT:n ominaisuus	**Riski/kontrolli vaikutus**
Prosessoinnin lisääntynyt nopeus mahdollistaa yhä suurempien informaation määrien prosessoinnin	Virheet suurenevat ja niiden havaitseminen vaikeutuu
Transaktioiden oikea-aikaisuus eliminoi puskurin virheiden korjaamiseksi	Virheet vaikuttavat keskeneräisiin liiketoimintointo prosesseihin; järjestelmät eivät enää ole ihmisen kontrolloimia
Suhteellinen joustamattomuus suunnittelussa	Viivyksemätön toiminta virheen sattuessa vaikeutuu. Laadullisten prosessien kehittäminen tärkää
Tehokkaiden ja vaikutusvaltaisten työkalujen helppokäyttöisyys sekä laaja-alainen levinneisyys	Ihmiset ilman riittävää ymmärrystä pystyvät käyttämään tehokkaita työvälineitä. Tämä luo kontrollimahdollisuuksia, mutta myös riskejä
Laaja-alainen toiminnallisuuden sisällyttäminen pieniin sovelluksiin, kuten mobiiliratkaisut	Muutosten teon mahdollisuus merkittäviin prosesseihin ilman systemaattista kontrollointia järjestelmään pääsystä, tiedon tallennuksesta sekä tiedon prosessoinnin mahdollisuuksista
Muutos yrityskohtaisesti kehitetyistä järjestelmistä laaja-alaisiin toiminnanohjausjärjestelmiin (ERP) sekä vastaaviin	Riippuvuus ulkopuolisiin toimittajiin kehityksestä ja korjauksista lisääntyy.
Päätöksentekojärjestelmien kehityksen lisääntyminen	Lisääntynyt riski merkittävissä päätöksenteon prosesseissa.
Lisääntyneet mahdollisuudet käyttää järjestelmiä	Lisääntyneet yhdistymispisteet (access

paikasta ja ajasta riippumatta	points) lisäävät tarvetta sekä fyysisille, että loogisille kontrolleille
Tallennusmedian haavoittuvuus	Lisää ympäristö, että loogisten ja fyysisten kontrollien tarvetta
Informaation ja kommunikaation konvergenssi	Vaikuttaa siihen, miten ihmiset työskentelevät. Muuttaa tavanomaiset prosessit toimia ja kommunikoida.
Informaatioteknologisten komponenttien, kuten infrastruktuurin, ohjelmistojen, tiedon ja toimintojen keskittäminen	Vähentää kontrollipisteiden määrää, mutta lisää haavoittavuuden riskiä; luvaton käyttö ja tahattomat vahingot lisääntyvät
Järjestelmäkomponenttien jakelu ja tiedon levittämisen lisääntyneet mahdollisuudet	Luo epäyhtenevyyttä, version hallinta ongelmia, tiedon saannin kontrolloinnin vaikeutuminen, tiedon eheyden vaarantuminen.
Eri järjestelmien käytön yhdentyminen, järjestelmien käytettävyyden toisesta järjestelmästä mahdollistuminen	Lisääntynyt riski tunkeutua järjestelmään toisen järjestelmän kautta
Internetin lisääntynyt käyttö liiketoiminnassa organisaatioiden ja yksilöiden välillä	Lisääntynyt liiketoiminnallinen riski kontrollitoimintojen puutteellisuudesta ja toiminnan hallitsemattomuudesta johtuen
Lähdetiedon puutteellisuus tai puuttuminen	Heikentää tai poistaa kirjaus ketjun (audit trail), jonka tulee todentaa tapahtuma(t)
Kohdetiedon puuttellisuus tai puuttellinen kirjaus ketju	Lisääntynyt tarve erikoisosaamiselle tiedon oikeellisuuden todentamiseksi
Automatisoidut kirjaukset kirjanpidossa	Lisää riippuvuutta järjestelmistä, vähentää ihmislähtöistä kontrollia. Lisää tiedon kompleksisuutta ja hallittavuutta
Riippuvuus IT:stä kilpailuedun saavuttamisessa	Suurentaa seuraamuksia sekä tiedostomattomia IT-riippuvuudesta

	aiheutuvia riskejä
IT-strategian sekä liiketoimintastrategian eroavuudet	Lisää vaillinnaista päätöksentekoa liiketoiminnassa ja luo riskejä, mikäli IT:n toimintaa ei ymmärretä täysin
Ylemmän johdon vastuun puute tietojärjestelmäkontrolleista	Lisää tiedostamattomia liiketoiminnallisia riskejä
Uusien toimintojen kehittäminen vasten IT-toimintoja	Lisää tarvetta koulutukselle riskien tiedostamiseksi
Uudenlaiset liiketoiminnalliset käytännöt, jotka perustuvat liiketoiminannan ja IT:n tehokkaalle integraatiolle	Moniosaamisen tarve korostuu. Liiketoiminannan ja IT:n yhteistoiminnallisuuden ymmärtäminen yhä tärkeämpää

LIITE 2. YLEISET IT-KONTROLLIT

Taulukko 9. Kontrolliympäristön toiminnot. ISACA (2005a)

	Kontrolliympäristö	COBIT - viittaus
	IT strateginen suunnittelu	
1.	Onko johto laatinut strategisen suunnitelman, jolla varmistetaan IT:n tukeminen liiketoimintaa?	PO1.4
2.	Viestiikö IT:stä vastaava taho IT - suunnitelmista liiketoimintaprosessien omistajille ja muille keskeisille osa-puolille organisaatiossa?	PO1.2 PO6.5
3.	Pitääkö IT:stä vastaava taho yritysjohdon tietoisena meneillä olevista aktiviteeteistä, haasteista ja riskeistä? Jaetaanko tämä informaatio myös hallitukselle?	PO1.2 PO6.5
4.	Arvioiko IT:stä vastaava taho edistymistään vasten liiketoimintastrategiaa ja onko reagointi reaktiivista tavoitteiden saavuttamiseksi?	PO1.3 ME1.2
	IT prosessit, organisaatio ja yhteydet	
5.	Onko IT-vastaavilla riittävät tiedot ja taidot täyttää tehtävänsä?	PO7.2 PO7.4
6.	Onko relevantit järjestelmät ja niiden omistajat tunnistettu?	PO4.9
7.	Onko IT - organisaation roolit tunnistettu, kuvattu ja ymmärretty?	PO4.6
8.	Ymmärtääkö ja hyväksyykö IT - henkilöstä vastuunsa sisäisestä kontrollista?	PO4.6 PO6.1 ME2.2
9.	Onko tiedon yhteneväisyydestä vastaavien rooleista kommunikoitu vastaavien liiketoiminnan vastaavien kanssa, ja ovatko he hyväksyneet nämä vastuut?	PO4.9 PO6.5
10.	Onko IT - johto implementoinut roolit ja vastuut, jotta tehtävien eriyttäminen varmistaa, ettei	PO4.11

