TURUN YLIOPISTO
Kauppakorkeakoulu

Digitalisaation vaikutus väärinkäytösriskeihin ja sisäiseen valvontaan

Laskentatoimen ja rahoituksen
pro gradu -tutkielma

Laatija:
Teemu Muurinen

Ohjaajat:
Prof. Kari Lukka
KTM Erkki Lassila

23.1.2022
Turku

Pro gradu -tutkielma

Oppiaine: Laskentatoimi ja rahoitus
Tekijä: Teemu Muurinen
Otsikko: Digitalisaation vaikutus väärinkäytöksiin ja sisäiseen valvontaan
Ohjaajat: Prof. Kari Lukka, KTM Erkki Lassila
Sivumäärä: 90 sivua
Päivämäärä: 23.1.2022

Tämä tutkielma tarkastelee digitalisaation vaikutusta yrityksen sisäiseen valvontaan ja väärinkäytöksiin. Väärinkäytöksillä tarkoitetaan tekoa, jolla tavoitellaan itselle tai muille epärehellistä etua. Väärinkäytöksessä käytetään yleensä apuna vilppiä, petosta tai huijausta. Sisäisellä valvonnalla organisaatiot pyrkivät muun muassa estämään ja havaitsemaan väärinkäytöksiä. Sen tavoitteena on varmistaa yrityksen omien sääntöjen ja strategian sekä organisaatiota koskevien lakien ja säännösten noudattaminen. Sisäisestä valvonnasta vastaa organisaation ylin johto, ja valvonnan tulee kattaa koko organisaatio

Digitalisaatio on tuonut kauaskantoisia muutoksia yrityksen toimintaan ja markkinoihin. Järjestelmien ja prosessien ollessa yhä vahvemmin riippuvaisia digitalisaatiosta on yritysten huomioitava muutosten tuomat uudet riskit. Digitalisaatio on tuonut sekä liiketoimintaan että valvontaan liittyviä hyötyjä, mutta se aiheuttaa samalla myös uudenlaisia riskejä, joihin yritysten on valmistauduttava.

Tutkielma on toteutettu tapaustutkimuksena, jossa kohdeyrityksenä on Suomessa toimiva tilitoimisto. Empiirinen aineisto kerättiin haastattelemalla neljää yrityksen työntekijää yhteensä seitsemän kertaa. Lisäksi tutkielmassa käytettiin muuta yrityksen sisäistä materiaalia, kuten koulutuksia ja ohjeita. Empiirinen osuus keskittyy tarkastelemaan tilitoimiston ja asiakasyrityksen välistä palvelusuhdetta. Näissä suhteissa väärinkäytökset ovat molemmille osapuolille kriittinen riski, jota valvonnan avulla pyritään minimoimaan. Siten on tärkeää tarkastella digitalisaation tarjoamia apuvälineitä sisäisen valvonnan tueksi, mutta myös sen tuomia uudenlaisia väärinkäytöksiin liittyviä riskejä. Tutkimuksen kohdeyritys on panostanut vahvasti sähköisten taloushallintopalveluiden tarjoamiseen. Yrityksellä on käytössään monia eri taloushallinnon järjestelmiä, joiden kautta se tarjoaa palveluita asiakkailleen.

Tutkimuksen empiirisen osan perusteella väärinkäytösten peruslogiikassa ei näytä tapahtuneen suuria muutoksia digitalisaation myötä. Väärinkäyttäjillä on kuitenkin käytössään yhä kehittyneempiä digitaalisia työkaluja. Siten digitalisoituminen pakottaa etenkin sähköisiin järjestelmiin vahvasti nojaavia organisaatioita tarkastelemaan toimintojaan kokonaisvaltaisesti, sillä digitaalisissa prosesseissa ja järjestelmissä saattaa piillä heikkouksia, joita väärinkäyttäjät pyrkivät hyväksikäyttämään. Esimerkiksi tiettyyn järjestelmään liittyvät riskit koskevat myös muita kyseiseen järjestelmään linkittyviä järjestelmiä ja prosesseja. Organisaatioiden tulee varautua näihin riskeihin sekä ennaltaehkäisevästi että luomalla toimintasuunnitelmat riskien realisoitumisen varalle. Valvonnan näkökulmasta on tärkeää kartoittaa jatkuvasti prosesseihin liittyviä riskejä ja päivittää tarvittaessa riskien valvontatoimenpiteitä. Tutkielman empirian mukaan kohdeyrityksessä on hyvät valmiudet ja potentiaali hyödyntää digitalisaatiota valvonnassa. Myös digitalisaation riskejä on tunnistettu hyvin, mutta valvontaa tukeville automaatiotyökaluille koettiin olevan tarvetta. Lisäksi yrityksessä nähtiin tarve parantaa tietoturvaan liittyvää koulutusta ja kulttuuria.

Avainsanat: sisäinen valvonta, väärinkäytökset, digitalisaatio

SISÄLLYSLUETTELO

KUVIOLUETTELO

TAULUKKOLUETTELO

1 Johdanto

1.1 Johdatus aiheeseen

Väärinkäytökset ovat olennainen riski mitä tahansa yritystoimintaa harjoitettaessa, ja ilmi tullessaan suuret tapaukset nousevat nopeasti otsikoihin sekä Suomessa että maailmalla. Viime aikoina palstatilaa ovat saaneet esimerkiksi Nordean ja Danske Bankin tapaukset (ks. MTV 11.9.2020; MTV 17.11.2020; Yle 19.9.2018). Kaksi Nordean työntekijää tuomittiin petoksesta, jossa asiakkaiden tileille murtauduttiin pankin omien järjestelmien avulla. Erään asiakkaan tililtä miehet onnistuivat viemään lähes 700 000 euroa, ja syyttäjän mukaan tekijät olivat aikeissa murtautua useiden muidenkin asiakkaiden tileille. Danske Bank sen sijaan joutui otsikoihin, kun paljastui, että vuosina 2007–2015 pankin Viron-yksikön kautta oli kierrätetty miljardeja euroja rahanpesutarkoituksessa. Danske Bank totesi omassa selvityksessään epäonnistuneensa epäilyttävien rahavirtojen alkuperän selvittämisessä sekä rahanpesun estämisessä. Pankin oman selvityksen mukaan valvontajärjestelmän pettäminen johtui useasta syystä, muun muassa johdon reagoimattomuudesta ja Viron-yksikössä käytössä olleista erilaisista IT-järjestelmistä.

Näiden esimerkkien tarkoituksena on havainnollistaa toimivan valvontajärjestelmän sekä epäkohtiin reagoimisen tärkeyttä. Lisäksi Nordean tapaus havainnollistaa petoksissa usein ilmeneviä piirteitä: pääsy yrityksen tietojärjestelmiin, useamman henkilön yhteistyö ja tietotaitoa vaativa turvamekanismien kiertäminen. Valvonnan pettäminen sekä siitä aiheutuvat väärinkäytökset ovat yritykselle strategisia riskejä, jotka realisoituessaan voivat johtaa oikeudellisiin seurauksiin ja saattavat pahimmassa tapauksessa uhata sen koko liiketoimintaa. Suorien vaikutusten lisäksi väärinkäytökset vaikuttavat yleiseen työilmapiiriin, organisaation brändiin sekä liikesuhteisiin (PwC 2018). Väärinkäytökset ovat kansainvälinen ongelma, sillä tapauksia selvitettäessä ulkomailta tulevien varojen alkuperää on usein vaikea, ellei miltei mahdotonta saada selville. Esimerkiksi Danske Bankin tapauksessa haasteita koitui lisäksi lainsäädännön maakohtaisista eroavaisuuksista sekä ajallisesta ulottuvuudesta, sillä yli kymmenen vuotta vanhoja tilisiirtoja saattaa esimerkiksi järjestelmien vaihtumisen takia olla vaikea selvittää.

Vuodesta 1996 lähtien joka toinen vuosi julkaistu Association of Certified Fraud Examinersin (ACFE) väärinkäytösraportti auttaa hahmottamaan yrityksissä tapahtuvien väärinkäytösten lukumäärää ja taloudellisia mittasuhteita. Vuosien 2014, 2016 ja 2018

raportit antavat jokainen samansuuntaisia viitteitä: tutkimuksiin osallistuneet yritykset arvioivat menettävänsä keskimäärin 5 % tuotoistaan vuosittain väärinkäytösten seurauksina. Väärinkäytösten aiheuttamat rahalliset mediaanitappiot vaihtelivat USD 130 000 ja USD 150 000 välillä. Yli viidenneksessä tapauksissa yritysten tappiot ylittivät miljoona dollaria.

Yrityksen näkökulmasta väärinkäytöksiin liittyy strateginen riski, jonka realisoituessa oikeudelliset ja taloudelliset seuraukset saattavat pahimmassa tapauksessa uhata sen koko liiketoimintaa. Toimintaa suunnitellessaan ja organisoidessaan yrityksen on tehtävä riskienkartoitustoimenpiteitä ja huomioitava niin ikään väärinkäytösten mahdollisuus. Organisaation henkilöstön, järjestelmien ja toiminnan strategianmukaiseen ohjaamiseen johto käyttää erilaisia ohjausjärjestelmiä (engl. *Management Control Systems*). Nämä järjestelmät ovat laajoja ja usein monimutkaisia kokonaisuuksia, jotka näkökulmasta riippuen saattavat käsittää pitkälti kaiken organisaation sisällä tapahtuvan valvonnan ja ohjauksen, kuten laaduntarkkailun, strategian kehityksen sekä työntekijöiden valvonnan. Yrityksessä tapahtuvan toiminnan valvonta ja ohjaaminen eri järjestelmin on väärinkäytösten minimoinnin ja havaitsemisen kannalta avainasemassa, sillä väärinkäytöksen tapahtuminen tarkoittaa usein jonkin ohjausjärjestelmän pettämistä.

Laskentatoimen kirjallisuudessa ei ole yksiselitteistä määritelmää johdon ohjausjärjestelmille, ja eri yhteyksissä ohjausjärjestelmillä voidaan tarkoittaa hyvin erilaisia järjestelmiä tai konsepteja. Määrittelyiden erot voivat liittyä esimerkiksi siihen, mitkä järjestelmät lasketaan ohjausjärjestelmiksi tai mihin tarkoitukseen ohjausjärjestelmää käytetään. Esimerkiksi Simons (1995, 5) määrittelee johdon ohjausjärjestelmät formaaleina, tietoon perustuvina rutiineina ja menettelyinä. Näitä käytetään Simonsin näkemyksen mukaan ihmisten toiminnan ohjaamiseen tiedon perusteella. Malmin ja Brownin (2008, 290) näkemys ohjausjärjestelmistä on samankaltainen, joskin laajempi. Toisin kuin Simons, heidän määritelmässään ohjausjärjestelmiä voivat olla myös muut kuin tietoon perustuvat järjestelmät. Yhteistä näille näkemyksille on kuitenkin se, että ohjausjärjestelmiksi voidaan katsoa sellaiset kokonaisuudet, joita johto käyttää yrityksessä tapahtuvan toiminnan ohjaamiseen ja siihen vaikuttamiseen.

Sen sijaan Chenhall (2003, 3) omaksuu määritelmän, jonka mukaan MCS käsittää johdon laskentatoimen järjestelmät (engl. *Management Accounting Systems*) sekä muita

organisaation kontrollijärjestelmiä, kuten klaanikontrollin (engl. *clan controls*). Tämä näkemys on olennaisesti laajempi kuin edellä esitetyt Simonsin tai Malmin ja Brownin määritelmät, sillä se sisältää esimerkiksi tiedon tuottamiseen ja päätöksenteon tukemiseen käytettäviä järjestelmiä, joita organisaation toimijat käyttävät tavoitteidensa saavuttamiseen.

Sisäinen valvonta (engl. *internal control*) on keskeinen ohjausjärjestelmä etenkin väärinkäytösten ehkäisyssä ja havaitsemisessa (PwC 2018). Nimensä mukaisesti sisäisellä valvonnalla yrityksen johto valvoo ja arvioi organisaation toimintaa. Sisäisen valvonnan tavoitteena on valvoa säännösten, lakien sekä yrityksen omien tavoitteiden ja normien noudattamista. (Ikäheimo ym. 2014, 117–119 ; Sihvonen ja Uusi-Hautamaa 2019, 99–100.) Varsinkin suuremmissa yrityksissä sisäinen valvonta on välttämätön toiminto, jolla voidaan vähentää väärinkäytöksen mahdollisuuksia, ja heikon sisäisen valvonnan on osoitettu olevan yhteydessä kasvaneeseen väärinkäytösriskiin. (Ruankaew 2016, 475; Bonny ym. 2015). Erityisesti 2000-luvun alkupuolen suuret kirjanpitoskandaalit, kuten Enronin ja Parmalatin tapaukset toimivat katalysaattoreina väärinkäytösten vastaisen sääntelyn tiukentumiselle sekä Euroopassa että Yhdysvalloissa. Näiden tapausten seurauksena yrityksille on asetettu korkeampia standardeja ja vaatimuksia väärinkäytösten estämiseksi. Yhtenä esimerkkinä tästä voidaan pitää sisäisen valvonnan järjestämistä ja organisointia koskeva raportointi. Lainsäädännön tiukentamisen ja sisäisten valvontajärjestelmien parantamisen avulla on pyritty niin sijoittajien kuin yrityksen oman aseman turvaamiseen. (Wolfe & Hermanson 2004, 38; Sihvonen & Uusi-Hautamaa 2019, 66–68.)

Digitalisaatio on viime vuosikymmenten suuri muutosvoima, jolla on ollut ja tulee suurella todennäköisyydellä olemaan kauaskantoisia vaikutuksia niin yhteiskunnan, organisaatioiden kuin yksittäisten henkilöidenkin näkökulmasta. Yhä kasvavalla vauhdilla etenevä digitaalinen kehitys asettaa siten alati muuttuvia haasteita ja vaatimuksia myös yritysjohdolle. (Bankewitz ym. 2016, 58.) Digitalisaation ansiosta monet yrityksen prosessit pohjautuvat nykyään erilaisille tietojärjestelmille, joiden toiminnasta yritysten prosessit ovat riippuvaisia (Stoel & Muhanna 2011). Näiden järjestelmien valvonta ja ylläpito on elintärkeää myös yrityksen sisäisen valvonnan kannalta, sillä heikkoudet tietojärjestelmien valvonnassa ovat usein sidoksissa valvonnan ja ohjauksen puutteeseen myös muualla yrityksessä (Klamm & Weidenmier Watson 2009, 2).

Digitalisaatio tarjoaa siten uudenlaisia keinoja väärinkäytöksille, kuten alussa mainitussa Nordean tapauksessa, jossa työntekijät käyttivät tietokoneille asennettua vakoiluohjelmaa käyttäjätietojen urkkimiseen. Esimerkiksi tämänkaltaisten uhkien estämiseksi ja havaitsemiseksi yrityksen sisäisen valvonnan on yhä tärkeämpää kattaa myös yrityksen digitaalinen ympäristö. Samalla digitalisaation tuomat työkalut, kuten automatiikka ja analytiikka voivat tarjota keinon havaita perinteisempiä väärinkäytöksiä.

1.2 Tavoite ja tutkimuskysymykset

Kuten edellä on havainnollistettu, koskettavat väärinkäytökset kaikenkokoisia yrityksiä, ja digitalisaatio on tuonut yrityksille liiketoimintamahdollisuuksien lisäksi myös uudenlaisia riskejä. Väärinkäytösten vaikutus yrityksen toimintaan, talouteen ja imagoon on selvän negatiivinen, joten yrityksillä on intressi sekä ehkäistä niitä että suorittaa jälkikäteistä tutkintaa ja tarkastuksia. Alussa esiteltyjen esimerkkiuutisten avulla on havainnollistettu, miten valvonnan heikko organisointi tai pettäminen saattaa johtaa suuriin väärinkäytösvyyhteihin. Yrityksen johdolla on siis selkeä intressi organisoida ohjausjärjestelmänsä ja sisäinen valvontansa tehokkaalla tavalla.

Tutkimuksen kohdeyhtiö on Suomessa toimiva tilitoimisto, joka tarjoaa muun muassa taloushallinnon, kirjanpidon ja palkanlaskennan palveluita yrityksille ja muille organisaatioille. Taloushallinto on monissa organisaatioissa pitkälti sähköistä, ja kohdeyritys tarjoaa asiakkailleen aktiivisesti digitaalisia taloushallinnon palveluita. Lisäksi esimerkiksi kirjanpitoon kohdistuva valvonta on avainasemassa taloudellisten väärinkäytösten estämisessä, joten vahvasti digitalisoitunut tilitoimisto tarjoaa otollisen ympäristön tarkastella digitalisaation vaikutuksia. Paperiseen taloushallintoon verrattuna digitalisaatio mahdollistaa muun muassa huomattavasti laajemman valvonnan ja seurannan tietojärjestelmien ja työkalujen avulla. Samalla yrityksen riskiympäristö muuttuu toimintaympäristön mukana, minkä vuoksi yritysten täytyy jatkuvasti tunnistaa näitä uudenlaisia riskejä.

Tutkielman tavoitteena on selvittää, millaisia muutoksia digitalisaatio on tuonut yrityksen sisäiseen valvontaan, ja miten se on muuttanut väärinkäytösriskejä. Nykytilan selvittämisen lisäksi tutkielmassa pyritään selvittämään mahdollisia tulevaisuuden kehityssuuntia ja digitalisaation sisäiseen valvontaan tuomia mahdollisuuksia. Valvontaa ja väärinkäytöksiä tarkastellaan empiirisesti tilitoimiston ja asiakasyrityksen välisessä suhteessa.

Tutkimuskysymykset, joiden avulla edellä mainittuihin tavoitteisiin pyritään, on määritelty seuraavasti:

1. Miten digitalisaatio on vaikuttanut yritysten väärinkäytösriskeihin?
2. Millaisia vaikutuksia digitalisaatiolla on sisäiseen valvontaan?

Tutkielman sisältöteoria pohjaa sekä väärinkäytösten että sisäisen valvonnan teoriaan. Tutkielman pyrkii parantamaan ymmärrystä digitalisaation vaikutuksesta näihin teorioihin peilaamalla empiiristä aineistoa sisältöteoriaan. Samalla tutkielma tarjoaa kohdeyrityksen katsauksen digitalisaation hyödyntämiseen yrityksen ohjauksessa ja asiakassuhteiden valvonnassa sekä auttaa tunnistamaan seuraavia todennäköisiä kehitysaskelia tällä saralla.

Koska tilitoimiston liiketoimintaprosessi muodostuu palvelutuotannosta, jossa esimerkiksi kirjanpitäjillä on pääsy asiakasyritysten taloudellisiin tietoihin, tarkastellaan tutkielman empiirisessä osuudessa väärinkäytöksiä tilitoimiston ja asiakasyrityksen välisessä suhteessa. Siten tutkielmassa tarkastellaan sekä sisäisiä että ulkoisia väärinkäytöksiä. Sisäisellä väärinkäytöksellä tarkoitetaan yrityksen sisällä työskentelevän henkilön toteuttamaa väärinkäytöstä, kun taas ulkoisessa väärinkäytöksessä tekijä on yrityksen ulkopuolinen taho, kuten asiakas tai toimittaja. Kuten luvussa 2 havainnollistetaan, väärinkäytöksinä voidaan pitää monenlaisia tekoja. Tässä tutkielmassa keskitytään tarkastelemaan vain taloudellista haittaa aiheuttavia tekoja, jolloin esimerkiksi epäeettinen toiminta, josta ei koidu suoria taloudellisia seurauksia, jää tarkastelun ulkopuolelle.

1.3 Tutkielman metodologia

Tutkielma on toteutettu laadullisena tapaustutkimuksena, joka on yleinen tutkimusstrategia etenkin johdon laskentatoimessa. Tapaustutkimukselle tyypillistä on tutkimuskohteiden pieni lukumäärä. Niiden tavoitteena on yleensä tuottaa uudenlaisia näkökulmia, tulkintoja tai ratkaisuja sekä saada syvempi näkemys tutkittavaan aiheeseen. (Lukka 2005, 376.) Tähän pohjaten tapaustutkimus soveltuu sisäisen valvonnan ja väärinkäytösten tutkimiseen. Nämä saattavat olla yritykselle arkaluontoisia ja monimutkaisia aiheita, jolloin niiden ymmärtämiseksi on syytä perehtyä yritykseen syvällisesti. Esimerkiksi Ratsula (2020) ja Arwinge (2014) ovat tutkineet sisäistä valvontaa tapaustutkimuksen avulla.

Tutkimusotteeltaan tämä tutkielma sopii parhaiten toiminta-analyyttisen tutkimusotteen alle. Toiminta-analyyttiset tutkimukset nojaavat vahvasti empiiriseen aineistoon, ja tutkimusote on luonteeltaan tavallisesti deskriptiivistä, selittävää. Toiminta-analyyttiselle tutkimukselle luonteenomaista on myös ainakin osittainen luopuminen tieteelliselle tutkimukselle tyypillisestä objektiivisuusvaatimuksesta. Siten tutkimukseen sisältyy tietty määrä subjektiivista ainesta. (Lukka 1991, 167). Tämän tutkielman tarkoituksena on ensisijaisesti kuvata digitalisaation vaikutusta sekä nykyisyyteen että tulevaan kehitykseen. Kuten toiminta-analyyttisessä tutkimuksessa yleensä, myös tämän tutkielman kontribuutio perustuu laadullisen empiirisen aineiston analyysiin. Toisaalta tutkielmassa esitellään erilaisia malleja ja viitekehyksiä sekä väärinkäytöksiin että sisäiseen valvontaan, ja pohditaan niiden suhdetta toisiinsa.

Tutkielmaa varten on haastateltu yrityksessä työskenteleviä asiantuntijoita. Kohdeyrityksen sekä haastateltavien taustoja avataan tarkemmin luvussa 4.1. Aineiston keruu on toteutettu avoimilla haastatteluilla ja teemahaastatteluilla. Haastatteluiden lisäksi empiriaosuuden tukena on käytetty muita lähteitä, kuten sähköpostikeskusteluja sekä yrityksen sisäistä materiaalia, kuten tiedotteita ja koulutusmateriaalia.

1.4 Tutkielman rakenne

Tutkielma koostuu kuudesta luvusta. Johdannon tehtävänä on johdatella lukija aiheeseen, esitellä tutkimuskysymykset ja motivoida tutkimus. Toinen ja kolmas luku muodostavat tutkielman teoreettisen viitekehyksen.

Tutkielman toinen luku käsittelee väärinkäytöksiä. Luvussa esitellään lyhyesti yleisimpiä väärinkäytöstyyppejä, väärinkäytösten luokittelua sekä väärinkäytöksiin johtavia tekijöitä. Luvussa esitellään myös tunnetuimpia väärinkäytösten arviointiin ja tutkimiseen käytettyjä malleja, joiden avulla havainnollistetaan esimerkiksi väärinkäytösten taustatekijöitä, syitä ja niille altistavia riskejä.

Kolmas luku käsittelee yrityksen sisäistä valvontaa ja sen merkitystä väärinkäytösten estämisessä. Ensimmäisissä alaluvuissa havainnollistetaan sisäisen valvonnan rooli osana johdon ohjausjärjestelmäkokonaisuutta, ja esitellään sisäisen valvonnan historiallista kehitystä. Luvussa esitellään kaksi sisäisen valvonnan mallia, Simonsin (1995; 2014) sekä COSOn (2013) luomat viitekehykset.

Luvussa neljä käsitellään digitalisaation tuomia riskejä sekä sen vaikutusta sisäiseen valvontaan ja COSO-malliin. Luvun tavoitteena on esitellä digitalisaation luomia kyberriskejä ja niiden eroa muunlaisiin riskeihin. Lisäksi luvuissa esitellään menetelmiä, joiden avulla näitä riskejä voidaan minimoida yrityksen ohjauksen avulla. Luku keskittyy sisäiseen valvontaan ja yrityksen ohjaukseen, eikä siinä käsitellä muita kyberriskien minimointiin käytettäviä keinoja, kuten vakuuttamista.

Viidennessä luvussa esitellään tutkielman empiirisen osuuden aineisto. Kuudes luku kokoaa yhteen aineistosta tehdyt havainnot ja tulokset, joita verrataan teoreettiseen viitekehykseen. Seitsemännessä luvussa summataan tutkielman tärkeimmät asiat.

2 Taloudelliset Väärinkäytökset yrityksissä

2.1 Väärinkäytösten määrittely ja luokittelu

2.1.1 Mitä tarkoitetaan väärinkäytöksellä?

Arkikielessä väärinkäytökset ymmärretään tavallisesti esimerkiksi petoksen tai kavalluksen kaltaisina tekoina. On kuitenkin olennaista pohtia, mitä väärinkäytöksellä tarkoitetaan eri konteksteissa, sillä eri konteksteissa väärinkäytöksille löytyy useita määrittelyjä.

Väärinkäytös on terminä kuvaava, mutta määritelmällisesti sitä saattaa olla hankala rajata. Se viittaa yleisesti epätoivottuun, sääntöjen tai ohjeiden vastaiseen toimintaan, jolla on negatiivisia vaikutuksia toiminnan kohteelle. Varsinkin englanninkielisessä kirjallisuudessa käytetään usein sanaa *fraud*, petos, kuvaamaan väärinkäytösten kaltaisia tilanteita. Väärinkäytös on kuitenkin terminä kattavampi kuin suomen kielen sana petos (ks. Rae & Subramaniam 2008; Dorminay 2012). Petosta voidaan kuitenkin hyvin pitää yhdenlaisena väärinkäytöstyyppinä

Toisaalta pelkkä sääntöjen vastainen käytös ei kuitenkaan automaattisesti tarkoita väärinkäytöstä. Inhimilliset erehdykset ja virheet eivät ole väärinkäytöksiä, sillä virheeseen ei sisälly samanlaista tahallisuutta tai tarkoituksenmukaisuutta kuin esimerkiksi petokseen. Huolimattomuuden ja tarkoituksellisuuden välinen raja on kuitenkin käytännössä ajoittain häilyvä, ja näissä tapauksissa asia jää usein oikeuden päätettäväksi. (Sihvonen & Uusi-Hautamaa 2019, 15.)

Sihvonen ja Uusi-Hautamaa (2019, 15–17) huomauttavat kuitenkin, että joissain tilanteissa toimintaa voidaan pitää väärinkäytöksenä, vaikkei teko täyttäisi oikeudellista määritelmää tahallisuudelle. Samoin tietynlaisia tahallisia tekoja voidaan pitää väärinkäytöksinä, vaikkeivat ne täyttäisi minkään rikoksen tunnusmerkistöä. Tämänkaltaisesta toiminnasta Sihvonen ja Uusi-Hautamaa käyttävät ilmausta epäeettinen ja arvojen vastainen toiminta.

Yleinen tapa lähestyä väärinkäytöstä terminä on lainsäädännön kautta. Kansainvälisten tilintarkastusstandardien (ISA 240) mukaan tilipäätöksissä olevat virheet ovat seurausta väärinkäytöksistä (engl. *fraud*) tai erheistä (engl. *error*). Väärinkäytös viittaa tässä tarkoitukselliseen (engl. *intentional*) toimeen ja vilpin (engl. *deception*) käyttöön

epäreilun tai laittoman edun saavuttamiseksi. Standardi käsittelee lähinnä tilinpäätöspetosta (engl. *financial statement fraud*), joka on eräs väärinkäytöksen muoto. Erilaisia väärinkäytösmuotoja käsitellään tarkemmin luvussa 2.1.2. IAS 240 -standardin määritelmän perustana on siis tarkoituksellinen epärehellinen toiminta. Samankaltaista tulkintaa käyttää myös Institute of Internal Auditors (IIA 2017, 23), jonka mukaan väärinkäytökselle luonteenomaista on vilppi, salailu tai luottamuksen pettäminen. Huomionarvoista on, että IIA:n määritelmästä on nimenomaisesti rajattu pois väkivallan tai fyysisen voiman käyttöön perustuvat teot. Tavoitteena väärinkäytöksissä on tämän määritelmän mukaan esimerkiksi rahan, omaisuuden tai edun saaminen taikka maksujen tai seuraamisten välttäminen.

Myös kansallinen lainsäädäntömme on huomioinut väärinkäytöksiä: rikoslakiin on kirjattu petoksia, kavalluksia ja rahanpesua kriminalisoivia pykäliä, ja korruptioon liittyvää säädäntöä sisältyy useisiin eri lakeihin, kuten osakeyhtiölakiin, kirjanpitolakiin ja tilintarkastuslakiin. (Rikoslaki 28§, 32§, 36§; Korruptiontorjunta.fi.)

Lainsäädännön ulkopuolelle jää kuitenkin liuta tekoja, jotka eivät välttämättä johda rikosoikeudellisiin seuraamuksiin, mutta joita voidaan pitää väärinkäytöksinä. Eettisesti kyseenalainen toiminta, kuten yrityksen arvojen ja sääntöjen rikkominen voidaan mieltää väärinkäytökseksi, vaikkei kyseinen teko olisi varsinaisesti lainvastainen eikä siten johtaisi oikeudelliseen rangaistukseen. Väärinkäytökset voidaan siten mieltää erilaisia rikoksia kattavaksi, mutta rikosta laajemmaksi termiksi. (Ratsula 2016a, 249; Sihvonen & Uusi-Hautamaa 2019, 14; 17.)

2.1.2 Väärinkäytöstyyppejä

Väärinkäytöksiä voidaan havainnollistaa ja luokitella eri tavoin. Yleinen tapa tarkastella väärinkäytöksiä on niiden tekotapojen mukaan. Association of Certified Fraud Examiners (ACFE) on käyttänyt raporteissaan väärinkäytöspuu-kaaviota, joka jakaa väärinkäytökset kolmeen päätyyppiin: korruptioon, varojen väärinkäyttöön ja tilinpäätöksiin liittyviin väärinkäytöksiin (engl. *financial statement fraud*). Nämä väärinkäytösten päätyypit on jaettu edelleen alakategorioihin ja edelleen yksittäisiin väärinkäytöstekoihin. Vaikkei kaavio ole tyhjentävä, antaa se esimerkin kattavasta jaottelusta.

