Haaga-Helia
ammattikorkeakoulu Oy

Taloushallinnon sähköistymisen ja digitalisoitumisen tuomat riskit ja niiden hallinta taloushallinnon työntekijän näkökulmasta

Pauli Martinmaa

28.5.2017

Haaga-Helia
ammattikorkeakoulu Oy

Tiivistelmä

Tekijä(t)
Pauli Martinmaa

Koulutusohjelma
Liiketalous/tradenomi

Raportin/Opinnäytetyön nimi	**Sivu- ja liitesivumäärä**
Taloushallinnon sähköistymisen ja digitalisoitumisen riskit taloushallinnon työntekijän näkökulmasta	50 + 3

Taloushallinnon ja teknologian nopea kehitys mahdollistaa uusia riskejä, jotka vaativat omia hallintakeinojaan. Tämän työn tavoitteena on tutkia näitä uusia riskejä ja niiden hallintaa taloushallinnon työntekijöiden näkökulmasta.

Taloushallinto on organisaation taloudellisia tapahtumia seuraava kokonaisuus, josta tehdään yrityksen ja sen sidosryhmien kannalta tärkeitä raportteja. Taloushallinnon voi jakaa ulkoiseen ja sisäiseen taloushallintoon, joista ulkoinen on ulkoisille sidosryhmille kohdennettua laissa määriteltyä taloushallintoa, ja sisäinen yrityksen omaan käyttöä varten olevaa vapaamuotoista taloushallintoa. Taloushallinnossa on monia osaprosesseja, kuten myyntilaskutus, ostolaskutus, palkanlaskenta ja pääkirjanpito. Taloushallinto on kehittynyt kohti sähköisempää ja digitaalisempaa taloushallintoa. Sähköisessä taloushallinnossa toimintaa tukee internet, tietotekniikka ja sovellukset, ja digitaalisessa taloushallinnossa kaikki prosessit pyritään automatisoimaan mahdollisimman tehokkaasti esimerkiksi järjestelmien erilaisten ratkaisujen avulla. Digitaalisessa taloushallinnossa tieto siirtyy järjestelmien, osastojen, osaprosessien ja sidosryhmien välillä sähköisesti ja mahdollisimman automatisoidusti. Pitkälle digitalisoituneessa taloushallinnossa osaprosessit ovat kaikki samassa järjestelmässä ja tiedostomuodossa, ja niiden tiedot yhdistyvät suoraan pääkirjanpitoon, arkistoon ja raportointiin automaattisesti.

Sähköisen ja digitaalisen taloushallinnon tuomat uudet riskit liittyvät sähköisen ja digitaalisen muotonsa johdosta hyvin paljon tietoteknisen tietoturvan riskeihin. Nämä riskit voidaan jakaa tahallisiin ja tahattomiin riskeihin. Tahalliset riskit ovat rikollisten tekemiä hyökkäyksiä ja rikoksia, kuten tiedon varastaminen, väärinkäyttö ja manipulointi, laitteiston varastaminen ja virukset. Tahattomat riskit voidaan jakaa esimerkiksi inhimillisiin virheisiin, ympäristöhaittoihin ja tietokonejärjestelmien vikoihin. Näiden riskien hallintaa varten yritys tarvitsee strategian, joka sisältää riskien estämisen, torjunnan, toteutuneiden riskien havaitsemisen ja valvomisen, laajenemisen estämisen, toipumisen, oikaiseminen, tietoisuuden ja strategian noudattamisen. Tarkempia hallintakeinoja ovat esimerkiksi palomuurit, koulutus, kontrollit ja kulunvalvonta.

Työn tutkimus on luonteeltaan kvalitatiivinen, ja sen tekomuoto on avoin kyselylomake sähköpostin välityksellä. Kyselyyn vastanneet ovat neljä taloushallinnon kokemusta omaavaa henkilöä. Kyselylomakkeessa on yksitoista kysymystä, jotka hakevat tavoitteeseen liittyviä vastauksia.

Tuloksista voi tehdä vastanneiden pohjalta huomioita kohdattujen riskien tietoperustaa vähemmästä määrästä, tahattomien riskien suuremmista vaikutuksista tahallisiin riskeihin verrattuna ja tiedonsäilytyksen riskin korkeammasta merkittävyydestä vastaajien mielestä sähköisessä ja digitaalisessa taloushallinnossa. Riskienhallinta on vastaajien mielestä taloudellisen tilanteen ja kokemuksen lisäksi hyvin paljon riippuvainen käytettävissä olevasta ajasta. Riskienhallinta tuloksien mukaan on koulutuksen ja ohjeiden kannalta kiinni niiden tekijöiden lisäksi erityisesti vastaanottavan henkilön ominaisuuksista. Riskienhallintaa ei kannata tulosten mukaan vähätellä, ja sitä pidetään vastanneiden ja heidän työpaikkojen mielestä yhä tärkeämpänä taloushallinnon kehitykseen liittyvänä asiana.

Asiasanat
sähköinen taloushallinto, riski, riskienhallinta, digitalisaatio

Sisällys

1 Johdanto

Teknologian jatkuva kehitys, uudet keksinnöt ja uudet ratkaisut tehostavat ja auttavat jokapäiväisessä elämässämme. Myös taloushallinnon laitteet, järjestelmät ja toimintatavat ovat olleet muutoksen alla. Kehityksen ja muutoksien kautta tulee myös uusia mahdollisuuksia erilaisille riskeille. Uudet riskit tarvitsevat mahdollisesti kokonaan uusia riskienhallintakeinoja, tai esimerkiksi vanhojen riskienhallintakeinojen päivittämistä.

Olen kuullut lähiaikoina (2016 kevät - 2017 syksy) hyvin monien yritysten uusivan taloushallinnon järjestelmiään tai kehittävänsä niiden toimintaa muilla tavoin, kuten esimerkiksi strategian ja käytettävien laitteiden muutoksilla. Jotkin yritykset ovat edelleen vasta sähköistämässä taloushallintoaan, jolloin muutos on vielä merkittävämpi. On siis hyvä tietää uusia järjestelmiä hankkiessa, taloushallintoa sähköistäessä tai uuteen yritykseen mennessä, mitä riskejä on olemassa ja miten niitä kannattaa hallita.

1.1 Opinnäytetyön tavoite

Opinnäytetyön tavoitteena on selvittää taloushallinnon sähköistymisen ja digitalisoitumisen tuomat riskit ja niiden hallinta taloushallinnon työntekijän näkökulmasta. Riskeissä ei kuitenkaan huomioida sisäisiä tahallisia riskejä, josta voi lukea tarkemmin luvussa viisi. Koska näkökulmia on aiheeseen monia, keskityn asiaan lähinnä taloushallinnossa työskentelevän henkilön näkökulmasta.

Aihe on ajankohtainen, koska esimerkiksi Euroopan komission järjestämän ICT 2015 (Innovate, Connect & Transform) työryhmän yksi ehdotuksista yksityisen ja julkisen hallinnon tietovirtojen parantamiseen oli erityisesti riskienhallinnan parantaminen. Opinnäytetyön aiheen ajankohtaisuutta tukee myös esimerkiksi 12. – 14.5. maailmanlaajuisesti levinnyt kiristysohjelma. Helsingin Sanomien mukaan 15.5. mennessä verkkohyökkäyksen kohteita oli yhteensä 200 000, ja uhreja oli jopa 150:ssä eri maassa. Haittaohjelma häiritsi merkittävästi esimerkiksi Britannian ja Indonesian sairaaloita ja Espanjan, Portugalin ja Argentiinan teleyhtiöitä. Muita hyökkäyksen kohteita olivat ainakin Venäjän sisäministeriö, kuljetusyhtiö FedEx, autonvalmistajat Renault ja Nissan ja Saksan rautatieyhtiö Deutsche Bahn. Suomessa 10 000 konetta vastaan yritettiin hyökätä, mutta vain harva hyökkäyksistä onnistui mahdollisesti uusien palomuurien päivitysten ansiosta. Haittaohjelma levisi pääosin sähköpostin liitetiedoston välityksellä, esittämällä olevansa esimerkiksi kiireellinen lasku. (Lassila 2017, A23 – A24)

1.2 Tämän opinnäytetyön rakenne

Työn tietoperusta -osassa selvitetään ensin mitä taloushallinto on ja miten se on kehittynyt. Tämän jälkeen työssä määritellään mahdollisimman tarkasti mitä eroa on taloushallinnon sähköistymisellä ja digitalisoitumisella. Opinnäytetyössä käydään myös läpi mitä kaikkea digitaalisessa taloushallinnossa on. Määrittelyn jälkeen keskitytään tarkemmin sähköistymisen ja digitalisoitumisen tuomiin riskeihin ja niiden hallintaan.

Tutkimusosuus alkaa empiirisen tutkimuksen toteutuksella, jossa esitetään tutkimuksen taustat, tutkimuksen toteutus, tutkimukseen osallistuneet ja tarkemmat rajaukset tutkimukselle. Tämän jälkeen luvusta kuusi alkaa tehdystä tutkimuksesta saadut tulokset, ja luvussa seitsemän, eli pohdintaosuudessa, vertaillaan tuloksia tietoperustaan ja tehdään siitä mahdollisia johtopäätöksiä. Pohdintaosuuden lopussa on myös arviointia opinnäytetyön heikkouksista, vahvuuksista ja yleisestä onnistuneisuudesta. Lähdeosuudesta voi tarkastella tarkemmin opinnäytetyön tietoperustassa käytettyjä kirjallisia ja verkossa olevia lähteitä, jonka jälkeen työn lopussa on vielä viimeiseksi liitteet.

2 Taloushallinto ja sen osat

Ensiksi on tärkeää määritellä taloushallinto. Taloushallinnon voi määritellä organisaation taloudellisia tapahtumia seuraavaksi järjestelmäksi, joka mahdollistaa toiminnasta raportoinnin. Taloushallinto jaetaan ulkoiseen ja sisäiseen laskentatoimeen. Sisäisessä laskentatoimessa tuotetaan tietoa enimmäkseen johdon tarpeita ja käyttöä varten, kun taas ulkoisessa laskentatoimessa aikaansaatu tieto on tarkoitettu monille sidosryhmille, kuten viranomaisille, asiakkaille ja omistajille. (Lahti & Salminen 2014, 15 - 24.)

2.1 Sisäinen laskentatoimi

Sisäistä laskentatoimea kutsutaan myös johdon laskentatoimeksi. Se tuottaa tietoa tukemaan yrityksen päätöksentekoa. Tämä tieto eroaa ulkoisen laskentatoimen muodostamasta tiedosta, koska se on vapaamuotoista ja vapaaehtoista. Sisäisen laskentatoimen tekemä tieto ei siis ole lain säätämää, ja sitä käytetään nykytilanteen arvioinnin lisäksi myös tulevaisuuden arviointiin. Se on myös yleensä nimensä mukaan tarkoitettu vain yrityksen sisäiseen omaan käyttöön eikä ulkoiseen julkiseen käyttöön. Raportteja tehdään sisäisessä laskentatoimessa tiheämmin, jotta ne olisivat päätöksentekoa varten ajan tasalla. Sisäinen laskentatoimen tiedon perusteella muodostetaan budjetit, kustannuslaskelmat, hinnoittelulaskelmat, investointilaskelmat ja ennusteet. Esimerkiksi kustannuslaskelmassa voidaan vertailla kustannuksia eri yksiköiden, tuotteiden tai palveluiden mukaan. Investointilaskelmalla pyritään arvioimaan pitkäaikaishankkeiden kannattavuutta. (Jormakka, Koivusalo, Lappalainen & Niskanen 2015, 13.)