	yksilö voi vaarantaa kriittistä prosessia?	
	IT-henkilö resurssien johtaminen	
11.	Onko IT-organisaatio omaksunut yrityksen mallin humaaneista toiminnoista?	PO6.1 PO7.1
	Käyttäjien opastus ja koulutus	
12.	Mahdollistaako IT - organisaatio toistuvia koulutusmahdollisuuksia joissa käydään lävitse eettisiä toimintoja, järjestelmä turvallisuuskäytäntöjä sekä turvallisuusvastuita?	PO7.4 DS7.1
	Ohjelmistojen hankinta ja ylläpito	
13.	Onko organisaatiossa ohjelmistojen kehitysprosessi?	PO8.3 AI2.3 AI2.4
14.	Ohjelmistojen kehitysprosessissa määritellään uuden järjestelmän mahdollisten vaikutusten arviointi suhteessa olemassa oleviin järjestelmiin?	PO 6.4 AI2 AI6.2
15.	Ohjelmistojen kehitysprosessi on määritelty kontrollikäytännöt?	AI1 AI2.3
16.	Ohjelmistojen hankinta on linjassa yrityksen strategian kanssa	PO4.3 AI3.1
17.	Ohjelmistojen luottettavuudeen kehittämiseksi käyttäjät osallistuvat soveltuvin osin ohjelmisto-kehitykseen.	AI1 AI2.1 AI2.2 AI7.2
18.	Kontrollien tarkoituksenmukaisuuden takaamisesi suoritetaan jälkiarviointeja	AI7.12
19.	Ohjelmistoja ja järjestelmiä kehitetään ja hankitaan yleisen hankintastrategian mukaisesti	AI2
20.	On olemassa dokumentointi, että kehitetyt	AI3

	talouden sovellukset ovat tarkoituksenmukaisia	
	Operaatioden mahdollistaminen	
21.	Organisaatiolla on asetettu käytännöt ohjelmistojen kehitykseen, kontrollointiin, muutoksiin etc.	PO6.1 & 6.3 PO8.1 & 8.2 PO8.3 AI6.1 & DS13.1
22.	Yritys kehittää, ylläpitää ja operoi järjestelmiä yrityksen käytännön mukaisesti	PO6.1 & 6.3 PO8.1 & 8.2 PO8.3 AI6.1 & DS13.1
	Ratkaisujen ja muutosten asentaminen ja valtuuttaminen	
23.	Yrityksessä on asetettu testausstrategia	AI7.2 AI7.4 AI7.6 AI7.7
24.	Järjestelmien kuormitustestaus on suoritettu	AI7.2
25.	Eri järjestelmien rajapinnat on testattu	AI7.5
26.	Konversiot testataan alku- sekä kohdejärjestelmässä	AI7.5
	Muutosten hallinta	
27.	Ohjelmistomuutosten hallinta on standardoitua	AI6.1 & 6.2 AI 6.4 & 6.5 AI7.3 & 7.8 AI7.9 & AI7.10 AI7.11
28.	Pikamuutokset dokumentoidaan	AI6.3 AI7.10
29.	Kontrollien asettamisesta vastaa ainoastaan valtuutettu	AI.8
30.	IT johto varmistaa informaatio eheyden ja turvallisuuden järjestelmäimplementoinneissa	AI6.2 AI7.4

		AI7.9
	Palvelutasojen määritys ja hallinta	
31.	Talouden raportoinnin tueksi on määritelty palvelutasot	DS1.2 DS1.3 DS1.5 DS1.6
32.	Palveluiden arvioimiseksi on viitekehys	DS1.1 DS1.3
	Kolmannen osapuolen palveluiden hallinta	
33.	Palveluissa on määritelty vastaava henkilö	DS2.2
34.	Ulkoistettujen toimintojen arviointi ja valinta perustuu yrityksen käytäntöihin	PO1.4 PO6.3 DS2
35.	IT johto varmistaa ulkoistettujen palveluiden turvallisuuden ja kontrollien riittävyyden	DS2.3
36.	Kolmannen osapuolen sopimuksissa on huomioitu riskit ja kontrollit	DS2.3
37.	Kolmannen osapuolen palveluiden sopimuksia arvioidaan säännöllisesti	DS2.3
38.	Kolmannen osapuolen turvallisuutta arvioidaan säännöllisesti	ME2.6
39.	IT johto varmistaa ulkoistettujen palveluiden turvallisuuden ja kontrollien riittävyyden	DS2.3

	Järjestelmäturvallisuuden takaaminen	
40.	Informaationturvallisuus - käytännöt on asetettu	PO6.3 PO6.5 DS5.2
41.	Turvallisuuden arvioimiseksi on olemassa viitekehys	PO82. DS5.2
42.	IT-turvallisuussuunnitelma on yhtenevä yrityksen strategian kanssa.	DS5.2
43.	IT-turvallisuussuunnitelmaa pidetään yllä säännöllisesti muutosten tapahtuessa	DS5.2
44.	Järjestelmien käyttäjien autentikoimiseksi on olemassa proseduuri kaikissa tilanteissa	DS5.2 DS5.4
45.	Autentikoimisen tehokkuuden arvioimiseksi on olemassa proseduurit	DS5.3 DS5.4
46.	Käyttäjätilien sulkemiseksi ajallaan ja oikein on olemassa proseduuri	DS5.4
47.	IT johto on asettanut riittävät lokit järjestelmä-uhkien tunnistamiseksi	DS5.5
48.	Tehtävien eriyttämiseksi on olemassa proseduuri	DS5.3 DS5.4
49.	Eri fasiliteettien pääsynvalvonta on asetettu viitekehys	DS12.2 DS12.3

50.	IT-turvallisuussuunnitelma on yhtenevä yrityksen strategian kanssa.	DS5.2
	Konfiguraatioiden hallinta	
51.	Käyttäjät voivat käyttää ainoastaan määriteltyjä ohjelmistoja työasemilla	DS9.2
52.	Toiminnot koskien järjestelmien turvallisuutta on konfigiuroitu oikein	DS5.3 DS5.4 DS5.10
53.	Käytönhallinta koskien informaation käsittelyä on konfiguroitu oikein ja kattavasti	DS5.4
54.	IT johto on asettanut käytännöt organisaation järjestelmien turvallisuuden takaamiseksi	DS5.9
55.	Ohjelmistojen ja verkkojen hyväksymistestausta suoritetaan säännöllisesti	AI3.2 AI3.3
	Ongelmien ja tapausten hallinta	
56.	IT johto on asettanut käytännöt ongelmien ja tapausten hallintaan	DS8
57.	Ongelmien hallinta tuottaa selkeän audit trailin tapausten ja ongelmien selvittämiseksi	DS10.2
58.	Turvallisuustapahtumiin vastaaminen on nopeaa	DS5.6 DS8.3 DS10.1 DS10.3
59.	IT johto on asettanut käytännöt organisaation järjestelmien turvallisuuden takaamiseksi	DS5.9