Kuvio 1 Väärinkäytöspuu, ACFE 2020

ACFE:n vuoden 2020 raportin mukaan reilusti suurin osa, 86 % tutkituista tapauksista, sisälsi varojen väärinkäyttöä, kun taas korruptioon (43 %) ja tilinpäätöspetoksiin liittyviä (10 %) väärinkäytöksiä tuli ilmi lukumääräisesti huomattavasti vähemmän. Toisaalta kuitenkin tilinpäätöspetosten aiheuttamat rahamääräisen mediaanitappiot olivat tutkimuksen mukaan moninkertaiset muunlaisten väärinkäytösten aiheuttamiin tappioihin verrattuna. Varojen väärinkäyttö sen sijaan aiheutti pienimmät mediaanitappiot. Nämä eri väärinkäytöstapojen mittasuhteet ovat pysyneet ACFE:n raporttien mukaan hyvin samansuuruisina vuodesta toiseen. (ACFE 2020; 2018; 2016). Huomattavaa kuitenkin on, että raportin mukaan monet väärinkäytöstapaukset voivat sisältää useamman kategorian alle kuuluvia tekoja.

Korruptio yhdistetään arkikielessä yleensä etenkin lahjuksiin. Lyhyesti korruptiona voidaan pitää etujen tavoittelua tavalla, joka sisältää vaikutusvallan väärinkäyttöä (Korruptiontorjunta.fi). ACFE:n (2020) väärinkäytöspuussa korruptio voi ilmetä erilaisina eturistiriitoina, lahjuksina, laittomina palkkioina tai kiristyksenä. Näistä kolme viimeistä ovat hyvin samantapaisia, mutta eivät synonyymejä. Lahjonta viittaa pyrkimykseen vaikuttaa toisen tahon päätöksentekoon tarjoamalla esimerkiksi rahaa. Laiton palkkio on hyvin lähellä lahjontaa, mutta termi viittaa tapauksiin, joissa palkkio annetaan päätöksentekijälle vasta päätöksen teon jälkeen. Kiristystapauksissa taas päätöksentekijään pyritään vaikuttamaan etukäteisesti esimerkiksi uhkailemalla tai vaatimuksilla. (Wells 2017, 254.) Eturistiriitatilannetta, jossa henkilöllä on mahdollisuus vaikuttaa johonkin transaktioon tavalla, josta koituu hänelle itselleen hyötyä organisaation kustannuksella (Wells 2017, 282). Eturistiriidat voivat näyttäytyä muun

muassa kaksoisrooleina, jossa esimerkiksi yksi henkilö toimii samanaikaisesti julkisella puolella päättävässä virassa, ja on samalla omistajana yksityisessä yrityksessä. Eturistiriita syntyy, mikäli hän voi käyttää julkista virkaansa edistääkseen yksityisen yrityksensä toimintaa. Myös esimerkiksi ystävien tai sukulaisten suosiminen päätöksiä tehdessä voi täyttää korruption tunnusmerkit. Samoin korruptioksi voidaan mieltää kartellit ja muu laiton kilpailun vääristäminen. (Korruptiotorjunta.fi.)

Varojen väärinkäyttö (engl. *asset misappropriation*), on ACFE:n raporttien mukaan ollut viime vuosien ylivoimaisesti yleisin väärinkäytöstyyppi. Myös PwC:n (2020, 2018) tilastossa varojen väärinkäyttö on yleisimpiä sisäisten väärinkäytösten muotoja. Varojen väärinkäyttö tarkoittaa tässä yrityksen omaisuuden tai resurssien anastamista tai käyttöä väärin tarkoituksiin, esimerkiksi varkauden, petoksen tai kavalluksen kautta. ACFE (2020) jakaa varojen väärinkäytön kahteen kategoriaan, rahavarojen väärinkäyttöön ja muiden varojen, kuten raaka-aineiden väärinkäyttöön. Rahavaroihin liittyvät väärinkäytökset käsittävät muun muassa rahojen varastamisen, kavaltamisen ja perusteettomat kulukorvaukset. Muihin varoihin voi niin ikään liittyä varastamista sekä esimerkiksi omaisuuden luvatonta omaan käyttöön ottamista. Toisin sanoen varojen väärinkäyttö on terminä laajempi kuin varkaus tai kavallus, ja se käsittää näiden lisäksi yrityksen omaisuuden luvattoman hyödyntämisen omiin tarpeisiin (Wells 2017, 46).

Väärinkäytösten liittyessä tilinpäätöksiin käytetään englanninkielisessä kirjallisuudessa ja lainsäädännössä usein termiä *financial statement fraud*. ACFE:n (2020) mukaan tilinpäätökseen liittyvät väärinkäytökset ovat melko epätavallisia, mutta ilmi tullessaan ne usein paljastuvat laajamittaisiksi ja aiheuttavat suuret tappiot yritykselle. ACFE:n (2020) väärinkäytöspuussa tilinpäätöksiin liittyvät väärinkäytökset johtuvat tilinpäätösinformaation väärinarvostamisesta, joko liian suurina tai liian pieninä. Esimerkkejä näistä ovat tekaistut myynnit tai kulut, tai omaisuuserien väärinarvostaminen. ISA 240 -standardi antaa samankaltaisen kuvan tilinpäätösväärinkäytöksistä: sen mukaan petollinen taloudellinen raportointi tarkoittaa informaation tahallista vääristämistä joko tietoja lisäämällä, muuttamalla tai poisjättämällä.

Edellä esitellyt väärinkäytöskategoriat eivät ole tyhjentäviä tai toisiaan poissulkevia. Väärinkäytöstapaukset ovat monesti monimutkaisia, ja yksittäinen tapaus voi sisältää useampiin edellä esiteltyihin kategorioihin laskettavia tekoja (ACFE 2020). Tämä koskee

etenkin useamman kuin yhden tekijän toteuttamia kompleksisia ja hyvin suunniteltuja väärinkäytösjuonia. Tällaiset suunnitelmat ovat usein hyvin peiteltyjä ja siksi haastavia havaita (Bonny ym. 2015, 447).

Toinen tapa tarkastella väärinkäytöksiä on tekijän näkökulmasta, eli siitä, kuka väärinkäytöksen tekee. Tässä tutkielmassa tarkastellaan muun muassa yrityksen sisäisiä väärinkäytöksiä (engl. *occupational fraud*), jonka määritelmässä korostuu yrityksen sisäisen aseman hyödyntäminen henkilökohtaisen hyödyn saavuttamiseksi (ACFE 2020; Wells 2017, 2). Tekijät voidaan jakaa esimerkiksi heidän asemansa mukaan, jolloin puhutaan työntekijöiden (engl. *employee fraud*), johtajien (engl. *management fraud*) tai omistajien (engl. *owner/executive fraud*) tekemistä väärinkäytöksistä (ISA 240; ACFE 2020). Edellä mainitut tekijät ovat organisaation sisällä, jolloin puhutaan sisäisistä tai ammatillisista väärinkäytöksestä (engl. *internal/occupational fraud*). Kuten luvussa 2.2.2 havainnollistetaan, on henkilön asema vahvasti sidoksissa valtaan ja sitä kautta mahdollisuuteen kiertää tai hyväksikäyttää organisaation ohjausmenetelmiä tai kontrolleja. Sisäisten väärinkäytösten lisäksi tekijä voi kuulua johonkin yrityksen sidosryhmistä, jolloin puhutaan ulkopuolisista väärinkäytöksistä (engl. *external fraud*). Yleisimpiä yrityksen ulkopuolisia väärinkäyttäjiä ovat asiakkaat ja liiketoimintakumppanit, kuten tavarantoimittajat (PwC 2020).

Väärinkäytökset voidaan luokitella myös sen mukaan, kenelle niistä koituu hyötyä. Ratsulan (2016a, 251–252) mukaan väärinkäytökset voivat joko hyödyttää tai haitata yrityksen toimintaa. Molemmissa tapauksissa tekijän tavoitteena on kuitenkin saavuttaa etua itselleen tai lähipiirilleen. Ratsula mainitsee muun muassa varkauden, lahjusten vastaanottamisen ja kirjanpidon väärentämisen esimerkkeinä tilanteista, joissa hyötyjänä on ainoastaan väärinkäytöksen tekijä. Organisaatio saattaa hänen mukaansa sen sijaan hyötyä esimerkiksi tilanteista, joissa annetut lahjukset sujuvoittavat sen liiketoimintaa tai yrityksen varoja on arvostettu tarkoituksellisesti väärin.

Väärinkäytöksiä tapahtuu kaiken kokoisissa yrityksissä. Pienet yritykset ovat kuitenkin ACFE:n (2020) raportin mukaan alttiimpia väärinkäytöksille yleisesti pienempien resurssien ja heikomman kontrollin takia, mutta erityisesti laskutukseen, kuitteihin ja maksuihin liittyvät väärinkäytösriskit ovat pienissä yrityksissä merkittävästi korkeammat. Ergin ja Erturan (2019, 36) huomauttavatkin, että pörssilistatuissa yhtiöissä tehdyt väärinkäytökset nousevat median kautta helposti suuren yleisön tietoisuuteen, kun

taas pienissä ja keskisuurissa yrityksissä vastaavat tapaukset jäävät vain korkeintaan yrityksen lähipiirin tietoon. Tämä on ongelmallista sikäli, että pienet ja keskisuuret yritykset muodostavat valtaosan kaikista yrityksistä, ja ne ovat alttiimpia väärinkäytöksille vähäisten ja puutteellisten ohjausjärjestelmien takia. Tämä saattaa johtaa vääristyneeseen kuvaan väärinkäytösten yleisyydestä ja niiden luonteesta. ACFE:n raportin (2020) mukaan alle 100 henkilöä työllistävissä pienyrityksissä väärinkäytösten aiheuttama mediaanitappio, USD 150 000 oli suurempi kuin yli 10 000 henkilöä työllistävissä suuryrityksissä, joissa vastaava tappio oli USD 140 000. Yritykset, joiden henkilöstömäärä oli näiden väliltä, kokivat verrattain pienemmät mediaanitappiot. Kun huomioidaan yrityksen koko, kärsivät pienyritykset suhteessa huomattavasti enemmän väärinkäytöksistä kuin vastaavan tappion kohtaava suuryritys.

2.2 Miksi väärinkäytöksiä tapahtuu? – Työkaluja ja viitekehyksiä

Seuraavissa alaluvuissa esitellään eräitä yrityskirjallisuudessa yleisesti tunnettuja väärinkäytösten viitekehyksiä. Väärinkäytösmallien tutkimushistoria ulottuu 1900-luvun puolivälin tienoille, kun Edwin Sutherland (1949) ja Donald Cressey (1953) julkaisivat ensimmäisiä laajamittaisia tutkimuksia valkokaulusrikollisuudesta. Viime vuosikymmeninä kehitettyjen uusien mallien avulla pystytään yhä paremmin selittämään väärinkäytösten syntyä sekä selvittämään niiden tapahtumiseen johtaneita tekijöitä. Yrityksen kannalta ongelmallista kuitenkin on, ettei väärinkäytösten riskejä pystytä tarkankaan valvonnan avulla täysin poistamaan. Tehokkaalla valvonnalla väärinkäytöksiin liittyviä riskejä voidaan kuitenkin olennaisesti pienentää ehkäisemällä sekä suorittamalla jälkikäteistä valvontaa (Ratsula 2016a, 255; ACFE 2020).

Väärinkäytösten ehkäisyn keskiössä on niiden juurisyiden ymmärtäminen. Väärinkäytösten syitä on tutkittu yhtä pitkään kuin valkokaulusrikollisuuttakin, ja yleisen konsensuksen mukaan yleisimpiä syitä väärinkäytöksille ovat erilaiset tekijän taloudelliseen tilanteeseen liittyvät tekijät (Bonny ym. 2015, 458; 460). Ratsulan (2016a, 253) mukaan myös esimerkiksi yllättäen avautuva tilaisuus tai kokeilunhalu saattavat johtaa väärinkäytökseen. Lisäksi esimerkiksi päihteiden väärinkäyttö ja tekijän luonteeseen liittyvät tekijät saattavat vaikuttaa väärinkäytöksen syntyyn (Bonny ym. 2015, 458). Ratsulan (2016a, 253) mukaan useat väärinkäytökset saavat alkunsa tekijän kokemasta tarpeesta, mutta epärehellistä toimintaa usein jatketaan myös alkuperäisen

tarpeen tyydyttämisen jälkeenkin. Tätä puoltaa myös ACFE:n vuoden 2020 raportti, jonka mukaan tyypillinen petos kestää keskimäärin 14 kuukautta ennen paljastumistaan.

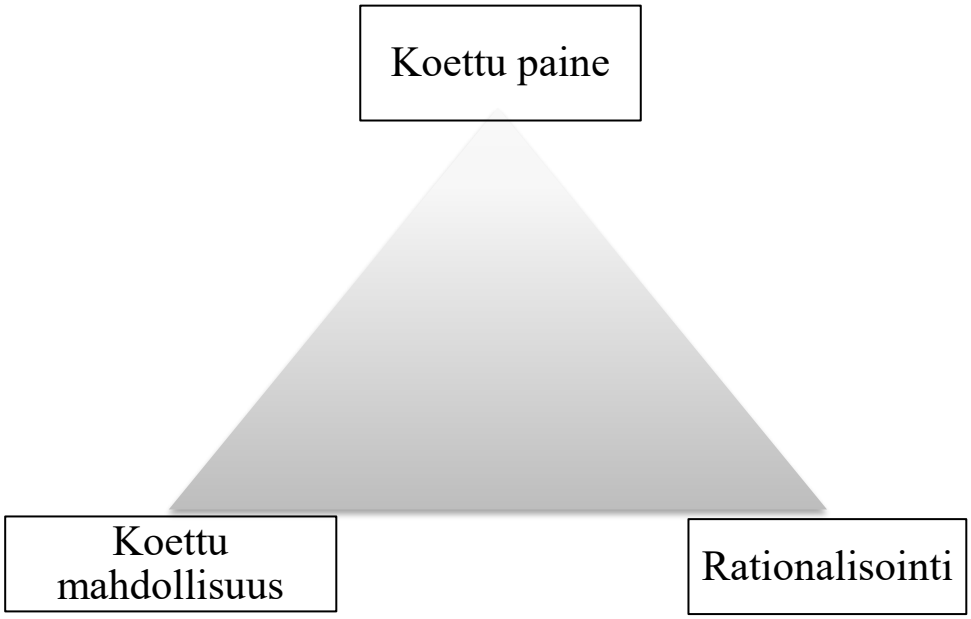
Etenkin luvussa 2.2.1 esiteltävä väärinkäytöskolmio on ollut uraauurtava malli, johon monet myöhemmät sovellukset pohjautuvat. Vousinasin (2019, 374) mukaan on kuitenkin tärkeää huomata, ettei kaikkia väärinkäytöstapauksia pystytä selittämään yhden mallin avulla. Lisäksi yhteiskunnan muutokset ovat tuoneet oman vaikutuksensa myös väärinkäytöksiin, jonka takia myös väärinkäytöksiä tulkitsevia malleja on päivitettävä huomioimaan moderni liiketoimintaympäristö.

Vertaamalla alkuperäistä väärinkäytöskolmiota myöhemmin kehitettyihin malleihin, kuten väärinkäytöstimanttiin tai väärinkäytösasteikkoon, on myöhemmin kehitetyissä malleissa huomattavissa persoonallisuudelle annettu vahvempi painoarvo. Esimerkiksi Rezaee ja Riley (2010) korostavat yksilön persoonan, henkilökohtaisen etiikan ja luottamuksen laatua väärinkäytöstapauksissa. Varsinkin avainhenkilöstön tunteminen ja henkilöiden luonteenpiirteiden sekä taipumusten arviointi ja seuranta ovat Wolfen ja Hermansonin (2004, 40) mukaan tärkeä osa-alue väärinkäytösriskien hallinnassa. Allanin (2003, 40) mukaan numeraalisen datan analysointi ei väärinkäytösten selvittämisessä riitä, vaan sen lisäksi asiaa selvittävien henkilöiden tulisi pyrkiä ymmärtämään teon kontekstia tekijän näkökulmasta: mitkä tekijät ovat saattaneet ajaa tekijän väärinkäytöksen tekoon, mistä hänen mahdolliset taloudelliset ongelmansa johtuvat, ja millainen hänen todellinen persoonallisuutensa on.

2.2.1 Fraud triangle – Väärinkäytöskolmio

Kenties tunnetuin väärinkäytösten havainnollistamiseen käytetty viitekehys on pitkälti Donald Cresseyn (1953) tutkimuksiin perustuva väärinkäytöskolmio. Yksinkertaisuutensa ja sovellettavuutensa ansiosta väärinkäytöskolmiota voidaan hyödyntää eri toimialoilla ja erilaisissa organisaatioissa, ja viitekehys on otettu osaksi esimerkiksi Yhdysvaltojen SAS-tilintarkastusstandardeja. (Dorminey ym. 2010, 18–19.) Cresseyn tutkimusten kohteena olivat väärinkäytöksen tekoon johtavat olosuhteet. Myöhemmin väärinkäytöskolmion teorian muodostaneet tutkimukset tarkastelivat elementtejä, joiden samanaikainen olemassaolo mahdollistaa väärinkäytöksen. (Ruankaew 2016, 474; Ratsula 2016a, 253.) Laajamittaisen käyttönsä lisäksi malli on toiminut pohjana muille väärinkäytösmalleille, kuten myöhemmin esiteltävälle

väärinkäytöstimantille. Väärinkäytöskolmiota voidaan siten pitää uraauurtavana viitekehyksenä väärinkäytösten kirjallisuudessa.



Kuvio 2 Väärinkäytöskolmio, Dorminey ym. 2010, 19.

Väärinkäytöskolmion kolme elementtiä ovat koettu paine (engl. *perceived pressure*), koettu mahdollisuus (engl. *perceived opportunity*) sekä toiminnan rationalisointi (engl. *rationalization*). Yksilön kokema paine viittaa motiiviin tai ajuriin, joka saa tai pakottaa yksilön toteuttamaan väärinkäytöksen. Yleensä väärinkäytöskolmion paine viittaa yksilön henkilökohtaisiin taloudellisiin paineisiin, kuten yllättäviin menoihin, elämiseen yli varojen tai muiden henkilökohtaisten ongelmien aiheuttamiin taloudellisiin seurauksiin. Näiden yksilöllisten, muilta usein piiloteltavien ongelmien ratkaisemiseksi saattaa yksilö sopivien olosuhteiden vallitessa turvautua väärinkäytökseen. (Dorminey ym. 2010, 18–19; Vousinas 2019, 373.) Taloudellisten paineiden lisäksi yksilö voi kohdata ei-taloudellisia paineita, kuten esimerkiksi työhön liittyviä sekä päihde- tai muihin riippuvuuksiin liittyviä paineita (Lokanan 2015, 203). Olennaista on, että yksilöt kokevat erilaisia paineita, jotka voivat liittyä muun muassa heidän yksityiselämäänsä tai asemaansa yrityksessä (Ruankaew 2016, 475). Esimerkiksi työntekijät voivat kohdata suorituspaineita esimiehiltään, ja omistajat ja ylin johto saattavat kokea tulosvastuun tuomaa painetta heikosti menneen tilikauden tai investoinnin seurauksena.

Koettu mahdollisuus väärinkäytökseen voidaan jakaa kahteen osa-alueeseen: organisaatioon ja yksilöön liittyviin tekijöihin. Otollisen väärinkäytösmahdollisuuden avautuminen saattaa johtua esimerkiksi heikosta valvonnasta tai vääränlaisesta organisaatiokulttuurista (Wolfe & Hermanson 2004, 38; Dorminey ym. 2010, 19). Kontrollin ja valvonnan puute saattaa siis avata potentiaaliselle tekijälle väylän väärinkäytökseen. Toisaalta jotta yksilö kykenisi hyödyntämään järjestelmien heikkoutta, täytyy uskoa siihen, että hän kykenee tekemään väärinkäytöksen jäämättä kiinni (Vousinas 2019, 373). Lisäksi hänen tulee asemaltaan tai kyvyiltään riittävän pätevä pystyäkseen hyväksikäyttämään organisaation heikkouksia (Rae & Subramaniam 2008, 106). Tekijän tulee siis muun muassa olla riittävän varma omista kyvyistään, sekä olla sopivassa asemassa organisaatiossa ollakseen riittävän vakuuttunut väärinkäytöksen onnistumisesta.

Väärinkäytöskolmion kolmas elementti, rationalisointi tarkoittaa yksilön muodostamaa perustelua tai oikeutusta väärinkäytökselle. Jotta potentiaalinen väärinkäyttäjä voisi toteuttaa aikeensa, tulee hänen kyetä oikeuttamaan ja moraalisesti perustelemaan tekonsa itselleen. Kuten koettu paine, rationalisointi on hyvin yksilöllinen prosessi, jota on vaikea todeta ja ehkäistä organisaation käytössä olevin perinteisin keinoin (Dorminey 2010, 19).

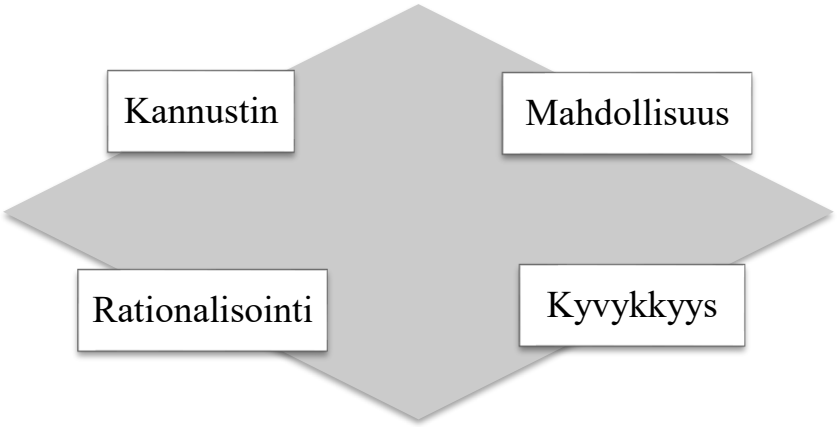
Jotta väärinkäytös realisoituisi, tulee jokaisen kolmion osa-alueen olla yhtä aikaa olemassa. Pelkkä taloudellinen ahdinko tai kyky perustella yrityksen varojen luvaton lainaaminen ei teorian mukaan johda väärinkäytöksen realisoitumiseen. (Vousinas 2019, 373.) Väärinkäytöskolmion viitekehyksen mukaan tyypillinen väärinkäyttäjä on siten taloudellisissa vaikeuksissa oleva henkilö, joka on havainnut mahdollisuuden helpottaa omaa tilannettaan sekä kykenee perustelemaan itselleen toimintansa oikeellisuuden.

Väärinkäytöskolmio on hyvä apuväline väärinkäytösten tutkijoille sekä organisaatioille, ja erityisen käytännöllinen se on tapahtuneiden väärinkäytösten taustatekijöitä selitettäessä. Vaikka kolmion avulla voidaan selittää monien väärinkäytöstapausten luonnetta ja syitä, on mallilla muutamia olennaisia heikkouksia (Vousinas 2019, 373–374). Esimerkiksi Dorminey ym. (2010, 19) huomauttavat väärinkäytöskolmion olevan yksinään riittämätön väärinkäytösten estämisessä, sillä etenkin yksilön kokemaa painetta ja yksilön rationalisointiprosessia on käytännössä mahdotonta tarkkailla. Toiseksi huolimatta väärinkäytöskolmion pelkistetystä ulkoasusta ja muuttujien pienestä lukumäärästä on väärinkäytösten sattuminen monien tekijöiden summa. Monimutkaisten

ja toisistaan riippuvien muuttujien vuoksi esimerkiksi heikko sisäinen kontrolli ei aina johda väärinkäytöksiin, ja toisaalta tehokkaatkaan sisäisen valvonnan järjestelmät eivät kykene täysin estämään väärinkäytöksiä. (Rae & Subramaniam 2008, 106; Sihvonen ja Uusi-Hautamaa 2019, 157.) Väärinkäytöskolmio ei siis välttämättä pysty tarjoamaan käyttäjälleen varsinaista viitekehystä sisäisen valvonnan tai ohjaustoimenpiteiden parantamiseen. Osittain näiden puutteiden johdosta väärinkäytöskolmiolle on kehitetty täydentäviä ja korvaavia viitekehyksiä, kuten seuraavassa alaluvussa esiteltävä väärinkäytöstimantti.

2.2.2 Fraud diamond – Väärinkäytöstimantti

Väärinkäytöstimantin esittelivät alun perin Wolfe ja Hermanson (2004) vastineena väärinkäytöskolmiolle, joka toimii pohjana neliulotteiselle viitekehykselle. Uuden viitekehyksen tavoitteena oli kehittää ja laajentaa kelvollisesti toimivaa väärinkäytöskolmion konseptia. Timantin muut ulottuvuudet ovat käytännössä samat kuin väärinkäytöskolmiossa. Koetun paineen Wolfe ja Hermanson ovat korvanneet kannustimelle (engl. *incentive*), joka kuitenkin sisällöltään vastaa väärinkäytöskolmion koettua painetta: yksilö kokee halun tai tarpeen toteuttaa väärinkäytös. Varsinainen kontribuutio muodostuu kuitenkin Wolfen ja Hermansonin neljännestä elementistä, kyvykkyydestä (engl. *capability*), joka liittyy yksilön kykyihin ja luonteenpiirteisiin toteuttaa väärinkäytös. Wolfe ja Hermanson (2004, 38) perustelevat neljännen ulottuvuuden lisäämistä tietyn yksilön henkilökohtaisten ominaisuuksien merkityksellä. Vaikka väärinkäytöstimantin muut ulottuvuudet olisivat olemassa, on väärinkäytöksen toteutumisen kannalta oleellista, kykeneekö potentiaalinen väärinkäyttäjä havaitsemaan ja hyödyntämään tarjoutuvan mahdollisuuden väärinkäytökselle. Mikäli potentiaalisella väärinkäyttäjällä ei ole vaadittavia persoonallisuuteen ja osaamiseen liittyviä ominaisuuksia, laskee se Wolfen ja Hermansonin (2004, 39) mukaan väärinkäytöksen riskiä huomattavasti.



Kuvio 3 Väärinkäytöstimantti, Dorminey ym. 2010, 22.

Wolfe ja Hermansonin (2004) kyvykkyys muodostuu ainakin kuudesta osa-alueesta. Yksilön kykyyn tehdä väärinkäytös vaikuttaa ensinnäkin henkilön asema. Esimerkiksi tietyt työtehtävät tai korkea asema yrityksessä saattavat tarjota ainutlaatuisen mahdollisuuden hyödyntää yrityksen järjestelmien heikkouksia. ACFEn (2020, 38) raportin mukaan tekijän asema yrityksessä vaikuttaa todennäköisiin tappioihin hyvin vahvasti: rivityöntekijän tekemän väärinkäytöksen mediaanitappio oli n. USD 60 000, kun taas omistajan tai johtohenkilön vastaava summa oli kymmenkertainen, USD 600 000. Korkeammassa asemassa olevalla henkilöllä on siis usein mahdollisuus suuremman väärinkäytöksen tekemiseen.

Toiseksi henkilön täytyy pystyä havaitsemaan ja hyväksikäyttämään yrityksen sisäisen valvontajärjestelmän heikkouksia. Onnistuneeseen väärinkäytökseen vaaditaan Wolfen ja Hermansonin (2004) mukaan yleensä hyvin usein hyvää koulutustaustaa, pitkähköä työkokemusta sekä luovuutta. Tietotaidon avulla potentiaalinen väärinkäyttäjä pystyy hyödyntämään asemaansa sekä pääsyään yrityksen järjestelmiin.

Wolfe ja Hermanson (2004) korostavat taitojen ja aseman lisäksi myös persoonallisuuden merkitystä väärinkäytöksien toteuttamisessa. Itseluottamuksen ja egon merkitys liittyy henkilön uskallukseen toteuttaa suunnittelemansa väärinkäytös. Itsevarma henkilö uskoo pystyvänsä toteuttamaan väärinkäytöksen, tai kiinni jäädessään selittämään tekonsa ja pääsemään siten pälkähästä.

Neljäs kyvykkyyden osa-alue on henkilön kyky suostutella tai pakottaa muita henkilöitä osalliseksi väärinkäytöstään. Wolfen ja Hermansonin (2004, 40) mukaan vakuuttavasti esiintyvä väärinkäyttäjä kykenee suostuttelemaan toisia yhteistyöhön tai painamaan huomaamansa väärinkäytöksen villaisella. Allan (2003) on artikkelissaan esitellyt

erilaisia potentiaalisia väärinkäyttäjätyyppejä. Allanin luokittelussa tyypeiltään erilaiset ihmiset käyttävät eri metodeja suostutellessaan muita ihmisiä peittämään väärinkäytöksiään. Esimerkiksi kiusaaja-tyyppi turvautuu usein pelotteluun ja painostukseen koettaessaan taivutella muita mukaan väärinkäytökseensä.

Väärinkäyttäjän on osattava myös valehdella. Valehtelijan on ensinnäkin kyettävä kertomaan uskottavia ja vakuuttavia valheita, ja toiseksi hänen on pysyttävä johdonmukaisena valheissaan.

Viimeinen Wolfen ja Hermansonin (2004) kyvykkyyden aspekti on paineensietokyky. Väärinkäytösten tekeminen on hyvin stressaavaa, ja siihen liittyy erilaisia alati läsnä olevia riskejä. Jatkuva valehtelu ja asioiden salailu on kuluttavaa, ja väärinkäytöksen onnistumisen kannalta on olennaista, ettei tekijä murru paineen alla.

Wolfe ja Hermanson (2004, 41–42) suosittelevat yrityksiä arvioimaan johto- ja avainhenkilöiden persoonallisuuksia ja kykyjä, jotta uudet mahdollisuudet ja etenkin uhat voidaan tunnistaa. Tarkastelemalla henkilön toimintaa ja reaktioita eri tilanteisiin voi yritys saada syvempää tietoa hänen persoonastaan. Etenkin avainhenkilöiden rekrytointitilanteissa käytetään usein erilaisia taustatarkistuksia, joiden avulla pyritään varmistumaan toisen osapuolen luotettavuudesta (Ratsula 2016a, 260–261). Organisaation on Wolfen ja Hermansonin (2004, 42) mukaan myös kyettävä reagoimaan, mikäli herää epäilys tietyn henkilön mahdollisesta kyvystä tai taipumuksesta toteuttaa väärinkäytös. Tällöin yritys voi käyttää useita erilaisia hienovaraisia toimenpiteitä, joilla varmistutaan esimerkiksi kyseisen henkilön työn laadusta tai tulojen ja menojen alkuperästä.