2.2 Ulkoinen laskentatoimi

Ulkoista laskentatoimea kutsutaan myös rahoittajan laskentatoimeksi. Siinä tuotetaan, muokataan ja kerätään informaatiota ulkoisille sidosryhmille. Sidosryhmiä voivat olla esimerkiksi sijoittajat, lainanantajat, asiakkaat ja verottaja. He ovat kaikki omalla tavallaan kiinnostuneita yrityksen taloudellisesta tilasta ja muusta yrityksen talouteen liittyvästä tiedosta. Omistajat, eli sijoittajat, haluavat tietää miten hyvin heidän sijoittamansa omaisuutta hoidetaan, ja miltä tulevaisuuden näkymät vaikuttavat. Lainanantajia, velkojia ja tavarantoimittajia kiinnostaa enemmän maksukyky ja miten yritys suoriutuu velvoitteistaan. Merkittävät ja pitkä aikaiset asiakkaat ovat pääsääntöisesti kiinnostuneita kumppanuuden toisen osapuolen taloudellisesta tilasta. Samoin myös verottaja haluaa tietää verotuksen kannalta oleellisen tiedon yrityksen taloudellisesta tilasta. Jotta ulkoisen laskentatoimen raportoima tieto olisi luotettavaa, vertailtavaa, seurattavaa ja todennettavaa on se määritelty tarkoin lailla. Kirjanpito, eli muistiin merkitseminen, ja sen perusteella tehty tilinpäätös ovat tärkeä osa talouden raportointia. Sitä säätelevät enimmäkseen kirjanpitolaki ja -

asetus, mutta ulkoiseen laskentatoimeen liittyy myös monia muita lakeja esimerkiksi verotukseen liittyen. Ulkoisen laskentatoimen tärkeimpiä raportteja ovat ainakin tuloslaskelma, tase, rahoituslaskelma ja veroilmoitus. (Jormakka ym. 2015, 12.)

2.2.1 Kirjanpito ja tilinpäätös

Kirjanpidolla ja sitä määrittelevillä laeilla pyritään varmistamaan merkityn tiedon luotettavuus, jotta sidosryhmät voivat käyttää ja hyödyntää tätä tietoa. Kirjanpito tulee toteuttaa hyvän kirjanpitotavan mukaisesti, mikä tarkoittaa kirjanpitolain noudattamista. Jokainen Suomessa liiketoimintaa harjoittava on kirjanpitolain mukaan kirjanpitovelvollinen. KILA, eli kirjanpitolautakunta, on tärkeässä osassa kirjanpitolain ja hyvän kirjanpitotavan tulkitsemisessa. Tämän lisäksi on olemassa periaatteita, jotka auttavat edelleen kirjanpidon määrittelemisessä. Näitä periaatteita on kolmenlaisia: rajoittavia periaatteita, mittausperiaatteita ja eettisiä periaatteita. Rajoittavat periaatteet rajaavat mikä tieto kuuluu kirjanpitoon tallennettavaksi, mittausperiaatteet määrittelevät arvojen olennaisuutta ja tärkeyttä ja eettiset periaatteet sisältävät lyhennettynä varovaisuuden, todennettavuuden, merkityksellisyyden ja johdonmukaisuuden. Lait, periaatteet ja säännöt yhdessä varmistavat, että kirjanpidossa tuotettu tieto on oleellista, ymmärrettävää ja asianmukaista. Tämä tieto kertoo yrityksen taloudellisesta tilasta, taloudellisesta historiasta, tarkemmin eri omaisuuksista ja tapahtumista. Kirjanpidon tieto on myös hyödyllistä tulevaisuuden suunnittelua ja arviointia varten. (Ikäheimo ym. 2012, 30 – 31;Tomperi 2013, 10 - 11.)

Kirjanpidon tuotokset jaetaan virallisesti tilikausittain, jotka kestävät yleensä 12 kuukautta, mutta voivat olla lyhyempiä tai pidempiäkin toimintaa aloittaessa ja lopettaessa. Kun tilikausi päättyy, tekee yritys tilinpäätöksen. Tilinpäätöksessä on tuloslaskelma, tase, rahoituslaskelma ja liitetiedot. Tilinpäätös pitää päivätä ja allekirjoittaa, ja sen ohelle liitetään toimintakertomus. (Kinnunen ym. 2006, 19.)

Tilikautena tehdyt kirjanpidon kirjaukset päätetään tase ja tuloslaskelmaan. Tase kuvaa yrityksen tilikauden päättymishetkistä taloudellista asemaa. Tätä asemaa voidaan mitata esimerkiksi vakavaraisuudella, joka on oman ja vieraan pääoman suhde. Mitä enemmän yrityksellä on suhteessa vierasta pääomaa, esimerkiksi velkaa, sitä enemmän niistä voi koitua jatkuvia kustannuksia. Tuloslaskelma puolestaan kuvaa nimensä mukaan tilikauden aikana syntynyttä tulosta. Tulos on menojen ja tulojen suhde, ja yritys voi tehdä tämän suhteen perusteella voittoa tai tappiota. Tuloslaskelma on tärkeä kannattavuuden arvioinnin kannalta. (Kinnunen ym. 2006, 12.)

2.2.2 Osakirjanpidot ja niiden yhteys pääkirjanpitoon

Rahaprosessien eri vaiheet muodostavat taloushallinnon, ja niitä kutsutaan myös osaprosesseiksi. Taloushallinnon osaprosessit voidaan jakaa esimerkiksi myyntilaskutukseen, ostolaskutukseen, matkalaskutukseen, rahaliikenteeseen, palkkojenlaskuun, vaihto-omaisuuden laskentaan, käyttöomaisuuden laskentaan ja pääkirjanpitoon. (Mäkinen & Vuorio 2002, 85.)

Myyntilaskutuksessa lasku tehdään, lähetetään, vastaanotetaan maksu ja kirjataan tapahtumat kirjanpitoon. Myyntilaskutukseen voidaan myös liittää perintätoimet, eli myöhästyneiden maksujen tilanteen kysely ja aiheettomasti viivästyneiden maksujen perintä. Manuaalisesti tehtynä myyntilasku joudutaan tulostamaan ja lähettämään postissa postileiman kanssa, jonka lisäksi kirjanpidon kirjaukset joudutaan yksitellen hoitamaan käsin. (Helanto, Kaisaniemi, Koskinen, Kuntola & Siivola 2013, 44.)

Ostolaskutusprosessi sisältää ostolaskun vastaanottamisen, sen maksamisen, kirjanpidon merkintöjen tekemisen ja tositteiden arkistoinnin. Ostolaskutusprosessiin voidaan myös liittää ostotilausten tekeminen ja hoitaminen. Paperisesti tehtynä ostolaskutusprosessissa lasku vastaanotetaan postitse, kierrätetään fyysisesti hyväksyttävänä, maksetaan nettipankissa ja kirjataan kirjanpitoon käsin. (Helanto ym. 2013, 45.)

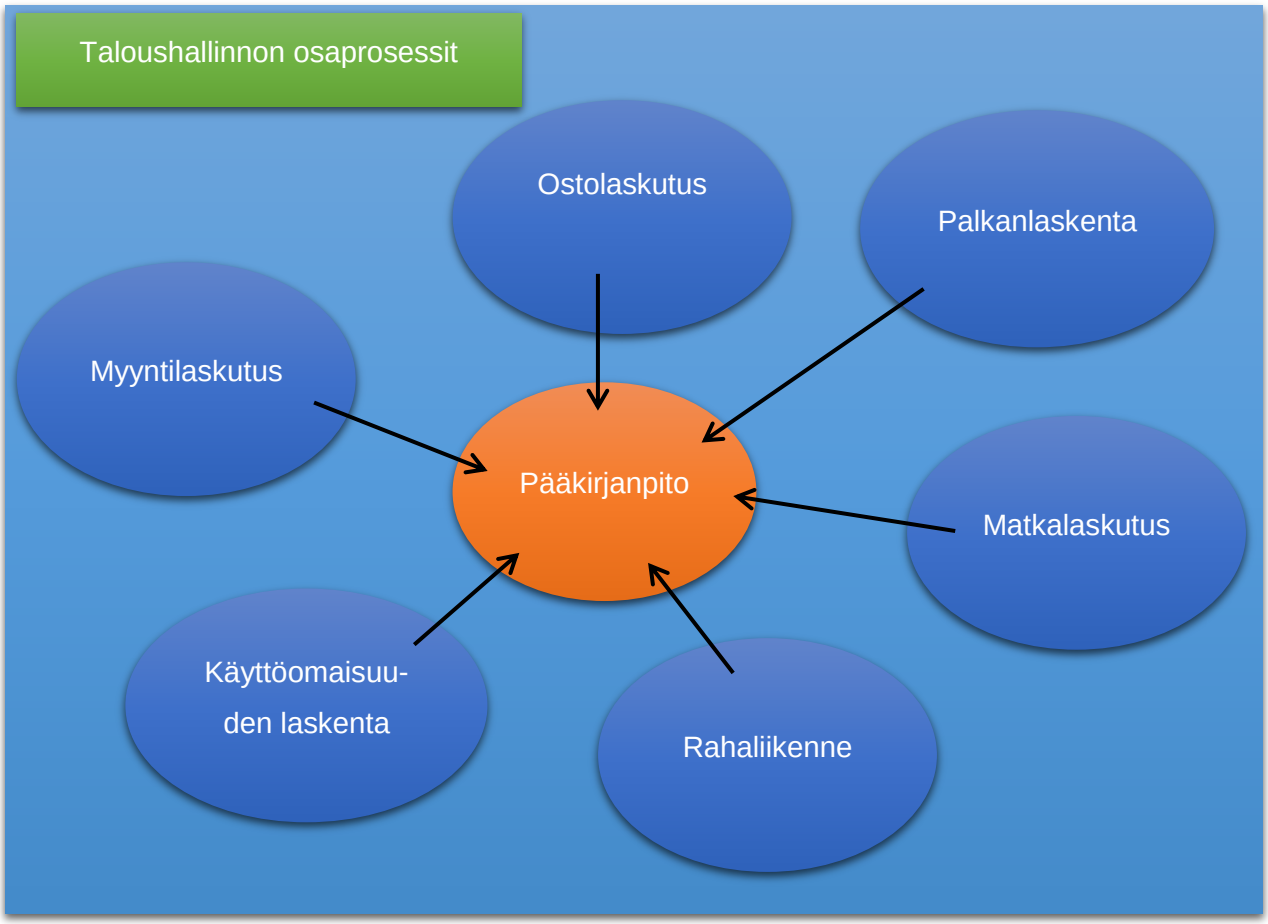
Laki määrittelee Suomessa matkakustannuksiin liittyvät verovapaat korvausten rajat. Matkustaja voi myös itse maksaa kuluja työmatkalla, jotka työnantaja korvaa kulukorvauksina. Matkalaskuihin liittyvät myös kululaskut, jotka ovat työntekijöiden itse ostamia pienhankintoja. Matkakorvauksia ovat esimerkiksi päivärahat ja kilometrikorvaukset. (Lahti & Salminen 2008, 98.)