	Tiedon hallinta	
60.	Tiedon hallintaan on asetettu yrityksen käytännöt	DS11.1 DS11.2 DS11.6
61.	Johto on asettanut käytännöt luottamuksellisen informaation suojaamiseksi	DS11.6
62.	Arkistointi on määritelty ja dokumentoitu	DS11.2
63.	Tiedon varmuuskopioimiseksi on asetettu johdon toimesta käytäntöjä	DS11.5
64.	Informaation palauttamista testataan säännöllisesti	DS11.5
65.	Tiedon rakenteen muutokset ovat hyväksyttyjä ja dokimentoituja	AI6
	Operaatioiden hallinta	
66.	IT-operaatioille on asetettu yrityksessä käytännöt johdon toimesta	DS13.1 DS13.2
67.	Järjestelmätapahtumista on olemassa riittävästi lokitietoa	DS13.3
68.	Informaation täydellisyyttä koskien on asetettu käytännöt järjestelmissä	DS11.1 DS11.3
69.	Tiedon varmuuskopioimiseksi on asetettu	DS11.5

	johdon toimesta käytäntöjä	
	Loppukäyttäjätoiminnot	
70.	Loppukäyttäjien toiminnoille on asetettu yrityksessä käytännöt	
71.	Loppukäyttäjätoiminnot, kuten esimerkiksi excelsheetit on dokumentoitu ja säännöllisesti arvioitu oikeellisuuden näkökulmasta	
72.	Loppukäyttäjätoiminnot varmistetaan säännöllisesti	
73.	Loppukäyttäjätoiminnot on suojattu	
74.	Loppukäyttäjätoimintojen input ja output informaatio varmennetaan säännöllisesti	

LIITE 3. KYSYMYSLOMAKKEET

Sovellustason kysymykset

Vastaaminen

Arvioi miten kysymyksessä esitetty osa-alue on tällä hetkellä yrityksessä.
Vastaa asteikolla 1-5.

1 - osa-aluetta ei ole tunnistettu yrityksessä tärkeäksi

2 - osa-alue on tunnistettu, mutta sitä ei pidetä tärkeänä

3 - osa.alue on tunnistettu, mutta toiminta on hajanaista ja rajoittuu yksittäisten ihmisten toimintoihin

4 - osa-alue on tunnistettu ja koetaan tärkeäksi. Toiminta on säännöllistä ja määriteltyä

5 - osa-alue on tunnistettu ja koetaan erittäin tärkeäksi. Toimintaa arvioidaan ja kehitetään jatkuvasti.

Kysymyksiä yhteensä 21 kappaletta

1. Ostotilaukset kohdistuvat ainoastaan hyväksytyille tilauksille

   Vastaus:

2. Ostotilaukset on syötetty oikein

   Vastaus:

3. Kaikki ostotilaukset syötetään ja prosessoidaan

   Vastaus:

4. Ostotileille (ostoreskontra) kirjatut summat esittävät ostettuja tuotteita ja palveluita

   Vastaus:

5. Ostotilien summat on laskettu ja kirjattu oikein

   Vastaus:

6. Kaikkien vastaanotettujen tuotteiden ja palveluiden määrät on syötetty ja prosessoitu

   Vastaus:

7. Kaikkien vastaanotettujen tuotteiden ja palveluiden summat on tallennettu oikealle ajanjaksolle

   Vastaus:

8. Ostoreskontran sisältöä on korjattu vain oikeasta ja perustellusta syystä
   Vastaus:

9. Hyvityslaskut ja muut muutokset on tarkasti kirjattu ja tallennettu

   Vastaus:

10. Kaikki hyvityslaskut ja muut muutokset syötetty ja prosessoitu

    Vastaus:

11. Kaikki hyvityslaskut ja muut muutokset on kirjattu oikealle ajanjaksolle

    Vastaus:

12. Maksusuoritukset tehdään vain vastaanotetuille tuotteille ja palveluille

Vastaus:

13. Maksut suoritetaan oikeille toimittajille

Vastaus:

14. Maksusuoritukset on laskettu ja kirjattu

Vastaus:

15. Kaikki maksusuoritukset tallentuvat

Vastaus:

16. Maksusuoritukset kirjataan oikealle ajanjaksolle

Vastaus:

17. Toimittajarekisteriin tehdään vain oikeat muutokset

Vastaus:

18. Kaikki toimittajarekisterin muutokset prosessoidaan ja tallennetaan

Vastaus:

19. Toimittajarekisterin muutokset ovat oikeellisia

Vastaus:

20. Toimittajarekisterin muutokset prosessoidaan ajallisesti oikein

Vastaus:

21. Toimittajarekisteri on ajan tasalla

Vastaus:

Aktiviteettitason kysymykset

Vastaaminen

Arvioi miten väittämässä esitetty osa-alue on tällä hetkellä yrityksessä.

Vastaa asteikolla 1-5.

1 - osa-aluetta ei ole tunnistettu yrityksessä tärkeäksi

2 - osa-alue on tunnistettu, mutta sitä ei pidetä tärkeänä

3 – osa-alue on tunnistettu, mutta toiminta on hajanaista ja rajoittuu yksittäisten ihmisten toimintoihin

4 - osa-alue on tunnistettu ja koetaan tärkeäksi. Toiminta on säännöllistä ja määriteltyä

5 - osa-alue on tunnistettu ja koetaan erittäin tärkeäksi. Toimintaa arvioidaan ja kehitetään jatkuvasti.

Kysymyksiä yhteensä 56 kappaletta

1. Organisaatiossa on järjestelmien kehitys – suunnitelma, joka kattaa mm. organisaation prosessoinnin oikeellisuus sekä luottamuksellisuus vaatimukset.

   Vastaus:

2. Organisaatiossa on olemassa kehityssuunnitelma / tietämys, jossa määritellään uusien järjestelmien hankkimisen tai olemassa olevien järjestelmien suurien muutosten kehitysperiaatteet.

   Vastaus:

3. Kehityssuunnitelmassa on kontrollivaatimukset, joita järjestelmäkehityksessä pitää noudattaa.

Vastaus:

4. Yrityksessä on olemassa järjestelmä hankinnassa prosessi, jossa uuden järjestelmän hankinnassa arvioidaan sen linjatumista yrityksen strategisten tavoitteiden kanssa.

   Vastaus:

5. Järjestelmien käyttäjät osallistuvat järjestelmäkehitykseen, jolla varmennetaan tarkoituksenmukaisten järjestelmien kehittäminen.