2.2.3 MICE-malli

Kranacherin ym. (2011) esittelemä MICE-malli pyrkii väärinkäytöstimantin tavoin täydentämään väärinkäytöskolmion teorian aukkoja tarkastelemalla yksilön motiiveja toteuttaa väärinkäytös. Näitä motivaatioita voidaan tarkastella MICE-mallin ulottuvuuksien kautta. Mallin kehittämisen taustalla oli etenkin väärinkäytöskolmion kyvyttömyys selittää tapauksia, joissa väärinkäytöksen tekijällä ei ollut merkittäviä henkilökohtaisia taloudellisia ongelmia. Väärinkäytöskolmion teoria olettaa väärinkäytöksen motivaation olevan aina yksilön henkilökohtainen ja jakamaton taloudellinen paine. Tämä näkemys on kuitenkin helposti kyseenalaistettavissa,

esimerkiksi Allan (2003, 40) huomauttaa ettei väärinkäytöksen motivaatio usein ole pelkästään taloudellinen. MICE-mallin avulla voidaan tarkastella väärinkäyttäjän motivaatioita pelkkiä taloudellisia paineita laajemmasta näkökulmasta, joten sitä voidaan hyödyntää esimerkiksi väärinkäytöskolmion teorian lisänä. (Dorminey ym. 2012, 562, 564.)

Akronyymi MICE muodostuu sanoista raha (engl. *money*), ideologia (engl. *ideology*), painostus (engl. *coercion*) ja ego tai oikeus (engl. *ego/entitlement*) (Dorminey ym. 2010, 21). Raha ja oman egon pönkittäminen ovat yleisiä osatekijöitä useimmissa väärinkäytöstapauksissa, ja nämä liittyvät läheisesti esimerkiksi väärinkätöstimantin paine ja kyvykkyys -osa-alueisiin. Usein väärinkäytösten taustalla on esimerkiksi oman taloudellisen aseman parantaminen tai vaikutusvallan kasvattaminen. Ideologia on Dormineyn ym. (2012, 563) mukaan hieman harvinaisempi motivaation lähde, mutta he esittävät kaksi tyyppiesimerkkiä ideologian vaikutuksesta. Heidän mukaansa esimerkiksi yksilön negatiivinen suhtautuminen verotukseen saattaa laskea kynnystä verojen kiertämiseen. Toinen esimerkki liittyy sen sijaan ekstremismiin, kuten ääriuskonnollisuuteen liittyvään terrorismiin, jota usein rahoitetaan rahanpesun avulla. Ideologia voi myös Dormineyn ym. (2010,) mukaan liittyä yksilön tarkoitusperiin, joita hän pitää oikeutettuina. Tarkoitus pyhittää keinot -ajattelua voidaan käyttää siten argumenttina oikeuttamaan väärinkäytökset. Painostuksen kohteeksi joutuneet henkilöt voivat joutua osallistumaan väärinkäytökseen vasten tahtoaan tai olemaan ilmoittamatta asiasta eteenpäin.

2.2.4 Fraud scale – Väärinkäytösasteikko

Väärinkäytösasteikko on Albrechtin ym. (1984) kehittämä työkalu, jonka avulla väärinkäytöksen todennäköisyyttä voidaan arvioida tarkastelemalla mallin elementtien, paineiden (engl. *pressure*), mahdollisuuksien (engl. *opportunity*) sekä henkilökohtaisen rehellisyyden (engl. *personal integrity*) suhteita toisiinsa. Kuten monet muut mallit, pohjautuu myös väärinkäytösasteikko osin väärinkäytöskolmioon rehellisyyden korvatessa rationalisoinnin (Dorminey ym. 2010, 19.)

Mallin avulla voidaan arvioida väärinkäytöksen riskiä tarkastelemalla asteikon kolmea kriteeriä samanaikaisesti. Esimerkiksi korkeat paineet, väärinkäytöksen helppous ja henkilön epärehellisyys altistavat suuremmille riskeille kuin tasapainoisemmassa

tilanteessa, jossa paineet ovat pienemmät, sisäinen valvonta hyvällä tasolla ja yritys on perillä työntekijöidensä persoonallisuudesta.

Dormineyn ym. (2010, 20) mukaan yksilön rehellisyyden tarkastelu rationalisoinnin sijaan helpottaa organisaatioiden työtä, sillä rehellisyyttä on todennäköisesti helpompi havaita ja arvioida kuin yksilön omaa rationalisointia. Tämä onnistuu heidän mukaansa lähinnä yksilön toimintaa seuraamalla, eli oppimalla tuntemaan henkilön persoonallisuuden sekä tavat tehdä päätöksiä ja reagoida erilaisiin tilanteisiin. Yksilön oma etiikka ja rehellisyys ovat avainasemassa väärinkäytösten toteuttamisessa ja ne liittyvät pitkälti myös potentiaalisen väärinkäyttäjän käymään sisäiseen dialogiin väärinkäytöksen rationalisoinnista. Henkilön aiemman käytöksen tarkastelu antaa siten osviittaa hänen rehellisyydestään. Rehellisyys vaikuttaa Dormineyn ym. (2012, 562) mukaan suoraan väärinkäytökseen rationalisointiin, sillä korkean integriteetin omaava henkilö on luultavasti vähemmän altis rationalisoimaan epäeettistä toimintaansa. Tästä näkökulmasta rehellisyys voidaan heidän mukaansa nähdä myös väärinkäytöskolmion rationalisointielementin edelleen jalostamisena.

Vaikka väärinkäytösasteikon osa-alueet ovat hyvin lähellä väärinkäytöskolmion vastaavia, on kuitenkin huomattava, että mallien käyttötarkoitus on hieman erilainen. Väärinkäytöskolmio on melko yleisluontoinen malli, ja sitä voidaan käyttää eri tarkoituksiin, kun taas väärinkäytösasteikko on luotu tukemaan nimenomaisesti väärinkäytöksen todennäköisyyden arviointia. Tämän lisäksi se soveltuu erinomaisesti etenkin tilinpäätöksiin liittyvien väärinkäytösten arviointiin, joissa yksilön kokeman paineen havainnointi on usein helpompaa verrattuna muunlaisiin väärinkäytöstyyppeihin (Vousinas 2019, 374; Dorminey ym. 2010, 19–20.)

3 Sisäinen valvonta ja väärinkäytösten estäminen

3.1 Johdon ohjausjärjestelmät ja sisäinen valvonta

Laskentatoimen kirjallisuudessa on erilaisia määritelmiä johdon ohjausjärjestelmille, ja näkökulmien moninaisuuden sekä selvyyden vuoksi on syytä havainnollistaa erilaisten määrittelyjen eroja. Etenkin englanninkielisessä kirjallisuudessa erilaisia kontrolliin liittyviä termejä, kuten *management control, organisational control* ja *strategic control*, käytetään kuvaamaan samankaltaisia tai jopa päällekkäisiä asioita. Yksiselitteistä määritelmää termille johdon ohjausjärjestelmä ei siis ole. Ongelmana on, että eri yhteyksissä ohjausjärjestelmillä tarkoitetaan eri asioita. Yleisellä tasolla ohjausjärjestelmiä voidaan pitää johdon apuvälineinä, jolla organisaatiota pyritään ohjaamaan kohti tavoitteitaan esimerkiksi sopeutumalla muuttuvaan toimintaympäristöön ja minimoimalla riskejä (Merchant & Otley 2007, 785). Kun ylätason sijaan tarkastellaan mitä toimintoja ohjausjärjestelmät pitävät sisällään, on tutkijoiden käyttämissä määritelmissä huomattaviakin eroja. Määrittelyiden erot voivat liittyä esimerkiksi niiden laajuuteen eli siihen, mitkä järjestelmät lasketaan ohjausjärjestelmiksi, tai mihin tarkoitukseen ohjausjärjestelmää käytetään. Ohjausjärjestelmien määritelmille yhteistä on niiden muodostuminen erilaisista ohjausmenetelmistä, joiden avulla johto ohjailee organisaation toimintaa. Ohjausmenetelmät voivat olla yksinkertaisia, kuten ohjeiksi kootut toimintamenetelmät tai monimutkaisempia, kuten erilaiset suorituksen mittausjärjestelmät. (Merchant & Otley 2007, 786.)

Esimerkiksi Simons (1995, 5) määrittelee johdon ohjausjärjestelmät seuraavasti:

> MCS are the formal, information-based routines and procedures manager use to maintain or alter patterns in organizational activities.

Näitä formaaleja järjestelmiä käytetään siis Simonsin mukaan ihmisten toiminnan ohjaamiseen tiedon perusteella. Merchantin ja Otleyn näkemykseen verrattuna Malmin ja Brownin (2008, 290) näkemys ohjausjärjestelmistä on samankaltainen, joskin laajempi. Toisin kuin Simonsin määritelmässä, Malmi ja Brown hyväksyvät ohjausjärjestelmiksi myös muunlaiset kuin tietoon perustuvat järjestelmät. Malmin ja Brownin (2008) viitekehys koostuu viidestä kontrollityypistä: suunnittelusta, kyberneettisistä kontrolleista, palkitsemisjärjestelmistä, hallinnollisista kontrolleista sekä kulttuurisista

kontrolleista. Suunnittelu tarkoittaa etukäteistä kontrollia, jonka avulla toimintaa pyritään ohjaamaan ennalta määritettyyn suuntaan. Kyberneettinen kontrolli muodostuu toiminnan mittaamisesta sekä mittauksesta saadun tiedon vertaamisesta ennalta asetettuihin standardeihin. Tämän tiedon pohjalta toimintaa pyritään usein muuttamaan. Palkitsemisjärjestelmien tavoitteena on motivoida organisaation henkilöstöä työskentelemään tiettyjen tavoitteiden eteen palkitsemalla tavoitteiden saavuttamisesta. Kulttuurinen kontrolli koostuvat arvoista, uskomuksista ja normeista, jotka vaikuttavat työntekijöiden käyttäytymiseen.

Yhteistä ja olennaista Simonsin sekä Malmin ja Brownin näkemyksille on se, että ohjausjärjestelmiksi voidaan katsoa sellaiset kokonaisuudet, joita johto käyttää yrityksessä tapahtuvan toiminnan ohjaamiseen ja siihen vaikuttamiseen. Huomionarvoista on, että joitain järjestelmiä voidaan käyttää eri tavoin eri yrityksissä. Mikäli järjestelmän on tarkoitus tuottaa informaatiota päätöksentekoon, ei sitä silloin Simonsin tai Malmin ja Brownin määritelmän mukaan voida pitää ohjausjärjestelmänä, sillä se ei itsessään ohjaa ihmisten käyttäytymistä.

Sen sijaan Chenhall (2003, 3) omaksuu määritelmän, jonka mukaan johdon ohjausjärjestelmät (engl. *management control systems*) käsittää johdon laskentatoimen järjestelmät (engl. *management accounting systems*) sekä muita organisaation kontrollijärjestelmiä, kuten klaanikontrollin (engl. *clan controls*). Klaanit viittaavat tässä organisaatiokulttuurin ala- tai mikrokulttuureihin, joita tietyt ryhmät organisaatiossa voivat muodostaa. Chenhallin (2003) näkemys on olennaisesti laajempi kuin edellä esitetyt Simonsin tai Malmin ja Brownin määritelmät, sillä se sisältää esimerkiksi tiedon tuottamiseen ja päätöksenteon tukemiseen käytettäviä järjestelmiä, joita organisaation toimijat käyttävät tavoitteidensa saavuttamiseen.

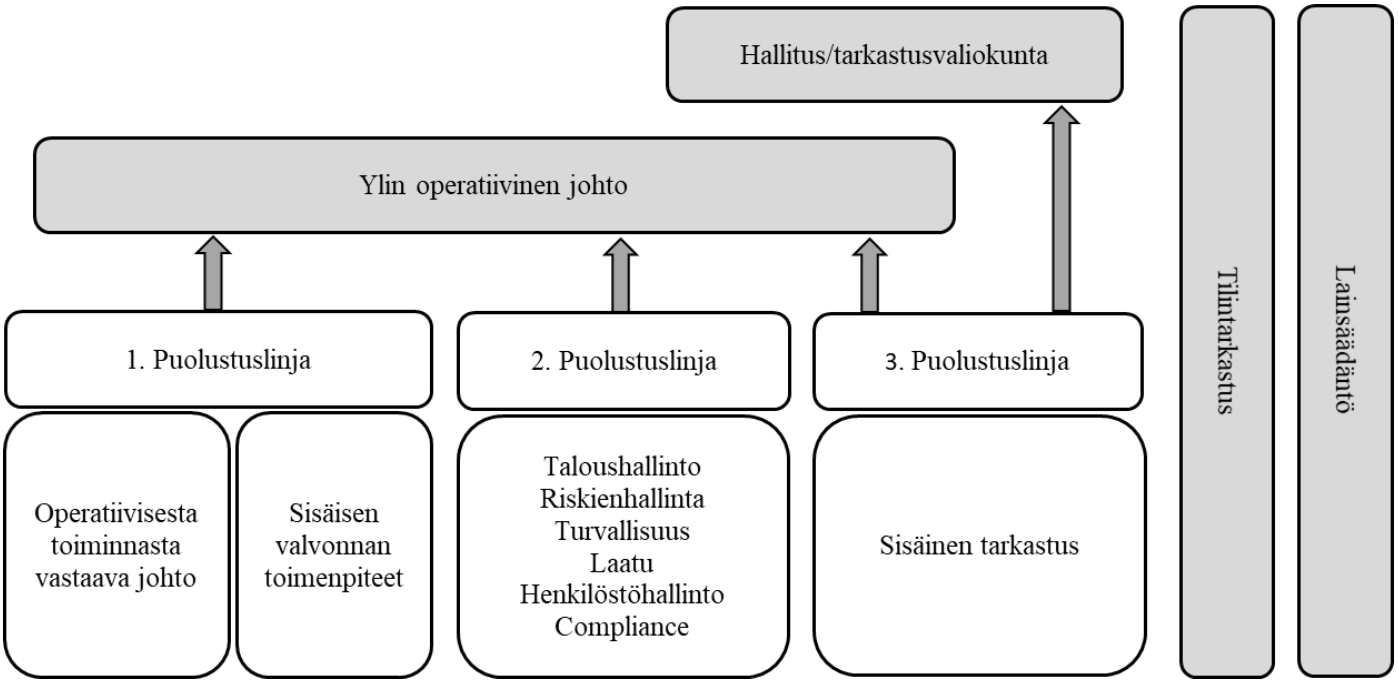
Organisaation ohjaus voi keskittyä myös tavoitteiden asetantaan. Tällöin ohjausmenetelmät keskittyvät työntekijöiden tehtäviin ja työn kannustimiin, ja tavoitteena on työntekijöiden ja yrityksen tavoitteiden yhdenmukaisuus (engl. *goal congruence*). Esimerkiksi Flamholtz ym. (1985, 35–36) määrittelevät organisaation kontrollin melko mekanistisesta näkökulmasta, jossa kontrollijärjestelmien tavoitteena on saada työntekijät työskentelemään organisaation tavoitteiden eteen. Järjestelmien tehtävänä on minimoida työntekijöiden omien ja yrityksen tavoitteiden ristiriidat, ja siten parantaa toiminnan tehokkuutta.

Tässä tutkielmassa sisäinen valvonta sopii parhaiten Malmin ja Brownin (2008) määritelmään johdon ohjausjärjestelmille. Kuten myöhemmin luvussa 3.2 havainnollistetaan, on sisäinen valvonta perinteisesti nähty mekanistisena, formaalina kontrollina, joka keskittyy kirjanpidon oikeellisuuden varmistamiseen sekä organisaation fyysisen omaisuuden turvaamiseen. Esimerkiksi luvussa 3.2 esiteltävä Simonsin (1995) sisäisen valvonnan viitekehys edustaa tätä näkökulmaa. Myöhempi sisäisen valvonnan kirjallisuus on kuitenkin nostanut esiin formaalin ja mekanististen kontrollin rinnalle esimerkiksi epäformaaleja ohjaustoimenpiteitä ja kulttuurin vaikutuksen sisäiseen valvontaan. Simons (1995) toki huomioi muun muassa kulttuurisen kontrollin yrityksen ohjauksen kannalta tärkeinä seikkoina, mutta niiden vaikutusta sisäiseen valvontaan ei kuvata. Sen sijaan luvussa 3.3 esiteltävä COSO-viitekehys on olennaisesti laajempi ja monimutkaisempi kuvaus sisäisestä valvonnasta, ja se huomioi esimerkiksi kulttuurin ja johdon suhtautumisen vaikutuksen sisäiseen valvontaan.

3.1.1 Sisäisen valvonnan rakenne

Sisäinen valvonta on yrityksen ohjausjärjestelmä, jonka avulla yrityksen johto ohjaa organisaation henkilöstön toimintaa (Ratsula 2016a, 13). Sisäisellä valvonnalla yrityksen johto valvoo organisaation toimintaa sekä lakien, strategian sekä sisäisten säännösten noudattamista. (Ikäheimo ym. 2014, 117–119 ; Sihvonen & Uusi-Hautamaa 2019, 99–100.) Sisäinen valvonta on jatkuva prosessi, ja sitä toteutetaan samanaikaisesti kaikkialla organisaatiossa. Käytännön tasolla se toteutuu esimerkiksi esimiesten valvoessa alaisiaan ja johdon seuratessa eri yksiköiden suoritusmittareita poikkeamien varalta. Ratsula 2016a, 13–14.) Sisäistä valvontaa toteutetaan kaikissa yrityksissä jossain muodossa. Suuremmissa yrityksissä sisäinen valvontajärjestelmä saattaa olla hyvin formaali, ja sitä ohjaavat organisaation omien tarpeiden lisäksi myös listayhtiöiden hallinnointikoodi sekä lainsäädäntö (esim. Osakeyhtiölaki 6:2 ja 6:16). Pienemmissä yrityksissä valvonta on sen sijaan usein vapaamuotoisempaa, eikä se välttämättä sisällä lainkaan formaaleja tai dokumentoituja ohjausmenetelmiä. (Ikäheimo ym. 2014, 120.) Sisäisen valvonnan järjestäminen on yrityksen hallituksen, toimitusjohtajan ja ylimmän johdon vastuulla. Kuten luvussa 3.2.2 havainnollistetaan, edellä mainitut tahot luovat sisäisen valvonnan suuntaviivat, jotka alemman operatiivisen johdon toimesta otetaan käytäntöön. (Ratsula 2016a 54, 67–68.)

Sisäisen valvonnan roolia sekä kontrolliin liittyvien vastuiden jakamista voidaan tarkemmin havainnollistaa alla olevalla puolustuslinjamallilla. Malli tukee hyvin esimerkiksi myöhemmin luvussa 3.3 esiteltävää COSOn sisäisen valvonnan viitekehystä havainnollistamalla sisäisen valvonnan vastuunjakoa. Tämän vastuunjaon tulee olla riittävän selkeä, jotta organisaation jäsenet ja sen sisäiset ryhmät ymmärtävät oman osuutensa riskienhallinnassa ja kontrollissa. (COSO 2015, 1.) Samalla mallin vastuujako toimii pohjana eri ryhmien väliselle yhteistyölle, jotta sisäisen valvonnan aukot sekä päällekkäisyydet pystytään eliminoimaan (IIA 2013, 1). Mallin lähtökohta on, että hallitus on viime kädessä vastuussa sisäisen valvonnan toimivuudesta, ja ylin johto sekä toimitusjohtaja vastaavat sen järjestämisestä ja päivittäisestä toiminnasta (Sihvonen & Uusi-Hautamaa 2019, 73). Ylin johto ja hallitus on kuvattu mallin yläosassa. He eivät ole varsinaisesti osa puolustuslinjoja, vaan toimivat suuntaviivojen antajina ja valvovat sisäisen valvontajärjestelmän toimintaa. He ovat kuitenkin lopullisessa vastuussa sisäisen valvonnan toimivuudesta. Mallissa hallituksen ja ylimmän johdon tehtävänä on suunnitella, toteuttaa ja valvoa sisäisen valvontajärjestelmän toimintaa. (COSO 2015, 4.)



Kuvio 4 Puolustuslinjamalli, mukaillen IIA 2013, 2; Ratsula 2016a, 56.

Mallin alaosa jakautuu kolmeen linjaan. Ensimmäinen puolustuslinja käsittää operatiivisesta liiketoiminnasta vastuussa olevan johdon ja esimiehet (Ratsula 2016a, 55). Ensimmäisen linjan tehtävänä on omistaa ja hallita riskejä. (COSO 2015, 2.) Operatiiviset johtajat ja esimiehet ovat vastuussa riskeihin vastaamisesta päivittäisessä työskentelyssä. Heidän tehtävänään on tunnistaa, arvioida ja kontrolloida riskejä, sekä huolehtia sisäisen valvonnan toimenpiteiden toteuttamisesta vastuualueellaan. (IIA 2013, 3.) Ensimmäinen puolustuslinja siis sijoittuu jokapäiväiseen liiketoimintaan, jossa johtajat, esimiehet ja työntekijät ovat jatkuvasti tekemisissä riskien ja ohjausmenetelmien kanssa.

Toinen puolustuslinja koostuu erilaisista tukitoiminnoista, joiden tehtävä sisäisen valvonnan näkökulmasta on tukea riskienhallintaa ja tarkkailla oman vastuualueensa riskejä. Lisäksi ne voivat tuottaa tietoa johdolle ja hallitukselle muun muassa riskeistä, sisäisen valvonnan tilasta ja ohjausmenetelmien tehokkuudesta. (Ratsula 2016a, 78; COSO 2015, 6.) Toiseen puolustuslinjaan kuuluvat toiminnot ovat eri organisaatioissa erilaisia, mutta yleensä suuremmissa yrityksissä toiseen puolustuslinjaan kuuluvat esimerkiksi riskienhallinta- ja *compliance* -funktiot sekä taloudellisista riskeistä ja raportoinnista vastaavat yksiköt (IIA 2013, 4). Nämä toiminnot ovat erillään varsinaisesta liiketoiminnasta ja siten ensimmäisestä puolustuslinjasta, mutta tyypillisesti ne ovat operatiivisen johdon valvonnan alaisia. (COSO 2015, 6).

Viimeinen, kolmas puolustuslinja muodostuu itsenäisestä ja riippumattomasta varmennustoiminnosta, jonka virkaa yleensä toimittaa sisäinen tarkastus. Sen tehtävänä on tuottaa ylimmälle johdolle riippumatonta tietoa ensimmäisen ja toisen puolustuslinjan toiminnasta. (Ratsula 2016a, 85.) Tällä pyritään varmistamaan, että sisäinen valvonta toimii johdon ja hallituksen linjan mukaisesti. Sen tehtävänä ei siten ole ohjata, johtaa tai suunnitella ohjausmenetelmiä, vaan tuottaa objektiivista informaatiota päätöksentekijöiden käyttöön. (COSO 2015, 3; 8.)

Mallin oikealle laidalle jäävät ulkoiset tekijät, kuten tilintarkastaja sekä lainsäätäjät. Vaikka ne eivät ole osa organisaatiota, vaikuttavat ne organisaation toimintaan ja muun muassa sisäiseen valvontaan. Lainsäätäjät asettavat yrityksille vaatimuksia johtamistapaan ja sisäiseen valvontaan liittyen, ja tilintarkastajat saattavat huomata esimerkiksi raportointiin liittyviä asioita, joita organisaation sisällä ei ole huomattu. Siten nämä ulkoiset toimijat voidaan nähdä ylimääräisinä puolustuslinjoina. (COSO 2015, 9.)

3.1.2 Sisäisen valvonnan tausta ja merkitys

Perinteisesti sisäinen valvonta on liitetty vahvasti taloudelliseen ja laskentatoimen kontrolliin, etenkin taloudellisen raportoinnin luotettavuuden varmistamiseen sekä yrityksen varojen turvaamiseen (Maijoor 2000, 104–105; Arwinge 2014, 18). Tämä kapeampi määritelmä pohjautuu Ratsulan (2020, 40) mukaan etenkin kirjanpidon ja tilintarkastuksen teoriaan, jonka mukaan tilintarkastajien tehtävänä on perinteisesti ollut velvollisuuksiensa täyttäminen tiettyjen standardien puitteissa. Tämä teoreettinen pohja on suoraan vaikuttanut sisäisen valvonnan määritelmiin ja käytännön soveltamiseen.

Sisäisen valvonnan ensimmäiset määritelmät ovat 1900-luvun alkupuoliskolta, ja näissä määritelmissä korostuivat nimenomaan kirjanpidon ja taloudellisen informaation oikeellisuus. Esimerkiksi AIA:n (1936) julkaisussa sisäinen valvonta on määritelty seuraavasti:

> …those measures and methods adopted within the organization itself to safeguard the cash and other assets of the company as well as check the clerical accuracy of the bookkeeping.

AIA:n vuoden 1936 määritelmän mukaisesti sisäisen valvonnan tehtävänä on varojen turvaaminen sekä kirjanpidon oikeellisuuden varmistaminen. Tämä määritelmä edustaa perinteistä näkemystä sisäisen valvonnan roolista, jota käsitellään tarkemmin luvussa 3.2.

Heierin ym. (2005, 45–46) mukaan sisäistä valvontaa pyrittiin 1900-luvun alkupuolella kehittämään tilintarkastajan toiminnan tueksi. Jatkuvaluonteinen sisäinen valvonta nähtiin keinona pienentää tilintarkastuksen kustannuksia ja vähentää tilintarkastajan työmäärää. Tämän lähestymistavan vahva asema on puolestaan vaikuttanut sisäisen valvonnan kirjallisuuteen, joka on tilintarkastustaustansa takia keskittynyt raportoinnin luotettavuuteen. (Ratsula 2020, 42–43). Tästä näkökulmasta sisäinen valvonta keskittyi palvelemaan tilintarkastusprosessin tehokkuutta, ja sen tavoitteena on liiketoimissa ja prosesseissa ilmenevien virheiden ja epäsäännönmukaisuuksien ehkäiseminen, jonka kautta varmistetaan tilinpäätösten riittävä luotettavuus (Merchant & Otley 2007, 787; Arwinge 2014, 18).

Erityisen sisäisen valvontajärjestelmän tarve selkiytyi Heierin ym. (2005, 49) mukaan viimeistään 1900-luvun puolivälissä, kun organisaatioiden sisäisiä petoksia ja väärinkäytöksiä alkoi tulla enenevässä määrin ilmi. Myös väärinkäytösten sekä valkokaulusrikollisuuden tutkimuksen ensimmäiset merkittävät kehitysaskeleet, kuten

väärinkäytöskolmio, sijoittuvat 1900-luvun puoliväliin. Nykyään sisäinen valvonta on olennainen osa yrityksen johtamisjärjestelmiä sekä sen riskienhallintaa. Parhaimmillaan tehokkaasti riskejä minimoiva sisäinen valvonta tarjoaa yritykselle kilpailuetua, kun se pystyy tarttumaan liiketoimintamahdollisuuksiin, jotka heikomman kontrollin tapauksessa todettaisiin liian riskialttiiksi. (Moeller 2013, 2.)

Sisäisellä valvontajärjestelmällä on tärkeä rooli väärinkäytösten vastaisessa työssä. Vahvan sisäisen valvonnan avulla organisaatio voi vähentää väärinkäytösten todennäköisyyttä. Peilaten väärinkäytöstimantin teoriaan, väärinkäytösten riskiä pienennetään kohdistamalla toimia timantin eri osa-alueisiin. Yrityksellä on eittämättä hyvin rajalliset mahdollisuudet puuttua esimerkiksi yksilön taloudelliseen tilanteeseen. Sen sijaan esimerkiksi mahdollisuuksiin ja yksilön kykyyn tehdä väärinkäytös voidaan sisäisen valvonnan ohjaustoimenpitein puuttua. Esimerkiksi Bonnyn ym. (2015, 459) tutkimuksessa haastatellut, väärinkäytöksistä kiinni jääneet henkilöt mainitsivat heikkojen ohjausmenetelmien vaikuttaneen merkittävästi tai vähintään kohtalaisesti väärinkäytöksen toteuttamiseen. Sen sijaan kukaan väärinkäyttäjistä ei pitänyt ohjausmenetelmiä irrelevantteina, mikä myös osaltaan alleviivaa sopivien menetelmien tärkeyttä. Samoin PwC:n (2020) raportin mukaan väärinkäytösten torjuntaan etukäteen tehdyt investoinnit vähentävät väärinkäytösten aiheuttamia vahinkoja. Yritykset, joissa oli selkeät protokollat väärinkäytösten varalle, säästivät sekä väärinkäytösten aiheuttamissa suorissa kustannuksissa että niiden aiheuttamien vahinkojen korvauskustannuksissa. Kuten luvussa 2.2.1 havainnollistettiin, altistaa heikosti toimiva sisäinen valvontajärjestelmä organisaation todennäköisemmin suuremmille väärinkäytösriskeille. Zakarian ym. (2016, 1158) mukaan huonosti toimiva sisäinen valvonta vähentää väärinkäyttäjän kiinnijäämisriskiä, ja siten saattaa lisätä väärinkäytöksen houkuttelevuutta. Tätä taustaa vasten sisäinen valvonta vaikuttaa väärinkäytösten todennäköisyyteen, sekä niiden vahinkoihin yhtäältä ennaltaehkäisevillä toimenpiteillä että toisaalta erilaisten tarkastusten avulla, jolloin indikaattoreita tapahtuneista väärinkäytöksistä etsitään jälkikäteen. Tätä mekaniikkaa avataan tarkemmin seuraavissa alaluvuissa.