Palkanlaskenta voi olla yrityksessä virallisesti osana joko taloushallintoa tai henkilöstöhallintoa. Palkat ja muut henkilöstökulut ovat monilla yrityksillä jopa suurimmat kuluerät, mistä syystä niitä seurataan tarkasti kirjanpidossa ja raportoinnissa erilaisilla tunnusluvuilla ja mittareilla. Tarkemmin määriteltynä palkanlaskenta sisältää yleensä ainakin itse palkkojen laskemisen ja kirjaamisen, niiden maksamisen, ennakonperinnän, viranomaisraportoinnin ja näihin liittyvän tiedon arkistoinnin. Palkanlaskentaan liittyy useita lain ja sopimusten määräämiä periaatteita ja sääntöjä, ja itse palkkakin voi sisältää bonuksia, luontaisetuja ja esimerkiksi sairasajan tai loma-ajan palkkaa. Palkanlaskenta ilman sähköistymistä toimii irrallaan kirjanpidosta. Palkkoja laskiessa pitää itse palkkojen lisäksi ottaa huomioon lukuisia asioita, kuten esimerkiksi ylityöt, erilaiset korvaukset ja työsuhde-etuudet. (Helanto ym. 2013, 37.)

Organisaatioissa yhdet mahdollisesti vähemmälle huomiolle jäävistä prosesseista ovat matka- ja kululaskuprosessit. Ne syntyvät työntekijöille oikeutetuista matkakulukorvauksista ja heidän tekemistään pienhankinnoista. Tämänlaisia korvauksia ovat muun muassa kilometrikorvaukset, päiväraha, majoituskulut, matkaliput, edustuskulut, neuvottelukulut ja toimistohankinnat. Verolainsäädäntö määrittelee verovapaat matkakustannukset, joiden käsittelyssä yrityksillä tapahtuu helposti virheitä. Monesti matka- ja kululaskuprosessi liitetään osaksi palkanlaskentaa yrityksen sisällä, eikä sille välttämättä anneta merkittävästi huomiota. Tästä huolimatta näiden kulujen määrä yhteenlaskettuna voi olla yllättävänkin merkittävä yrityksen toiminnassa. (Lahti & Salminen 2008, 110 - 115.)

Pääkirjanpidossa eri taloushallinnon prosessien tapahtumat kirjataan lakisääteisesti yhdeksi kirjanpidon kokonaisuudeksi. Tästä voi nähdä esimerkin kuvio yhdestä sivulla seitsemän. Eri prosessien kirjanpitoja kutsutaan osakirjanpidoiksi. Kirjanpidossa käytetään muistiotositteita, joihin merkitään ja päivitetään esimerkiksi poistot, arvonlisävero ja jaksotukset. Tositteet ovat asiakirjoja, joilla todennetaan liiketapahtuma selvässä muodossa. Niissä pitää olla ainakin numeroituja ja niistä pitää löytyä päiväys. Jos aiemmin kirjanpidon tositteista annetut esimerkit eivät ole tuttuja, määritellään ne tässä vielä tarkemmin. Poistot tehdään käyttöomaisuudelle, jolle voidaan arvioida pitkäaikainen vaikutusaika. Käyttöomaisuuden hankintamenoarvo poistetaan vaikutusajan loppuun mennessä. Käyttöomaisuutta voi olla esimerkiksi koneet, rakennukset ja laitteet. Arvonlisäverolla verotetaan tuotteesta tai palvelusta nimensä mukaan arvoltaan kasvanutta osuutta. Yritykset voivat vähentää myymänsä tuotteen arvonlisäverovelasta sen oston aikana maksetun arvonlisäveron, jotta kustakin arvonnoususta maksetaan vain kerran veroa. Jaksotuksessa aktivoidaan kirjanpidossa tulot ja menot niille tilikausille, joihin ne oikeasti kuuluvat. (Lahti & Salminen 2008, 128.)

Pääkirjanpidon tieto jaetaan yleisellä tasolla tilikausien, tositelajien tai konsernin sisäisten yritysten mukaan. Tositelajit taas määritellään eri osakirjanpitojen, kuten esimerkiksi myyntireskontran, mukaan. Kirjanpidossa on myös muita perustietoja, kuten tilit, seurantakohteet, toimittajat, tuotteet, projektit ja päiväykset. Eri kirjanpidon tileistä muodostuva tilikartta ja erityiset seurantakohteet suunnitellaan raportoinnin tarpeiden perusteella niin, että ainakin viralliset tulos- ja taselaskelman vaatimukset täyttyvät. Suomessa käytetäänkin pienissä ja keskisuurissa yrityksissä usein Liikekirjuri-tilikarttaa, koska se on tehty täyttämään tulos- ja taselaskelmien viralliset säädökset ajankohtaisesti. (Lahti & Salminen 2008, 129.)



Kuvio 1 – Taloushallinnon osaprosessit ja niiden yhdistäminen pääkirjanpitoon (Lahti & Salminen 2008)

3 Taloushallinnon sähköistyminen ja digitalisoituminen

Seuraavaksi on tärkeää määritellä mitä tarkoittaa sähköistyminen ja digitalisoituminen. Digitaalinen -sanan sijasta saatetaan käyttää puhekielessä myös sanaa sähköinen taloushallinto tai paperiton taloushallinto, mutta tarkalleen ottaen näissä on kuitenkin eroja. Digitaalisuus viittaa sähköisen tiedon erilaiseen käyttämiseen, kuten esimerkiksi sähköisen tiedon käsittelyyn, siirtämiseen ja varastointiin. Tämän tekemiseen tarvitaan ohjelmistokielellä kirjoitettuja ohjelmia tai sovelluksia. Digitaalisen tiedon käsittely on yleensä nopeampaa kuin paperisen, ja se kulkee tietoverkoissa langallisesti tai langattomastikin. Yritysten välistä sähköistä ja automatisoitua tiedonvälitystä kutsutaan organisaatioiden väliseksi tiedonsiirroksi (OVT), ja sitä käytetään esimerkiksi tilausten, maksuliikenteen ja verotuksen yhteydessä. E-liiketoiminnalla tarkoitetaan tuotteiden tai palveluiden kauppaa netissä, mikä tunnetaan yleisemmin verkkokauppana. E-liiketoiminnassa asiakas tunnistetaan esimerkiksi verkkopankkitunnuksella tai sivustolle luodulla käyttäjätunnuksella. Yritykset tunnistautuvat viranomaisten sähköisiin palveluihin, kuten Verohallinnon palveluihin, omilla Katso -tunnisteillaan. Sanna Lahden ja Tero Salmisen kirjoittaman kirjan mukaan Digitaalisen taloushallinnon vakiintunut määritelmä on seuraava: (Lahti & Salminen 2014, 15 - 24.)

”*Digitaalisella taloushallinnolla tarkoitetaan taloushallinnon kaikkien tietovirtojen ja käsittelyvaiheiden automatisointia ja käsittelyä digitaalisessa muodossa.”* (Lahti & Salminen 2014, 24.)

Se on myös muotoiltu käytännössä ymmärrettäväksi seuraavasti:

”*Konkreettisesti digitaalinen taloushallinto on prosessi, joka koostuu ihmisten tekemisistä, töiden organisoinnista, tietojärjestelmistä ja teknologioista sekä mahdollisimman suoraviivaisista toimintaketjuista, joissa automatisoinnin tavoitteena on poistaa turhat ja päällekkäiset käsittelyvaiheet digitaalisessa muodossa olevan taloushallintomateriaalin käsittelystä.*” (Lahti & Salminen 2014, 25.)

Taloushallinnon sähköistyminen viittaa työn tehostamiseen erilaisilla sähköisillä toiminnoilla ja palveluilla kuten internetillä, tietotekniikalla ja sovelluksilla. Sitä kuvataan digitaalisen taloushallinnon esiasteeksi, ja on vähemmän automatisoitunut esimerkiksi sisältäen paperien skannausta tai yhtyeensopimattomia ohjelmia. Digitaaliselle taloushallinnolle ominaista sähköiseen verrattuna on varsinkin verkkolaskutus, jossa täsmäytys, tiliöinti ja hyväksyntä voidaan automatisoida. (Lahti & Salminen 2014, 25.)

Taloushallinnon sähköistyminen ja digitalisoituminen on levinnyt Suomessa laajalle, mutta hitaammin kuin aikaisemmin oli monien ennustuksien mukaan oletettu esimerkiksi paperilaskujen sähköistymisen osalta. Verkkolaskujen osuus oli vuonna 2013 Suomessa julkisella sektorilla 40 % ja yrityksillä 15 %. Suomessa on erityisesti kehitetty pankki- ja maksuliikennejärjestelmiä, esimerkiksi yhtenäisillä pankkistandardeilla. Euroopassa vuonna 2013 verkkolaskuja oli vain 20 % julkisten hankintojen laskuista ja 13 % kuluttajalaskuista, mikä antaa osittain kuvaa sähköistymisen levinneisyydestä. (Lahti & Salminen 2014, 28 - 30.)

3.1 Digitaalisen taloushallinnon sisältö ja perusteet

Jotta yrityksen taloushallinto voi kutsua itseään digitaaliseksi, on sen saavutettava monia asioita. Ensinäkin digitaalisessa taloushallinnossa kirjanpito- ja taloushallintomateriaali käsitellään ja tallennetaan sähköisesti. Tieto siirtyy sekä eri sisäisten järjestelmien, osastojen ja osaprosessien välillä, että myös ulkoisten sidosryhmien välillä sähköisesti ja mahdollisimman automatisoidusti. Tämän lisäksi digitaalisessa taloushallinnossa tositteet ja arkistointi ovat sähköisessä muodossa. Eri prosessien automatisoinnit vähentävät henkilöresurssien tarvetta itse lukujen ja laskujen kirjaamiseen, mutta lisää tarvetta järjestelmien uusien sääntöjen luomiseen ja erilaisten erikoistapausten hoitamiseen. On ennustettu, että jopa puolet Suomen taloushallintoon liittyvistä työpaikoista saattaisi kadota tulevaisuudessa. Taloushallinnon digitalisointi tekeekin normaalisti prosesseista 30 – 50 % tehokkaampaa. (Lahti & Salminen 2014, 26 – 28, 32.)

Vaikka yritys tekisi itse kaikkensa taloushallintonsa mahdollisimman täydellisen digitalisoimisen eteen, voivat sidosryhmät vaikeuttaa sitä esimerkiksi lähettämällä paperilaskuja. Muita ongelmia voivat olla myös sopivien järjestelmien ja ohjelmien löytäminen sekä uuden monimutkaisen teknologian oppiminen. Tulevien paperilaskujen määrää voi vähentää pyytämällä toimittajilta verkkolaskuja, tai joissain tapauksissa jopa pakottaa heitä siihen. Esimerkiksi Tanskassa valtionhallinnolle voi lähettää pelkästään verkkolaskuja. (Lahti & Salminen 2014, 26 - 28.)