   Vastaus:

6. Käyttöönoton jälkeisiä arviointeja suoritetaan, joissa arvioidaan järjestelmäkontrollien riittävyyttä ja järjestelmän tarkoituksen mukaisuutta.

   Vastaus:

7. Yrityksessä on olemassa hankintaprosessi ohjelmistojen ja järjestelmien osalta.

   Vastaus:

8. Yrityksessä on olemassa dokumentaatio keskeisimmistä IT- prosesseista.
   Vastaus:

9. Organisaatiossa on olemassa menettelytapa ja ohjeistus ohjelmistokehitykseen, ohjelmisto muutoksiin, käyttöoikeuksien hallintaan ohjelmistoissa ja tietokannoissa, joita ylläpidetään säännöllisesti ja jotka johto hyväksyy.

   Vastaus:

10. Ohjelmistojen kehityksessä, ylläpidossa ja käytössä noudatetaan yrityksen yleistä ohjeistusta.

Vastaus:

11. Yrityksessä on olemassa testausstrategia ohjelmisto muutosten osalta, jolla varmennetaan muutosten tarkoituksenmukaisuus ja oikeellisuus.

    Vastaus:

12. Liitynnät eri osapuolien ja eri järjestelmien välillä varmennetaan säännöllisesti tiedon oikeellisuuden takaamiseksi.

    Vastaus:

13. Tietojen konvertointi varmennetaan alkuperäisen ja kohteen välillä säännöllisesti.

    Vastaus:

14. Ohjelmistojen sekä järjestelmien muutokset on standardoitu, hyväksytty ja dokumentoitu vasten yrityksen politiikkaa.

    Vastaus:

15. Välittömät ohjelmistomuutokset dokumentoidaan.

    Vastaus:

16. Käyttöoikeuksien osalta on olemassa riittävät kontrollit.

    Vastaus:

17. Ohjelmistoasennusten / järjestelmähankkeiden yhteydessä varmennetaan olemassa olevan informaation turvallisuus ja oikeellisuus.

    Vastaus:

18. Taloudellisen raportoinnin osalta on määritelty IT - palvelutasot, jotka tukevat taloudellisen raportoinnin osapuolten vaatimuksia.

Vastaus:

19. IT-palvelutasojen tarkoituksenmukaisuutta arvioidaan säännöllisesti.

Vastaus:

20. Kolmannen osapuolen palveluissa on määritelty henkilö, joka vastaa palvelun valvonnasta, ylläpidosta ja kehityksestä.

Vastaus:

21. Kolmannen osapuolen palveluiden osalta suoritetaan toimittaja-arviointia parhaan palvelun saamiseksi.

Vastaus:

22. Toimittajien arviointiin sisältyy taloudellinen arviointi ja luotettavuus.

Vastaus:

23. Kolmannen osapuolten palveluiden sopimuksissa on huomioitu riski- ja turvallisuuskontrollit liittyen yritysten tietojärjestelmiin ja tietoliikenteeseen.

Vastaus:

24. Kolmannen osapuolten palveluille on asetettu yrityksen yleiset tietojärjestelmävaatimukset.

Vastaus:

25. Toimintaa kolmannen osapuolen palveluiden osalta arvioidaan säännöllisesti.

Vastaus:

26. IT:n osalta on tehty säännöllisesti ylläpidetty turvallisuussuunnitelma.

    Vastaus:

27. IT - turvallisuus suunnitelmaa päivitetään säännöllisesti vastamaan muuttuneita olosuhteita.

    Vastaus:

28. Käyttöoikeuksien hallinnasta pidetään yllä dokumentaatioita.

    Vastaus:

29. Autentikoimisen kattavuuden takaamiseksi on olemassa proseduuri.

    Vastaus:

30. Käyttäjien hallinta on ajantasaista ja dokumentoitua kaikkien järjestelmien osalta.

    Vastaus:

31. Käyttöoikeuksien myöntämisen osalta on olemassa kontrolliprosessi

    Vastaus:

32. Käyttäjä on todennettavissa kiistattomasti kaikissa transaktioissa.

    Vastaus:

33. Tetoliikennekontrollit ovat kattavia ja riittäviä torjumaan ulkopuolisten pääsy yrityksen verkkoon.

    Vastaus:

34. Järjestelmäturvallisuuden osalta on riittävästi lokeja, joista transaktiot voidaan todentaa.

Vastaus:

35. Järjestelmien fyysinen turvallisuus on varmennettu ja määritelty.

Vastaus:

36. Henkilöstö käyttää ainoastaan hyväksyttyjä ohjelmistoja.

Vastaus:

37. Järjestelmäinfrastruktuuri sisältäen tietoliikenteen sekä muut yrityksen verkkoon sisältyvät laitteet on konfiguroitu estämään luvaton käyttö kaikilta osin.

Vastaus:

38. Tietovarastot ja tietokannat on suojattu luvattomalta käytöltä.

Vastaus:

39. Yrityksessä on organisaation laajuiset virusten ja haittaohjelmien torjunta proseduurit?.

Vastaus:

40. Yrityksessä järjestetään säännöllistä kontrollien testaamista konfiguraation osalta.

Vastaus:

41. IT – organisaation toimesta on määritelty toimintamalli ongelmien ja virheiden seuraamiseen.

Vastaus:

42. Järjestelmässä sattuneen kirjanpidollisen virheen osalta voidaan jäljentää audit trail tai vastaava tapahtumaketju.

Vastaus:

43. Virhetilanteisiin (esimerkiksi virheellisen raportin syntyminen) reagoidaan nopeasti ja selvitetään virheen lähde.

Vastaus:

44. Tiedon jakamiseen, säilyttämiseen sekä replikointiin on määritelty hallittu prosessi.

Vastaus:

45. Luottamuksellinen tieto on suojattu sekä fyysisesti, että loogisesti.

Vastaus:

46. Tedon säilyttämiseen ohjelmien, dokumenttien, raporttien sekä viestien osalta on määritelty aikajaksot ja tiedon arkistointi on ohjeistettu sekä varmennettu.

Vastaus:

47. Johto asettanut tiedon varmuuskopioinnille vaatimuksia.

Vastaus:

48. Tiedon palauttamista testataan säännöllisin aikavälein.

Vastaus:

49. Tietorakenteiden muutokset ovat hallittuja sekä dokumentoituja.

Vastaus:

50. IT - operaatioiden hallinnasta on olemassa dokumentoitu standardi.

Vastaus:

51. Kriittisten järjestelmien osalta muodestetaan riittävä loki.Esimerkiksi laskun maksatusohjelmasta.

    Vastaus:

52. Järjestelmätapahtumien lokista muodostetaan yhtenäinen, kronologinen tapahtumasarja transaktion toteamiseen syötteestä tulosteeseen.