3.2 Sisäisen valvonnan perinteinen näkökulma

Etenkin varhaisemmassa laskentatoimen kirjallisuudessa sisäinen valvonta on yleensä nähty yrityksissä omana irrallisena toimintonaan. Viime vuosikymmeninä on kuitenkin

yleistynyt ajatus sisäisestä valvonnasta osana yrityksen ohjausjärjestelmäkokonaisuutta, jolloin sisäinen valvonta toimii yhteystyössä muiden ohjausjärjestelmien kanssa. Samoin myös sisäisen valvonnan käsite on laajentunut perinteisestä kirjanpidon ja tilintarkastuksen kontrollista sekä aineellisen omaisuuden suojaamisesta, ja uudempi sisäisen valvonnan kirjallisuus on kiinnittänyt enemmän huomiota sosiaalisiin koontrolleihin osana sisäistä valvontaa. Ratsulan (2020, 44) mukaan perinteinen lähestymistapa käsittää sisäisen valvonnan lähinnä virheiden sekä väärinkäytösten ehkäisemisenä, huomaamisena ja korjaamisena.

Esimerkiksi Simonsin (2013; 1995) näkemys sisäisestä valvonnasta edustaa perinteistä tyyliä, jossa sisäinen valvonta linkittyy vahvasti kirjanpitoon ja tilintarkastukseen, ja pyrkii eliminoimaan niissä tapahtuvia virheitä toiminnan sujuvuuden varmistamiseksi. Simonsin (2013, 280; 1995, 84–85) viitekehyksessä sisäinen valvonta keskittyy yrityksen varojen suojaamiseen sekä yrityksen informaation luotettavuuden varmistamiseen. Sisäisen valvonnan Simons (2013, 280) määrittelee seuraavasti:

> The policies and procedures designed to (1) ensure reliable accounting information and (2) safeguard company assets.

Sisäinen valvonta palvelee etenkin Simonsin *Levers of Control* -mallin diagnostista ohjausta. *Levers of Control* -viitekehyksessä diagnostinen ohjaus on yrityksen toiminnan seurantaa ja poikkeamiin reagoimista, ja diagnostiset kontrollijärjestelmät toimivat usein palautesilmukoiden (engl. *feedback loop*) kautta. Diagnostinen ohjaus on varsinkin perinteisesti toiminut yrityksen ohjauksen selkärankana, ja sen tavoitteena on ennen kaikkea ennustettavuuden ja tavoitteiden saavuttaminen. Diagnostiset kontrollit ovat formaaleja tietojärjestelmiä, joilla johtajat valvovat yrityksen toimintaa. (Simons 1995, 59.)

Simonsin mukaan sisäisen valvonnan ohjausmenetelmät voidaan jakaa kolmeen luokkaan:

- Rakenteelliset turvamekanismit
- Henkilöstöön liittyvät turvamekanismit
- Järjestelmien turvamekanismit

Rakenteellisten turvamekanismien liittyvät esimerkiksi tehtävien eriyttämiseen, sisäiseen tarkastukseen sekä päätös- ja muihin valtuutuksiin. Niiden tehtävä on taata yrityksen varoja ja tietoja käsittelevien henkilöiden riittävät valtuudet. (Simons 2013, 280.)

Henkilöstöön liittyvillä turvamekanismeilla varmistutaan yrityksen työntekijöiden riittävästä osaamistasosta ja heidän käytettävissään olevista resursseista. Nämä mekanismit voivat sisältää esimerkiksi riittävän koulutuksen ja avaintehtävien vuorottelun. (Simons 2013, 283.)

Järjestelmien turvamekanismit liittyvät sen sijaan yrityksen järjestelmissä olevan tiedon luotettavuuteen, riittäviin kirjausketjuihin (engl. *audit trail*) sekä pääsyn rajoittamiseen yrityksen tietokantoihin. Näiden toimenpiteiden avulla varmistetaan transaktioiden sekä johdon raportoinnin ajantasaisuus ja oikeellisuus. (Simons 2013, 282; 1995, 84–85.) Sisäinen valvonta turvamekanismeineen palvelee yrityksen ohjausjärjestelmiä, ja takaamalla esimerkiksi tietojen oikeellisuutta varmistaa muiden ohjausjärjestelmien toiminnan (Simons 1995, 85).

Simonsin näkemys sisäisestä valvonnasta nojaa vahvasti teknisiin ohjausmenetelmiin, joiden avulla virheitä ja poikkeamia pyritään havaitsemaan. Ratsula (2020, 48) huomauttaa, että ainoastaan teknisiin menetelmiin nojaava järjestelmä saattaa toimia vajavaisesti verrattuna myös sosiaalista ja informaalia kontrollia hyödyntävään sisäiseen valvontajärjestelmään. Simonsin (1995, 86) viitekehyksessä sosiaalinen kontrolli on osa johdon ohjausta, ja sisäinen valvonta taas tästä erillinen järjestelmä, joka luo pohjan johdon ohjausjärjestelmien toiminnalle.

Yllä esitetty perinteinen sisäisen valvonnan konsepti on uudemman laskentatoimen kirjallisuuden myötä laajentunut sisältämään laskentatoimen ja kirjanpidon ohjaustoimenpiteiden lisäksi myös muita kontrollin muotoja (Maijoor 2000, 105). Kun sisäisen valvonnan kirjallisuus aiemmin nojasi vahvasti laskentatoimen ja tilintarkastuksen teoriaan, on uudempi sisäisen valvonnan kirjallisuus saanut vaikutteita esimerkiksi riskienhallinnan, johdon ohjauksen ja organisaatioiden tutkimuksesta. Näiden tutkimusalojen teoriat ovat osaltaan vaikuttaneet sisäisen valvonnan kirjallisuuden kontrollikäsityksen laajenemiseen (Ratsula 2020, 49; Maijoor 2000, 105.) Kontrollikäsityksen laajenemisen ja sisäisen valvonnan merkityksen korostumisen myötä kasvoi myös tarve uusille viitekehyksille, jotka tarkastelevat mekanistisen ohjauksen lisäksi myös muunlaisia sisäiseen valvontaan liittyviä ohjausmekanismeja.

Mekanistisella ohjauksella tarkoitetaan näkökulmaa, jossa ohjausjärjestelmien menetelmät ovat formaaleja johdon käyttämiä instrumentteja. Nämä instrumentit nähdään yksilöinä, eikä mekanistinen katsantokanta huomioi ohjausmenetelmien vaikutuksia muihin menetelmiin. (van der Meer-Kooistra & Scapens 2008, 367.)

3.3 COSO-malli: sisäisen valvonnan laaja näkökulma

Treadway Commissionin alun perin vuonna 1992 esittelemä sisäisen valvonnan COSO-viitekehys on Suomessakin laajasti käytössä oleva sisäisen valvonnan viitekehys, jota yritykset voivat käyttää apuna sisäisen valvontansa järjestämisessä. Viitekehystä täydennettiin myöhemmin, ja vuonna 2013 julkaistiin päivitetty versio. Päivitetyn mallinperusidea on kuitenkin sama kuin alkuperäisessä. Suurin muutos alkuperäiseen malliin oli 17 periaatetta, joiden tavoitteena oli selkiyttää mallin käyttäjille sisäisen valvonnan komponenttien toimintaa ja käyttöönottoa. Nämä periaatteet esitellään yksityiskohtaisemmin tulevissa alaluvuissa.

COSOn sisäisen valvonnan malli on tarkoituksella luotu yleisluontoiseksi, jolloin sen soveltaminen erilaisissa organisaatioissa olisi mahdollista (Moeller 2013, 37). Samalla mallin tehokas hyödyntäminen vaatii käyttäjältään hyvää tuntemusta niin itse mallista kuin sitä käyttävästä yrityksestäkin.

COSO (2013) määrittelee sisäisen valvonnan seuraavasti:

> Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.

COSOn sisäisen valvonnan määritelmä on olennaisesti Simonsin (2013) vastaavaa laajempi, sillä Simonsin määritelmässä sisäinen valvonta on oma erillinen kokonaisuutensa, joka palvelee diagnostista ohjausta. Simonsin malli koostuu pitkälti kirjanpidollisista ja fyysisistä toimenpiteistä, jotka liittyvät pitkälti tiedon oikeellisuuteen ja näin varmistavat muiden ohjausjärjestelmien toiminnan. Verrattuna COSO-malliin, Simonsin näkemys on melko yksipuolinen, sillä sisäisellä valvonnalla on tiedon oikeellisuuden lisäksi monia muitakin funktioita. COSO-mallissa sisäinen valvonta on jatkuva prosessi, joka kattaa koko organisaation ja sen kaiken toiminnan. Myös Moellerin (2013, 3) mukaan sisäinen valvonta voidaan määritellä jatkuvina toisiinsa liittyvinä toimintoina yrityksen sisällä, eikä niinkään omana irrallisena systeeminään. Ratsulan

(2016, 14) mukaan sisäinen valvonta muodostuu kaikilla organisaation tasoilla jatkuvasti toteutettavista ohjausmenetelmistä, joiden avulla hallitaan riskejä ja ohjataan organisaatiossa tapahtuvaa toimintaa. Nämä menetelmät ovat hyvässä valvontajärjestelmässä usein rakennettu sisään liiketoimintaprosesseihin, jolloin niiden erottaminen selkeästi omaksi järjestelmäkseen saattaa olla hankalaa.

COSO-mallissa sisäinen valvonta on kuvattu kuutiona. Kuution päällimmäinen sivu kuvaa tavoitteita, joita tehokkaalla sisäisellä valvonnalla pyritään saavuttamaan. Mallin oikea sivu kuvaa organisaation rakennetta, sillä sisäisen valvonnan tulee kattaa kaikki organisaation tasot. Kuution julkisivussa on esitetty sisäisen valvonnan komponentit, jotka kuvaavat sisäisen valvonnan toimintaa käytännössä.

Kuvio 5 Sisäisen valvonnan COSO-viitekehys (COSO 2013)

Sisäisen valvonnan tavoitteiden tehtävänä on tukea yrityksen toimintaa ja sen strategisia tavoitteita. Julkisivussa esitetyt sisäisen valvonnan komponentit sisältävät ne välineet, joilla taas sisäisen valvonnan tavoitteet pyritään saavuttamaan. Monet sisäisen valvonnan toimenpiteet voivat tukea yhtä, kahta tai kaikkia kolmea sisäisen valvonnan tavoitetta, ja

monet toimenpiteet ovat myös vuorovaikutussuhteessa toisiin toimenpiteisiin sekä sisäisen valvonnan tavoitteiden saavuttamiseen.

COSO-mallia voidaan käyttää työkaluna, kun yrityksen johto kuvaa ja suunnittelee omaa sisäistä valvontajärjestelmäänsä. Se tarjoaa joustavan lähtökohdan sisäisen valvonnan tarkasteluun, ja sen periaatteita voidaan käyttää ja soveltaa erilaisissa organisaatioissa. Samoin sen avulla voidaan tarkastella yrityksen valvontajärjestelmälle asetettavia tavoitteita, vaatimuksia sekä niitä riskejä, joihin valvonnalla pyritään vastaamaan. (Ratsula 2016a, 58.)

Vaikka COSO-mallissa sisäinen valvonta nähdään jatkuvana ja itseään toistavana prosessina, on sillä myös selkeä kehämäinen etenemistapa. Kuten seuraavissa alaluvuissa havainnollistetaan, ovat mallin komponentit riippuvaisia toisistaan. Esimerkiksi valvontatoimenpiteisiin kuuluvat ohjausmenetelmät on suunniteltava arvioitujen riskien perusteella tehokkaan sisäisen valvonnan saavuttamiseksi. Mikäli organisaation ohjaustoimenpiteet suunnitellaan perehtymättä riskeihin, toimii sisäinen valvonta tehottomasti eikä se kykene saavuttamaan tavoitteitaan. Tehoton toiminta myös kuluttaa organisaation resursseja turhaan. (Sihvonen & Uusi-Hautamaa 2019, 92.)

3.3.1 Sisäisen valvonnan tavoitteet, komponentit ja rakenne

Kuution yläsivulla on jaoteltuna sisäisen valvonnan tavoitteet, liiketoiminnan (engl. *operations*), raportoinnin (engl. *reporting*) ja *compliance*-tavoitteet. On huomattava, että vaikka mallissa tavoitteet on esitetty omissa laatikoissaan, kontekstista riippuen yksittäinen tavoite voi liittyä useampaan kuin yhteen kategoriaan. Esimerkiksi tietyin väliajoin tuotettava kauden loppuraportti voidaan käyttötarkoituksesta riippuen lukea raportoinnin tavoitteisiin. Mikäli raportti tukee operatiivisen johdon toimintaa, voidaan se lukea myös liiketoiminnan tavoitteisiin. (Moeller 2013, 35.)

Liiketoimintaan liittyvät tavoitteet liittyvät organisaation päivittäisen toiminnan tehokkuuteen. (COSO 2013). Sisäisen valvonnan tehtävänä on sopivien ohjausmenetelmien avulla auttaa yritystä saavuttamaan asettamansa liiketoiminnan tavoitteet. Tavoitteet asetetaan aliyksiköille, kuten divisioonille ja liiketoimintayksiköille, johtamalla ne organisaatiotason tavoitteista. Liiketoiminnan tavoitteet voivat liittyä esimerkiksi prosessien ja laadun parantamiseen,

kustannussäästöihin tai asiakkaiden ja työntekijöiden tyytyväisyyteen. (Moeller 2013, 34.)

COSO-mallissa sisäisen valvonnan tavoitteena on myös turvata yrityksen raportoinnin luotettavuus. Yritykset tuottavat raportteja sekä sisäiseen että ulkopuoliseen käyttöön, kuten sijoittajille. Lisäksi raporttien sisältämä informaatio voi olla taloudellista tai ei-taloudellista. Ulkoisen raportoinnin on noudatettava esimerkiksi voimassa olevia kirjanpitosäädöksiä, kun taas sisäisen raportoinnin tehtävänä on muun muassa palvella yrityksen tavoitteita ja strategiaa. (COSO 2013; Moeller 2013, 33–34.) COSO-malli koki vuoden 2013 päivityksessä myös raportoinnin osalta muutoksia, sillä alkuperäinen COSO-malli keskittyi lähinnä organisaation ulkopuolelle suuntautuvaan taloudelliseen raportointiin. Tältä osin päivitettyä versiota voidaan pitää alkuperäistä kattavampana. (Sihvonen & Uusi-Hautamaa 2019, 82.)

Compliance-kategorian tavoitteet liittyvät yritystä koskevan lainsäädännön ja muun sääntelyn noudattamiseen (COSO 2013). Yrityksen sisäiset säännöt ja ohjeet ohjaavat sen henkilöstön toimintaa näiden säännösten mukaiseksi. Sääntöjen noudattamista voidaan valvoa esimerkiksi sisäisen tarkastuksen ja laadunvalvonnan avulla. (Moeller 2013, 34.)

COSOn sisäisen valvonnan mallin julkisivun muodostavat sen sisäisen valvonnan komponentit. Nämä komponentit ovat:

- Ohjausympäristö (engl. *control environment*)
- Riskien arviointi (engl. *risk assessment*)
- Valvontatoimenpiteet (engl. *control activities*)
- Informaatio ja viestintä (engl. *information & communication*)
- Seurantatoimenpiteet (engl. *monitoring activities*)

Vuoden 2013 päivitettyyn COSO-malliin lisätyt 17 periaatetta perustuvat kukin omaan komponenttiinsa. COSOn (2013) mukaan ottaessaan käyttöön mallin periaatteet ja sisäisen valvonnan komponentit organisaatio kykenee järjestämään sisäisen valvontansa tehokkaasti. Sihvosen ja Uusi-Hautamaan (2019, 83) mukaan mallin tehokas käyttöönotto ainakin mallin periaatteiden läpikäymisen, sopeuttamisen oman organisaation kontekstiin ja sisäiseen valvontaan liittyvien vastuiden kirjaamisen. Mallin komponentit ovat suorassa yhteydessä toisiinsa, ja sekä komponentit että niihin liittyvät periaatteet palvelevat jokaista sisäisen valvonnan tavoitetta. Organisaatio pyrkii kohti

liiketoiminnan, raportoinnin sekä *compliance*-tavoitteitaan sisäisen valvonnan avulla, joten sisäisen valvonnan komponentit kuvaavat niitä toimia, joita organisaation täytyy tavoitteidensa saavuttamiseksi tehdä. (COSO 2013.)

COSO-mallin oikean sivun dimensio kuvaa organisaation rakennetta. Sisäinen valvonta kattaa mallin mukaisesti koko organisaation itsensä, sen divisioonat, liiketoimintayksiköt ja funktiot. Organisaation kontrollin tulisi kattaa kaikki organisaation tasot, ja niiden tulisi olla yhteneväisiä halutun sisäisen valvonnan tason saavuttamiseksi. (Moeller 2013, 36–37). Organisaation rakenteen ja sisäisen valvonnan suhdetta voidaan tarkastella myös aiemmin luvussa 3.1 esitellyn kolmen puolustuslinjan mallin avulla. Esimerkiksi COSOn viitekehyksen avulla organisaatio voi määritellä itselleen sopivan sisäisen valvonnan mallin, ja hyödyntää puolustuslinjamallia määritellessään sisäisen valvonnan vastuujaon. Yleisluontoisena mallina COSOn viitekehys soveltuu eri organisaatioille niiden rakenteesta riippumatta. Organisaation tavoitteet sekä sisäisen valvonnan komponentit tulee ulottaa kaikille tasoille aina yritystasolta yksittäisiin toimintoihin ja funktioihin.

3.3.2 Ohjausympäristö

Ohjausympäristö on yrityksen sisäisen valvonnan perusta. Se muodostuu yrityksen sisäisistä standardeista, prosesseista ja rakenteista. COSOn (2013) mukaan yrityksen ylin johto on vastuussa sisäisen valvonnan linjan luomisesta. Niin kutsuttu *tone at the top* vaikuttaa pitkälti sisäisen valvonnan onnistumista, ja sen tavoitteena on selventää johdon asettama sisäisen valvonnan tavoitetila myös yrityksen alemmille tasoille. Ohjausympäristö ulottuu koko organisaation läpi, ja sisältää siten esimerkiksi yrityksen eettiset ohjeet, palkitsemisjärjestelmät sekä suoritusmittarit. Alemman tason operatiivisen johdon sekä esimiestien tehtävän taas on kommunikoida johdon sisäisen valvonnan linja oman vastuualueensa alaisille (Ratsula 2016, 95).

COSOn (2013) ohjausympäristöön liittyvät seuraavat periaatteet:

1. Organisaation sitoutuminen lahjomattomuuteen ja eettisiin arvoihin.
2. Hallitus on riippumaton yrityksen johdosta ja varmistaa sisäisen valvonnan toiminnan.
3. Johto luo rakenteet, raportointikanavat, valtuudet ja vastuut tavoitteiden saavuttamiseksi.
4. Osaavien henkilöiden värväämineni, kehittäminen ja sitouttaminen organisaatioon.

5. Yksilöt ovat vastuussa sisäisen valvonnan toiminnasta.

Yllä olevia periaatteita soveltamalla organisaatio kykenee COSOn mukaan luomaan toimivan ja koko organisaation kattavan ohjausympäristön, joka toimii perustana yrityksen sisäiselle valvonnalle. Yksittäisen organisaation ohjausympäristöön vaikuttavat monet sisäiset ja ulkoiset tekijät, kuten organisaation historia, arvot, markkinat ja toimintaympäristö (Moeller 2013, 42). Sen periaatteiden mukaisesti ohjausympäristön muotoutumiseen vaikuttavat vahvasti organisaation ylätason linja eli *tone at the top*. Tähän linjaan vaikuttavat johdon muodollisen viestinnän lisäksi vahvasti myös ei-muodollinen esimerkki sekä johdon käytännön toiminta. (Ratsula 2020, 54; Ratsula 2016b; Lamberton ym. 2005.)

Sihvonen ja Uusi-Hautamaa (2019, 84–85) korostavat myös keskijohdon suhtautumisen, ns. *tone in the middle*, tärkeyttä. Esimerkiksi hallituksen viestit saattavat jäädä rivityöntekijälle etäiseksi, ja oman lähiesimiehen esimerkki ja käytös saattavat vaikuttaa työntekijöihin huomattavasti enemmän. Tästä syystä johdon on pystyttävä jalkauttamaan haluamansa sisäisen valvonnan linja keskijohdon kautta työntekijöille.

Vahvan ohjausympäristön luomalla organisaatio kestää paremmin sekä sen sisäisen että sen ulkoisen toimintaympäristön aiheuttamia paineita. Ohjausympäristö voidaan mieltää myös sisäisen valvonnan kulttuuriksi, jolloin oikeanlainen ja johdon tavoittelema kulttuuri palvelee myös muita sisäisen valvonnan komponentteja. (Moeller 2013, 42.) Tähän ajatukseen pohjaten sisäisen valvonnan onnistuminen on pitkälti kiinni organisaation kulttuurista. Vahva ohjausympäristö tukee muiden mallin komponenttien toimintaa. Samalla kuitenkin heikolla tai puutteellisella ohjausympäristöllä on vastaavasti negatiivinen vaikutus muihin komponentteihin. (Klamm & Weidenmier Watson 2009, 3.)

3.3.3 Riskien arviointi

Riskien arvioinnin tarkoituksena on tunnistaa yrityksen toimintaa uhkaavia riskejä sekä toimenpiteitä näiden riskien minimoimiseksi (Ratsula 2016a, 61). COSOn (2013) määritelmän mukaan riski tarkoittaa jonkin organisaatiolle epäsuotuisan tapahtuman todennäköisyyttä. Riskien arviointi on jatkuva ja iteratiivinen prosessi, jolla pyritään tunnistamaan ja arvioimaan organisaation tavoitteita uhkaavia riskejä, ja se muodostaa pohjan organisaation riskienhallinnalle.

Riskien arviointi on sidoksissa organisaation tavoitteisiin. Johdon on kirjattava sisäisen valvonnan tavoitteet riittävän selkeästi, jotta niihin liittyviä riskejä voidaan tarkastella. (COSO 2013; Sihvonen & Uusi-Hautamaa 2019, 85.)

Riskien arvioinnin periaatteet ovat:

6. Organisaation tavoitteiden selkeä määrittely.
7. Tavoitteisiin liittyvien riskien tunnistaminen.
8. Väärinkäytösten mahdollisuuden arviointi.
9. Toimintaympäristön muutosten tunnistus ja arviointi.

Riskien arvioinnin komponenttiin liittyvät periaatteet lähtevät liikkeelle organisaation tavoitteiden selkiyttämisestä, ja pyrkivät kiinnittämään mallin käyttäjän huomion näihin tavoitteisiin liittyviin riskeihin (Ratsula 2020, 55). Periaatteet huomioivat sekä sisäisiä että ulkoisia riskejä korostamalla väärinkäytöksiä sekä toimintaympäristön muutosten tuomat uhkia. Näiden riskien tunnistaminen vaatii organisaatiolta uusien muutosten ja ilmiöiden jatkuvaa seurantaa ja tunnistamista. Riskien tunnistamisen lisäksi niiden tarkempi analyysi muodostaa pohjan näiden riskien hallinnalle (Ratsula 2020, 55).

Väärinkäytösriskiä voidaan arvioida hyödyntämällä esimerkiksi luvussa 2 esiteltyjä malleja. Kuten muidenkin riskien myös väärinkäytösriskien arvioimisen lähtökohtana on tunnistaa erilaiset väärinkäytöstyypit. COSO-malli painottaa etenkin omaisuuseriin liittyvien väärinkäytösten, korruption ja raportoinnin vääristelyn riskejä (Moeller 2013, 69–70). Tunnistamisen lisäksi organisaation on arvioitava omaa sisäistä kulttuuriaan ja työympäristöään, ja miten todennäköistä tietyn väärinkäytöksen tapahtuminen on. Esimerkiksi väärinkäytöskolmion avulla voidaan arvioida työntekijöiden kokemia paineita ja kannustimia sekä mitä mahdollisia tilaisuuksia tietynlaiseen väärinkäytökseen on. (Ratsula 2016, 116–117.)

3.3.4 Valvontatoimenpiteet

Kuten aiemmin on todettu, hallituksen luoman linjan ja politiikan tavoitteena on asettaa organisaatiolle suuntaviivat sisäisen valvonnan suhteen. Johdon tehtävänä on jalostaa nämä laajemmat suuntaviivat organisaation politiikoiksi ja menettelytavoiksi, joiden mukaan toimimalla organisaatio pyrkii kohti hallituksen asettamia tavoitteita. (Ratsula 2020, 56.) Näitä käytännön tason sääntöjä ja menettelytapoja kutsutaan valvontatoimenpiteiksi, joita toteutetaan kaikilla organisaation tasoilla sekä kaikissa

yksiköissä ja toiminnoissa. Toimenpiteitä voidaan jaotella esimerkiksi ehkäiseviin ja paljastaviin sekä manuaalisiin ja automaattisiin ohjausmenetelmiin. (COSO 2013.) Valvontatoimenpiteiden tehtävänä on pienentää aiemmin arvioituja organisaation tavoitteita uhkaavia riskejä. (Moeller 2013, 73).

COSO-mallin ohjausmenetelmien taustalla on usein käytäntö tehtävien eriyttämisestä, jolloin esimerkiksi maksujen hyväksymiseen tarvitaan aina useampi henkilö. Erilaisia menetelmiä ovat myös esimerkiksi muut hyväksymisvaltuudet, varmistukset sekä suorituksen arviointi. (Moeller 2013, 73; COSO 2013.) Lisäksi valvontatoimenpiteet voivat sisältää fyysisiä toimenpiteitä, kuten aineellisten omaisuuserien suojaaminen ja kulkuvaltuudet (Ratsula 2020, 57).

Valvontaympäristöön liittyvät seuraavat periaatteet:

10. Sopivien valvontatoimenpiteiden valinta ja kehittäminen.
11. Yleisten teknologiaan liittyvien toimenpiteiden valinta ja kehittäminen.
12. Valvontatoimenpiteiden jalkauttaminen politiikoiden ja menettelytapojen avulla.

Valvontaympäristöön liittyvät periaatteet ohjaavat organisaatiota tunnistamaan, valitsemaan ja dokumentoimaan sille sopivia ohjausmenetelmiä, joiden avulla tunnistettuja riskejä pyritään minimoimaan (Moeller 2013, 74; Sihvonen & Uusi-Hautamaa 2019, 92). Yleensä tunnistetut ja käyttöönotettavat menetelmät dokumentoidaan kirjalliseen muotoon, jotta varsinkin suuremmissa organisaatioissa niiden kommunikointi helpottuu. Toisaalta organisaatiokulttuuriin vahvasti juurtunutta toimintatapaa ei välttämättä tarvitse kirjallista dokumentaatiota, mikäli sitä pidetään organisaatiossa itsestäänselvyytenä. (Ratsula 2016a, 119–120.)

Organisaation ohjausmenetelmät on aina määriteltävä yrityksen omat lähtökohdat huomioiden, joten yleisesti pätevää, kaikille organisaatioille sopivaa menetelmäkokoelmaa ei ole olemassa. Hyväksi havaittuja käytäntöjä voi toki kopioida ulkopuolelta tai organisaation sisältä, mikäli ne sopivat kyseiseen yksikköön. (Sihvonen & Uusi-Hautamaa 2019, 92–93.) Valvontatoimenpiteiden tarkoituksena on pienentää organisaatioon kohdistuvia riskejä, joten toimenpiteet on suunniteltava aiemmin tunnistettujen riskien perusteella. Näin tarvittavat menetelmät voidaan kohdistaa niihin toimintoihin, joissa niitä todella tarvitaan. (Ratsula 2016a, 120–121.) Kun sopivat

toimenpiteet on tunnistettu ja valittu, otetaan ne käyttöön politiikkojen ja menettelytapojen avulla. Politiikoilla määritellään, mikä toiminta organisaatiossa on odotettua tai sallittua, ja menettelytavoilla näitä politiikoita toteutetaan käytännössä (Moeller 2013, 83).

3.3.5 Informaatio ja kommunikointi

Informaation hankinta, tuottaminen ja vaihdanta on COSO-mallin mukaan elintärkeää organisaation sisäisen valvonnan toiminnan kannalta. Johto käyttää itse luomansa tiedon lisäksi myös organisaation ulkoisista sekä sisäisistä lähteistä saatua tietoa sisäistä valvontaa koskevan päätöksenteon tukena. (COSO 2013.) Informaatiolla on valtava vaikutus yritysten päätöksenteon ja toiminnan laatuun. Sisäisen valvonnan yhtenä tehtävänä on siten taata organisaatiossa käytettävän informaation relevanttius ja laatu. (Ratsula 2020, 58.)

Kommunikaatio on prosessi, joka tässä yhteydessä tarkoittaa informaation jatkuvaluontoista jakamista ja välittämistä. Sisäisen valvonnan näkökulmasta tiedon on päästävä virtaamaan organisaatiossa sekä vertikaalisesti johdon ja työntekijöiden välillä että horisontaalisesti eri yksiköiden välillä. (COSO 2013) Tehokkaalla kommunikaatiolla esimerkiksi johdon linjan mukaiset tavoitteet ja vastuut kyetään välittämään henkilöstölle, jolloin kukin työntekijä ymmärtää oman vastuualueensa ja roolinsa sisäisen valvonnan kannalta. (Ratsula 2016a 130.)

Informaatioon ja kommunikointiin liittyvät periaatteet ovat:

13. Laadukkaan ja relevantin informaation tuottaminen ja hankkiminen, ja tiedon käyttö sisäisen valvonnan tukemiseen.
14. Informaation, kuten sisäisen valvonnan tavoitteiden ja vastuiden kommunikointi organisaation sisällä.
15. Kommunikointi ulkoisten osapuolten kanssa sisäiseen valvontaan liittyvistä asioista.

Informaatio ja kommunikointi -komponentti tukee toiminnallaan muita COSO-mallin komponentteja edistämällä tiedon kulkua ja jakamista organisaatiossa (Moeller 2013, 88–89). Organisaation on tunnistettava, minkälaista informaatiota se tarvitsee toimintansa tueksi, ja tarkasteltava sekä sisäisiä että ulkoisia informaatiolähteitään. Sen on myös

huolehdittava käytettävän informaation ajantasaisuudesta, relevanttiudesta ja laadukkuudesta. (Ratsula 2016a, 131.)