Taloushallintojärjestelmän hankkiminen on yleensä suuri ja kallis projekti yritykselle. Vaihtoehtoina on erilaisia valmiita järjestelmäpaketteja tai yritykselle omanlainen räätälöity kokonaisuus. Uusi taloushallintojärjestelmä voi tehdä työstä merkittävästi tehokkaampaa, mutta se tarvitsee hyvän käyttöönottototeutuksen ja sen pitää täyttää yrityksen toiminnalliset tarpeet. Pienet yritykset tarvitsevat yleensä yksinkertaisempia ja suppeampia kirjanpitojärjestelmiä, joita käytetään tilitoimiston tai pilvipalvelun kautta. Keskisuuret yritykset

räätälöivät ja mukauttavat enemmät taloushallintojärjestelmiään vaativimpiin tarpeisiinsa, joita ovat esimerkiksi monipuolisempi ja laadukkaampi raportointi sekä varastonhallinta. Suuremmilla järjestelmillä on Suomessa vähemmän tarjoajia kuin pienemmillä. Suuryrityksien tarpeisiin taas sopii parhaiten erityiset operatiiviset järjestelmät tai ERP -ohjelmistot. ERP -ohjelmistot, joka on lyhenne englanninkieliselle käsitteelle enterprise resource planning, ovat eri integroitujen prosessien toimintoja käsitteleviä toiminnanohjausjärjestelmiä. Toiminnanohjausjärjestelmät voivat sisältää eri moduuleina esimerkiksi kirjanpitoa, projektinhallintaa, henkilöstöhallintaa, sisäistä laskentaa ja varastonhallintaa, mutta taloushallinto on yleensä näistä tärkeintä. ERP -ohjelmisto voikin korvata useita eri ohjelmia ja järjestelmiä yhdistämällä ne yhdeksi kokonaisuudeksi. (Lahti & Salminen 2014, 36 – 42)

Järjestelmän voi joko hankkia lisenssinä yritykselle, tai ostaa pilvipalveluna. Jos järjestelmälisenssi ostetaan itselle, voi sen asentaa itse tai siirtää vastuun ulkoistamalla laitteet ja ohjelmistot. IT-palveluiden ulkoistaminen on ollut Suomessa kasvussa. Pilvipalvelut ovat ohjelmisto- ja tietotekniikkapalveluita, joita käytetään netin kautta. Myös niidenkin käyttö on yleistynyt. Pilvipalvelun päivityksestä, toiminnasta, kehityksestä ja muusta ylläpidosta vastaa sen palveluntarjoaja. Lainsäädännön muutokset, teknologian kehitys ja tehokkuuden parantaminen tekevät päivitysten saannista pilvipalvelun kautta hyödyllistä ja nopeaa sitä käyttävälle yritykselle verrattuna muihin vaihtoehtoihin. Suuremmat yritykset voivat käyttää private cloud -tyyppistä pilvipalvelua, jossa järjestelmä on eristetty sen omaan käyttöön. Varsinkin konsernit hyötyvät keskittäen taloushallintonsa yhteen pilvipalveluun, pitämällä eri yritysten järjestelmät samalla päivitystasolla ja yhteensopivina. (Lahti & Salminen 2014, 44 - 47.)

Verkkolaskut ovat sähköisesti lähetettäviä laskuja, joita voi vastaanottaa yrityksen lisäksi myös kuluttaja. Ne sisältävät yleensä dataa ja laskun kuvan, jota käytetään esimerkiksi arkistoinnissa. Verkkolaskujen lähettäminen ja vastaanottaminen ulkomailta ei ole vielä kehittynyt yhteiseen formaattiin, joten niiden käyttö on vähäisempää kuin oman maan sisäisillä verkkolaskuilla. Verkkolaskujen lähettäminen ja vastaanottaminen paperilaskujen sijasta on kustannustehokkaampaa materiaalisäästämisen, käsityön tarpeen vähenemisen ja alhaisempien maksuliikenne- ja arkistointikulujen takia. Vastaanotetut paperilaskut joudutaan skannaamaan, jonka jälkeen laskun tiedot, kuten eräpäivä, summa ja viitenumero, syötetään järjestelmään joko käsin tai automaattisella älyskannauksella. (Lahti & Salminen 2014, 63 - 65.)

3.2 Digitaalinen taloushallinto prosesseittain

Digitaalisen taloushallinnon voi jakaa paperisen taloushallinnon tapaan osaprosesseihin, mutta näiden osaprosessien toteutustapoihin on tullut kehityksen myötä paljon muutoksia. Kirjanpidon osaprosessien lisäksi digitaaliseen taloushallintoon kuuluu ainakin raportointi ja arkistointi. Tässä opinnäytetyössä ei keskitytä taloushallintoon johdon tai esimiesten näkökulmasta, joten tässä osuudessa ei erikseen käydä taloushallinnon johtamista läpi.

3.2.1 Osto- ja myyntilaskutus digitaalisessa taloushallinnossa

Yritysten yksi suurimmista resursseja vievistä taloushallinnon osista on ostolaskujen käsittely. Paperiset ostolaskut yleensä skannataan sähköiseen muotoon, mikä on hitaampaa kuin verkkolaskujen prosessointi. Vaikka Suomessa ostolaskujen käsittelyyn käytetään vielä erillisiä ohjelmia, liitetään niitä myös enemmän osaksi ERP -järjestelmää. Ostolaskujen sähköinen prosessointi alkaa laskun vastaanottamisella järjestelmään, jonka jälkeen se tiliöidään automaattisesti tai manuaalisesti. Tämän jälkeen ostolasku lähetetään tarkastettavaksi ja hyväksyttäväksi kiertoon järjestelmässä mahdollisten automaattisten kiertolistojen mukaan. Yritys itse määrittelee hyväksymismenettelyn, ja se on yleensä kaksiportainen. Kun lasku on mennyt kierrosta läpi, se menee automaattisesti ostoreskontraan ja maksuun. Kehitystä ostolaskujen käsittelyssä tapahtuu muun muassa automatiikan lisäämisessä, käsittelyn liittämisen ERP -järjestelmiin moduuliksi ja kirjaamisen perilaitteiden yhdentämistä. Yksi tärkeistä osista järjestelmässä, ostolaskuihin liittyen, on toimittajarekisteri, mikä on hyvä pitää ajan tasalla pankkitietojen, sovittujen maksuehtojen ja esimerkiksi ennakkoperintärekisterin suhteen. Muita ylläpidettäviä tietokantoja ovat ainakin tilikartta, kustannuspaikat ja muut kohdistustiedot kuten projektitieto. Sähköiset laskut voivat tulla virheellisenä järjestelmävian tai inhimillisen virheen sattuessa. Jos saaduista ostolaskuista puuttuu jotain tietoja, voi niiden käsittely hidastua merkittävästi nopeasta automatiikasta huolimatta. (Lahti & Salminen 2014, 55 - 62.)

Myyntilaskutusprosessi on tärkeää suorittaa ajallaan, jotta yritys voi maksaa myös omat laskunsa ajoissa. Jos myyntilaskuissa tapahtuu merkittäviä virheitä, voi se helposti haitata imagoa ja asiakkaiden luottamusta yritystä kohtaan. Myyntilaskun tekemisen, lähettämisen ja arkistoinnin lisäksi myös sen vastaanotto, kuittaus ja maksusuoritus ovat osa myyntilaskutusprosessia. Verkkolaskutus on kaikista yleisintä suuremmilla yrityksillä, mutta useat pienetkin yritykset käyttävät sitä. Sähköisten myyntilaskujen prosessit ovat nykyään jo melko automatisoituja, mutta esimerkiksi sisäisissä laskuissa ja uuden verkkokaupan liittämisessä vanhaan toimintaan on vielä kehittämistä. Toisin kuin ostolaskuissa, myyntilaskujen sähköistäminen ei yleensä vähennä taloushallinnosta muodostuneita kuluja merkittävästi. Myyntilaskut eivät vaadi paperisena työvoimaa tai resursseja kovasti enempää,

vaan ainoastaan säästetään paperi- ja postituskuluissa. Myyntilaskutusprosessin digitalisoinnilla kuitenkin vähennetään virheitä, nopeutetaan myyntilaskujen laatimista ja esimerkiksi arkistointi tapahtuu sähköisesti ja automaattisesti. Kasvavien yritysten kannattaa sähköistää myyntilaskutus ja verkkokauppa mahdollisimman aikaisessa vaiheessa, jottei myyntilaskutuksesta myöhemmin synny kontrolloimatonta ja sähköistämisestä vaikeampaa. (Lahti & Salminen 2014, 78 - 100.)

3.2.2 Maksatus digitaalisessa taloushallinnossa

Maksutapahtumien käsittelyä ja välitystä pankin ja yrityksen välillä kutsutaan maksuliikenteeksi. Maksuliikenteessä yritys käyttää taloushallintojärjestelmää ja pankki tiliotteita ja viitemaksutiedostoja. Yrityksestä uloslähtevää maksuliikennettä ovat esimerkiksi ostolaskut ja palkat, kun taas sisään tulevia ovat esimerkiksi asiakkaiden maksut ja käteismyynnistä tehdyt tilitykset. Suomen maksukäyttäytyminen on mitattu yhdeksi nopeimmista, ja maksuliikenneinfrastruktuuriamme pidetään yleisesti hyvin kehittyneenä. Yritys voi käyttää joko lisämoduulia nykyisessä järjestelmässään tai hankkia kokonaan erillisen ohjelmiston maksuliikenteen hallitsemiseen. Vaikka erillisohjelmistot, eli Middleware -ohjelmistot, voivat olla itsessään kehittyneempiä, moduulit toimivat suoraan osana koko taloushallinnon järjestelmää eikä niitä tarvitse yhteen sovittaa tai liittää muihin järjestelmän osiin yhtä hankalasti. (Lahti & Salminen 2014, 115 - 120.)