    Vastaus:

53. Loppukäyttäjiä varten on määritelty konsernin laajuinen tietoturvallisuuspolitiikka.

    Vastaus:

54. Käyttäjäkohtaisten modifikaatioiden kuten esimerkiksi tulosteiden ja raporttien toiminnallisuus on dokumentoitu ja varmistettu.

    Vastaus:

55. Käyttäjäkohtaiset modifikaatiot varmennetaan säännöllisesti ja ne on suojattu luvattomalta käytöltä.

    Vastaus:

56. Käyttäjäkohtaisten modifikaatioiden tuottama informaatio on varmennettu ennen merkityksellistä käyttöä. (kuten esimerkiksi raportin tietojen oikeellisuuden varmennus)

    Vastaus:

Ylimmän tason kysymykset

Vastaaminen

Arvioi miten väittämässä esitetty osa-alue on tällä hetkellä yrityksessä. Vastaa asteikolla 1-5.

1 - osa-aluetta ei ole tunnistettu yrityksessä tärkeäksi

2 - osa-alue on tunnistettu, mutta sitä ei pidetä tärkeänä

3 - osa-alue on tunnistettu, mutta toiminta on hajanaista ja rajoittuu yksittäisten ihmisten toimintoihin

4 - osa-alue on tunnistettu ja koetaan tärkeäksi. Toiminta on säännöllistä ja määriteltyä

5 - osa-alue on tunnistettu ja koetaan erittäin tärkeäksi. Toimintaa arvioidaan ja kehitetään jatkuvasti.

Kysymyksiä yhteensä 23 kappaletta

1. IT:n osalta on luotu strateginen suunnitelma, jossa kuvataan mitä ja miten IT tukee / vaikuttaa yrityksen strategisiin tavoitteisiin, kustannuksiin ja riskeihin.

   Vastaus:

2. IT-organisaatio toimii yhteistyössä liiketoiminnan eri osa-alueiden (hankinta, myynti, tuotanto, etc.) päättäjien kanssa tavoitteenaan luoda ymmärrys IT:n synnyttämistä mahdollisuuksista ja riskeistä.

   Vastaus:

3. IT – organisaatio kommunikoi säännöllisesti aktiviteeteista, haasteista, mahdollisuuksista sekä riskeistä IT:ssä talousjohdon kanssa.

   Vastaus:

4. IT – organisaation toimintaa arvioidaan säännöllisesti vasten yrityksen strategisia tavoitteita.

   Vastaus:

5. IT – organisaatiossa on riittävä osaaminen ja tietämys täyttää IT:lle asetetut tavoitteet.

   Vastaus:

6. Keskeisimmät järjestelmät, informaatio sekä niiden omistajuus on määritelty (omistajuudella tarkoitetaan tässä yhteydessä kehitys- / järjestelmä vastuussa olevia henkilöitä)

   Vastaus:

7. IT organisaation roolit ja vastuut on määritelty, dokumentoitu ja päivitetty säännöllisesti.

   Vastaus:

8. IT – organisaation yksilöt ymmärtävät roolinsa ja vastuunsa sisäisestä kontrollista.

   Vastaus:

9. Informaation oikeellisuudesta ja omistajuudesata kommunikoidaan eri osa-alueiden päättäjien kesken säännöllisesti.

   Vastaus:

10. IT - organisaatio on määritellyt roolit ja vastuut (segregation of duties) kriittisten prosessien osalta ehkäisemään väärinkäytöksiä.

    Vastaus:

11. IT - organisaatio on omaksunut ja edistänyt yrityksen kulttuuria informaation luottamuksellisuuden ja oikeellisuuden hallinnassa.

    Vastaus:

12. IT - organisaatio vastaa siitä, että järjestelmien loppukäyttäjät ovat tietoisia järjestelmien oikeellisesta käytöstä sekä tietoturvallisista toimintatavoista.

    Vastaus:

13. IT – organisaatio arvioi säännöllisesti käytäntöjä sekä toimintamalleja vasten liiketoiminnan muutoksia.(esimerkiksi organisaation laajentuminen)

    Vastaus:

14. IT:n arvioimiseksi on olemassa määritelty viitekehys/prosessi, jonka avulla arvioidaan kontrollien kattavuutta ja toimintaa IT - prosesseissa.

    Vastaus:

15. Yrityksessä arvioidaan lakien ja säädösten vaikutusta IT – organisaatioon.

    Vastaus:

16. IT – organisaatiossa on määritelty prosessi / viitekehys, jota käytetään säännöllisesti arvioimaan riskejä, jotka vaarantavat taloudellisen raportoinnin?

    Vastaus:

17. IT – organisaatio määrittelee säännöllisen riskiarvioinnin perusteella riskien liiketoiminnallista vaikutusta.

    Vastaus:

18. IT:n aiheuttamille riskeille on olemassa varautumis- sekä palautumissuunnitelma.

    Vastaus:

19. Keskeisimmät IT – prosessit on määritelty ja kuvattu.

    Vastaus:

20. IT-toiminnoille ja -prosesseille on olemassa laadun varmistussuunnitelma (IT:n tuki liiketoiminnalle).

    Vastaus:

21. IT – organisaatio on määritellyt mittariston päivittäisen toiminnan arvioimiseksi.

    Vastaus:

22. IT – organisaatio arvioi säännöllisesti palveluidensa tuottamista ja saatavuutta.

    Vastaus:

23. IT –organisaatiossa on yleisten ja sovelluskontrollien osalta järjestetty säännöllinen auditointi.

    Vastaus:

LIITE 4. COBIT:N KONTROLLITAVOITTEET

COBIT:n kontrollitavoitteet ITGI (2006d) mukaan:

Entiteettitaso

Riskienhallinnan prosessi PO9

1. Liiketoimintariskianalyysi
    a. johdon tulee asettaa viitekehys riskien tunnistamiselle
    b. viitekehyksessä tulee luoda perusta, kuinka merkittävimmät riskit johdetaan hyväksyttävälle tasolle
    c. Johdon tulee huolehtia, että viitekehystä pidetään yllä säännöllisesti
2. Riskianalyysin periaatteet
    a. riskien merkittävyyden arvioinnin perusteet
    b. vastuiden määrittely
    c. riskianalyysin laadunhallinta
3. Riskien tunnistaminen
    a. riskianalyysin tulee keskittyä riskin syy/seuraus – suhteeseen
    b. riskien tunnistamisprosessin tulee sisältää sekä kvantitatiivista, että sopivissa määrin kvalitatiivista riskiarviointia
    c. riskien tunnistamisen tulee kattaa liiketoimintaympäristön, lain ja säädökset, teknologian, kolmannen osapuolen palvelut sekä yrityksen henkilöstön
4. Riskien mittaaminen

   a. riskien mittaaminen tulee perustua luotettavaan kvantitatiiviseen sekä kvalitatiiviseen informaatioon

   b. yrityksen riskinsietokyky tulee arvioida

5. Riskisuunnitelma

   a. Riskianalyysin tulee tuottaa varautumissuunnitelma löydetyille riskeille, jossa huomioidaan liiketoiminnallinen merkittävyys ja täten tuotetaan kustannustehokkaita kontrollitoimenpiteitä

6. Riskien siedettävyys

   a. Riskien hyväksymisen osalta tulee määritellä keskeisimmät keinot, esimerkiksi vakuutukset, riskien siedettävyystason asettamiseksi

Aktiviteettitaso

Toimintojen hallinnan prosessi DS13

1. Käytännöt ja ohjeistukset operaatioista

   a. IT – operaatioiden käytäntöjen määrittely ja ylläpito ja varmistaminen, että IT-organisaation kaikki henkilöt ovat niistä tietoisia.