Tiedon laadun lisäksi organisaation tulee varmistaa kommunikaation tehokkuus sekä organisaation sisällä että sen ulkopuolelle. Sisäisessä kommunikaatiossa korostuu etenkin organisaation tavoitteiden ja niihin kuuluvien vastuiden informoiminen niistä vastaaville tahoille. Tehokkaalla sisäisellä kommunikaatiolla johto pystyy viestittämään sisäisen valvonnan suuntaviivat ja toimenpiteet henkilöstölle, ja samalla alleviivaamaan sisäisen valvonnan tärkeyttä ja roolia organisaatiossa. Esimerkiksi luvussa 4.3.4 esiteltyjen politiikkojen ja menettelytapojen jalkauttamisen onnistuminen on hyvin riippuvainen tehokkaasta ja loogisesta kommunikaatiojärjestelmästä. (Moeller 2013, 96.)

Ulkopuolelle suuntautuvan kaksisuuntaisen kommunikoinnin tavoitteena on sekä viestiä että kerätä informaatiota, joka liittyy organisaation tavoitteisiin. Esimerkiksi osakkeenomistajat, asiakkaat ja viranomaiset ovat ulkoisen kommunikaation kannalta tärkeitä toimijoita. (Moeller 2013, 100.) Organisaatiolla on siis oltava olemassa vakiintuneet kanavat tai menetelmät, joilla ulkoista kommunikointia käydään.

3.3.6 Seurantatoimenpiteet

Organisaation on COSO-mallin mukaan alati seurattava ja arvioitava sisäisen valvontansa toimintaa ja suoriutumista (Ratsula 2020, 62). Tähän käytetään jatkuvaa tai erillisiä arviointeja, tai näiden yhdistelmää. Arvioinneilla varmistetaan kunkin sisäisen valvonnan komponentin toimivuus. Jatkuva arviointi integroidaan kuhunkin organisaation liiketoimintaprosessiin, ja tämän arvioinnin avulla prosesseista saadaan ajankohtaista informaatiota. Erilliset arvioinnit sen sijaan toteutetaan tietyin väliajoin, ja niiden laajuus sekä tiheys riippuu muun muassa prosessiin kohdistuvasta riskistä sekä jatkuvan arvioinnin laadusta. Arviointien tuloksia verrataan esimerkiksi johdon ja hallituksen ennalta asettamaan kriteeristöön, ja havaittujen puutteiden perusteella sisäistä valvontaa pyritään kehittämään eteenpäin. (COSO 2013.)

Seurantatoimenpiteisiin liittyvät seuraavat periaatteet:

16. Sisäisen valvonnan komponenttien toimintaa arvioidaan jatkuvilla ja/tai erillisillä arvioinneilla.
17. Sisäisen valvonnan puutteita arvioidaan ja kommunikoidaan asiasta vastaaville tahoille.

Seurantatoimenpiteillä pyritään jälkikäteisesti varmistamaan sisäisen valvonnan toiminta, havaitsemaan sen mahdolliset puutteet sekä korjaamaan ja kehittämään sisäistä valvontajärjestelmää (Sihvonen & Uusi-Hautamaa 2019, 97). Organisaatio voi arvioida vaikkapa tietyn liiketoiminnon tai ohjausmenetelmän toimintaa suorittamalla sisäisen tarkastuksen tälle alueelle. Mikäli tällaisessa erillisarvioinnissa havaitaan puutteita, tulee ne raportoida eteenpäin ja tarvittaessa suorittaa uusi tarkastus myöhemmin. Jatkuvat arvioinnit sen sijaan tulee rakentaa osaksi organisaation prosesseja, jolloin toiminnan arviointi on jatkuvaa, rutiininomaista ja reaaliaikaista. (Moeller 2013, 108–109.) Seurantatoimenpiteillä on tärkeä rooli pitää organisaation sisäinen valvonta ajan tasalla.

4 Digitalisaatio yritystoiminnan muutosvoimana

Digitalisaatio voidaan nähdä liiketoimintaympäristöä muuttaneena tekijänä, jolla on ollut parin viime vuosikymmenen aikana käänteentekevä vaikutus niin yritysten sisäisiin prosesseihin kuin globaaleihin markkinoihinkin (Betti & Sarens 2020, 200). Nykyään tietotekniikan merkitys voi päivittäisen toiminnan tuen lisäksi olla joillekin yrityksille jopa kilpailuvaltti (Damiandes 2005, 77). Myös sisäisen valvonnan ja väärinkäytösten näkökulmasta digitalisaatio on tuonut mukanaan uudenlaisia mahdollisuuksia ja uhkia. Rutiininomaisten ja standardisoitujen työtehtävien automatisointi on mahdollistanut inhimillisen osaamisen suuntaamisen monimutkaisempiin tehtäviin. Teknologian avulla monia yrityksen prosesseja voidaan kokonaisvaltaisesti tehostaa, ja paremman tiedon ansiosta epävarmuus päätöksenteossa vähenee. (Bredmar 2017, 115; 122.)

Digitalisaatiolla viitataan yleensä uusien teknologisten innovaatioiden lisääntymiseen ja yleistymiseen, joiden avulla digitaalisessa muodossa olevaa dataa voidaan hyödyntää. Bankewitzin ym. (2016, 58) mukaan digitalisaatio käsittää esimerkiksi datamäärän lisääntymisen (*big data*), paremman analytiikka- ja prosessointikapasiteetin sekä informaatiovirtojen kasvamisen. Bainesin ym. (2018, 401) laveassa määritelmässä digitalisaatio tarkoittaa digitaalisen teknologian hyödyntämistä. Teknologian avulla voidaan automatisoida, kiihdyttää ja vahvistaa kommunikaatiota, liiketoimintaprosesseja sekä sosiaalista muutosta. Nykyään tietojärjestelmiä ja perustason IT-osaamista voidaan pitää elinehtona käytännössä kaikille yrityksille. Sen sijaan riittämättömät investoinnit sekä järjestelmiin että osaamiseen voivat helposti jättää yrityksen epäsuotuisaan kilpailuasemaan sen kilpailijoihin verrattuna. (Stoel & Muhanna 2011, 285.) Siten digitalisaatio on yritysten näkökulmasta helppo nähdä lähteenä sekä mahdollisuuksille että riskeille.

4.1 Digitalisaatio ja yrityksen riskit

Digitaalisia työkaluja käytetään jo laajalti esimerkiksi organisaation toiminnan tehostamiseen. Samalla uusia teknologisia innovaatioita voidaan kuitenkin käyttää myös epätoivottuihin tarkoituksiin. Erilaiset digitalisaation tuomat riskit ovat digitalisoituneissa organisaatioissa kriittinen ongelma, ja mitä vahvemmin organisaation toiminta nojaa tietojärjestelmiin, sitä alttiimpi se on kyberriskeille (Betti & Sarens 2020, 202; Eling & Schnell 2016, 476).

Digitalisoitumiseen liittyviä riskejä kutsutaan usein kyberriskeiksi tai kyberuhiksi. Ne liittyvät sähköisiin tietoverkkoihin ja virtuaaliseen todellisuuteen eli internetiin, mikä osaltaan erottaa kyberriskit muista yritysten riskeistä. Tyypillinen esimerkki tällaisesta kyberuhasta on tietomurto. Lisäksi ne eroavat monista muista riskeistä ensinnäkin aineettoman luonteensa takia. (Eling & Schnell 2016, 476.) Yleisellä tasolla voidaan todeta, että digitalisaatio on yhtäältä tuonut tekijöille parempia työkaluja toteuttaa esimerkiksi kyberrikoksia, ja toisaalta se on lisännyt potentiaalisten kohteiden määrää, kun useammat prosessit ja laitteet ovat yhteydessä verkkoon esimerkiksi Asioiden Internetin (engl. *Internet of Things*) kautta (EY 2017).

Yritysten prosessit ovat digitalisaation myötä tulleet yhä riippuvaisempia tietojärjestelmistä ja teknologiasta, ja monilla yrityksillä on usein käytössään valtavasti erilaisia internetiin yhteydessä olevia järjestelmiä ja laitteita. Toisiinsa yhteydessä olevat järjestelmät, niiden monimutkaisuus sekä alati muuttuvat ja lisääntyvät kyberuhat ovat radikaalisti lisänneet tarvetta tietojärjestelmien turvamekanismeille. (Stoel & Muhanna 2011, 281.) Kun prosessit ja järjestelmät liittyvät toisiinsa digitalisaation kautta yhä tiiviimmin, liittyy myös niiden turvallisuus ja yrityksen riskiympäristö samalla yhä tiiviimmin kyberturvallisuuteen. Tämä aiheuttaa ongelmia etenkin tilanteissa, kun kehitys tapahtuu teknologia edellä turvallisuusaspektin jäädessä taustalle. (Salminen 16.2.2017.) Linkittyneisyyden seurauksena esimerkiksi turvallisuuspuutos yhdessä järjestelmässä aiheuttaa automaattisesti epäsuoran riskin myös siihen liittyneille toisille järjestelmille. Toisin sanoen, vaikka digitalisaatio on tuonut hyötyjä yritystoimintaan ja prosesseihin, tarvitaan yrityksissä yhä kokonaisvaltaisempaa ymmärrystä sen tuomista haasteista ja etenkin turvallisuuteen liittyvistä vaatimuksista. Nykyiset toisiinsa linkittyneet järjestelmät ovat huomattavasti hankalampia johtaa ja hallita kuin digitalisaatiota edeltäneet erilliset ja rajatut järjestelmät. Yksittäisissä yrityksissä digitalisaation vaikutuksen kokonaisvaltaisen arvioinnin laiminlyönti saattaa siis johtaa kielteisiin seurauksiin. (Donghui 2021, 4; EY 2017.)

Uusi teknologia, ohjelmistot ja niihin liittyvä osaaminen mahdollistavat uudenlaisten riskien ja väärinkäytöskeinojen syntymisen. PwC:n (2020) mukaan kyberrikokset ovat yleistyneet, ja niiden vahingot vaikeuttavat huomattavasti yritysten toimintaa. Samoin PwC:n (2018) mukaan etenkin pohjoismaissa kyberrikollisuus on kasvanut viime vuosina, ja se on ottanut paikkansa yhtenä yleisimmistä taloudellisten väärinkäytösten muodoista. Kehittynyt teknologia tarjoaa väärinkäyttäjille uudenlaisia, vaikeammin

torjuttavia työkaluja ja menetelmiä. Siten yritykset joutuvat tasapainoilemaan toisaalta alati kasvavien vaatimusten ja turvallisuuden kanssa (Damianides 2005, 77). Esimerkiksi kyberhyökkäykset voidaan luokitella tavallisiin, edistyneisiin ja esiin työntyviin (engl. *emergent*) hyökkäyksiin. Tavallisissa hyökkäyksissä hyödynnetään helposti saatavilla olevia työkaluja eivätkä ne vaadi korkeatasoista osaamista, kun taas edistyneissä hyökkäyksissä käytetään hyväksi monimutkaisia välineitä. Niiden tekijät ovat yleensä kokeneempia ja ammattitaitoisempia kuin tavallisten hyökkäyksien tekijät. Esiin työntyvissä hyökkäyksissä taas hyödynnetään kaikkein uusimman teknologian vielä tunnistamattomia heikkouksia, ja tämänkaltaiset hyökkäykset vaativat erityistä tutkimusta kyseisen teknologian heikkouksiin. Näitä, samoin kuin edistyneitäkin hyökkäyksiä, toteuttavat ammattitaitoiset tekijät kuten rikollisjärjestöt tai kansallisvaltiot. (EY 2017.)

Riskinäkökulmasta huomionarvoinen tekijä ovat yrityksen datavarat, jotka riittävän turvallisuuden saavuttamiseksi on tunnistettava ja suojattava. Taustalla tässä on tietoturva-asiantuntija Mikko Hyppösen (16.2.2020) se, ettei täydellisen tietoturvallisia järjestelmiä pystytä luomaan. Siten yrityksen hallinnoimaan tietoon liittyy aina riskejä ja heikkouksia. Datavarantojen haavoittuvuudet voivat realisoitua esimerkiksi datan menettämisenä, vuotamisena tai muuttamisena. Taustalla realisoitumisessa voi olla inhimillinen virhe, tarkoituksellinen väärinkäytös tai puutteellinen kirjaus. (Damianides 2005, 83.) Yritysten on siten suojattava datansa asianmukaisesti, varmistettava mahdollisuus datan palauttamiseen sekä varauduttava datan vuotamiseen.

Yksittäisten yritysten kohtaamien riskien lisäksi vahva riippuvuus digitalisaatiosta muodostaa riskejä myös yleisemmällä tasolla. Vaikka laajamittaisten skenaarioiden todennäköisyys ovat huomattavasti pienemmät, ovat ne silti mahdollisia. Eling ja Schnell (2016, 480–481) nostavat artikkelissaan 2010-luvulla tapahtuneita laajamittaisia vahinkoja, joiden seurauksena esimerkiksi suuressa osassa Afrikkaa internet-yhteydet katkesivat vuorokaudeksi. Vastaavia tapauksia on sattunut myös Euroopassa ja Aasiassa. Vaikka täydelliset maailmanlaajuiset tietokatkot ovat heidän mukaansa hyvin epätodennäköinen, ovat laajamittaiset alueelliset katkokset tulevaisuudessa edelleen mahdollisia. Edellä mainittujen skenaarioiden ongelmana Eling ja Schnell näkevät puutteellisen varautumisen. Koska kaikki tämän hetken yritystoiminta on vähintäänkin osittain riippuvainen tai tietoverkoista, johtaisi internetin katkeaminen myös esimerkiksi

viestinnän, pilvipalveluiden, nettisivujen ja tietoverkkoon sidoksissa olevan tuotannon lamaantumiseen (Eling & Schnell 2016, 481; Strickland 2021).

4.2 Digitalisaation vaikutus yrityksen ohjaukseen ja valvontaan

4.2.1 Digitalisaatio ja yrityksen ohjaus

Teknologian murros on tuonut ja tuo edelleen organisaatioiden käyttöön yhä tehokkaampia työkaluja, joita käytetään sekä itse liiketoimintaprosesseissa että yritysten tukitoiminnoissa. Kun suuri osa yritysten prosesseista on digitalisoitu, täytyy myös sisäisen valvonnan ulottua yrityksen digitalisoiduille osa-alueille. Kuten edellisessä alaluvussa mainittiin, kytkeytyvät yritysten järjestelmät nykyään usein toisiinsa, jolloin kyberturvallisuus koskettaa myös niitä yrityksen osa-alueita, jotka eivät ole digitalisoituja. Tähän pohjaten digitalisaation uhkiin varautuminen ei voi nojata vain teknisiin ohjausmenetelmiin, vaan sen tulisi olla keskeinen osa yritysten riskienhallintastrategiaa (Kyberturvallisuuskeskus 4.2.2020). Siten digitalisaation riskien käytännön valvonta ja ohjaus ei voi olla vain yrityksen IT-osaston vastuulla, vaan sen onnistuminen vaatii Elingin ja Schnellin (2016, 479–480) mukaan jatkuvaa osastojen välistä kommunikointia. Teknisten ja teknologisten ratkaisujen lisäksi tarvitaan myös muunlaisia menetelmiä. Esimerkiksi henkilöstön riskitietoisuus, salasanapolitiikka ja huolimattomuuksien ehkäisy seurannan avulla ovat tärkeitä perusasioita kyberturvallisuuden kannalta. Tärkeää on, että yrityksellä on visio kyberturvallisuudestaan: mitä kyberturvallisuus käsittää ja miten se nivoutuu osaksi yrityksen liiketoimintastrategiaa ja kulttuuria. (EY 2017.)

Mitä tulee kyberriskien hallintaan, Eling ja Schnell (2016) ehdottavat klassista riskienhallinnan prosessia, joka muistuttaa osittain COSO-mallia. Tämä malli alkaa alkutilanteen ja kyberriskien hallinnan tavoitteiden määrittelystä. Yrityksen on esimerkiksi tunnistettava erityisen arvokkaat varallisuuserät, kruununjalokivet (engl. *crown jewels*), ja pyrittävä suojaamaan ne asianmukaisesti (EY 2017).

Toinen vaihe on tunnistaa yrityksen prosesseihin ja varoihin liittyvät riskit, sekä näiden riskien lähteet ja niiden tuottamat uhat. Uhkien tunnistamista ja seurantaa on toteutettava jatkuvasti, sillä kyberriskit ja kyberhyökkäyksien metodit muuttuvat jatkuvasti (EY 2017).

Kolmas vaihe Elingin ja Schnellin mallissa on riskianalyysi, jossa voidaan tarkastella riskien kokonaisvaltaista vaikutusta yrityksen toimintaan esimerkiksi erilaisten skenaarioiden avulla. Kuten COSO-mallissa myös kyberriskien tunnistamisessa voidaan käyttää erilaisia työkaluja ja viitekehyksiä.

Neljäs vaihe on riskien käytännön hallinta: miten välttää, siirtää, minimoida ja vastata riskeihin. Nimenomaan kyberriskien kohdalla Eling ja Schnell näkevät riskien minimoinnin olevan tehokas metodi. Minimointia voidaan tehdä esimerkiksi virustorjunnan ja toimintaprotokollien avulla.

Viimeisenä vaiheena mallissa on riskien seuranta. Kyberriskien dynaamisen, nopeasti muuttuvan luonteen vuoksi seuranta on Elingin ja Schnellin mukaan avainasemassa esitetyssä riskienhallintamallissa. Seurannassa korostuu tehokas kommunikaatio ja informaation jakaminen, jolla taataan kaikkien organisaation jäsenten valveutuneisuus kyberriskeistä.

Prosessitason suunnitelmien lisäksi yritykset tarvitsevat myös teknisiä ratkaisuja toimintansa suojaamiseksi. Erilaisten analytiikkaan ja tekoälytekniikkaan perustuvien uudenlaisten työkalujen, kuten anomalia-analyysien avulla yritykset saavat yhä ajankohtaisempaa tietoa yrityksen toiminnasta, ja pystyvät siten yhä paremmin muun muassa puuttumaan poikkeamiin. Esimerkiksi data-analytiikkaa voidaan hyödyntää suurten tietomassojen käsittelyyn ja analysointiin, jota voidaan tehdä esimerkiksi poikkeamien havaitsemiseksi (Sihvonen & Uusi-Hautamaa 2019, 143). PwC:n (2018) mukaan vasta melko harvoissa yrityksissä kuitenkin käytetään edistyksellistä teknologiaa väärinkäytösten torjuntaan. Tutkituista yrityksistä esimerkiksi vain 7 % hyödyntää tekoälyä, ja 10 % big dataa väärinkäytösten estämiseen. Kolmasosa tutkimuksen yrityksistä kuitenkin joko suunnitteli tai oli ottamassa käyttöön edellä mainittuja työkaluja, mikä voi osaltaan indikoida kehittyneempien työkalujen yleistymistä lähivuosina. Näiden teknologioiden käyttöönotto ei kuitenkaan ole vailla haasteita. Esimerkiksi kyberturvallisuuteen liittyen yritysten ongelmaksi voi muodostua sellaisen riittävän kompetenssin ja osaamisen haaliminen, jonka avulla organisaatio pystyisi torjumaan jatkuvasti kehittyviä teknologisia uhkia. (Betti & Sarens 2020, 202.) Lisäksi väärinkäytösten torjunnassa jo käytettävää teknologiaa on mahdollista hyödyntää nykyistä huomattavasti paremmin. PwC:n (2020) raportin mukaan tekoälyä hyödyntävistä yrityksistä yli kolmasosalla onkin vaikeuksia löytää sille käyttöä

nimenomaan väärinkäytösten torjunnassa. Raportin mukaan teknologia ei siten yksistään riitä väärinkäytösten torjuntaan, vaan vähintään yhtä merkityksellistä on teknologian hyödyntämistä tukevat prosessit ja rakenteet sekä tarvittava osaaminen.

Reaaliaikaisuuteen tähtäävän seurannan, kehittyneiden analytiikkatyökalujen ja muiden uhkien minimointiin tähtäävien menetelmien lisäksi yrityksen tulee myös varautua kyberuhkien realisoitumiseen. Erilaiset uhkiin liittyvät vastausmekanismit, kuten datan varmuuskopiointi, palomuurit ja tietoympäristön riittävä suojaaminen ulkopuolisilta antavat yritykselle mahdollisuuden toimia välittömästi uhan havaittaessa tai realisoituessa. Ennakoiva varautuminen uhkien toteutumiseen sekä teknisin ratkaisuin että toimintamallein auttaa siten minimoimaan kyberriskien vaikutusta. (Donghui 2021, 4.) Yhtenä ennakkotoimenpiteenä yritys voi toteuttaa käytännön harjoittelua ja testausta, jolla voidaan selvittää esimerkiksi henkilöstön osaamista ja käyttäytymistä muun muassa tietojenkalastelua kohdattaessa. Käytännön testauksella voidaan selvittää tiettyjä kehityskohteita niin henkilöstön koulutustarpeissa kuin järjestelmissä ja teknologisissa kontrolleissakin. (EY 2017.)

4.2.2 Digitalisaatio ja COSO-malli

Digitalisaatio on vaikuttanut myös sisäisen valvonnan teoriaan. Tätä muutosta kuvastaa esimerkiksi tarve päivittää alkuperäinen vuoden 1992 COSOn sisäisen valvonnan malli alle kaksi vuosikymmentä sen julkistamisesta. Etenkin internetin nopea yleistyminen liiketoiminnassa 1990- ja 2000-luvuilla, ja sitä edeltäneiden *mainframe*-tietokoneiden poistuminen korostivat tarvetta mallin parantamiselle. (Moeller 2013, 29–30.) Luvussa 4.3.4 esiteltyihin valvontatoimenpiteisiin kuuluvat olennaiselta osalta myös organisaation tietojärjestelmiin liittyvät toimenpiteet. Organisaation ohjausmenetelmät voidaankin jakaa IT-menetelmiin ja muihin, kirjanpidon ja johtamisen yleisiin ohjausmenetelmiin (Stoel & Muhanna 2011, 283). Sisäisen valvonnan kontekstissa tietojärjestelmiin liittyvää valvontaa ja ohjausta kutsutaan usein IT-kontrolliksi (engl. *IT control*). IT-kontrolli muodostuu muun muassa tietojärjestelmiin liittyvistä IT-valvontatoimenpiteistä tai IT-menetelmistä. IT-menetelmiä ovat kaikki ne ohjausmenetelmät, jotka koskevat yrityksen tietojärjestelmiä sekä prosesseja ja infrastruktuuria, joiden avulla tietoja tai dataa käsitellään. (Chang ym. 2014, 187; Stoel & Muhanna 2011, 281; 284).

IT-menetelmien tavoitteena on varmistaa IT-ympäristön tehokas ja turvallinen toiminta, sekä valmistautua mahdollisiin uhkiin ja poikkeustilanteisiin (Ratsula 2016a, 240–241).

Samalla erityisesti tietoturvaan liittyvät ohjausmenetelmät ylläpitävät tietojärjestelmien ja niissä olevan datan luotettavuutta, saatavuutta ja oikeellisuutta (Chang ym. 2014, 188). Tietojärjestelmiin liittyvien menetelmien tärkeydestä kertovat esimerkiksi Klammin ja Weidenmier Watsonin (2009) tutkimus, jonka keskiössä olivat sisäisen valvonnan heikkoudet. Tutkimuksen mukaan yrityksissä, joiden IT-menetelmät oli heikkoja, paljastui myös muiden ohjausmenetelmien merkittäviä puutteita. Myös Stoel ja Muhanna (2011, 285) painottavat, että IT-kontrollin heikkous heijastuu helposti paitsi tilinpäätösinformaation laatuun, myös yrityksen liiketoimintaan. Lisäksi huomionarvoista on, että tietojärjestelmiin liittyvien väärinkäytösten ja tietomurtojen riski usein lisääntyy, mitä vahvemmin organisaation toiminta on digitalisoitunut (Betti & Sarens 2020, 202). Tätä taustaa vasten IT-kontrollin merkitystä on hankalaa ylikorostaa. Näiden ohjausmenetelmien toiminnan tai toimimattomuuden vaikutus on sitä suurempi, mitä riippuvaisempia sen prosessit ovat tietojärjestelmistä.

IT-menetelmät voivat olla luonteeltaan yleisiä tai liittyä tiettyihin sovelluksiin, mutta olennaista on, että menetelmät kattavat koko organisaation tietojärjestelmäympäristön (Moeller 2013, 85). Yleiset IT-menetelmät kattavat organisaation tietojärjestelmäympäristön sekä tietojärjestelmiin liittyvät prosessit. Niiden avulla määritellään esimerkiksi IT-hallinnon roolit ja vastuut, tietoturvallisuuteen liittyvät prosessit sekä uusien järjestelmien käyttöönotot (Ratsula 2016a, 242). Nämä menetelmät luovat yleiset suuntaviivat sekä pohjan tarkemmille, sovelluskohtaisille ohjausmenetelmille. Käytännössä yleisten menetelmien luonne riippuu organisaatiosta itsestään ja sen IT-infrastruktuurista. (Moeller 2013, 182.)

Sovelluskohtaiset menetelmät liittyvät esimerkiksi yksittäisissä järjestelmissä olevaan dataan (Chang ym. 2014, 187). Niillä säädellään esimerkiksi tiedon keräämistä, syöttöä ja käsittelyä järjestelmissä, ja niiden tavoitteena on varmistaa tiedon laatu, kattavuus ja oikeellisuus. Samoin sovelluksiin liittyvillä menetelmillä varmistetaan, että vain valtuutetuilla henkilöillä on pääsy sovelluksen sisältämiin tietoihin. (Ratsula 2016a, 245.)

Tehokkaan IT-kontrollin lisäksi digitalisaatio on korostanut myös toimivien seurantatoimenpiteiden merkitystä. Kuten luvussa 3.3.6 esitettiin, on seurantatoimenpiteiden tehtävänä pitää organisaation sisäinen valvonta ajan tasalla. Toimintaympäristön muutos, jota digitalisaatio on nopeuttanut, tuo mukanaan uudenlaisia riskejä, joista organisaation on oltava tietoinen. Yrityksen on siten seurattava

ja arvioitava esimerkiksi sisäistä verkkoympäristöään jatkuvasti puutteiden havaitsemiseksi (Donghui 2021, 4). Puutteelliset seurantatoimenpiteet voivat rapauttaa sisäisen valvonnan tehokkuutta, jos käytössä olevat ohjausmenetelmät ja riskien arviointiprosessi eivät vastaa nykyistä toimintaympäristöä. (Klamm & Weidenmier Watson 2009, 4.) Toimintaympäristön muutoksen lisäksi myös liiketoimintamallit ovat usein dynaamisia. Siten organisaation sisältä kumpuavat muutokset luovat tarpeen sisäisen valvonnan ja riskien jatkuvalle seurannalle. (PwC 2020.) Yrityksen on siten kyettävä seuraamaan ja valvomaan prosessien ja ohjausmenetelmien toimintaa reaaliaikaisesti niiden toiminnan luotettavuuden turvaamiseksi (Sihvonen & Uusi-Hautamaa 2019, 118).

5 Empiirinen analyysi

5.1 Empiirinen tutkimusasetelma ja metodit

Tutkielman empiirinen analyysi keskittyy tarkastelemaan sisäistä valvontaa ja väärinkäytösten ehkäisyä tilitoimiston ja asiakasyrityksen suhteessa tilitoimiston näkökulmasta. Nykyään monet yritykset ulkoistavat tukitoimintojaan keskittyen ydinliiketoimintaansa, jolloin jokin toinen yritys hoitaa esimerkiksi ulkoistavan yrityksen taloushallinnon. Näissä suhteissa perinteiset organisaatiorajat hämärtyvät, ja organisaatioiden rajapinnassa valvonta saattaa olla haastavaa.

Tutkielman kohdeyrityksenä on Suomessa toimiva tilitoimisto. Yrityksellä on toimipisteitä ympäri Suomea, ja se työllistää satoja henkilöitä. Tilitoimistojen prosessit ovat yleisesti pitkälti digitalisoituneet. Suurin osa yrityksen asiakkaiden kirjanpidosta ja palkkahallinnosta toimii sähköisten järjestelmien avulla, mutta yritys palvelee edelleen myös täysin paperista kirjanpitoa pitäviä asiakkaita. Yritys tarjoaa asiakkailleen lukuisien palveluntarjoajien sähköisiä taloushallintojärjestelmiä, ja esimerkiksi kotisivujensa markkinointiviestinnässä se painottaa sähköisen taloushallinnon hyötyjä asiakasyrityksille.

Taulukko 1, Haastattelut

	Tehtävä	**Päivämäärät**	**Haastattelujen kesto**
Haastateltava A	Johtaja, verotus ja yritysjärjestelyt	5.10.2021 11.10.2021	30min 36min
Haastateltava B	Laadunvalvonnan asiantuntija	6.10.2021 14.10.2021	30min 1 h 4min
Haastateltava C	Laadunvalvonnan asiantuntija	13.10.2021 21.10.2021	39min 1 h 3min
Haastateltava D	Kehityspäällikkö, IT	8.11.2021	53min

Tutkielmaa varten haastateltiin yhteensä neljää tilitoimistossa työskentelevää henkilöä. Haastateltava A toimii johtajana verotus- ja yritysjärjestelytiimissä, ja osallistuu myös yrityksen riskienhallinnan suunnitteluun. Haastateltavat B ja C työskentelevät yrityksen laadunvarmennuksen parissa asiantuntijoina. Laadunvalvonnan tavoitteena on varmistaa

yrityksen liiketoimintaprosessien, kuten kirjanpidon asianmukainen toiminen. Haastateltava D toimii yrityksen kehitystiimissä kehityspäällikkönä, ja vastaa osaltaan yrityksen IT-kehityksestä.