Taloushallinnon järjestelmät laskevat vastaanotettujen laskujen tai syötettyjen tietojen ja sääntöjen pohjalta useimmat uloslähtevät maksut automaattisesti, mutta veroluontoiset erät ja jotkin poikkeustapaukset on syötettävä ohjelmiin kokonaan käsin. Yrityksen luottokorteilla tehdyt ostot voidaan laittaa joko työntekijän itsensä vastuulle, jotta tämän on pakko kirjata ostoistaan kulu- tai matkalasku kuitteineen, tai yrityksen vastuulle maksettavaksi, jolloin vastaanotetun luottokorttilaskun tiedot voidaan kirjata automaattisesti annettujen kohdistuksien pohjalta. Ulosmenevien laskujen tekemisessä ja hallinnassa voi vähentää virheitä hajauttamalla tehtäviä ja oikeuksia eri työntekijöille, käyttämällä kaksoishyväksyntää ja seuraamalla säännöllisesti järjestelmän toimittajarekisterin muutoksia. Sisään tuleva maksuliikenne on järjestelmien avulla hyvin automatisoitua kun käytetään kotimaisia maksuviitteitä. Ulkomaalaiset laskut ja virheelliset laskut joudutaan yleensä kohdistamaan manuaalisesti. Kassamyynnin tuotoilla on olemassa väärinkäytösriski, jolla tarkoitetaan käteisen menoa muualle kuin tarkoitettuun kohteeseen. Tätä riskiä voi vähentää esimerkiksi vertaamalla kassajärjestelmän kassaraporttia, kassatyöntekijän laskemaa rahamäärää ja pankkiin vietyä pankkityöntekijän laskemaa rahamäärää toisiinsa. Digitalisoituneessa taloushallinnossa kassamyynti voi automaattisesti mennä kirjanpitoon ja myyntireskontraan pankin rahansiirron yhteydessä. Tämä on joko mahdollista käyttämällä ERP -

järjestelmää ja lähettämällä saman viitteen kassajärjestelmästä sekä pankkiin että taloushallintoon, tai liittämällä kassa- ja talousjärjestelmät suoraan toisiinsa. Verkkokauppa liitetäänkin yleensä myyntireskontraan suoraan. Kassaennusteet on mahdollista automatisoida taloushallinnon järjestelmästä esimerkiksi myyntilaskujen tai tilauskannan perusteella. Tilauskantaan pitää tällöin päivittää saadut tilaukset ja niistä tehdyt maksamissuunnitelmat. (Lahti & Salminen 2014, 121 - 129.)

3.2.3 Palkanlaskenta, matkalaskuprosessi ja kululaskuprosessi digitaalisessa taloushallinnossa

Palkanlaskentaa varten yleensä ostetaan erillinen palkanlaskentajärjestelmä tai erillisiä ohjelmistoja, mutta esimerkiksi pienet yritykset saattavat käyttää taloushallintojärjestelmän mukana tullutta palkanhallinta -osuutta. Joka tapauksessa palkanlaskenta saattaa olla hyvä sähköistää ja digitalisoida, koska sen merkittävyyden ja lukuisien eri prosessien takia kaiken käsin tekeminen on aikaa vievää eikä välttämättä kovin tehokasta. Palkanlaskentaprosessi alkaa ensin työaika- ja palkka-aineiston keräämisellä palkanlaskentaan, jossa tämä tieto pitää yleensä tarkastaa ja hyväksyä järjestelmän kierron kautta. Kun tieto on saatu, voi sen tulkintaan käyttää tulkintaohjelmistoa, mikä auttaa tiedon tulkinnassa ja sen oikeaan muotoon muuttamisessa. Tulkintaohjelmiston voi saada osaksi käyttämäänsä palkanlaskenta- tai työajanhallintaohjelmistoon, tai sen voi hankkia kokonaan erillisenä ohjelmana. (Lahti & Salminen 2014, 135 -139.)

”Monissa organisaatioissa ja useilla toimialoilla tämä on erittäin vaativa ja monimutkainen vaihe… …Tulkintavaihe on yksi keskeisimmistä ja tärkeimmistä asioista, kun tavoitellaan automatisoitua palkanlaskentaprosessia. Valitettavan usein tämä vaihe on jäänyt ratkaisematta osana digitaalista palkanlaskentaprosessia tai se on toteutettu huonosti. Tällöin palkanlaskijat tai assistentit tekevät erilaista tapahtumien tulkintaa täysin manuaalisesti.” (Lahti & Salminen 2014, 139.)

Itse palkanlaskentaa ohjelmat osaavat oikein syötetyillä tiedoilla ja säännöillä laskea automaattisesti. Näitä prosesseja voi valvoa ja tarkistaa ohjelmalla itsellään. Laskemisen jälkeen tulevan raportoinnin ja arkistoinnin voi myös tehdä ohjelmaa käyttäen, mutta maksamisen tekee maksuliikennejärjestelmä sinne siirretyn tiedon perusteella. Työntekijälle annettava ansiolaskelman, eli palkkalaskelman, voi lähettää Suomessa sähköisesti verkkopankin, sähköpostin tai eKirje ja iPosti palveluiden kautta. Myös erilaiset viranomaisraportit verottajalle, vakuutusyhtiölle ja verottajalle voi lähettää tiedonsiirtona sähköisesti. Palkanlaskennan digitalisoituminen on kehittynyt monilta osin. Varsinkin uusien työajanhallintaohjelmistojen kehitys on lähiaikoina ollut merkittävää ja esimerkiksi henkilö- ja työsuhdetietojen ylläpitoa on pyritty saamaan ylläpidettyä vain yhdessä paikassa vähentäen siihen liittyviä mahdollisia riskejä. Myös kulkukorttijärjestelmiä ja älypuhelimia pyritään

liittämään muuhun digitaaliseen taloushallintoon paremmin. Prosessin digitalisoituminen on vielä hitaasti etenevää pienempien ja keskikokoisten yritysten kohdalla, mutta halvemmat pilvipalveluratkaisut ja verohallinnon vaatimukset saattavat nopeuttaa niitä tulevaisuudessa. (Lahti & Salminen 2014, 140 - 150.)

Matkalaskuprosessin keskittäminen sähköiseen matkalaskujärjestelmään helpottaa muun muassa sen merkittävyyden ja määrän seuraamisessa. Jotta matka- ja kululaskujen sähköistäminen olisi hyödyllistä, tarvitsee ohjelma niihin liittyvät erilaiset säännöt, kirjanpidon tilit, hyväksymisprosessit ja henkilötiedot ajantasaisina. Vaikka järjestelmät ja ohjelmat ovat kehittyneet, matkalaskujen käsittely ja luominen tehdään kuitenkin usein esimerkiksi Excelillä tai jopa pelkästään paperisesti. Taloushallinnon ohjelmilla voi laskea päivärahan ja muita matkakululaskelmia syöttämällä ensin tarvittavat tiedot, kuten lähtö- ja paluuajat, ajokilometrit tai ilmaiset ateriat. Kuten muissakin prosesseissa, matkalaskuprosessin saattaa joutua ostamaan järjestelmään erillisenä moduulina. (Lahti & Salminen 2014, 101 - 109.)

Kululaskut jaetaan omilla maksuvälineillä ostettuihin ja yrityksen maksuvälineillä ostettuihin tuotteisiin ja palveluihin. Ne jaetaan ohjelmissa edelleen yleensä eri valmiisiin kululajeihin. Järjestelmien avulla luottokorttitapahtumat voidaan käsitellä parhaimmillaan automaattisesti kohdistamalla ja kirjaamalla ne tehtyjen määritelmien mukaan. Järjestelmä auttaa kulu- ja matkalaskujen prosessia myös tallentamalla kaikki kuitit sähköisesti järjestelmään liittäen ne suoraan laskuille, lakisääteisten raporttien automaattinen ajo ja lähetys sekä esimerkiksi tarkastaminen ja hyväksyntä tapahtuvat kätevämmin sähköisesti. Nykyään työmatkalla voi myös kuvata kuitit älypuhelimella ja lähettää ne heti järjestelmään estäen niiden katoamisen. (Lahti & Salminen 2014, 110 - 115.)

3.2.4 Käyttöomaisuuskirjanpito digitaalisessa taloushallinnossa

Käyttöomaisuuskirjanpidossa kirjatuista pitkäaikaisista investoinneista tehdään poistoja suunnitelman mukaisina poistoina ja ELV, eli elinkeinoverolain mukaisina, -poistoina. Käyttöomaisuutta ovat yleisesti ne yrityksen investoinnit, joita aiotaan hyödyntää vähintään kolme vuotta. Poistot vähentävät investoinnin kirjanpidollista arvoa poistetun arvon verran, mikä kuvastaa käyttöomaisuuden normaalia arvon laskemista esimerkiksi käytön ja kulumisen takia. Suomessa suuret yritykset voivat käyttää tähän prosessiin käyttöomaisuusohjelmia ja ainakin pienet yritykset käyttävät siihen usein ihan pelkästään Excel -ohjelmaa. Kuten monet muutkin taloushallinnon järjestelmän osat, käyttöomaisuuskirjanpidon voi hankkia joko moduulina nykyiseen järjestelmään, tai ostaa sitä varten kokonaan uusi ohjelma. Samoin tässäkin tilanteessa moduuli yleensä sopii paremmin aikaisempaan

järjestelmään ja helpottaa eri prosessien yhdistämistä, mutta erillinen ohjelma voi joissain tapauksissa olla tarkempi ja kehittyneempi juuri käyttöomaisuuskirjanpidossa. Molemmilla vaihtoehdoilla voi kuitenkin esimerkiksi tehdä automaattiset käyttöomaisuusraportit ja laskea kätevästi poistoihin liittyvät laskelmat. (Lahti & Salminen 2014, 131 - 134.)

3.2.5 Pääkirjanpito digitaalisessa taloushallinnossa

Eri taloushallinnon prosessit kirjataan yleensä lopulta pääkirjanpitoon. Pääkirjanpidon automatisointi voi parantaa raportteja, helpottaa aikataulujen kanssa ja vähentää inhimillisiä virheitä. Pääkirjanpito on yhteydessä muun muassa ostoreskontraan, myyntireskontraan, kassakirjanpitoon ja palkkakirjanpitoon, joista siirretään tietoa tietyin väliajoin. Muut taloushallinnon järjestelmän osat liitetään pääkirjanpitoon joko moduuleina tai erillisillä yhteyksillä. Järjestelmän sisäiset moduulit ovat siinä mielessä kätevämpiä, että ne lähettävät tietoa valmiiksi yhteensopivassa muodossa. Jokaista liiketapahtumaa vastaa sekä pääkirjanpidon tosite, että osakirjanpidon kirjaukset liiketapahtumaan liittyen. Pääkirjanpidon tositteissa, eli muistiotositteissa, on merkittyinä laskutavat, joiden avulla on saatu kirjanpitoon laitettu summa. Näitä tositteita syntyy esimerkiksi kurssieroja, jaksotuksia ja täsmäytyksiä laskettaessa. Pääkirjanpito on kokoelma eri prosessien kirjauksista, mutta toiminnallisesti se ohjaa niiden kirjaukset oikeille tileille ja raportoinnin tasoille, täsmäyttää kokonaisuuden osakirjanpidon liiketapahtumiin ja tarkistaa virheet. Koska pääkirjanpidolla on suuri rooli koko taloushallinnon kokoamisessa, tarkastamisessa ja raportoinnissa, on sen tehostaminen digitalisoitumisen avulla myös merkittävää. Raportointi tehdään digitaalisessa taloushallinnossa mahdollisimman automaattiseksi, mutta siinä kiinnitetään myös huomiota tiedon oikeanlaiseen tallennukseen, käyttöön, jakamiseen ja luotettavuuteen. (Lahti & Salminen 2014, 150 - 157.)