2. Töiden aikataulutus

   a. Töiden organisointi ja priorisointi liiketoiminnan vaatimusten mukaisesti.

3. IT infrastruktuurin valvonta

   a. Käytäntöjen määrittäminen koskien IT infrastruktuurin valvontaa ja riittävän jäljitystiedon tallentaminen.

4. Luottamukselliset tulosteet ja laitteet

    a. Riittävien suojauksien varmistaminen luottamuksellisten tulosteiden ja laitteiden osalta.

5. Laitteiston ennakoiva ylläpito

    a. Käytännöistä sopiminen, että laitteistoa ylläpidetään oikea-aikaisesti eikä reaktiivisesti.

6. Liiketoiminnan vaatimukset tiedonhallinnalle

    a. Raporttien tarkoituksenmukaisuuden varmistaminen liiketoiminnan vaatimusten mukaisesti.

Muutosten hallinnan prosessi AI6 ja muutosten asentamisen prosessi AI7

1. Standardit ja proseduurit muutoksissa

    a. Muutospyyntöjen standardoitu käsittely.

2. Arviointiin, priorisointiin ja valtuuttamiseen vaikuttaminen

    a. Kaikkiin muutospyyntöihin vastaaminen, niiden priorisoinnin ja luokittelun käytännöt.

3. Seurannan ja raportoinnin muutostaso

    a. Järjestelmien ja prosessien muutosten järjestelmällinen seuraaminen.

4. Muutospäätökset ja dokumentointi

    a. Järjestelmämuutosten osalta muutoksen dokumentointi sekä järjestelmän käyttäjäohjeiden ylläpito.

5. Implementointisuunnitelma

a. Muutoksen tekemisen hyväksyntä /informointi muutoksen kohteena olevilta tasoilta.

6. Tuotantoon nostaminen

a. Muutoksen hyväksyminen tarkoituksenmukaiseksi ennen käyttöönottoa.

7. Ohjelmistojulkaisut

a. Ohjelmistojulkaisun vaatimien toimintojen läpikäynti.

8. Järjestelmäjakelu

a. Järjestelmäpäivitysten kontrollointi.

9. Muutosten tallennus ja jäljitys

a. Järjestelmämuutosten seurantainformaation muodostaminen.

Palvelutasojen määrityksen ja hallinnan prosessi DS1

1. Palveluiden määritys

a. Liiketoiminnallisia vaatimuksia vastaavien palveluiden määrittäminen.

2. Palvelutason sopimukset

a. Määrittely ja hyväksyntä IT palvelun palvelusopimuksesta, joka pohjautuu käyttäjän tarpeisiin ja IT:n mahdollisuuksiin.

3. Palvelutason seuranta ja raportointi

a. Säännöllinen palvelutason tarkoituksenmukaisuuden arviointi.

4. Palvelutason sopimusten tarkastelu

a. Sopimuksen toteutumisen seuranta sisäisesti ja ulkoisesti.

Loppukäyttäjät – prosessi AI7

1. Koulutustarpeen tunnistaminen
    a. Kehitystarpeiden mukaisen koulutuksen ja opastuksen määrittely.
2. Opastuksen ja koulutuksen järjestäminen
    a. Riittävän ja kattavan koulutuksen järjestäminen.
3. Annetun koulutuksen arviointi
    a. Koulutuksen ja opastuksen riittävyyden arviointi.

Järjestelmäturvallisuuden takaamisen prosessi DS5

1. IT – käytäntöjen johtaminen
    a. IT – turvallisuuden johtaminen yrityksen ylimmällä tasolla, jotta turvallisuustoimet ovat liiketoiminnan vaatimusten edellyttämällä tasolla.
2. Tavoitteiden ja suunnan viestiminen IT:ssä
    a. IT:n tavoitteiden viestintä organisaation kaikilla tasoilla.
3. IT – turvallisuussuunnitelma
    a. Sisältää liiketoiminnan vaatimukset, IT konfiguraation määritelmän, informaation vaarantavien riskien määritelmät sekä IT riskikulttuurin määritelmän yrityksessä.
4. IT – standardit ja laatukäytännöt
    a. IT – toimintojen laadun määrittely.

5. Identiteetin hallinta
    a. Käyttäjien yhdistäminen järjestelmässä tapahtuneisiin toimintoihin tulee olla aukoton.
6. Käyttäjätilien hallinta
    a. Reaaliaikainen käyttöoikeuksien hallinta.
7. Tiedon hallinnan turvallisuusvaatimukset
    a. Tiedon turvallisuustasojen kuvaaminen ja kontrollointi.
8. Verkkoturvallisuus
    a. Turvallisuutta parantavien tekniikoiden järjestelmällinen hallinta.
9. Turvallisuustestaukset ja valvonta
    a. IT turvallisuuden säännöllinen testaaminen ja valvonta.
10. Fyysisen turvallisuuden arvioiminen
    a. Riittävien fyysisten kontrollien valvonta.
11. Kulunvalvonta osana fyysistä turvaamista
    a. Laitteiston, kuten esimerkiksi palvelinten, ympäristön kontrollointi.

Ongelmien hallinnan prosessi DS10

1. Palvelukeskus
    a. Käyttäjäpyyntöjen hallinnan keskittäminen.
2. Käyttäjäpyyntöjen rekisteröinti
    a. Käyttäjäpyyntöjen dokumentoinnin järjestäminen.

3. Tapahtumien laajentaminen

    a. Ongelmien, joita ei voida välittömästi selvittää, jatkoselvityksen käytännöt.

4. Selvityspyyntöjen päättäminen

    a. Kattava käyttäjäpyyntöjen käsittely ja käsittelyn päättämisen käytönnöt.

5. Suunnan analysointi

    a. Käyttäjäpyyntöjen ryhmittely ja valvonta. Edesauttaa johtoa määrittelemään käyttäjätuen tarvetta.

6. Ongelman jäljitys ja laajuus

    a. Ongelmien jäljitettävyysinformaation varmistaminen sekä ongelman kattavuuden selvittäminen.