5.2 Aineiston keruu

Tutkielman aineisto on kerätty haastattelemalla yrityksessä työskenteleviä henkilöitä. Haastateltavat valittiin tutkielmaan heidän osaamisensa sekä työnkuvansa perusteella. Kriteereinä tässä olivat esimerkiksi ymmärrys yrityksen kontrolliympäristöstä, riskienhallinnasta ja olennaisista tilitoimistoympäristössä kohdattavista väärinkäytösriskeistä. Haastattelut toteutettiin etäyhteyksin, ja ne nauhoitettiin sekä litteroitiin analysoinnin helpottamiseksi. Haastateltava D:tä lukuun ottamatta kutakin henkilöä haastateltiin kahdesti. Ensimmäinen haastattelukierros oli lyhyt, vapaamuotoinen keskustelu aiheesta, ja tarkoituksena oli kartoittaa lähemmin haastateltavan taustaa ja osaamista. Lisäksi tavoitteena oli löytää relevantteja teemoja ja pointteja, joista keskusteltiin syvemmin toisella haastattelukierroksella. Kaksivaiheisen haastattelun ajatuksena oli myös antaa haastateltaville aikaa pohtia aihetta ja valmistautua varsinaiseen haastatteluun. Toisen haastattelukierroksen haastatteluissa käytettiin apuna kysymysrunkoja, jotka löytyvät tutkielman liitteistä. Kysymysrunkojen avulla tutkimuskysymysten kannalta relevanttia tietoa pyrittiin löytämään. Lisäksi toisella haastattelukierroksella keskusteltiin syvällisemmin niistä teemoista, jotka nousivat ensimmäisessä haastattelussa esiin.

Toinen haastattelukierros ja pääasiallinen aineiston keruu toteutettiin teemahaastatteluin. Teemahaastattelut etenevät tavallisesti ennalta määriteltyjen teemojen ja kysymysten kautta, mutta kysymysten tarkka asettelu saattaa vaihdella haastattelusta toiseen. Verrattuna esimerkiksi strukturoituun kysymyspatteristoon teemahaastattelu antaa enemmän tilaa haastateltavan omille näkemyksille sekä vastausten yhteydessä mahdollisesti ilmenevien, ennalta arvaamattomien alateemojen käsittelylle. Ennalta määritellyt teemat kuitenkin pitävät haastattelun tutkittavassa aiheessa. Tutkielma tarkastelee monimutkaisia sekä eri yrityksissä eri tavoin ilmeneviä aiheita, on loogista antaa haastateltavien kertoa avoimesti omia näkemyksiään, jolloin tarkasteltavista teemoista saattaa nousta uusia teemoja, joita tutkielman tekijä ei ole huomannut.

Tutkielman toissijaisina lähteinä käytettiin yrityksen sisäistä koulutus- ja tiedotusmateriaalia, kuten videokoulutuksia, tiedotteita, uutisia ja kirjallista

koulutusmateriaalia. Tutkielman tekijän työ kohdeyrityksessä mahdollisti pääsyn näihin aineistoihin, eivätkä ne ole saatavilla yrityksen ulkopuolisille.

5.3 Kohdeyrityksen taustatilanne

Yritys on viime vuosina laajentunut melko aggressiivisesti sekä orgaanisen kasvun että yritysostojen avulla. Yritysostoja varten yrityksellä on olemassa selkeä haltuunottoprosessi, jonka mukaisesti yritysostot toteutetaan. Prosessin tarkoituksena on varmistaa ostettavan toiminnan yhteensopivuus konsernin toiminnan kanssa, ja jalkauttaa yrityksen toimintatavat ja strategia ostettavaan yksikköön.

Toinen yrityksen toimintaan vaikuttava taustatekijä on yrityksen strateginen ratkaisu olla ohjelmistoriippumaton. Tämä tarkoittaa sitä, ettei yritys ole lukittunut yhteen tiettyyn järjestelmään tai ohjelmistotoimittajaan, vaan tarjoaa asiakkailleen palveluita eri järjestelmissä ja ympäristöissä. Lisäksi joidenkin asiakkaiden kohdalla taloushallinto suoritetaan asiakkaan omassa IT-ympäristössä. Järjestelmien ja ohjelmistojen määrä ja niiden väliset erot, sekä erot kullekin asiakkaalle toteutettavissa palveluissa tuovat tiettyjen etujen lisäksi myös haasteita etenkin toiminnan valvonnan näkökulmasta.

Yrityksellä on olemassa teknologiastrategia, jonka mukaisesti sen toiminnassa pyritään hyödyntämään ja tulevaisuudessa aktiivisesti lisäämään digitaalisia työkaluja. Tästä merkkinä ovat lukuiset järjestelmiin ja digitaalisiin työkaluihin liittyvät kehitysprojektit, joista osa on otettu osittain käyttöön, osa tulee lähiaikoina pilottivaiheeseen ja osa on vielä suunnittelupöydällä. Teknologiastrategiassa on huomioitu myös turvallisuusaspekti, mutta esimerkiksi erillistä tietoturvastrategiaa yrityksellä ei ole.

5.4 Digitalisaation vaikutus riskeihin

Taloushallinnon siirtyminen digitaalisiin järjestelmiin on tuonut muutoksia niin väärinkäytösten riskeihin ja tekotapoihin kuin niiden valvontaankin. Taloudellisia väärinkäytöksiä kyetään yhä paremmin valvomaan ja havaitsemaan analytiikan avulla. Osassa taloushallinnon ohjelmistoja on jo sisäänrakennettuna hyvät ominaisuudet esimerkiksi tietynlaisten poikkeamien etsimiseen. (Haasteltava A.) Sähköisten järjestelmien myötä tilisiirtojen ja vastaavien kirjanpidon toimien tekeminen on helppoa ja nopeaa. Helppous ja nopeus saattavat avata helposti hyödynnettävän tilaisuuden esimerkiksi kavallukseen, mutta sekä haastateltava A että D huomauttivat, että

sähköisessä järjestelmässä tehdyt huonosti peitellyt väärinkäytökset tulevat todennäköisesti hyvinkin nopeasti ilmi. Esimerkiksi väärinkäytöksestä kielivän poikkeaman huomaamiseen saattaa kulua aikaa, mutta mikäli järjestelmään tallentuu loki- ja muita tietoja, on näiden jälkien seuranta nopeaa.

Vaikka analytiikan avulla pystytään havaitsemaan etenkin yksinkertaisia virheitä helposti, on huomattavasti haastavampaa huomata tapauksia, joissa väärinkäytöksiä pyritään peittelemään. Samoin digitaalisten työkalujen avulla saattaa olla hankala havaita väärinkäytöksiä, jotka tapahtuvat sellaisessa kohdassa prosessia, johon digitaalisuus ei ulotu. Esimerkiksi käteiseen rahaan liittyvät väärinkäytökset, kuten kassan kavaltaminen saattaa hyvin toteutettuna jäädä pelkin teknologisin valvontamenetelmin huomaamatta. Haastateltava A kertoi esimerkin tapauksesta, jossa hyvällä paikalla sijainnut ravintola ei tuottanut oletettua voittoa. Lukuja tarkasteltaessa huomattiin yrityksen katteen olevan kummallinen. Lopulta yritys asennutti valvontakamerat, jonka jälkeen erään työntekijän huomattiin vetävän käteiskassaa välistä. Tällaisessa tilanteessa, jossa maksutiedot eivät siirry sähköiseen järjestelmään, väärinkäytöksen toteaminen puhtaasti digitaalisella valvonnalla on haastavaa, mutta käytettäessä yhdessä fyysisten menetelmien kanssa voidaan valvontaa tehostaa huomattavasti.

Yleisellä tasolla Haastateltava D näkee, ettei tällä hetkellä käytössä oleva teknologia ole olennaisesti muuttanut väärinkäytösten perustekijöitä. Kohdeyrityksessä näiden tapauksien valvonta ja havainnointi on tällä hetkellä pitkälti jälkikäteistä, mutta kehityksen suunta on kohti reaaliaikaisempaa valvontaa. Kuitenkin väärinkäyttäjillä on käytössään uusia välineitä, ja sähköiset järjestelmät mahdollistavat erilaisten väärinkäytösten tekemisen.

> Ehkä tavat on muuttunut, se miten niitä väärinkäytöksiä tehdään, mutta logiikka taustalla on sama kuitenkin.
>
> Kun toimitaan sähköisissä järjestelmissä, niin jos sinulla on riittävästi käyttöoikeuksia niin sä pystyt tekemään kerralla isomman väärinkäytöksen tai huijauksen, siirtää vaikka sadoilta asiakkailta rahat omalle tilille. Totta kai sä jäät siitä sitten myös kiinni, eli se on aika paljon kiinni myös siitä mitä tehdään.
>
> (Haastateltava D)

Tätä taustaa vasten on etenkin monimutkaisempien väärinkäytösten havaitseminen nojaa yksittäisten havaintojen sijaan esimerkiksi kaavamaisuuksien ja toistuvien epäilyttävien

seikkojen etsimiseen. Sen sijaan Haastateltava A näkee, ettei yksittäisten kirjanpidon toimien tarkastelu ole välttämättä edes mielekästä.

> Pitäisi enemmän päästä tietyllä tavalla yksittäisestä datasta tietoanalyyseihin, prosessin valvojaksi ja sitten havaita siellä poikkeamia tai vääristymiä.
>
> (Haastateltava A)

Koska tiedon ja erilaisten järjestelmissä tehtävien toimien määrät ovat valtavia, tarvitaan valvonnan väistämättä digitaalisia työkaluja, mikäli valvontaa halutaan tehdä kattavasti. Ohjelmistoyritysten tarjoamissa valmiissa taloushallinnon järjestelmissä on työkaluja poikkeamien havaitsemiseen. Tarkempaa ja laajempaa valvontaa varten tarvitaan kuitenkin kehittyneempiä automaatio- ja analytiikkatyökaluja, kuten robotteja, jotka kykenevät hakemaan järjestelmistä tietoa ja esittämään sen esimerkiksi mittaristona. (Haastateltava A.)

Vaikka teknologia tarjoaa nyt ja tulevaisuudessa työkaluja väärinkäytösten estämiseen, liittyy siihen jo itsessään riskejä. Kun digitaalisia järjestelmiä ja työkaluja kehitetään ja otetaan käyttöön nopealla tahdilla ominaisuudet edellä, saattaa esimerkiksi tietoturvaan jäädä aukkoja. Samaan aikaan myös alati paranneltavat kehitystyökalut mahdollistavat helpomman ja nopeamman kehittämisen, mikä edelleen saattaa kohdistaa huomion kehitykseen itseensä, jolloin laajemman kontekstin ja taustan ymmärtäminen unohtuu. (Haastateltava D.) Turvallisuuden ja valvonnan näkökulmien laiminlyönti saattaa siten tarjota väylän potentiaalisille hyväksikäyttäjille.

Tilitoimiston ja yrityksen taloushallinnon näkökulmasta potentiaalisia väärinkäytöstapoja on runsaasti. Väärennettyjen laskujen lähettäminen tai maksaminen, tuplalaskutus tai kassavarojen kavaltaminen ovat esimerkkejä kirjanpitoon liittyvistä väärinkäytöksistä. Tämänkaltaiset väärinkäytökset saattavat näkyä muun muassa kassassa tai tileillä, mikä alleviivaa niiden seurannan tärkeyttä. (Haastateltava A).

Vaaralliset työyhdistelmät ovat yksi olennaisimmista riskeistä yritysten taloushallinnossa. Tällainen yhdistelmä syntyy, kun tietylle henkilölle on annettu liikaa oikeuksia tai valtuuksia. Haastateltava A kertoi esimerkkitapauksesta, jossa yrityksen hallitus ei pystynyt valvomaan toimitusjohtajan työtä. Toimitusjohtaja käytti kyseisessä yrityksessä huomattavaa valtaa, ja osallistui esimerkiksi laskujen maksattamiseen. Lopulta kyseinen toimitusjohtaja jäi kiinni, kun yrityksen toimittajia tarkastettiin ja

huomattiin, että yritys oli maksanut toimitusjohtajan nimissä olleiden yritysten valheellisia laskuja.

Asiakkaan ja tilitoimiston välisessä palvelusuhteessa vaarallisia työyhdistelmiä voidaan havaita tarkastelemalla esimerkiksi maksujen hyväksyntäprosessia, kuten edellä Haastateltava A:n esimerkissä. Sisäisellä prosessien tarkastuksella voidaan siis sekä ennaltaehkäistä että jälkikäteen havaita tällaisia työyhdistelmiä ja niihin liittyvää väärinkäyttöä. Työyhdistelmiä tarkasteltaessa kiinnitetään huomiota esimerkiksi maksuvaltuuksiin sekä prosessiohjeiden noudattamiseen. Toisaalta mikäli normaalista toimintatavasta poiketaan, on tärkeää dokumentoida syyt poikkeamiselle, jotta mahdolliset epäselvyydet vältetään. (Haastateltava C.) Tietty haaste vaarallisten työyhdistelmien ja valtuuksien hallinnassa on se, että jollakulla henkilöllä on kuitenkin oltava valtuudet esimerkiksi maksaa laskuja ja tehdä tilisiirtoja.

> Jollain pitää olla oikeus esimerkiksi maksujen lähettämiseen. Siinä tulee sitten se, että jos tällainen henkilö haluaa tehdä jotain väärinkäytöstä siellä, niin sitten täytyy jo softatasolla olla jotkut mekanismit, millä se estetään. Eli aina jonkun ihmisen pitää kuitenkin pystyä tietyt toimenpiteet tekemään.
>
> (Haastateltava D)

Joissain tapauksissa tietynlaisten vaarallisten valtuuksien kertymistä joillekin henkilöille ei ole tarkoituksenmukaista estää, jotta yrityksen prosessit sujuvat jouhevasti. Liian mutkikas prosessi ja liialliset valvontatoimenpiteet eivät ole siten tarkoituksenmukaisia, jolloin valvonnassa on nojattava esimerkiksi jälkikäteiseen valvontaan ja teknisiin ohjausmenetelmiin. Eräs mahdollinen tapa ehkäistä tämänkaltaisia väärinkäytöksiä liittyy tiedon avoimuuteen. Kun useampi ihminen, kuten kirjanpitäjä, tilintarkastaja että asiakasyrityksen henkilöt näkevät saman datan, vähentää se yksittäisen ihmisen halua ja mahdollisuutta väärinkäytöksen tekemiseen (Haastateltava A).

> Jos työntekijä tietää, että siinä on kamera yläpuolella, kassaa ja katteita seurataan tarkasti ja käydään läpi, niin näiden ennaltaehkäisevä vaikutus varmasti vähentää väärinkäytöksen riskiä.
>
> (Haastateltava A)

Tietynlaisia yrityksen liiketoimintaan ja siihen liittyvien henkilöiden välisiä asioita, jotka voivat vaikuttaa väärinkäytöksen tekemiseen on valvonnan näkökulmasta vaikea havaita. Esimerkiksi lähipiiriliiketoimiin liittyy olennaisia väärinkäytösriskejä. Näissä avoimuudella on tärkeä rooli riskien minimoinnissa. Asiakasyritystä arvioidessa on

otettava huomioon kyseisen yrityksen omistajat, edunsaajat ja heidän lähipiirinsä. Lisäksi on syytä selvittää tällaisten henkilöiden ja yritysten väliset toimet kuten saamis-, velka- ja vuokrasuhteet. Mikäli lähipiirin tai heidän yritystensä kanssa käydään kauppaa, on näitä kauppoja tarkasteltava esimerkiksi hintojen ja sisällön suhteen. (Haastateltava B.) Lähipiirin tarkastamista havainnollistaa aiemmin kerrottu Haastateltava A:n esimerkki, jossa toimittajien taustojen tarkastaminen johti väärinkäytöksen paljastumiseen. Tällaisessa tilanteessa tilitoimiston näkökulmasta on valvontatoimenpiteiden lisäksi olennaista, että yrityksen taloushallintoa hoitava työntekijä tuntee asiakkaansa. Toisaalta hankalammaksi asian tekee, mikäli väärinkäytös on suunniteltu huolellisesti ja valetoimittajana käytetään esimerkiksi jonkin toisen henkilön nimissä olevaa yritystä tai bulvaania. Tämänkaltaisia väärinkäytösriskejä on analytiikan keinoin hankala havaita, jolloin valvonta nojaa työntekijän ammattitaitoon. (Haastateltava A.)

Haastateltava B:n mukaan asiakkaat yleensä kertovat avoimesti muista omistamistaan yrityksistä tai suhteista lähipiirin yrityksiin, mutta tällaisten suhteiden kanssa on oltava hereillä, sillä ne eivät tule välttämättä kovin helposti ilmi muutoin. Lisäksi hyvin peiteltyjä väärinkäytössuunnitelmia voi olla hankala paljastaa, mikäli niihin kuuluu useampia yrityksiä.

> … asioita osataan tehdä tosi siististi, että näyttää että kaikki on hienosti, mutta siellä onkin joku mutka kuitenkin olemassa jossain.
>
> Ja kyllähän näissä yrityskuvioissa, että kuka laskuttaa ketä, voi olla aika monimutkaisiakin juttuja, että välillä täytyy paperille piirtää, että mikä on kenenkin myyntiä.
>
> (Haastateltava B)

Useissa tapauksissa voidaankin todeta, että mitä monimutkaisemmasta peittelyjärjestelystä on kyse, sitä vaikeampaa on väärinkäytöksen havaitseminen. Toisaalta monimutkaiset, useita yrityksiä sisältävät järjestelyt voivat toimia myös merkkinä esimerkiksi rahanpesusta. Oman haasteensa tähän voivat tuoda ulkomaankauppaa käyvät tai ulkomailla sijaitsevat yritykset. Näissä tapauksissa tilitoimiston on selvitettävä muun muassa se, käydäänkö kauppaa niin sanottuihin riskimaihin tai pakotelistalla oleviin maihin. (Haastateltava A.)

Tietynlaiset erityiset tilanteet kuten yrityskaupat ja konkurssit voivat aiheuttaa myös väärinkäytöksen riskejä. Tämänkaltaisissa tilanteissa valvonta on usein hyvin hankalaa.

Haastateltava A:n mukaan esimerkiksi konkurssitilanteet saattavat aiheuttaa katvealueita valvontaan, mikä puolestaan avaa mahdollisuuksia tai paineita erilaisille väärinkäytöksille.

5.5 Digitalisaation vaikutus kohdeyrityksen prosesseihin ja sisäiseen valvontaan

5.5.1 Liiketoimintaprosessin digitalisointi

Kohdeyritys on vahvasti digitalisoitunut tilitoimisto, ja yritys tarjoaa asiakkailleen erilaisia sähköisiä taloushallinnon palveluita. Huolimatta siitä, että yritys profiloituu digitaalisten palveluiden tarjoajaksi, on sillä asiakaskunnassaan myös paperista taloushallintoa käyttäviä asiakkaita. Yritys on panostanut kasvunsa myötä prosessiensa ja niiden ohjeiden määrittämiseen ja dokumentointiin, ja Haastateltava D:n mukaan näissä ollaan yrityksessä hyvällä tasolla.

Tilitoimistolla on olemassa haltuunottoprosessi, joka käydään läpi yrityksen tai organisaation tullessa tilitoimiston asiakkaaksi. Haltuunottoprosessi sisältää erilaisia huomioitavia asioita, ja sen mukana asiakassuhteessa otetaan käyttöön tietyt prosessit, joilla varmistetaan toiminnan luotettavuus. Laskujen asiatarkastus ja hyväksyminen on yksinkertainen mutta tehokas valvontamenetelmä, jonka perusajatus on siinä, ettei sama henkilö voi toimia sekä laskun tarkastajana että maksun hyväksyjänä, vaan prosessiin on sisällytettävä useampi henkilö. Ideaalitilanteessa tarkastusprosessissa on henkilöitä sekä asiakasyrityksestä että tilitoimistosta. (Haastateltava A.) Esimerkiksi laskua maksettaessa palveluprosessin yhtenä vaatimuksena on, että laskut ovat asiakkaan toimesta tarkastettu ja hyväksytty, jotta asiakkaan taloushallintoa hoitava tilitoimiston työntekijä voi ne maksaa. Jos taas asiakas pyytää kirjanpitäjää tekemään muita tilisiirtoja, tarvitaan tätäkin varten dokumentaatio asiakkaalta myöhempää tarkastelua varten. (Haastateltava B). Maksuprosessiin voidaan asettaa myös lisää kontrollipisteitä. Esimerkiksi tietyn rahasumman ylittävät maksut ja siirrot voidaan määritellä vaatimaan useamman henkilön hyväksynnän (Haastateltava A).

Selkeä haastatteluissa noussut teema liittyi kirjanpitäjien ammattitaitoon sekä asiakkaiden ja heidän toimintansa tuntemiseen. Asiakassuhteen ulkopuolisen henkilön on todennäköisesti vaikeampi arvioida muun muassa sitä, mitkä seikat ovat asiakkaan toiminnassa normaaleja ja mitkä tekijät saattavat olla merkkejä väärinkäytöksistä (h.

> Iso merkitys on työntekijän osaamisella ja sillä millaisen koulutuksen hän on saanut riskeihin liittyen, jotta hän esimerkiksi ymmärtää mikä on vaarallinen työyhdistelmä, tai kun tulee uusi toimittaja niin hänen täytyy tarkastaa sen taustat. Tämä vaatii paljon ja analytiikka ei tähän ihan pysty.
>
> (Haastateltava A)

Henkilöstön jatkuva kouluttaminen, asiakkaan tunteminen ja riskitietoisuus ovat tärkeässä roolissa esimerkiksi asiakkaan prosessien ja asiakassuhteen kriittisessä arvioinnissa. Tätä arvokasta tietoutta on kuitenkin vaikea lisätä muutoin kuin käytännön työn kautta.

> Siihen on hankalampi vaikuttaa, että kuinka hyvin niitä omia asiakkaita esimerkiksi tunnetaan.
>
> (Haastateltava C)
>
> Jos ei jostain tiedä, niin sellaiseen on aina hankalampi tarttua. Jos sä et tiedä, että miten jotain pitää tehdä niin mistä sä tiedät puuttua tai korjata?
>
> (Haastateltava C)

Asiakkaan tunteminen tapahtuu sekä käytännön asiakastyön että aktiivisen tiedonkeruun kautta. Edellä mainituissa seikoissa tullaan haastateltavien mukaan kuitenkin usein resurssikysymysten äärelle. Yrityksen on valittava, mihin koulutuksiin ja millaisiin työkaluihin investoidaan. Tähän on haastateltavien mukaan törmätty niin laadunvalvonnan ja ohjelmistokehityksen kuin koulutuksenkin kohdalla.

5.5.2 Laadunvalvonta ja digitalisointi

Tutkielman kohdeyrityksellä on oma laadunvarmennuksen yksikkönsä, jonka tehtävänä on tutkia ja tarkastaa yrityksen eri toimistojen työmetodeja ja varmistaa niiden yhdenmukaisuus olemassa olevien prosessiohjeiden ja standardien kanssa. Laadunvarmennuksen tavoitteena on varmistaa tuotetun palvelun laatu, ja samalla tunnistaa toiminnan kehityskohteita. Laadunvalvontaa toteutetaan tietyn väliajoin tehtävillä vuosisuunnitelman mukaisilla tarkastuksilla sekä tarpeen vaatiessa erityistarkastuksilla. Vuosisuunnitelman mukaiset tarkastukset toteutetaan standardoidusti vertailukelpoisen tiedon saamiseksi, kun taas erityistarkastukset voidaan suorittaa tietyn tarpeen, kuten havaitun laatupoikkeaman perusteella. (Haastateltava B; Haastateltava C.)

Käytännön tasolla suunnitelman mukaisessa laadunvarmennuksessa tarkastetaan valikoitujen asiakasyritysten kirjanpitoa, kuten laskuja ja tositteita, sekä tietyt hallinnolliset dokumentit, kuten esimerkiksi yhtiöjärjestys, lainoihin liittyvät asiakirjat ja vuokrasopimukset. Lisäksi tarkastettavan yrityksen kirjanpidolle tehdään erilaisia täsmäytyksiä, joilla osaltaan tarkistetaan kirjanpidossa olevien erien, kuten velkojen täsmääminen. Mikäli kirjanpidossa on virheitä, näkyvät ne eroina täsmäytysraporteilla. (Haastateltava B.)

Tarkastuksen kohteena olevasta toimistosta kultakin kirjanpitäjältä valikoituu muutama yritys, joiden kirjanpidon ja asiakaskansioon tallennetut dokumentit tarkastetaan. Kohdeyrityksellä on konserninlaajuiset ohjeet siitä, mitä ja millaisessa muodossa tietyt asiakirjat pitää asiakaskansiosta löytyä. Lisäksi tarkastukseen kuuluu toimiston työntekijöiden haastattelut. Paperista kirjanpitoa käyttävien asiakkaiden kohdalla prosessi vie enemmän aikaa, eikä välttämättä ole yhtä kattava kuin sähköisen kirjapidon asiakkailla, sillä järjestelmien kautta tapahtuva tarkastus on ajasta ja paikasta riippumatonta. Lisäksi tarkastaja pääsee tutkimaan kaikkia järjestelmään syötettyjä tositteita, ja tarkastamaan esimerkiksi niiden tiliöinnit. Tarkastuksen aikana prosessissa ilmenneet seikat kirjataan ylös, ja ne kootaan palautteeksi, joka käydään läpi tarkastuksen toimistokohtaisessa loppupalaverissa. Mikäli tarkastuksen aikana ilmenee puutteita tai huomautettavaa, otetaan se joko kyseisen työntekijän tai usein myös koko tarkastettavan toimiston kesken esiin. (Haastateltava B; Haastateltava C.)

Varsinaisen tarkastuksen jälkeen, noin 2–3 kuukauden kuluttua pidetään seurantatilaisuus, jolloin käydään esimerkiksi kirjanpitäjän kanssa läpi ne asiakkaat, jotka häneltä tarkastettiin. Seurannan tarkoituksena on varmistaa, että tarkastuksissa ilmenneisiin seikkoihin on reagoitu. (Haastateltava B.)

Erityiset tarkastukset nousevat yleensä esiin yksittäisistä laatupoikkeamista. Nämä tapaukset käydään yleensä läpi lähinnä esimiesten tai liiketoimintajohtajan kanssa, ja ne koskevat usein esimerkiksi tiettyyn yritykseen liittyviä toimintatapoja tai tiettyjä työkäytäntöjä. (Haastateltava C.)

Laadunvarmennuksen olennaisimpana haasteena tällä hetkellä koettiin varmennustyön vaatiman manuaalisen työn määrä. Suuri osa etenkin nimenomaan tarkastustyöstä tapahtuu käsin, ja vaikka sähköisen taloushallinnon järjestelmien avulla kirjanpidon tarkastelu on kätevää, on tarkastus kokonaisuudessaan työläs prosessi. Tällä hetkellä

kukin toimisto tarkastetaan noin joka toinen vuosi. Tämän johdosta laadunvarmennuksen data ei välttämättä ole kovin reaaliaikaista, mikä on tosin tunnistettu yhtenä kehityskohteena. Koska yrityksellä on tuhansia asiakkaita ja siten valtavasti tietoa valvottavana, vaikuttaa se väistämättä laadunvarmennuksen tarkkuuteen. (Haastateltava C.)

> Yksi selkeä riski tai ongelmakohta on se, ettei kattavuus ole niin suuri, että kaikki osuisi niin sanotusti haaviin.
>
> (Haastateltava C)

Haastateltava B:n mukaan laadunvarmennuksen tueksi olisi hyvä saada työkaluja, joilla voidaan hoitaa rutiininomaiset mutta aikaa vievät tarkastuksen osat. Konkreettisena esimerkkinä hän mainitsi kirjanpitäjille teetettyjen kyselymittausten automatisoinnin. Tähän asiaan on yrityksen toimesta jo tartuttu, ja kehitteillä on työkalu, joka pystyisi haarukoimaan kirjanpitäjän antamien kyllä/ei -vastausten mukaan tietyt yritykset jatkotarkastukseen. Toinen kehittämisen kohde Haastateltava B:n mukaan olisi työkalu, jolla voitaisiin tarkastaa, löytyykö asiakastietokannasta kunkin asiakasyrityksen kohdalta tarvittavat dokumentit. Tämänkaltaista tarkastusta on tähän asti tehty käsin, jolloin tarkastettavia kohteita joudutaan valikoimaan. Haastateltava B:n mukaan tämänlaisiin perusasioihin olisi hyvä saada apuvälineitä, jotta tarkastus voisi tulevaisuudessa kattaa koko asiakastietokannan. Edellä mainitun kaltaisiin haasteisiin on jo kehitteillä automaatiotyökaluja, jolla laadunvarmennusprosessia saataisiin muun muassa nopeutettua (Haastateltava D).

Laadunvarmennuksella tehtävä valvonta kohdistuu pääasiassa itse tilitoimiston liiketoimintaprosessiin ja siten välillisesti asiakkaisiin. Siten valvonnan näkökulmasta sellaisia prosessin osia, jotka tapahtuvat kokonaan asiakasyrityksessä on hankala seurata. Tämä koskee etenkin sellaisia tapahtumia ja toimia, jotka eivät taloushallinnon järjestelmän kautta näy tilitoimistolle. Esimerkiksi kirjanpitäjän kannalta kuitenkin oleellista on hoitaa oma tonttinsa, noudattaa prosessiohjeita ja dokumentoida tarvittavat tiedot, mikäli ne eivät automaattisesti tallennu järjestelmiin. (Haastateltava C).

Tällä hetkellä digitaalisia työkaluja käytetään laadunvarmennuksessa lähinnä siinä, kun tarkastajat valikoivat toimistoista tarkastuksen kohteeksi otettavia asiakasyrityksiä. Konserninlaajuisesta asiakasrekisteristä pystytään nykyisten työkalujen avulla haarukoimaan asiakasyrityksiä esimerkiksi koon, yritysmuodon, toimialan tai

liikevaihdon mukaan. Myös tässä asiassa on menty eteenpäin, sillä aiemmin asiakastietokannasta sai tulostettua vain valtavan Excel-tiedoston, jota tarkastajat joutuivat itse käsittelemään sopivia tarkastuskohteita etsiessään. Lopullisen tarkastuksen kohteeksi tulevat yritykset valitaan osittaisella satunnaisotannalla. Tarkastajat valitsevat toimiston asiakkaista tarkastettavat yritykset, ja tämä lista hyväksytetään toimiston palvelupäälliköllä, jotta mahdolliset erityistilanteet kuten poistuvat asiakkaat saadaan haarukoitua tarkastuksesta pois. (Haastateltava B, Haastateltava C.)