Kirjanpidon tositteiden yhteydessä järjestelmään tallennetaan myös sisäisen laskennan kannalta seurattavia seurantatasoja. Seurantatasoja ovat yrityksen toiminnan, seurannan, päätöksenteon ja budjetoinnin kannalta tärkeitä luokkia joihin informaatiota voi jakaa. Tasoina voivat olla esimerkiksi projekti, tuoteryhmä, kustannuspaikka ja toimipaikka. Mitä enemmän taloushallinnossa käytetään eri sisäisen laskennan seurantatasoja, sitä enemmän ne hidastavat kirjaamista ja vaativat järjestelmältä. Ulkoiseen raportointiin liittyvä arvonlisäveroraportointi perustuu arvonlisäverokirjauksiin kunkin verotason koodeilla. Nykyajan järjestelmissä ja ohjelmissa ei tarvitse enää perustaa erillisiä tilejä eri verokannoille, vaan alv:n koodi toimii omana tasonaan. EU-maiden ja sen ulkopuolisten maiden kanssa tehdessä kauppaa pitää kuitenkin käyttää niiden omia tilejään. (Lahti & Salminen 2014, 157 - 159.)

Pääkirjanpidon muistiotositteiden, jaksottamisen ja täsmäytyksen osittainen automatisointi nopeuttaa niiden hoitamista ja käsittelyä huomattavasti. Jaksotustositteiden purku, ennakkomaksujen jaksotus, Excel -tiedostojen lukeminen ja yhteisten kulujen vyörytys voidaan kaikki automatisoida nykyajan taloushallinnon järjestelmällä. Tositteiden purku pitää tehdä kirjanpidossa, jos se on jouduttu kirjaamaan manuaalisesti silloin kun juokseva kirjanpito on suljettu kuukausikaton takia. Täsmäytyksessä tarkistetaan, että osakirjanpidot täsmäävät pääkirjanpitoon. Kaikkien liiketapahtumien pitää olla pääkirjanpidossa, ja tilinpäätöksen pitää olla yhtenäinen tositteiden ja kirjanpitomerkintöjen kanssa. Täsmäyttämisen voi tehdä pankkitilien, pääkirjanpidon, osakirjanpidon ja niiden eri summien avulla. Täsmäyttäminen voidaan suorittaa automaattisemmin digitaalisessa taloushallinnossa, mutta se kannattaa myös automatisoidussa kirjanpidossa suorittaa useammin jotta järjestelmän mahdolliset viat huomataan tarpeeksi ajoissa. Ohjelma tai järjestelmä voi auttaa täsmäyttämistä tarkistuslaskelmilla, raporteilla, hälytysjärjestelmillä, välitileillä ja esimerkiksi seurantaominaisuuksilla. Kun tieto siirtyy järjestelmästä toiseen, voidaan niiden välisen tiedonsiirron täsmäyttää käyttämällä välitilejä. Välitilit pitävät kirjaa molemmissa järjestelmissä, joten niiden avulla voi huomata mahdolliset erot ja erojen määrät. Kuukausikatkot kannattaa suunnitella hyvin etukäteen, jotta kaikki tärkeät ja erääntyvät tehtävät saadaan ajoissa tehtyä katkoa ennen. Esimerkiksi käyttöomaisuushankintojen poistot voidaan automatisoida laskettavaksi etukäteen ennen katkoa, palkanlaskennan voi kirjata ennen katon aikaista maksamista ja vakiojaksotusten kirjaus voidaan myös automatisoida. Tuloslaskelman kuukausittaisen tarkistuksen voi myös tehdä ennen katkoa, jotta virheet ja poikkeamat saadaan korjattua ennen järjestelmän tietoliikenteen sulkemista. Joihinkin järjestelmiin saa myös ostolaskujen automaattisen kierrätysjärjestelmän, jolla kierrossa olevat ostolaskut voidaan jaksottaa kirjanpitoon. (Lahti & Salminen 2014, 160 - 166.)

3.2.6 Raportointi ja arkistointi digitaalisessa taloushallinnossa

Raportointi on tärkeä tapa informoida eri sidosryhmiä heitä kiinnostavista asioista, ja sen voi jakaa sidosryhmien perusteella sisäiseen ja ulkoiseen raportointiin. Sisäinen raportointi tehdään omalle johdolle tai muille työntekijöille esimerkiksi budjetointia tai strategiaa varten. Ulkoinen raportointi sisältää viranomaisraportit sekä omistajille, lehdistölle ja rahoittajille annettavat raportit. Vaikka ennen nämä kaksi eri raportointia saattoivat olla eri järjestelmissä, on nykyään normaalia että molemmat raportoinnit perustuvat samaan järjestelmään ja saman järjestelmän tietoihin. Ulkoisella raportoinnilla on lain määräämät vaatimukset tuloslaskelmalle, taselaskelmalle, pääkirja- ja päiväkirjaraportille ja esimerkiksi viranomaisilmoituksille. Viranomaisraportteja ovat veroilmoitukset, tullista raportointi ja arvonlisäveroilmoitukset. Digitaalisessa taloushallinnossa järjestelmään syötetyistä tiedoista voi tehdä automaattisia ja itse päivittyviä raportteja. Lukujen ja laskujen ulkopuoliset

kertomukset on tietenkin tehtävä käsin, joten mitään prosessia ei voi kokonaan automatisoida. Jotta raportointi onnistuu, tarvitsee muun kirjanpidon olla mahdollisimman virheetöntä ja yhteensopivaa järjestelmän sisällä. Pörssiyritysten on raportoitava konsernitilinpäätös IFRS -standardien mukaisena, mutta erilliset emoyhtiön ja tytäryhtiöiden tilinpäätökset tehdään oman maan kirjanpidon standardien mukaan verotusta varten. Taloushallinnon raportointi on kehittynyt digitalisoitumisessa eniten tiedonvarastoinnissa, käyttäjäkokemuksessa ja eri prosessien yhdistämisessä samaan ohjelmaan tai järjestelmään. Raportointi on myös kehittynyt paperittomuuden osalta, koska raporttiportaalit, raportointijärjestelmät ja sähköpostin kautta jaettavat raportit ovat kaikki toimivia ratkaisuja. Raporttiportaali on internetin kautta käytettävä raporttien tallennus- ja hakupaikka. Sen voi myös tehdä mahdollisesti muun tietoliikenneverkon tai intranetin välityksellä käytettäväksi. (Lahti & Salminen 2014, 171 – 175, 183 – 186.)

Sisäisellä raportoinnilla on merkittävä vaikutus yrityksen jatkuviin muutoksiin ja strategioihin. Se tukee eniten johtoa ja esimiehiä auttaen erityisesti nykytilanteen ja tulevaisuuden ennustamisen arviointia. Koska sisäinen raportointi perustuu tehtyyn kirjanpitoon, pitää järjestelmään tai ohjelmaan lisätä kaikki ne dimensiot mitkä haluaa myös näkyvän eriteltynä raportoinnissa. Jos järjestelmässä on siis eri dimensiot projekteille, toimipaikoille ja tuotteille, voi raportoinnissa esittää näiden eroavaisuuksia. Sisäinen raportointi auttaa myös tavoitteisiin tähtäävässä talousohjauksessa, eli budjetoinnissa. Budjetointia varten on omia ohjelmistoja ja moduuleita järjestelmiin. Ne voivat automaattisesti vastaanottaa tiedot muusta kirjanpidosta ja tehdä niiden perusteella vertailuja ja tunnuslukuja. Kontrolloinnissa digitalisoituminen auttaa hyväksymiskierroilla, käyttöoikeusrajoituksilla ja esimerkiksi syötettyjen tietojen tarkastusominaisuuksilla. (Lahti & Salminen 2014, 176 - 183.)

Digitaalisessa taloushallinnossa suurin osa arkistoinnista hoidetaan täysin sähköisesti, pois lukien lain paperisena määräämä tasekirja ja mahdollisten vastaanotettujen paperilaskujen skannaus järjestelmään. Kun arkistointi on tehty sähköisesti, on tiedon hakeminen, siitä raporttien tekeminen, sen säilyttäminen ja arkistoon pääseminen nopeampaa ja helpompaa. Kirjanpitoaineisto säilytetään järjestelmässä tilikauden loppumiseen asti, jonka jälkeen se tallennetaan pysyvään säilytykseen kahteen eri tietovälineeseen, joissa olevaa tietoa ei saa enää muuttaa. Muuttamisen voi estää esimerkiksi käyttämällä CD ROM- ja DVD- levyjä, joihin tiedon voi tallentaa vain kerran, tai asettamalla järjestelmään lukituksia tai estoja. Tieto pitää tallentaa selväkielisessä muodossa, joka tarkoittaa

”…että kirjanpitoaineiston säilyttämiseen käytetyn tietovälineen tyyppinen tietoväline on yleisessä käytössä ja että käytössä on laitteistoja ja ohjelmistoja, joiden avulla kirjanpitoaineisto on saatettavissa tietovälineeltä selväkieliseen muotoon.” (Lahti & Salminen 2014, 201.)

Yksi sähköisen arkistoinnin tehtävistä on siis tehdä arkistoidun tiedon etsimisestä, tarkastelemisesta ja edelleenkäsittelystä sähköisesti mahdollista tietyillä järjestelmillä, ohjelmilla tai esimerkiksi Excelillä. Näin digitaalisessa taloushallinnossa arkistoituja tositteita tai kirjanpitomerkintöjä ei tarvitse tulostaa lukemista varten. Muita sähköisen taloushallinnon arkistoinnin tehtäviä on rajata tarkkaan ketkä pääsevät lukemaan arkistoa ja päivittää pysyväksi jäävää arkisto vähintään tilikausittain aktiivisesti käytetystä tiedosta, eli aktiiviarkistosta. (Lahti & Salminen 2014, 200 - 203.)

4 Sähköisen ja digitaalisen taloushallinnon riskit ja niiden hallinta

Sähköisessä ja digitaalisessa taloushallinnossa käytetään erityisesti monia ohjelmia, järjestelmiä ja muuta tietotekniikkaa. Tästä syystä tietotekninen tietoturva on erittäin tärkeää niiden riskien ja riskienhallinnan kannalta. Tietoturva tarkoittaa tiedon ja tietojärjestelmien suojaamista luvattomalta pääsyltä, käytöltä, lukemiselta, muokkaamiselta, tallennukselta, tuhoamiselta, julkaisulta ja häirinnältä. Tietotekninen tietoturva on osa tietoturvaa, ja sisältää tiedon, verkon, tietokoneohjelmien ja muiden tietokonepohjaisten tietojärjestelmien suojelemista. Tietotekninen tietoturva pyrkii joko estämään tai minimoimaan uhan. (Turban, King, Lee, Liang & Turban. 2012, 488.)

Tietotekninen tietoturva voidaan jakaa uhkiin, suojaukseen ja hallintaan. Uhat voivat olla tahallisia tai tahattomia. Tahalliset uhat ovat verkon kautta tehtyjä rikoksia, ja niiden tavat muuttuvat usein ja nopeasti muun kehityksen ja rikollisuuden omien keksintöjen myötä. Internetin suojaus voi maksaa merkittävästi, joten yrityksen on osattava päättää, paljonko se investoi tietotekniseen tietoturvaan. (Turban ym. 2012, 493.)