7. Turvallisuustapahtumien määritys

    a. Riittävien lokitietojen tallentaminen.

8. Ongelmien tunnistaminen ja luokittelu

    a. Ongelmien luokittelu ja kriittisten ongelmien tunnistaminen ja käsittelyn tehostaminen.

9. Ongelmien päättäminen

    a. Määrittely onko ongelman aiheuttaja saatu selvitettyä ja korjattua.

LÄHDELUETTELO

Agrawal, R. & Johnson, C. & Kiernan, J. & Leymann, F. 2006. Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology. Teoksessa Data Engineering, 2006. ICDE '06. Proceedings of the 22nd International Conference on. April 3-7.

Altman, W. 2005. What's going on? [US Sarbanes-Oxley Act - company financial legislation]. Engineering Management Journal, Volume 6, 42-43.

Baumgartner, G. D, Hamilton, A. 2004. Healthcare Financial Management, Vol. 58 Issue 6, 34-36. Saataville www-osoitteessa: <http://search.epnet.com/login.aspx?direct=true&db=bsh&an=13308804 &loginpage=Login.asp >.

Blumme, N., Karhu, P., Kontula, L., Laitakari, J., Linna, M., Nordin, J., Sovasto, J., Tarvainen, J., Tikkanen, R., Turakainen, O., Urrila, A. & Vesa, J. 2005. Corporate Governance sisäisen valvonnan ja riskienhallinan näkökulmasta . Helsinki Edita Publishing Oy.

Changchit, C. & Holsapple C. W. & Madden D. L. 1999. Positive impacts of an intelligent system on internal control problem recognition. System Sciences, 1999. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on Volume Track6, 5-8 Jan. 1999.

Changchit, C. & Holsapple C.W. & Viator R. E. 2001. Transferring auditors' internal control evaluation knowledge to management, Volume 20, Issue 3, [online]. Viitattu 23.10.2006. Saaatavilla www-muodossa: <http://www.sciencedirect.com/science/journal/09574174>.

Damianides, M. 2005. Sarbanes-Oxley an IT governance: New guidance on IT control and compliance. Julkaisussa Information Systems Management

[online], [viitattu 3.5.2007]. Saatavilla www-muodossa <http://www.infosectoday.com/SOX/Damianides.pdf>

Daniel H. L. 2005. Contextual IT Business Value and Barriers: An E-Government and E-Business Perspective[online], [viitattu 3.5.2007]. Teoksessa System Sciences, 2005. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference on. Hawaii, 03-06 Jan. 2005. Saatavilla www-osoitteessa: <http://ieeexplore.ieee.org/iel5/9518/30166/01385497.pdf?tp=&arnumber=1385497&isnumber=30166>.

De Haes, S. & Van Grembergen, W. 2005. IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group. System Sciences, 2005. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference on. January 3-6.

Debreceny, R.S. 2006. Re-Engineering IT Internal Controls: Applying Capability Maturity Models to the Evaluation of IT Controls. System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on. January 4-7.

Ernst & Young. 2004. Emerging trends in Internal Control.

Financial Executives Research Foundation (FERF). 2003. What is COSO? Defining the Alliance That Defined Internal Control [viitattu 3.1.2007]. Saatavilla www-osoitteessa< http://www.coso.org/articles.htm>

Ginzberg, M. J. & Moulton, R. T. 1990. Information technology risk management. Information Technology, 1990. 'Next Decade in Information Technology', Proceedings of the 5th Jerusalem Conference on. October 22-25.

Gottschalk P. 2000. Strategic Management of IS/IT Functions: The Role of the CIO [online]. Teoksessa Proceedings of the 33rd Hawaii International

Conference on System Sciences - 2000.[online], [viitattu 3.2.2007]. Saatavilla www-osoitteessa: <http://ieeexplore.ieee.org/iel5/6709/20043/00926956.pdf?tp=&arnumber=926956&isnumber=20043>.

Hirsijärvi, S. & Remes, P. & Sajavaara, P. 2001. Tutki ja kirjoita. 6-7 painos. Helsinki: Tammi.

Hinz, D. J. & Malinowski J. 2006. Assessing the Risks of IT Infrastructure — A Personal Network Perspective. System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on Volume 8, 04-07 Jan. 2006 Page(s):172a - 172a.

Hussain, S.J. & Siddiqui, M.S. 2005. Quantified Model of COBIT for Corporate IT Governance. Information and Communication Technologies, 2005. ICICT 2005. First International Conference on. August 27-28.

ISACA. 2005a. IT Control Objectives for Sarbanes-Oxley [online]. Information Systems Audit and Control Association [viitattu 28.10.2006]. Saatavilla www-osoitteessa< http://www.isaca.org >.

ISACA. 2005b. Implementation tool set [online]. Information Systems Audit and Control Association [viitattu 26.10.2006]. Saatavilla www-osoitteessa< http://www.isaca.org >.

ITGI. 2006a. IT control objectives for Sarbanes-Oxley – Design and implementation of internal control over financial reporting – 2nd edition [online]. IT governance institute (ITGI) [viitattu 05.01.2007]. Saatavilla www-osoitteessa< http://www.itgi.org >.

ITGI. 2006b. Cobit mapping – Overview of international IT guidance, 2nd edition [online]. [viitattu 05.01.2007]. Saatavilla www-osoitteessa< http://www.itgi.org >.

ITGI. 2006c. Guidance for Boards of Directions and Executive Management [online]. [viitattu 05.01.2007]. Saatavilla www-osoitteessa< http://www.itgi.org >.

ITGI. 2006d. COBIT 4.0[online]. [viitattu 05.01.2007]. Saatavilla www-osoitteessa< http://www.isaca.org >.

Järvinen, P. & Järvinen, A. 2004. Tutkimustyön metodeista. Tampere: Opinpaja

Kaarst-Brown, M. L. & Kelly, S. 2005. IT Governance and Sarbanes-Oxley: The Latest Sales Pitch or Real Challenges for the IT Function? System Sciences, 2005. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference on. January 3-6.

Kan, A. R. 2003. Managing a multi-billion dollar IT budget. Software Maintenance, 2003. ICSM 2003. Proceedings. International Conference on. September 22-26.

Kauppa- ja teollisuusministeriö (KTM). 1997. Kirjanpitolaki. [viittattu 9.11.2006]. Saatavilla www-osoitteessa < http://www.finlex.fi/fi/laki/ajantasa/1997/19971336>.

KHT-yhdistys. 2003. Tilintarkastuskertomukset ja tilintarkastajan lausunnot. Jyväskylä: Gummerrus Kirjapaino Oy.

KHT-yhdistys. 2004. Tilintarkastusalan suositukset 2004. Jyväskylä: Gummerrus Kirjapaino Oy.

KPMG. 2001. Managing business continuity. [viitattu 2.12.2006]. Saatavilla www-osoitteessa <http://www.kpmg.com.au/aci/docs/bus-continuity.pdf>.