5.5.3 Tietotekniikka ja -järjestelmät

Järjestelmiin liittyvät ohjausmenetelmät ovat sähköisessä taloushallinnossa äärimmäisen tärkeitä. Etenkin käyttöoikeuksien, valtuutusten ja lokitietojen merkitys korostui kaikissa haastatteluissa. Kohdeyrityksen strategisena valintana on olla ohjelmistoriippumaton, jolloin asiakkaalle voidaan tarjota eri ohjelmistotoimittajien järjestelmiä. Valvonnan näkökulmasta monen järjestelmän käyttäminen tuo kuitenkin haasteita. Eri järjestelmät eroavat ominaisuuksiltaan ja ne sisältävät erilaisia työkaluja. Yhteinen haaste kuitenkin kaikille järjestelmille on proaktiivisen ja reaaliaikaisen valvonnan puute. (Haastateltava D.)

> Eli jos siellä tehdään jotain väärinkäytöstä, niin päästäisiin siihen heti kiinni jo siinä vaiheessa, kun se tapahtuu.
>
> (Haastateltava D)

Jälkikäteisessä valvonnassa nykyiset järjestelmät ovat kuitenkin hyvällä tasolla, vaikka parannettavaa edelleen löytyy. Esimerkiksi lokitietoja järjestelmässä tehdyistä toimista voisi Haastateltava D:n mukaan kertyä enemmänkin.

Yritys pyrkii tarjoamaan aktiivisesti asiakkailleen sähköisiä taloushallinnon palveluja. Yleisesti haastatteluissa sähköinen kirjanpito koettiin paremmaksi kuin paperinen, ja etenkin valvonnan kannalta sähköisessä kirjanpidossa nähtiin selviä hyötyjä. Ensinnäkin sähköisessä järjestelmässä olevia tietoja voidaan valvoa ja niihin pääsyä voidaan helposti rajoittaa. Toisaalta järjestelmissä oleva tieto on kaikkien järjestelmään pääsevien nähtävillä. Siten tiedot ovat tämän avoimuuden kautta ikään kuin automaattisen valvonnan alla, kun useat ihmiset näkevät sekä tiedot että niissä tehdyt muutokset. (Haastateltava A, Haastateltava C.) Sähköisissä kirjanpitojärjestelmissä raporteilta voidaan porautua yksittäisille tositteille ja niiden liitteisiin asti, mikä helpottaa

jälkikäteistä tarkastamista. Paperista kirjanpitoa tarkistettaessa esimerkiksi laadunvarmennuksen yhteydessä on paperiset tositteet skannattava ja lähetettävä. (Haastateltava B.) Sähköinen kirjanpito helpottaa ja nopeuttaa jälkikäteistä aineiston läpikäyntiä, ja mahdollistaa esimerkiksi laajemman tarkastamisen. Siten esimerkiksi kirjausketjujen (engl. *audit trail*) seuraaminen on huomattavasti helpompaa.

> Kyllä siinä sähköisessä kirjanpidossa on paljon enemmän mahdollisuuksia ja laajemmin pystyy katsomaan kaikkea.
>
> (Haastateltava B)

Digitalisoitumisen myötä yritys on panostanut monipuolisesti myös tietoturvaan. Prosessinäkökulmasta yrityksellä on esimerkiksi salasanapolitiikka, joka ohjaa työntekijöitä päivittämään salasanansa tietyin väliajoin. Lisäksi yrityksen työntekijöille on ohjeistettu esimerkiksi tietokoneiden ja työpuhelimien turvalliseen käyttöön liittyvissä asioissa ja asiakasmateriaalien säilyttämisestä. Sen sijaan teknisestä näkökulmasta yrityksessä on panostettu esimerkiksi verkkojen turvallisuuteen ja käyttöoikeuksien valvontaan. (Haastateltava D.)

Käyttöoikeuksien ja erilaisten valtuutustasojen avulla voidaan hallita sitä, millä henkilöillä on oikeus tehdä mitäkin järjestelmässä. Pääsyn kontrollointi tapahtuu kohdeyrityksessä sovellustuelle lähetettävän tiketin kautta, jolla työntekijä voi pyytää tietyn tasoisia oikeuksia, kuten katselu- tai muokkausoikeuksia yksittäisen asiakkaan järjestelmiin. Tiketistä jää myös dokumentaatio. (Haastateltava C). Käyttöoikeuksien hallintaan ollaan ottamassa yrityksessä käyttöön uutta prosessia, jossa käyttöoikeuspyyntöjen käsittely on keskitetty valvonnan parantamiseksi (Haastateltava D). Tästä kerrotaan lisää alaluvussa 5.6.1. Olennaista sähköisten järjestelmien kanssa toimisessa on, että käyttöoikeuksia valvotaan, jotta tiedetään ketkä järjestelmää käyttää ja mitä he siellä pystyvät tekemään (Haastateltava C). Yritys pyrkii ottamaan käyttöön kertakirjautumisen kaikissa mahdollisissa järjestelmissä. Tällä pyritään vähentämään eri käyttäjätunnusten ja salasanojen määrää ja siten helpottamaan niiden hallintaa. Samoin järjestelmissä pyritään ottamaan käyttöön monivaiheinen tunnistautuminen, jolloin työntekijä varmistaa sisäänkirjautumisen käyttäjätunnuksen ja salasan lisäksi esimerkiksi mobiilisovelluksella. (Haastateltava D.)

Tietyissä asiakassuhteissa taloushallinto on toteutettu siten, että esimerkiksi kirjanpitäjälle annetaan pääsy asiakasyrityksen järjestelmäympäristöön. Tämänkaltainen

järjestely vaatii yhteistyötä asiakkaan järjestelmävastaavan kanssa, jolloin myös järjestelmän valvonta jää käytännössä kokonaan asiakkaan vastuulle. (Haastateltava C.)

Sähköisen järjestelmän etuna on mahdollisuus reagoida nopeasti muuttuviin tilanteisiin. Haastateltava A kertoi tapauksesta, jossa erään yrityksen toimitusjohtaja jäi kiinni hänen omilta yrityksiltään tulleiden tekaistujen laskujen hyväksymisestä. Kyseessä oli hankalasti vältettävissä ollut työyhdistelmä, mutta asian tullessa ilmi kyseiseltä henkilöltä jäädytettiin heti järjestelmien käyttöoikeudet. Tämä kuvastaa hyvin sähköisten järjestelmien etua paperiseen kirjanpitoon verrattuna, sillä käyttöoikeuksien poistamisen jälkeen tekijä ei päässyt enää käsiksi aineistoon. Tällä estettiin esimerkiksi todisteiden muokkaaminen tai hävittäminen.

Yrityksen tarjoamat ohjelmistot keräävät tietoa järjestelmässä tehdyistä toimista. Näitä tietoja kutsutaan lokitiedoiksi. Ohjelmistosta riippuen käyttäjä voi tarkastella, kuka on tehnyt tietyn toimen, ja mihin aikaan. Lokitietojen hyödyt perustuvat Haastateltava C:n mukaan muun muassa siihen, että sähköisessä järjestelmässä tehdyistä toimista jää useimmiten jälki, jolloin järjestelmässä tehtyjen tai tietyn henkilön tekemien toimien jälkikäteinen tarkastelu on helppoa. Lokitietojen kannalta on olennaista, että kaikilla järjestelmää käyttävillä on henkilökohtaiset käyttäjätunnukset.

> Tavallaan kuulostaa perusasialta, mutta jokaisella henkilöllä on järjestelmiin mitä he käyttää, niin henkilökohtaiset käyttäjätunnukset, joka sitten mahdollistaa sen, että meillä jää ne lokitiedot ja muut paljon tarkemmin ylös.
>
> (Haastateltava D)

Tässä asiassa yritys on mennyt viime vuosien aikana eteenpäin, sillä yleisellä tasolla monissa yrityksissä ei edelleenkään huolehdita Haastateltava D:n mukaan riittävästi käyttäjätunnusten hallinnasta. Muun muassa tästä syystä myös kohdeyritys on panostanut käyttäjätunnusten hallintaan viime vuosina.

Yrityksellä on käytössä konserninlaajuinen julkinen raportointityökalu, johon on koottu eri toimistoista ja toimintojen, kuten palkanlaskennan ja kirjanpidon suoritusmittareita. Mittareille on asetettu tavoitetasot, joiden toteutumista seurataan konsernitasolla. Ne toimivat siten kontrollipisteinä, joiden avulla pystytään kohdentamaan tarvittaessa toimenpiteitä, mikäli esimerkiksi tietyn toimiston kohdalla havaitaan laatupoikkeama. Kyseistä raportointityökalua hyödynnetään yrityksen sisäisessä laskennassa, ja tiettyjä

työkalun ominaisuuksia tarjotaan palveluna myös asiakasyritysten omaan käyttöön. (Haastateltava C.)

5.6 Digitalisaatioon ja valvontaan liittyvät kehittämistoimet

5.6.1 Prosessinäkökulma

Laajemmassa kuvassa yrityksellä on Haastateltava D:n mukaan edistysaskelista huolimatta edelleen parantamisen varaa etenkin tietoturvallisen kulttuurin luomisessa ja kehittämisessä. Tähänkin haasteeseen on hänen mukaansa jo tartuttu, ja tavoitteena on kouluttaa henkilöstöä tietoturva-asioissa ja luoda tulevaisuudessa lisää koulutusohjelmia aiheesta. Kokonaisuutena tietoturva on toiminut toistaiseksi hyvin, eikä yrityksessä Haastateltava D:n mukaan ole kohdattu kovin suuria ongelmia. Yksittäisiä, pienempiä tapauksia on vuosien aikana kohdattu, mutta niiden pohjalta tietoturvaa ja valvontaa on aina kehitetty eteenpäin,

> Se lähtee sieltä ihan ylätasolta: miten meidän prosessit toimii? Ja tosiaan sitten lisäksi ihan yksittäisiä toimenpiteitä IT-näkökulmasta.
>
> (Haastateltava D)

Prosessien kehittäminen on kuitenkin aikaa vievää, ja uuden työnkulun luominen vaatii jo itsessään runsaasti työtä. Digitaalisessa ympäristössä on omanlaisensa haasteet, ja automatisoitavien prosessien vaikutus muuhun toimintaan on tärkeä tunnistaa.

> Haaste on se, että nyt kun tehdään automaatiota tai mitä tahansa prosessia, se vaatii paljon laajempaa kokonaisuuden ymmärtämistä kuin mitä aiemmin. Aikaisemmin jos on tehty verkkopankista yksittäisiä maksuja, niin se on selkeä. Mutta jos mietitään, että tuhansien asiakkaiden maksut pyörii jonkun järjestelmän kautta, niin niiden kaikkien asioiden huomioiminen vaatii isompaa kokonaisuuden ymmärtämistä.
>
> (Haastateltava D)

Yrityksessä on toteutettu noin vuosi sitten laaja tietoturvakartoitus, jossa tarkastettiin laajasti kaikki yrityksen prosessit. Tämän kartoituksen pohjalta yrityksessä luotiin tiekartta, jonka mukaan yrityksen tietoturvaa pyritään kokonaisvaltaisesti kehittämään. Tiekarttaan sisältyy esimerkiksi erilaisia IT-projekteja, kuten alaluvussa 5.6.2 esiteltävä DLP-järjestelmä. Järjestelmien lisäksi kehityskohteisiin lukeutuu muun muassa yrityksen käyttämien verkkojen seurannan ja tietoturvan kehittämistä sekä prosessien turvallisuuden kehittämistä. Esimerkiksi käyttöoikeuksien hallintaprosessia ollaan

rakentamassa uudelleen. Uudessa hallintaprosessissa käyttöoikeustiedot on viety yrityksen HR-järjestelmään, jonka kautta voidaan tarkastella kunkin työntekijän käyttöoikeuksia yhdessä paikassa. Käyttöoikeuksien lisäämiseen on luotu yhtenäinen prosessi, jossa työntekijän esimies tekee lähtökohtaisesti käyttöoikeuspyynnön, minkä jälkeen pyyntö käsitellään HR-järjestelmässä. Näin prosessiin lisätään uusi valvontataso eli esimies, kun aiemmin työntekijät ovat itse voineet pyytää käyttöoikeuksia tarvitsemiinsa järjestelmiin ja asiakkaisiin. Kun käyttöoikeustietoja voidaan hallinnoida yhdestä järjestelmästä käsin, myös niiden poistaminen esimerkiksi työntekijän työsuhteen päättyessä on helpompaa. (Haastateltava D.)

Tällä hetkellä yrityksellä ei ole yksittäistä henkilöä, joka vastaisi yrityksen tietoturva-asioista. Haastateltava D:n mukaan tietoturvapäällikön tai vastaavan henkilön tarpeesta on yrityksessä keskusteltu, mutta toistaiseksi tällaiselle positiolle ei ole nähty akuuttia tarvetta. Tällä hetkellä tietoturvaan liittyvät vastuut on hajautettu eri osastojen, kuten esimerkiksi IT-osaston, laadunvalvonnan ja kehitystiimin kesken.

Kohdeyritys on tutkielman tekohetkellä ottamassa käyttöön koko konsernin laajuista rahanpesun ehkäisemiseen ja estämiseen tähtäävää ohjelmaa, joka on osa yrityksen uudistuvaa riskienhallintaprosessia. Pääpaino tässä ohjelmassa on yrityksen asiakkaiden taustojen ja toiminnan tarkistaminen ja valvonta rahanpesun tunnistamiseksi ja havaitsemiseksi. Tavoitteena on siis oppia tuntemaan tilitoimiston asiakasyritykset prosessinmallin kautta, jolloin asiakassuhteeseen liittyviä riskejä voidaan paremmin tunnistaa. Prosessiin kuuluu esimerkiksi tiettyjen avaintietojen kerääminen asiakkaasta, asiakkaan edunsaajat ja suhteet muun muassa poliittisesti vaikutusvaltaisiin henkilöihin sekä muiden kysymysten kautta tehty riskiarvio.

Osana rahanpesun tunnistamis- ja ehkäisyohjelmaa on asiakkaiden taloushallintoa hoitavien työntekijöiden avuksi luotu lista indikaattoreista joihin työntekijöiden tulisi kiinnittää huomiota asiakkaidensa toimintaa arvioidessaan. Listassa on kymmeniä indikaattoreita, joiden avulla voidaan laajasti arvioida asiakasyrityksen toimintaa, taloushallintoa, edunsaajia ja omistajia. Matalan riskin indikaattoreita ovat esimerkiksi havaitut vaaralliset työyhdistelmät, käteispalkat tai epäilyt pimeästi tehdystä työstä. Korkeammasta riskistä voivat kertoa epätavallisen suuri tai pieni liikevaihto, monimutkaiset yritysrakenteet ja poikkeukselliset matkalaskut tai muut korvaukset. Merkittäviä riskiä indikoivat esimerkiksi yrityksen johtoon kuuluvat epäillyt tai tuomitut

rikolliset, havaittu tuplalaskutus tai epäilyt kytköksistä terrorismiin. Indikaattorilista on tarkoitettu työkaluksi asiakkaan taloushallintoa hoitaville tilitoimiston työntekijöille. Mikäli työntekijät kohtaavat listalla mainittuja indikaattoreita työssään, tulee heidän toimia prosessiohjeiden mukaisesti ja ottaa tarvittaessa yhteys esihenkilöön sekä riskinhallintatiimiin.

5.6.2 Järjestelmät ja työkalut

Laadunvarmennuksen haasteena on tällä hetkellä melko raskas manuaalinen tarkastusprosessi. Joiltain osin tarkastajien työtä on helpotettu sähköisten järjestelmien avulla, mutta molemmat Haastateltavat B ja C totesivat, että data-analytiikka ja automaatio toisivat merkittäviä aikasäästöjä heidän työhönsä.

> Aika paljon tehdään manuaalisesti tätä, ja se olisi yksi kehittämisen paikka. Kun käydään nyt yksittäin manuaalisesti läpi, niin data-analytiikka toisi paljon lisäarvoa ja ihan ajan säästöä meidän tarkastuksiimme.
>
> (Haastateltava C)

Haastateltava C:n mukaan ajansäästön lisäksi digitaalisten työkalujen toivottuna hyötynä olisi mahdollisuus tarkastelun lisäksi myös jalostaa dataa. Hänen mukaansa laadunvarmennuksessa tarkoituksena on tulevaisuudessa lisätä automaatiota, jotta varmennusprosessia saadaan nopeutettua ja laajennettua. Tällä hetkellä suurimmat digitaalisten työkalujen tarpeet liittyvät Haastateltava C:n mukaan tiedon läpikäymiseen ja jalostamismahdollisuuksiin. Toisin sanoen tavoitteena on saada automaation avulla suurempi määrä dataa, jota käsittelemällä ja analysoimalla saadaan kattavampaa seurantaa ja tiedon hyödyntämistä. Tätä parempaa tietoa voidaan käyttää päätöksenteossa, jotta tarkempaa seurantaa voidaan kohdentaa prosesseissa havaittuihin poikkeamiin.

Yksi konkreettinen esimerkki valvonnan ja tarkastuksen kehittämisestä on kohdeyrityksessä kehitetty täsmäytysrobotti, jota käytetään kirjanpidon tilien täsmäyttämiseen. Robotille syötetään halutun asiakkaan tiedot, joiden pohjalta se tarkastaa kirjanpitojärjestelmässä olevat tilit. Mikäli robotti huomaa kirjanpidossa eroja, antaa se raportissaan huomautuksen erottavasta tilistä. (Haastateltava B.)

Toinen yrityksessä lähinnä kirjanpitäjille jo kehitetty apuväline on työkalu, joka hakee automaattisesti kunkin asiakkaan kuukausittaiset veroyhteenvedot verottajan Omavero-

palvelusta ja tallentaa ne tiettyyn paikkaan. Tämän työkalun etu on lähinnä ajansäästöllinen. Koska yhdellä kirjanpitäjällä voi olla kymmeniä asiakkaita, on tämä koettu kuitenkin hyödylliseksi avuksi rutiinityötehtävän hoitamiseen. (Haastateltava B.)

Järjestelmien ja tietoturvan näkökulmasta yritykseen ollaan tulevaisuudessa tuomassa järjestelmäkokonaisuus, jonka tarkoituksena on turvata yrityksen tietokannat menettämisen varalta. Datan menettämisen ehkäisyjärjestelmän (engl. *data loss prevention system, DLP system*) tavoitteena on estää tietojen katoaminen yrityksen informaatioympäristössä. Toinen tietoturvaan liittyvä järjestelmä, jota ollaan tuomassa käyttöön, on salasanojen hallintajärjestelmä, jonka tarkoituksena on auttaa eri järjestelmiin olevien salasanojen tietoturvaa ja hallintaa. (Haastateltava D.)

6 Tutkimustulokset ja pohdinta

Tämän tutkielman tarkoituksena on vastata johdannossa esitettyihin tutkimuskysymyksiin tarkastelemalla tilitoimiston ja asiakasyrityksen välistä palvelusuhdetta. Tavoitteena on tarkastella, miten digitalisaatio on vaikuttanut väärinkäytösriskeihin ja valvontaan. Tutkimuskysymyksiin pyritään vastaamaan peilaamalla empiiristä aineistoa tutkielman luvuissa 2, 3 ja 4 esiteltyyn teoreettiseen pohjaan.

1. Miten digitalisaatio on vaikuttanut yritysten väärinkäytösriskeihin?
2. Millaisia vaikutuksia digitalisaatiolla on sisäiseen valvontaan?

Väärinkäytösten näkökulmasta digitalisaatio on tarjonnut toisaalta uudenlaisia mahdollisuuksia tehdä väärinkäytös, mutta samalla se on myös lisännyt kiinnijäämisen riskiä. Kuten haastatteluissa tuli ilmi, pystytään sähköisissä järjestelmissä tekemään nopeasti erilaisia toimia ja siten siirtämään esimerkiksi rahaa tai maksamaan laskuja. Sopivassa asemassa oleva henkilö pystyy siten tekemään lyhyessä ajassa paljon vahinkoa. Vaaralliset työyhdistelmät ovat etenkin pienemmissä yrityksissä tavallisia riskejä, ja niiden välttäminen on kirjallisuudessa laajalti tunnistettu (Ratsula 2016a, 44; Wells 2017, 86). Tietynlaisten riskitekijöiden, kuten vaarallisten työyhdistelmien suora ja etukäteinen havaitseminen digitaalisten työkalujen kuten analytiikan avulla on haastavaa, jolloin väärinkäytösten estämisessä korostuu taloushallinnon henkilöstön osaaminen, prosessien valvonnan suunnittelu ja muunlaiset valvontamenetelmät. Sen sijaan etenkin automatisoinnin ja analytiikan hyödyt tulevat haastatteluiden perusteella parhaiten esiin jälkikäteisessä väärinkäytösten havainnoinnissa, kun suurista datajoukoista etsitään virheitä tai poikkeamia. Väärinkäytösten ehkäisyssä taas auttavat parhaiten hyvin suunnitellut prosessit, joihin on sisäänrakennettu kontrollipisteitä. Esimerkiksi laskujen maksatukseen saavat osallistua vain järjestelmässä kyseisen valtuutuksen saaneet henkilöt, ja toisaalta maksuja ei voi lähettää ennen kuin toinen henkilö on ne järjestelmässä tarkastanut ja hyväksynyt. Sähköiset järjestelmät ovat siten mahdollistaneet sujuvammat taloushallinnon prosessit, joiden hallinta on helpompaa ja käyttäjien valtuuksia pystytään sekä ennalta määrittelemään tarkemmin ja toisaalta heidän tekemiään toimia pystytään jälkikäteen seuraamaan tarkemmin.

Haastatteluissa nousi esiin myös huomio tavoista, joilla digitaalisia valvontamenetelmiä voidaan kiertää. Väärinkäyttäjät saattavat välttää esimerkiksi viestinvaihtoa ja koettaa hoitaa asiansa puhelimitse tai kasvotusten dokumentaation välttämiseksi. Toinen riskialtis tapa on käteisen suosiminen ja sähköisten järjestelmien välttäminen. Väärinkäytöksiä, jotka kohdistuvat prosessien ei-digitaalisiin osiin on haastava huomata suoraan digitaalisten välineiden avulla. Valvonnan näkökulmasta prosesseihin liittyvien riskien analysointi ja oikeanlaisten valvontatoimenpiteiden valinta on tämänkaltaisissa tilanteissa avainasemassa (COSO 2013; Sihvonen ja Uusi-Hautamaa 2019, 92–93, Ratsula 2016a, 61). Kuten luvussa 5.4 esitetyssä käteiskassan kavallusesimerkissä havainnollistettiin, tehokas sisäinen valvonta vaatii erilaisten ohjausmenetelmien yhteistyötä ja koordinointia sekä prosessiin liittyvien riskien tunnistamista.

Haastateltava A mainitsi väärinkäytöksen toteutumiseen vaikuttavana yhtenä olennaisena seikkana siihen liittyvän tiedon avoimuuden. Kun sähköisessä järjestelmässä sama tieto on monen henkilön nähtävillä yhtä aikaa, ja tietoa muokatessa sen tekijästä jää jälki, voi tällainen tiedon avoimuus toimia väärinkäytöksen riskiä vähentävänä tekijänä. Riskiä voi vähentää tiedon näkevien ihmisten lukumäärän lisäksi heidän asemansa. Mikäli asiakassuhteessa saman tiedon näkee sekä asiakasyrityksessä että tilitoimistossa työskenteleviä henkilöitä, on väärinkäyttäjän hankalampi esimerkiksi suostutella muita olemaan huomioimatta toimiaan. Tätä voidaan peilata esimerkiksi Wolfen ja Hermansonin (2004) väärinkäytöstimantin mahdollisuus- ja kyvykkyys-aspekteihin. Kun tieto on monelle henkilölle avointa, vähentää se väärinkäyttäjän kykyä saada muut mukaan juoneensa. Tiedon avoimuus voidaan nähdä sekä kulttuurisena tekijänä että ohjausmenetelmänä, jolloin se toimii valvonnan osana ja siten vaikuttaa väärinkäytöstimantin mahdollisuuteen.

Toinen kiinnostava huomio Haastateltava A:lta oli näkemys tiettyjen ohjausmenetelmien olemassa olon vaikutus ihmisten käyttäytymiseen. Mikäli työntekijät tietävät, että toimintaa valvotaan aktiivisesti ja tarkasti, on ohjausmenetelmillä tietynlainen karkottava vaikutus potentiaalisiin väärinkäyttäjiin. Esimerkiksi tieto valvontakameroista tai kirjanpidon säännöllisistä tarkastuksista saattaa vähentää väärinkäyttäjän motivaatiota tehdä väärinkäytös. Näin teoriassa jälkikäteiseen valvontaan suunnitellut ja tarkoitetun menetelmät voivat toimia myös väärinkäytöksiä etukäteen ehkäisevinä tekijöinä, jolloin uusien ohjausmenetelmien käyttöönotto ja niistä tiedottaminen saattavat estää väärinkäytöksiä.

Olennainen osa sähköistä taloushallintoa ja sisäistä valvontaa ovat järjestelmien käyttöoikeudet ja niiden pohjalta kertyvät lokitiedot. Haastatteluiden perusteella kohdeyrityksessä ollaan melko hyvällä tasolla käyttöoikeuksien hallinnassa, ja prosessia kehitetään keskitetympään suuntaan, jossa tavoitteena on nopeamman reagoinnin mahdollisuus, lisääntynyt automaatio ja tehokkaampi käyttöoikeuksien valvonta. Ratsulan (2016a, 242–243) mukaan käyttäjäoikeuksia tulisi rajata siten, ettei työntekijöillä ole liian laajoja valtuuksia. Samoin tunnusten lainaamista ja yhteiskäyttötunnuksia tulisi välttää, ja olemassa olevat oikeudet tulisi dokumentoida. Tutkielman kohdeyritys on panostanut juuri tämänkaltaisten riskien minimointiin kehittämällä käyttöoikeuksien hallintaprosessia sekä ottamalla käyttöön kertakirjautumisen ja henkilökohtaiset tunnukset. Huomionarvoista on, että yritysostojen kautta kohdeyritys on päässyt näkemään muiden alan toimijoiden IT-kontrollin tasoa, joka haastatteluiden perusteella on monessa paikassa kohdeyritystä heikommalla tasolla.

Digitalisaatiota ei voida sen hyödyistä huolimatta pitää kokonaisvaltaisena ratkaisuna sisäisen valvonnan haasteisiin. Haastateltavien mukaan yksittäiset tekniset ratkaisut toimivat hyvin määriteltyjen prosessien pohjalta. Valvonnan suunnittelun lähtökohtana ei siis voi olla teknologisten apuvälineiden käyttö, vaan kunkin valvottavan prosessin tarpeet. Siten kokonaisvaltainen riskianalyysi ja sen pohjalta valittavat sopivat toimenpiteet ovat lähtökohta tehokkaalle valvonnalle. Tämä on tunnistettu myös sisäisen valvonnan kirjallisuudessa (Eling & Schnell 2016, 479–480), ja sama ajatus toimii myös COSOn (2013) viitekehyksen pohjana.

Kohdeyritys on haastatteluiden perusteella panostanut riskienhallintaan ja valvontaan sekä prosessien että yksittäisten ohjausmenetelmien näkökulmasta. Iso edistysaskel on käyttöönottovaiheessa oleva rahanpesun tunnistamis- ja ehkäisyohjelma, jonka tarkoituksena on tilitoimiston asiakkaisiin liittyvien riskien kartoittaminen. Prosessi on pyritty järjestämään tehokkaasti hyödyntämällä muun muassa asiakkaalle lähetettäviä automaattisia kyselyitä, joilla kerätään avaintietoja asiakasyrityksestä. Rahanpesun tunnistamisohjelman prosessi sekä sen yhteydessä esitellyt työkalut, kuten indikaattorilista voivat auttaa taloushallinnon työntekijöitä tunnistamaan myös väärinkäytöksille tyypillisiä riskejä. Toisaalta väärinkäytöksinä pidetyt teot, kuten väärennetyt laskut voivat liittyä myös rahanpesuun.

Toimiva tietoturva on vahvasti digitalisoituneille yrityksille elinehto. Kohdeyrityksessä on investoitu tietoturvaan tuomalla uusia järjestelmiä, kuten DLP-järjestelmä. Yritys on myös tuotteistanut tietoturvaa oman IT-ympäristön omaaville asiakkaille. Yritys tarjoaa VPN-ratkaisuja, joilla taloushallinnon työntekijä pääsee turvallisesti asiakkaan omaan IT-ympäristöön ja siten taloushallinnon järjestelmiin.

Vaikka tietoturva on toiminut haastatteluiden perusteella hyvin ilman suurempia ongelmia, on yrityksellä kuitenkin kehitettävää etenkin tietoturvallisen kulttuurin luomisessa. Kulttuurin merkitys on sekä väärinkäytösten että sisäisen valvonnan kirjallisuudessa nostettu erittäin tärkeäksi seikaksi (Ratsula 2016a, 297; Moeller 2013, 43). COSO-mallin ohjausympäristö mielletään usein sisäisen valvonnan kulttuurina. Ohjausympäristön laatimisesta ja muokkaamisesta vastaa pitkälti yrityksen ylin johto, mutta myös omalta osaltaan myös keskijohto ja operatiiviset työntekijät. Tähän peilaten saattaa olla, ettei yrityksen johto ole sisäisen valvonnan linjassaan korostanut tai huomioinut riittämiin tietoturvan roolia yrityksen toiminnassa ja välittänyt tätä viestiä koko organisaatioon. Kuten tutkielman luvussa 4 esitettiin, on teknologialla ja tietoturvalla olennainen merkitys nykypäivän liiketoiminnassa. Tämän vuoksi näihin liittyviin epäkohtiin on syytä reagoida jo ennen kuin ne johtavat ongelmiin.