4.1 Tietotekniset uhat

Sähköistä ja digitaalista toimintaa harrastavan yritys on altis turvallisuusriskeille, jotka tulevat sähköistä kautta tai vaikuttavat sähköisiin järjestelmiin, laitteisiin ja ohjelmiin. Tällaisia turvallisuusriskejä ovat esimerkiksi kyberhyökkäykset, kybervakoilu, hyökkäykset mobiililaitteisiin, kuten kännyköihin, internetin kautta tulevat huijaukset, hyökkäykset uuteen teknologiaan, kuten pilvipalveluihin, ja hyökkäykset verkkosovelluksiin. Yrityksillä pitää olla strategioita, turvatoimia ja tietämystä sähköisiä riskejä välttämistä ja toteutuneiden riskien aiheuttamien tilanteiden korjaamista varten. (Turban ym. 2012, 490.)

Kyberhyökkäykset voivat olla yksittäisten henkilöiden, yksittäisen tiimin, toisen yrityksen tai jopa jonkin valtion tekemiä sähköisiä hyökkäyksiä käyttämällä esimerkiksi tietokoneohjelmaa. Niiden tarkoituksena voi olla vakoilla tietoa, tuhota tietoa, varastaa verkon kautta omaisuutta, rikkoa ja haitata järjestelmiä tai saada taloudellista hyötyä hyväksikäyttämällä saatua tietoa. (Turban ym. 2012, 490 - 491.)

Internet-verkkoa ei alun perin suunniteltu turvaamaan sen käyttäjiä rikolliselta toiminnalta tai epäluotettavalta tiedolta, vaan sitä oli tarkoitus käyttää pienissä suljetuissa yhteyksissä. Siitä kuitenkin tuli maailman laajuinen osittain kontrolloimaton tiedonvälityksen keino. Internet käyttää paljolti verkkotunnussysteemiä (DNS = domain name system), jossa verk-

kotunnukset, eli verkkosivut, käännetään IP -osoitteille, eli käyttäjille. IP -osoitteet ovat internetiin otettavia laitekohtaisia yhteyksiä. Koska yhteyden lähteitä ei usein todenneta tai tarkisteta, eikä vastaanotettua tiedon eheyttä tarkisteta, ovat DNS systeemin verkkosivut alttiita hyökkäyksille. Verkkohyökkäysten määrä on lähtenyt kovaan kasvuun vuodesta 2009 lähtien ja ne ovat muuttuneet enemmän taloudellista etua hakeviksi. (Turban 2012, 491 - 492.)

Internetin pimeä talous on varastetun tiedon myymistä. Tiedot joita varastetaan ja myydään voivat olla esimerkiksi luottokorttitietoja, salasanoja ja sosiaaliturvatunnuksia. Symantec, Yhdysvaltalainen tietoturvaratkaisuja valmistava ja myyvä yhtiö, oli vuonna 2008 tehnyt tutkimuksen, jonka mukaan noin kolmekymmentä prosenttia internetin varastetun tiedon myynnistä kohdistuu luottokorttitietoihin. (Turban E ym. 2012, sivu 492 – 493.) Teknologian kehityksen ja innovaation myötä nykyiset järjestelmät ja ohjelmat kehittyvät, ja löydetään myös uudenlaisia ratkaisuja, kuten esimerkiksi pilvipalvelun käyttö taloushallinnossa, työasioiden liittäminen sosiaalinen mediaan ja langattomien yhteyksien käyttö. Uhat eivät kaikki myöskään ole ulkoisia, vaan niitä löytyy myös yrityksen sisäpiiristä. (Turban ym. 2012, 492 – 493.)

Pilvipalvelussa yrityksen käyttämät tiedot tai ohjelmat ovat pilvipalvelun tarjoajan palvelimella, eivätkä yrityksen omilla palvelimilla tai tietokoneilla. Pilvi on eri palvelimista ja tietokoneista muodostuva verkosto, johon pääsee internetin kautta tietokoneilla ja mobiililaitteilla. Facebook, Dropbox, Skype ja Office 365 ovat esimerkkejä pilvessä olevista palveluista. Tiedot säilyvät palveluntarjoajan pilvessä, vaikka sitä käyttävän asiakasyrityksen omat tietokoneet vioittuisivat. Pilvipalveluun pääsyn voi esimerkiksi rajata käyttämällä käyttäjätunnuksia, salasanoja ja kaksivaiheista tunnusta, jossa uudesta sijainnista tai laitteesta kirjautuessa pitää todentaa käyttäjätunnuksen omistus puhelimen kautta koodilla. (Elisa 2017.)

Ciscon, monikansallisen teknologian monialayhtiön, 2010 vuotuisen turvallisuusraportin mukaan kyberkriminaalit ja hakkerit ovat siirtäneet keskittymisensä Windowsin tietokoneista muihin käyttöjärjestelmiin ja mobiililaitteisiin, kuten kännyköihin ja tabletteihin. Saman raportin mukaan verkkorikollisten tekemät ansatilanteet ja huijaukset ovat edelleen toimineet. Teknologia mahdollistaa uusia tapoja käyttää hyväkseen verkkoa, järjestelmiä ja ihmisen haavoittuneisuutta tiedon varastamiseen ja vahingon tekoon. Hyökkäyksiä on myös helpompi tehdä halvoilla tai ilmaisilla työkaluilla. (Turban ym. 2012, 493-494.)

Tahattomat riskit voidaan jakaa inhimillisiin virheisiin, ympäristöhaittoihin ja tietokonejärjestelmien vikoihin. Inhimilliset virheet voivat sattua esimerkiksi laitteiston suunnittelussa,

ohjelmoinnissa, testauksessa, tiedon keräämisessä tai ohjeissa, ja ne voivat johtua kokemuksen puutteesta, huolimattomuudesta ja väärinymmärtämisestä. Ympäristöhaittoja ovat esimerkiksi sähkökatkokset, tulipalot ja myrskyt. Viat tietokonejärjestelmissä voivat johtua vaikkapa valmistuksesta tai huonosta materiaalista. (Turban ym. 2012, 495.)

Tahalliset uhat ovat rikollisten tekemiä hyökkäyksiä ja rikoksia, kuten tiedon varastaminen, tiedon väärinkäyttö ja tarkoituksellinen manipulointi, laitteiston tai ohjelmien varastaminen, virusten aiheuttama tuho, internethuijaukset ja tietokonejärjestelmiin kohdistuva vandalismi ja sabotaasi. Verkkohyökkäykset ovat internetin kautta tehtäviä rikoksia, joita verkkorikolliset tekevät muun muassa hakkeroimalla tai huijauksilla. Hakkeroinnissa tietokonejärjestelmään päästään sisälle luvattomasti. Kohteena voi olla ihminen, laite, verkko, tietokanta, ohjelma tai järjestelmä. Sähköpostin kautta tehdyt hyökkäykset ovat yleisiä, mutta myös uudet tavat hyökätä mobiililaitteisiin tai langattomiin yhteyksiin ovat yleistyneet. Yleiset heikkoudet verkkorikollisuutta kohtaan ovat salaamattomat kommunikaatiomuodot, päivittämättömät ohjelmat, palomuurin ja virustorjunnan käytön puute ja sovellusten huono turvallisuus. Yhtiön toiminta voi myös mahdollistaa heikkouksia liian vähällä koulutuksella ja tietoisuudella riskeistä ja niiden torjunnasta, kiinnittämällä liian vähän huomiota mobiililaitteiden turvallisuuteen ja käyttämällä väärin yhtiön tietokoneita ja verkkopalveluita. Kuviossa 2 on jaettu tärkeimmät tietotekniset riskit tahallisiin ja tahattomiin riskeihin. (Turban ym. 2012, 496 - 497.)

Kuvio 2 – Tietoteknisten riskien jakaminen tahallisiin ja tahattomiin riskeihin

Sähköiset hyökkäystavat voidaan jakaa teknisiin ja ei-teknisiin hyökkäystapoihin. Merkittäviä teknisiä tapoja ovat haittaohjelmat, luvaton pääsy kohteeseen, palvelunestohyökkäykset, roskaposti, vakoiluohjelmat, kohteiden kaappaukset, bottiverkot (web-robotit) ja roskaposti. Haittaohjelmat ovat tietokonejärjestelmiin tunkeutumista tai niiden vahingoittamista varten kehitettyjä ohjelmia. Ne pyrkivät toimimaan ilman tietojärjestelmän omistajan huomaamista tai suostumusta. Haittaohjelmiin kuuluvat muun muassa madot, virukset, ja Troijan hevoset. Madot ovat itsenäisesti toimivia isäntäjärjestelmän resursseja käyttävä ohjelma, jotka voivat kopioida itsensä automaattisesti seuraaviin hyökkäyskohteisiin. Virukset ovat ohjelmistokoodin osia, jotka liittävät itsensä isäntäohjelman osaksi. Troijan hevoset esittävät hyödyllistä ohjelmaa tai tiedostoa, mutta sisältävät piilotettuja haitallisia ominaisuuksia. Haittaohjelmat voivat tulla esimerkiksi sähköpostin, muistitikun, verkkoyhteyden tai verkkosivun kautta. Palvelunestossa (Englanniksi denial-of-service, lyhennettynä DoS) palveluun otetaan yhteyttä hyvin suurilla lukumäärillä, jonka tarkoituksena on hidastaa tai kaataa palvelun toiminta. Palvelunestossa voidaan myös käyttää ohjelmaa, joka tulvii kohdejärjestelmään tiedostopaketteja ylikuormittaakseen sen. Bottiverkossa jopa sadat tuhannet kaapatut verkkojärjestelmät asetetaan esimerkiksi lähettämään haittaohjelmia automaattisesti ja itsenäisesti. Roskapostia, eli spammia, voidaan käyttää esimerkiksi mainostamiseen tai haitallisten viestien ja ohjelmien levittämiseen. Arvioiden mukaan vuonna 2008 maailmassa lähetettiin 62 biljoonaa (tuhatta miljardia) roskapostia, ja vuonna 2009 90 % lähetetyistä sähköposteista oli roskapostia. (Turban ym. 2012, 500, 511.)

Ei-tekniset hyökkäystavat perustuvat sosiaaliseen manipulointiin, jossa ihmiset saadaan sosiaalisesti tai psykologisesti tekemään haluttuja tekoja tai paljastamaan salassa pidettävää tietoa. Näitä tapoja ovat esimerkiksi verkkourkinta (Englanniksi phishing), huijaukset ja identiteettivarkaudet. Verkkourkinnalla pyritään saamaan laittomasti salaista tietoa, kuten henkilöllisyystietoja, salasanoja ja luottokorttitietoja. Urkinnassa voidaan esittää olevansa pankin, sosiaalisen media-alan yhtiön, telekommunikaatioyhtiön tai luottokorttiyhtiön työntekijä, kohdehenkilön ystävä tai muu tietoa tarvitseva henkilö. On myös olemassa vale-nettisivuja, jotka esittävät aitoja palveluiden tarjoajien sivuja ja keräävät niihin syötettyjä tietoja omiin tarkoituksiinsa. Huijaukset toimivat verkon välityksellä helpommin, koska osapuolet eivät koskaan tapaa toisiaan henkilökohtaisesti. Huijauksista merkittäviä ovat verkossa vilpilliset tilaukset, joissa tilaajat esimerkiksi valehtelevat maksutiedot saadakseen tuotteet maksamatta. Identiteettivarkauksissa henkilöllisyystietoja varastetaan pystyäkseen esittäytymään kohdehenkilönä saadakseen rahaa tai muita hyötyjä. Varastettua identiteettiä voi käyttää esimerkiksi ostettaessa palveluita ja tuotteita, rahanpesussa tai tekemällä rikoksia toisen henkilötunnuksilla. Roskaposti on samanlaisia viestejä, joita lä-

hetetään massapostina eri tavoin kalastetuille sähköpostiosoitteille. (Turban ym. 2012, 501 - 508.)