KPMG. 2004a. Sarbanes-Oxley 404 - An Overview of the PCAOB's Requirements (Canadian Edition). [viitattu 4.12.2006]. Saatavilla www-osoitteessa < http://www.kpmg.ca/en/services/audit/sarbanes.html>.

KPMG. 2004b. Sarbanes-Oxley Section 404: Management Assessment of Internal Control and the Proposed Auditing Standards. [viitattu 4.12.2006]. Saatavilla www-osoitteessa <http://www.kpmg.ca/en/services/audit/sarbanes.html>.

KPMG. 2004c. Sarbanes-Oxley: a Closer Look. [viitattu 4.12.2006]. Saatavilla www-soitteessa <http://www.kpmg.ca/en/services/audit/sarbanes.html>.

KPMG. 2005. Corporate Governance sisäisen valvonnan ja riskienhallinnan näkökulmasta. Helsinki: Edita Puböishing Oy.

KPMG. 2005b. The compliance journey. [viitattu 2.12.2006]. Saatavilla www-osoitteessa <http://www.kpmg.com.au/aci/docs/compliance-journey200502.pdf>.

Kyrölä, T. 2001. Esimies ja tietoriskien hallinta. Juva: WS Bookwell Oy.

Laamanen, K. 2002. Johda liiketoimintaa prosessien verkkona – ideasta käytäntöön. Helsinki: Suomen laatukeskus Oy.

Larsen, M.H. & Pedersen, M.K. & Viborg Andersen, K. 2006. IT Governance: Reviewing 17 IT Governance Tools and Analysing the Case of Novozymes A/S. System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on. January 4-7.

Laudon, K.C. & Laudon J.P. 2000. Management information systems (kuudes painos). Upper Saddle River, New Jersey: Prentice-Hall, Inc.

Leppiniemi, J. 2000. Hyvä kirjanpitotapa. Porvoo: WSOY – Kirjanpainoyksikkö.

Leppiniemi, J. 1999. Tilinpäätös- ja verosuunnittelu. Porvoo: WSOY – Kirjanpainoyksikkö.

Lo, E.C. & Marchand, M. 2004. Security audit: a case study [information systems]. Electrical and Computer Engineering, Canadian Conference on Volume 1, 2-5 May 2004 Sivut:193 - 196 Vol.1

Mahnic, V. & Klepec, B. & Zabkar, N. 2001. IS audit checklist for router management performed by third-party. EUROCON'2001, Trends in Communications, International Conference on. 4-7 July 2001.

McGinnis, S.K. & Pumphrey, L. & Trimmer, K. & Wiggins, C. 2004. Sustaining and extending organization strategy via information technology governance. System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on. January 5-8.

McNurlin B.C. & Sprague, jr. R.H. 2002. Information Systems Management In Practice (Fifth edition). New Jersey: Pearson Education, Inc.

Miettinen, J. E. 1999. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari Oyj.

Norman, M. 2006. Sarbanes-Oxley section 404: A guide for management by internal controls practioners. [viitattu 4.12.2006]. Saatavilla www-osoitteessa < http://www.theiia.org/download.cfm?file=31866>

Nuuttila, E. 1997. Tietojärjestelmien tarkastuksen ja riskienhallinnan käsikirja. Jyväskylä: Gummerrus Kirjapaino Oy.

O'Donnell, Joseph B. & Rechtman, Yigal. 2005. Navigating the Standards for Information Technology Controls. CPA Journal; Jul2005, Vol. 75 Issue 7, sivut 64-69.

Opuscapita. 2007. Opuscapita Journal. [online]. [Viitattu 20.4.2007]. Saatavilla osoitteesta www.opuscapita.com

PriceWaterhouseCoopers (PWC). 2004. Sarbanes-Oxley Act: Section 404 Practical guidance for Management. [viitattu 4.12.2006]. Saatavilla osoitteessa < http://www.pwc.com/images/gx/eng/fs/1004soa.pdf>

Public Company Accounting Oversight Board (PCAOB). 2004. Auditing standard No. 2 – An audit of internal control over financial reporting performed in conjunction with an audit of financial statements. [viitattu 12.2.2007]. Saatavilla www-osoitteessa <http://www.pcaobus.org/Standards/Standards_and_Related_Rules/Auditing_Standard_No.2.aspx>

Ramamoorti, S & Weidenmier, M. L. 2004. The pervasive impact of information technolgy in internal auditing [online]. [viitattu 4.12.2006]. Saatavilla www-osoitteesta <http://www.theiia.org>

Ridley, G. & Young, J. & Carroll, P. 2004. COBIT and its utilization: a framework from the literature. System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on. January 5-8.

Riistama, V. 1999. Tilintarkastuksen teoria ja käytäntö (toinen painos). Porvoo: WSOY.

Rittenberg, L. E. & Miller, P. K. 2005. Sarbanes-Oxley section 404 work: Looking at the benefits[online]. [viitattu 5.1.2007]. Saatavilla osoitteesta < http://www.theiia.org>

Securities and exchange comission (SEC). 2006. Concept release concerning management's reports on internal control over financial reporting; proposed rule[viitattu 3.1.2007]. Saatavilla www-osoitteessa< http://www.sec.gov/rules/concept/2006/34-54122fr.pdf>

Sisäiset tarkastajat r.y. 1988. Suositukset sisäiselle tarkastukselle. Helsinki: Kirjapaino R. Lunkka

Spears, J.L & Cole, R.J. 2006. A Preliminary Investigation of the Impact of the Sarbanes-Oxley Act on Information Security. Teoksessa System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on. January 4-7.

Syrjälä, L. & Ahonen, S. & Syrjäläinen, E. & Saari, S. 1994. Laadullisen tutkimuksen työtapoja. Rauma: Kirjapaino West Point Oy

The Institute of internal Auditors (THEIIA). 2005. Sarbanes-Oxley section 404: A guide for management by internal controls practioners [viitattu 3.1.2007]. Saatavilla www-osoitteessa< http://www.theiia.org/download.cfm?file=31866.>

Vahtera, P. (1991) Automatisoitu kirjanpito, Gummerus Kirjanpaino Oy, Jyväskylä.

Volonino, L. & Kermis, G. F. & Gesner, G. H. 2004. Sarbanes-Oxley links IT corporate compliance. Proceedings of the Tenth American Conference on Information systems, New York, August 2004.

Yamamoto, R. & Yamamoto, K. & Ohashi K. & Inomata, J. 2006. Development of a business process modeling methodology and a tool for sharing business processes. Teoksessa Software Engineering Conference, 2005. APSEC '05. 12th Asia-Pacific 15-17 Dec 2005.

Yin, R. 2002. Case study research: design and methods – 3rd edition. California: Sage publications, Inc.