Kohdeyrityksellä ei ole tällä hetkellä henkilöä, joka vastaisi yrityksen tietoturvasta. Asiasta on Haastateltava D:n mukaan käyty keskusteluja, mutta tällaista positiota ei ole nähty toistaiseksi tarpeelliseksi, vaan vastuu tietoturvasta on jaettu useamman osaston kesken. Sinänsä kirjallisuuden valossa tämä ei ole ongelma, sillä toimiva valvonta vaatii joka tapauksessa tehokasta kommunikaatiota ja yhteistyötä eri osastojen välillä vaikka tietoturvan johtaminen olisikin vain yhden henkilön vastuulla. Tietohallinto on mahdollista järjestää keskitetysti, hajautetusti tai ulkoistetusti, mutta tehokkuuden kannalta tärkeää on, että roolit ja vastuut on määritelty selkeästi, ja IT:n toiminnalle ja kehittämiselle on olemassa strategia. (Ratsula 2016a, 240.) Eräs tapa järjestää IT:hen liittyvien riskien hallinta on Elingin ja Schnellin (2016, 479–480) mukaan luoda tietoturvasta ja kyberriskien hallinnasta vastaavan tietoturvapäällikön positio, mikä saattaisi selkeyttää tietoturvan kehittämistä.

Sisäinen laadunvarmennus näyttelee tärkeää roolia kohdeyrityksen sisäisessä valvonnassa. Haastateltujen henkilöiden mukaan laadunvarmennuksen tehtävä on varmistaa lakien, säädösten sekä laadittujen prosessiohjeiden noudattaminen sekä

tuotetun palvelun tasainen laatu. Tämä on hyvin lähellä myös esimerkiksi COSOn (2013) sisäisen valvonnan tavoitetta. Määritelmällisesti kohdeyrityksen laadunvarmennusfunktio ja siten haastateltavat B ja C sijoittuisivat kolmen puolustuslinjan mallissa kolmanteen puolustuslinjaan. Haastateltavat A ja D sen sijaan sijoittuvat mallissa toiseen puolustuslinjaan.

Haastattelujen perusteella laadunvarmennustyö on hyötynyt sähköisistä taloushallinnon järjestelmistä. Sähköisissä järjestelmissä olevien tietojen tarkastelu on kätevää, ja tietojen tarkastelussa voidaan siirtyä nopeasti tilitasolta yksittäisille tositteille ja kirjauksille, jonka lisäksi erilaisten liitetiedostojen ja tositteisiin liitettyjen kommenttien kautta voidaan tarkistaa kirjauksen tekijän perusteet toimilleen. Lisäksi järjestelmien lokitietoja voidaan hyödyntää jälkikäteen esimerkiksi tietyn henkilön toimia tarkastellessa.

Sähköisten järjestelmien voidaan siis nähdä parantaneen jälkikäteisen valvonnan tarkkuutta. Haastatteluissa kuitenkin nähtiin haasteena varmennuksen vaatima manuaalisen työn määrä. Tämän vuoksi tarkastukset pohjautuvat edelleen pitkälti satunnaisotantaan ja pistokokeisiin laajamittaisten automatisoitujen tarkastusten sijaan. Bettin ja Sarensin (2020) mukaan digitalisaatio on lisännyt sisäiseen tarkastuksen vaatimuksia ensinnäkin laajuuden ja toisaalta ketteryyden suhteen. Tehokkaan valvonnan saavuttamiseksi tarkastusten tulisi käsittää entistä laajempia alueita, ja toisaalta tarkastusten tulisi myös valmistua nopeammin. Haastatteluissa laadunvarmennuksen kohdalla esiin nousi tarve automaatiotyökaluille, joiden avulla tiettyjä rutiininomaisia tarkastuksen osia voitaisiin nopeuttaa, ja toisaalta analytiikkatyökaluille, joilla tarkastuksista saataisiin yhä enemmän hyötyä yritykselle.

Yhteenvetona voidaan todeta, että yritys on tällä hetkellä melko hyvällä tasolla digitalisaation hyödyntämisessä. Viime vuosina toteutettujen yritysostojen kautta kohdeyritys on saanut kattavan kuvan suomalaisten tilitoimistojen toiminnasta. Haastateltavien mukaan moniin muihin yrityksiin verrattuna tutkielman kohdeyrityksessä ollaan monessa asiassa näitä yrityksiä kokonaisvaltaisesti edellä etenkin järjestelmiin liittyvän sisäisen valvonnan suhteen. Esimerkiksi henkilökohtaiset käyttäjätunnukset ja lokitietojen kerääminen eivät ole Haastateltava D:n mukaan olleet monissa yrityksissä kovin pitkään itsestään selvyyksiä, vaikka sisäisen valvonnan kirjallisuudessa IT-kontrollin tärkeys on tunnettu jo jonkin aikaa (COSO 2013, Moeller 2013). Kuitenkin vaikka prosessi- ja järjestelmätasolla yritys on hyvällä tasolla ja näiden kehittämiseen

investoidaan haastatteluiden perusteella myös tulevaisuudessa, on valvonnan ja väärinkäytösten ehkäisyn näkökulmasta olennaista, että yrityksessä vallitsee tietoisuus ja oikeanlainen kulttuuri tietoturvan suhteen. Samoin nykyiseen hyvään tilanteeseen pohjaten yrityksellä on hyvät edellytykset kehittää toimintaansa eteenpäin ja lisätä digitalisaatiota koko organisaatiossa.

Tutkielman empiirisen aineiston perusteella vaikuttaa siltä, ettei digitalisaatiolla ole ollut suurta vaikutusta väärinkäytösten juurisyihin. Sen sijaan digitalisaatio on tuonut uusia välineitä ja keinoja väärinkäytösten tekemiseen, esimerkiksi järjestelmien ja prosessien heikkojen kohtien tai tietoturva-aukkojen hyväksikäyttämiseen. Sisäisen valvonnan näkökulmasta on tärkeä tunnistaa digitaalisissa järjestelmissä ja prosesseissa olevia riskejä ja heikkoja kohtia, ja tarkastella valvontatoimenpiteiden suunnittelussa niiden vaikutusta liiketoiminnan kokonaisuuteen yksittäisten prosessien lisäksi. Digitalisaatio on mahdollistaa muun muassa automaation, robotiikan ja analytiikan käytön valvonnan tukena. Tässä on kuitenkin omat haasteensa, sillä riskien ja heikkouksien tunnistaminen ei ole välttämättä yksioikoista, ja se nojaa edelleen vahvasti inhimilliseen osaamiseen. Lisäksi oikeanlaisen osaamisen haaliminen saattaa yrityksen näkökulmasta olla haastavaa. Toiminnan kehittämisessä törmätään usein myös resurssikysymyksiin, jotka tuovat oman haasteensa, kun yrityksissä pohditaan tärkeimpiä investointi- ja koulutuskohteita.

7 Yhteenveto

Tämän tutkielman tavoitteena oli selvittää, miten digitalisaatio on vaikuttanut yrityksen kohtaamiin väärinkäytösriskeihin ja yrityksen sisäiseen valvontaan. Tarkoituksena oli tarkastella kohdeyrityksen kautta tarkastella yhtäältä sitä, mitä muutoksia digitalisaatio on tähän mennessä tuonut yrityksen toimintaan ja toisaalta sitä, mitä vaatimuksia se asettaa yrityksen tulevalle kehitykselle.

Tutkielma lähti liikkeelle erilaisten väärinkäytösten määrittelystä ja luokittelusta. Väärinkäytöksellä tarkoitetaan yleisesti tekoa, jolla tavoitellaan epärehellistä tai laitonta hyötyä itselle tai muille. Väärinkäytöksen toteuttamisessa käytetään usein hyväksi muun muassa vilppiä, petosta tai huijausta.

Väärinkäytöksiä voidaan jaotella eri tavoin, esimerkiksi tekotapojen mukaan. ACFE (2020) käyttää jaottelee väärinkäytökset korruptioon, varojen väärinkäyttöön ja tilinpäätöksiin liittyviin väärinkäytöksiin. Nämä päätyypit ovat laveita, ja ne jakautuvat edelleen alatyyppeihin. Huomionarvoista on, etteivät nämä väärinkäytöstyypit ole toisiaan poissulkevia, vaan yhdessä väärinkäytöstapauksessa saattaa usein esiintyä useampaan eri kategoriaan kuuluvaa tekotapaa.

Väärinkäytökset voidaan jakaa myös tekijän mukaan työntekijöiden, johtajien ja omistajien tekemiin väärinkäytöksiin. Näissä väärinkäytöksissä puhutaan sisäisistä väärinkäytöksistä. Väärinkäytösten tekijä voi tulla myös yrityksen ulkopuolelta. Esimerkiksi asiakkaiden tai toimittajien tekemiä väärinkäytöksiä kutsutaan ulkopuolisiksi väärinkäytöksiksi.

Tutkielmassa perehdyttiin myös erilaisiin väärinkäytöksiä kuvaaviin viitekehyksiin. Kirjallisuudessa ensimmäisiä ja suosituimpia viitekehyksiä on väärinkäytöskolmio. Malli muodostuu kolmesta osa-alueesta, koetusta paineesta, koetusta mahdollisuudesta ja rationalisoinnista, ja se kuvaa elementtejä, joiden samanaikainen olemassaolo saattaa altistaa organisaation väärinkäytökselle. Väärinkäytöskolmion pohjalta on myöhemmin kehitetty uusia paranneltuja viitekehyksiä, kuten väärinkäytöstimantti ja MICE-malli, väärinkäytösten havainnollistamiseen ja arviointiin.

Tutkielman kolmannessa luvussa esiteltiin yrityksen sisäistä valvontaa. Sisäinen valvonta on olennainen ohjausjärjestelmä väärinkäytösten ehkäisemisessä ja havaitsemisessa, ja tutkielmassa se nähtiin ikään kuin vastavoimana väärinkäytöksille. Luvussa tarkasteltiin

sisäisen valvonnan historiaa ja kehitystä, ja esiteltiin kaksi sisäisen valvonnan viitekehystä. Simonsin (1995, 2013) viitekehys pohjaa hyvin perinteiseen käsitykseen sisäisestä valvonnasta. Sisäinen valvonta pohjaa alun perin kirjanpidon ja tilintarkastuksen teoriaan, ja sen tarkoituksena on perinteisesti nähty lähinnä tiedon oikeellisuuden varmistaminen, virheiden korjaaminen ja organisaation omaisuuserien suojaaminen. Simons käsittää sisäisen valvonnan omana mekanistisena toimintonaan, joka palvelee yrityksen diagnostista ohjausta.

COSOn (2013) sisäisen valvonnan viitekehys edustaa modernimpaa, kokonaisvaltaisempaa käsitystä sisäisestä valvonnasta. Sen mukaan sisäinen valvonta on koko organisaation kattava jatkuva prosessi, joka pohjautuu organisaation tavoitteisiin ja ulottuu kaikkiin organisaation prosesseihin ja koko henkilöstöön. Malli koostuu sisäisen valvonnan viidestä komponentista, jotka ovat ohjausympäristö, riskien arviointi, valvontatoimenpiteet, informaatio & viestintä sekä seurantatoimenpiteet. Sisäinen valvonta nähdään iteratiivisena, toistuvana prosessina, jossa edellä mainitut komponentit rakentuvat toistensa päälle.

Tutkielman viimeinen teorialuku käsittelee digitalisaatiota ja sen tuomaa muutosta yritystoimintaan. Digitalisaatiolla tarkoitetaan yleisesti teknologisten innovaatioiden lisääntymistä ja yleistymistä. Näiden innovaatioiden avulla jatkuvasti lisääntyvää digitaalista dataa voidaan hyödyntää.

Digitalisaatio on tuonut sekä riskejä että mahdollisuuksia. Digitalisaatioon liittyviä riskejä kutsutaan tavallisesti kyberriskeiksi. Yleistäen voidaan todeta, että mitä vahvemmin yritys on digitalisoitunut, sitä alttiimpi se on kyberriskeille. Monien yritysten prosessit ovat joko kokonaan tai osittain digitalisoituja. Kun prosessit ja järjestelmät ovat digitaalisesti linkittyneet toisiinsa, voidaan myös kyberriskien katsoa koskevan kaikkia järjestelmiä näiden linkkien välityksellä. Toisin sanoen, jos johonkin yrityksen järjestelmään kohdistuu kyberuhkia, koskevat ne järjestelmän linkkien kautta myös muita järjestelmiä. Kyberriskit koskevat laajasti niin yrityksen järjestelmiä, datavarantoja kuin liiketoimintaakin. Siksi yritysten on pyrittävä sekä minimoimaan näitä riskejä että varautumaan niiden realisoitumiseen. Tähän yritys tarvitsee sekä suunnitelmia prosessitasolla että erilaisia teknisiä ratkaisuja kuten analytiikkatyökaluja, palomuureja ja IT-ympäristöön liittyviä valvontatoimenpiteitä. Apuna yritykset voivat käyttää esimerkiksi COSO-malliin kuuluvia IT-menetelmiä.

Tutkielman empiirisessä osuudessa tarkasteltiin taloushallinnon palveluita tarjoavaa tilitoimistoa. Tutkielmaa varten haastateltiin neljää yrityksessä työskentelevää henkilöä. Lisäksi empiriassa käytettiin muuta yrityksen sisäistä materiaalia, kuten koulutusmateriaalia, ohjeistuksia ja sähköpostikeskusteluja. Empiirisessä analyysissä keskityttiin tarkastelemaan tilitoimiston ja sen asiakasyritysten välistä palvelusuhdetta. Tarkastelussa keskityttiin etsimään väärinkäytöksiin ja valvontaan liittyviä teemoja, ja pohtimaan digitalisaation vaikutusta niihin.

Vertaamalla empiiristä aineistoa ja kirjallisuuden teemoja voidaan todeta, että kohdeyritys on tunnistanut hyvin tärkeitä digitalisaation tuomia muutoksia yritystoimintaan ja pyrkinyt panostamaan tehokkaan valvontaympäristön luomiseen. Yritys on luonut asiakassuhteen hoitoon prosessimallin, jonka tarkoituksena on tuottaa laadukasta palvelua ja toimia työkaluna riskien minimoimisessa. Prosessin suunnittelussa on otettu huomioon digitalisaation tuomat vaatimukset esimerkiksi käyttäjätunnusten hallintaan liittyen.

Tällä hetkellä yritys hyödyntää runsaasti digitaalisia järjestelmiä prosesseissaan. Se on myös pyrkinyt tuomaan automaatiota esimerkiksi kirjanpitoprosessiin. Haastatteluissa nousi kuitenkin esiin tarve laadunvarmennuksessa käytettäville automaatiotyökaluille, joiden avulla tarkastustyötä kyettäisiin nopeuttamaan ja laajentamaan. Digitalisaation yhtenä suurena hyötynä nähdään yleisesti sekä kirjallisuudessa että käytännössä nimenomaan automaation ja analytiikan hyödyntäminen, joiden avulla rutiininomaiset tehtävät voidaan hoitaa nopeasti ja yrityksen hallinnoimaa dataa voidaan jalostaa arvoa tuottavaan käyttöön. Kohdeyritys on pyrkinyt ja pyrkii tulevaisuudessakin panostamaan teknologiaan toimintansa tehostamiseksi. Toinen tärkeä huomio liittyi yrityksen tietoturvaan ja sitä ympäröivään kulttuuriin. Järjestelmien ja prosessien tasolla yrityksen tietoturva on nähty toimivaksi, mutta haastatteluiden perusteella kehittämiskohteena voidaan nähdä tietoturvallisen kulttuurin luominen esimerkiksi koulutusten ja tietoturvaan liittyvän tiedottamisen kautta.

Väärinkäytöksiin digitalisaatio on tuonut myös omat muutoksensa. Nämä liittyvät tutkielman empirian perusteella väärinkäytösten tekotapoihin ja käytettävissä oleviin metodeihin. Samalla yritysten käyttöönottamista teknologisista järjestelmistä ja niihin liittyvistä prosesseista voi löytyä uudenlaisia heikkouksia, joita väärinkäyttäjät voivat käyttää hyväkseen. Väärinkäytösten merkkejä voidaan yrittää etsiä erilaisten työkalujen

avulla, kuten esimerkiksi haarukoimalla suuresta datamäärästä poikkeamia. Tärkeäksi teemaksi nousi myös asiakkaan toiminnan tunteminen. Jotta väärinkäytösriskejä voidaan vähentää, on prosessit suunniteltava riittävän yksinkertaisesti. Tällöin suureen tietomäärään tai monimutkaisten järjestelyjen taakse hankalampi piilottaa väärinkäytöksiä. Samoin tietyin valvontamenetelmin voidaan vähentää riskejä prosessin eri kohdissa, kuten tarkistamalla asiakasyrityksen tai sen toimittajien taustat.

Yrityksen on helpointa vaikuttaa niihin väärinkäytösten riskeihin, jotka sijaitsevat sen sisällä. Empiirisen analyysin perusteella ei kuitenkaan vaikuta siltä, että digitalisaatiolla olisi ollut vaikutusta väärinkäytösten syntymisen juurisyihin. Toisin sanoen, vaikka digitalisaatio on vaikuttanut siihen, *miten* väärinkäytöksiä toteutetaan, ei sillä ole ollut huomattavaa vaikutusta siihen, *miksi* väärinkäytöksiä tapahtuu.

8 Lähteet

ACFE (2020) Association of Certified Fraud Examiners. Report to the Nations: 2020 Global study on occupational fraud and abuse.

ACFE (2018) Association of Certified Fraud Examiners. Report to the Nations: 2018 Global study on occupational fraud and abuse.

ACFE (2016) Association of Certified Fraud Examiners. Report to the Nations: 2016 Global study on occupational fraud and abuse

AIA (1936) Examination of financial statements by independent public accountants. Accounting Trends and Techniques. https://egrove.olemiss.edu/aicpa_att , haettu 5.9.2021.

Albrecht S. – Howe K. – Romney, M. (1984) Deterring Fraud: The Internal Auditor's Perspective. Institute of Internal Auditors Research Foundation, Lake Mary.

Allan R. (2003) The human face of fraud: understanding the suspect is vital to any investigation. CA Magazine – Chartered Accountant. Vol 136, Nro. 4, s. 39-40.

Arwinge O. (2014) Internal Control in the Financial Sector – A Longitudinal Case Study of an Insurance Company. (PhD Dissertation) http://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-218906, haettu 4.7.2021.

Baines L. – Grinevih V. – Karatas-Ozkan M. (2018) Digitalisation and the role of the board. Research handbook on boards of directors. Edward Elgar Publishing Ltd. Cheltenham.

Bankewitz M. – Åberg C. – Teuchert C. (2016) Digitalization and Boards of Directors: A New Era of Corporate Governance? Business and Management Research. Vol. 5, Nro. 2, s. 58-69.

Betti N. – Sarens G. (2020) Understanding the internal audit function in a digitalised business environment. Journal of Accounting & Organizational Change Vol. 17, Nro. 2, s. 197-216.

Bonny P. – Goode S. – Lacey D. (2015) Revisiting employee fraud: gender, investigation outcomes and offender motivation. Journal of Financial Crime. Vol. 22 Nro. 4, s. 447-467.

Bredmar, K. (2017), Digitalisation of Enterprises Brings New Opportunities to Traditional Management Control, Business Systems Research, Vol. 8, Nro. 2, s. 115-125.

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

Chenhall R. (2003) Management control systems design within its organizational context: findings from contingency-based research and directions for the future. Accounting, Organizations and Society. Vol. 28, s. 127-168.

COSO (2015) Leveraging COSO Across the Three Lines of Defense. Committee of Sponsoring Organizations of the Treadway Commission & The Institute of Internal Auditors. https://www.coso.org/Pages/guidance.aspx, haettu 1.10.2021.

COSO (2013) Internal Control – Integrated Framework: Executive Summary. Committee of Sponsoring Organizations of the Treadway Commission. https://www.coso.org/Pages/guidance.aspx, haettu 9.6.2021.

Cressey D. (1953) Other People's Money: A Study in the Social Psychology of Embezzlement Free Press, Glencoe.

Damianides M. (2005) Sarbanes-Oxley and IT Governance: New Guidance on IT Control and Compliance. Information systems management. Nro. 22 (1), s.77-85

Donghui L. (2021) Problems and Countermeasures of Enterprise Internal Control in Big Data Environment. Journal of Physics: Conference Series.

Dorminey J. – Fleming S. – Kranacher M. – Riley R. (2010) Beyond the Fraud Triangle – Enhancing Deterrence of Economic Crimes. The CPA Journal. Vol. 80. Nro. 7, s. 16-23.

Dorminey J. – Fleming S. – Kranacher M. – Riley R. (2012) The Evolution of Fraud Theory. Issues in Accounting Education. Vol. 27, Nro. 2, s. 555-579.

Eling M. – Schnell W. (2016) What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance. Vol. 17 (5) s. 474-491

Ergin E. – Erturan I. (2019) Fraud Evasion Triangle: Why Can Fraud Not Be Detected? Journal of Accounting, Finance and Auditing Studies. Vol. 5/4, s. 35-45

EY (2017) Cybersecurity regained: preparing to face cyber attacks. *20th Global information security survey 2017-2018.* < https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/digital/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf>, haettu 20.10.2021.

Flamholtz E. – Das T. – Tsui A. (1985) Toward an integrative framework of organizational control. Accounting Organizations and Society. Vol. 10 (1) s. 35-50.

Heier J. – Dugan M. – Sayers D. (2005) A century of debate for internal controls and their assessment: a study of reactive evolution. Accounting History. Vol 10, Nro 3, s. 39-70.

Hyppönen M. (16.2.2017) Hyvä paha digitalisaatio: Verkkorikollisuuden monet kasvot. DNA Business. https://www.youtube.com/watch?v=3l7geUpnAv0, haettu 19.11.2021.

IIA (2017) International Standards for the Professional Practice of Internal Auditing. Institute of Internal Auditors.

IIA (2013) The Three Lines of Defense in Effective Risk Management and Control. Institute of Internal Auditors Position Paper, January 2013.

ISA 240. International Standard on Auditing 240 – The Auditor's Responsibility to Consider Fraud in an Audit of Financial Statements. 15.12.2004. https://www.ifac.org/system/files/downloads/2008_Auditing_Handbook_A080_ISA_240.pdf, haettu 20.9.2021.

Ikäheimo S. – Laitinen E. – Laitinen T. – Puttonen V. (2014) Yrityksen taloushallinto tänään. Vaasan Yritysinformaatio Oy. Vaasa.

Klamm B. – Weidenmier Watson M. (2009) SOX 404 Reported Internal Control Weaknesses: A Test of COSO Framework Components and Information Technology. Journal of Information Systems. Vol. 23, Nro. 2, s. 1-23.

Korruptiontorjunta.fi. Mitä on korruptio? https://korruptiontorjunta.fi/mita-on-korruptio, haettu 20.9.2021.

Korruptiontorjunta.fi Korruptiontorjunta Suomessa. https://korruptiontorjunta.fi/kansalliset-lait, haettu 20.9.2021

Kranacher, M. – Riley R. – Wells J (2011) Forensic Accounting and Fraud Examination. New York. John Wiley & Sons.

Kyberturvallisuuskeskus (4.2.2020.) Traficom nostaa kyberturvallisuuden yritysten hallitusten agendalle. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/traficom-nostaa-kyberturvallisuuden-yritysten-hallitusten-agendalle

Lamberton B. – Mihalek P. – Smith C. (2005) The Tone at the Top and Ethical Conduct Connection. Strategic Finance. Vol. 86, Nro. 9, s. 36-39.

Lukka, Kari (2005) Approaches to case research in management accounting: the nature of empirical intervention and theory linkage. Accounting in Scandinavia – the Northern Lights, Liber AB, Malmö.

Lukka, Kari (1991) Laskentatoimen tutkimuksen epistemologiset perusteet. Liiketaloustieteen aikakausikirja, Vol. 40 (2), 161–186.

Maijjoor S. (2000) The Internal Control Explosion. International Journal of Auditing. Vol. 4, s. 101-109.

Malmi T. – Brown D. (2008) Management control systems as a package – Opportunities, challenges and research directions. Management Accounting Research Vol. 19 s. 287–300

Merchant K. – Otley D. (2007) A Review of the Literature on Control and Accountability. Handbook of Management Accounting Research. Vol. 2. Elsevier Ltd. s. 785–802

Moeller R. (2013) Executive's Guide to COSO Internal Controls: Understanding and Implementing the New Framework, John Wiley & Sons Inc., Somerset.

Niemi P. (2018) Sisäinen tarkastus käytännössä. Helsinki. Alma.

Osakeyhtiölaki 2006/624 https://www.finlex.fi/fi/laki/ajantasa/2006/20060624 26.4.2021

PwC (2020) Fighting Fraud: A never-ending battle. PwC's Global economic Crime and Fraud Survey. Pricewaterhouse Coopers. https://www.pwc.com/fraudsurvey, haettu 27.9.2021

PwC (2018) Tunnista ja hallitse väärinkäytösriskit yrityksessäsi. PwC's Global Economic Crime and Fraud Survey 2018. PricewaterhouseCoopers. https://www.pwc.fi/fi/julkaisut.html, haettu 28.9.2021.

Rae K. – Subramaniam N. (2008) Quality of internal control procedures: Antecedents and moderating effect on organisational justice and employee fraud. Managerial Auditing Journal Vol. 23 Nro. 2, s. 104-124

Ratsula N. (2020) Interplay Between Technical and Social Control: Internal Control and SOX Compliance at Nokia. Turun Yliopiston julkaisuja. Turku

Ratsula N. (2016a) Yrityksen sisäinen valvonta. Edita Publishing Oy. Kerava.

Ratsula N. (2016b) Compliance – Eettinen ja vastuullinen liiketoiminta. Talentum. Helsinki.

Rezaee Z. – Riley R. (2010) Financial Statement Fraud : Prevention and Detection. Wiley. Hoboken.

Rikoslaki 1889/39 https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Ruankaew T. (2016) Beyond the Fraud Diamond. International Journal of Business Management and Economic Research. Nro. 7(1), s. 474–476.

Salminen M. (16.2.2017) Hyvä paha digitalisaatio: Verkkorikollisuuden monet kasvot. DNA Business. https://www.youtube.com/watch?v=3l7geUpnAv0, haettu 18.11.2021.

Sihvonen J. – Uusi-Hautamaa (2019) Väärinkäytökset yrityksissä – Ehkäise, havaitse, korjaa.

Simons R. (2014) Performance Measurement and Control Systems for Implementing Strategy Text and Cases: Pearson, Essex.

Simons R. (1995) Levers of Control – How Managers Use Innovative Control Systems to Drive Strategic Renewal. Harvard Business School Press. Boston.

Stoel M. – Muhanna W. (2011) IT internal control weaknesses and firm performance: An organizational liability lens. International Journal of Accounting Information Systems. Vol. 12 s. 280–304.

Strickland, J. (2021) What would happen if the internet collapsed? http://computer.howstuffworks.com/internet/basics/internet-collapse.htm, haettu 21.11.2021.

Sutherland E. (1949) White collar crime. New York. Holt, Reinhart, & Winston.

Vakuutusyhtiölaki 2008/522 https://www.finlex.fi/fi/laki/ajantasa/2008/20080521 26.4.2021

van der Meer-Kooistra J. – Scapens R. (2008) The governance of lateral relations between and within organisations. Management Accounting research. Nro. 19 s. 365–384

Vousinas G. (2019) Advancing theory of fraud: the S.C.O.R.E. model. Journal of Financial Crime Vol. 26 Nro. 1, s. 372-381

Wells J. (2017) Corporate Fraud Handbook: Prevention and Detection. John Wiley & Sons, Inc. New York.

Wolfe D. – Hermanson D. (2004) The Fraud Diamond: Considering the Four Elements of Fraud. The CPA Journal. Vol 74 Nro. 12, s. 38-42.

Zakaria K. – Nawawi A. – Salin A. (2016) Internal controls and fraud – empirical evidence from oil and gas company. Journal of Financial Crime Vol 23, Nro. 4, s. 1154-1168.

9 Liitteet

Haastattelurunko 1

- Millainen on yrityksen sisäisen valvonnan ympäristö?
- Millaisia sisäisen valvonnan toimenpiteitä yrityksen liiketoimintaprosesseihin liittyy?
- Onko yrityksellä olemassa väärinkäytöksiin ja niiden estämiseen liittyvää strategiaa?
- Millaisia väärinkäytöksiä yrityksen liiketoimintaan liittyy?
- Minkälaisia työkaluja tai apuvälineitä väärinkäytösten estämiseen tarvittaisiin?
- Millaiset väärinkäytöstyypit ovat yleisimpiä tilitoimistossa?
- Miten potentiaalisia väärinkäyttäjiä voidaan tunnistaa?

Haastattelurunko 2

- Mitä laadunvarmennuksella tehdään ja mitkä ovat sen tavoitteet?
- Millainen laadunvarmennusprosessi on käytännössä?
- Miten tarkastuksissa ilmenneisiin puutteisiin reagoidaan?
- Millaisia riskejä laadunvarmennuksella voidaan parhaiten havaita? Entä millaisiin riskeihin on haastava puuttua?
- Miten laadunvarmennuksessa huomioidaan väärinkäytöksiin liittyviä riskejä?
- Miten laadunvarmennusta pyritään kehittämään?
- Miten digitalisaatiota voidaan hyödyntää laadunvarmennuksessa?
- Miten paljon automaatiota hyödynnetään laadunvarmennuksessa, ja miten sitä voitaisiin hyödyntää tulevaisuudessa?
- Mitä haasteita tai ongelmakohtia laadunvarmennustyössä tällä hetkellä on?
- Millaisia hyötyjä sähköisessä taloushallinnossa on verrattuna paperiseen järjestelmään?

Haastattelurunko 3

- Millaisia työkaluja ja järjestelmiä yrityksessä käytetään toiminnan sisäiseen valvontaan?
- Miten yrityksessä huolehditaan tietoturvasta?
- Mitä asioita tietoturvan näkökulmasta voidaan tai aiotaan parantaa?
- Mitä haasteita tai ongelmia järjestelmiin ja tietoturvaan yrityksessä liittyy?

- Miten yritys pysyy ajan tasalla digitaalisessa kehityksessä?
- Onko yrityksellä tietoturvastrategiaa tai – suunnitelmaa?
- Miten yrityksessä hallinnoidaan käyttöoikeuksia?
- Miten digitalisaatio ja digitaaliset järjestelmät ovat vaikuttaneet väärinkäytösriskeihin?
- Millaisia riskejä automaatioon, järjestelmiin ja teknologiaan liittyy?