4.2 Tietoteknisten uhkien hallinta

Tietoteknisen tietoturvan toteutusta varten tarvitaan käytettävä teknologia ja suunniteltava turvallisuusstrategia, josta johto ja hallinto huolehtivat, ja jota muut työntekijät ja järjestelmien käyttäjät noudattavat. Itse teknologisesta puolesta vastaa usein yhtiön tietojärjestelmän osasto ja turvallisuuspalveluiden myyjät. Strategia sisältää riskien estämisen, torjunnan, toteutuneiden riskien havaitsemisen ja valvomisen, laajenemisen estämisen, toipumisen, oikaiseminen, tietoisuuden ja noudattamisen. Tässä materiaalissa estävillä toimenpiteillä tarkoitetaan tekoja jotka saavat rikolliset luovuttamaan ajatuksesta hyökätä tietyllä tavalla, esimerkiksi pelätessään jäävänsä kiinni. Torjunnalla estetään luvattomien käyttäjien, eli tunkeutujien, pääsy sisälle mihinkään järjestelmän osaan esimerkiksi vaatimalla salasanaa. Havainnoinnissa pyritään huomaamaan tehdyt hyökkäykset ja niiden onnistumiset mahdollisimman aikaisin ja tarkkaan. Mitä aikaisemmin hyökkäys huomataan, sitä nopeammin se voidaan korjata ja sitä vähemmän tuhoa se ehtii saada aikaan. Haitallisten vaikutusten leviäminen pitää estää sammuttamalla vähintään hyökkäyksen alla olevat osat, tai katkaisemalla yhteydet joita hyökkäys käyttää. Riskien tietoisuuden parantamisella autetaan kaikkia muita turvallisuusstrategian osia, ja pidetään huoli että niitä pystytään tietoisesti noudattamaan. Tietoisuutta voi parantaa esimerkiksi koulutuksella ja ohjeistuksilla. Noudattaminen koskee sekä annettuja ohjeita ja sääntöjä, että kokonaisuudessaan koko strategian yleistä noudattamista. (Turban ym. 2012, 499.)

Turvallisuustilanteen tapahduttua yhtiön ja sen työntekijöiden pitää toipua siitä. Mitä suurempi hyökkäys tai katastrofi, sitä tärkeämpää on nopea toipuminen. Liiketoimintaa ja työntekoa pitää pystyä jatkamaan jo ennen kuin tietojärjestelmät ovat kokonaan palautuneet, ja niiden palautuminen pitää olla nopeaa. Toipumista varten yhtiöllä pitää olla katastrofi- ja elpymissuunnitelma. Esimerkiksi joidenkin osien korvaaminen ja korjaaminen on parempi tapa elpyä kuin kokonaan uuden koneiston ja järjestelmän hankkiminen. Oikaisuvaiheessa mahdolliset ongelman aiheuttajat ja sen mahdollistaneet tekijät kuten tietoturva-aukot selvitetään ja korjataan. Jokaisessa vaiheessa ja tilanteessa on tärkeää myös riskitietoisuus ja sääntöjen noudattaminen, jotta turvallisuusstrategia toteutuisi suunnitellusti. Strategia pitää jatkuvasti päivittää uusien uhkien varalta, ja uudet järjestelmät ja koneet olisi hyvä testata heikkouksien varalta. (Turban ym. 2012, 499.)

Verkon ja järjestelmien turvaamista varten on käytettävä kulunvalvontaa. Kulunvalvonnalla määritellään kuka ja mikä pystyy todellisuudessa käyttämään kyseisessä verkossa olevia

ominaisuuksia ja tietoja. Se määrittelee myös mitä resursseja käyttäjä pääsee käyttämään ja millä tasolla, kuten esimerkiksi tiedostoja, ohjelmia, servereitä, laitteita ja verkkosivuja. Käyttötasoja voivat olla esimerkiksi lukeminen, katsominen, kopiointi, poistaminen, suorittaminen, muokkaaminen ja siirtäminen, ja ne voidaan määritellä käyttäjäkohtaisesti käytettävien resurssien kanssa. Kulunvalvonnassa on kaksi pää ominaisuutta, jotka ovat käyttöluvat, eli määritellyt oikeudet siihen mitä pääsee käyttämään, ja tunnistaminen, jossa käyttäjä tunnistetaan oikeaksi henkilöksi tai käyttäjäksi. Näiden toteuttamiseen voidaan käyttää esimerkiksi salasanoja, kortinlukijoita tai allekirjoituksia. (Turban ym. 2012, 518.)

Verkon kautta tulevia hyökkäyksiä vastaan voi puolustautua palomuurilla. Palomuuri on portti sisäisen ja ulkoisen verkon välissä. Sisäinen verkko sisältää luotettavat laitteet, verkot ja yhteydet, ja ulkoinen kaiken tuntemattoman ja ulkoisen verkon. Palomuuri tutkii vastaanotettavan tiedon ja yhteydet, ja päättää saako se mennä läpi vai ei. Verkolla voi olla monia palomuureja eri tasoilla, jotta esimerkiksi tiettyyn verkkoympäristöön päässeet hyökkäykset eivät automaattisesti pääse tärkeimpiin verkon osiin. Palomuureilla on eroja, esimerkiksi tietokoneen mukana ilmaiseksi tuleva palomuuri voi suojata ja toimia maksullista palomuuria huonommin. (Turban ym. 2012, 523.)

Sähköposti sisältää useita riskitekijöitä. Sillä vastaanotetut liitetiedostot voivat sisältää viruksia, roskaposti tulee suurimmaksi osaksi sen kautta ja sosiaaliset huijaukset tehdään usein sen välityksellä. Sähköpostia voi suojata palomuurilla, virustorjuntaohjelmalla ja roskapostia estävillä ohjelmilla. Viestejä voi myös salata maksullisilla palveluilla, jolloin niitä pystyy lukemaan vain tietyillä ohjelmilla tai koodeilla. Kaiken muun lisäksi lähtevää ja tulevaa sähköpostia voidaan suodattaa arkaluontoisen tai haitallisen tiedon perusteella, esimerkiksi jottei lähtevässä sähköpostissa voi olla henkilötunnuksia tai muita tärkeitä tunnuksia. Kuitenkin kaikesta tärkeintä on kouluttaa sähköpostin käyttäjät turvallisuudesta uhkia ja huijauksia vastaan. (Turban ym. 2012, 526.)

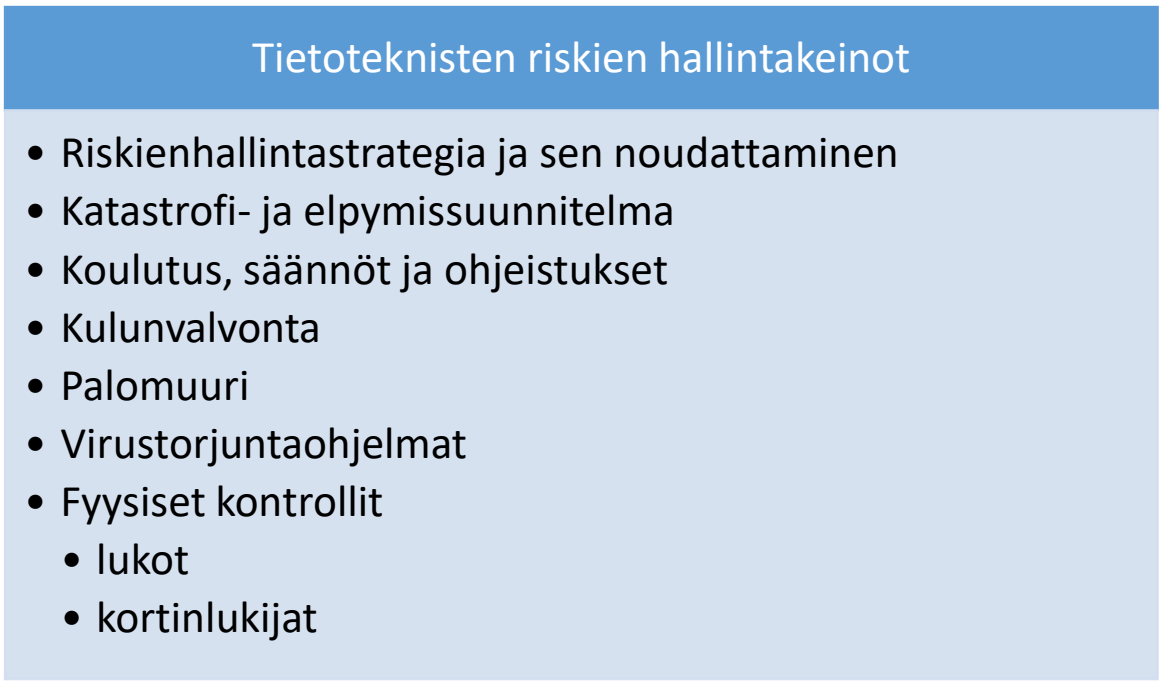
Verkon kautta tulevien uhkien lisäksi uhat voivat myös kohdistua fyysiseen tietotekniikkaan kuten tietokoneisiin, servereihin ja fyysisiin varakopioihin. Näitä uhkia varten pitää olla fyysisiä kontrolleja. Tietokeskusten ja tärkeiden laitteiden kannattaa olla vesitiiviillä ja palamattomalla paikalla, jonka lisäksi on käytettävä lukkosysteemejä ja esimerkiksi kortinlukijoita. Tulipaloja varten pitää suunnitella niiden estäminen, havaitseminen ja sammuttaminen, ja asentaa esimerkiksi sprinklereitä ja vaahtosammuttimia. Sähköinen laitteisto pitää pystyä sammuttamaan hätätilanteessa. (Turban ym. 2012, 527.)

Koska yritysten resurssit ovat rajalliset, eivät ne pysty täysin suojautumaa kaikilta mahdollisilta eri riskeiltä. Tästä syystä yrityksen pitää määritellä mitkä ovat sille merkittävimmät

riskit, ja mille se antaa vähemmän huomiota. Merkittävämpiä riskejä vastaan suojautumiseen käytetään enemmän resursseja. Arvioinnissa voi käyttää esimerkiksi viisivaiheista menetelmää:

1. Riskin oleellisuutta varten pitää ensin määritellä kohteiden, kuten rakennusten, ihmisten, laitteiston ja tiedon, vertailuarvot.
2. Toiseksi kaikki eri mahdolliset riskit, ulkoiset ja sisäiset, pitää määritellä ja luetella. Riskit voivat koitua tahallisesti tai tahattomasti.
3. Kolmanneksi pitää määritellä alttiuksia riskeille, eli heikkouksia, ja kuinka todennäköisesti niitä hyväksikäytetään. Heikkouksia voi löytyä esimerkiksi toimintatavoista, käytetyistä teknologioista ja laitteista tai yrityksen politiikasta.
4. Neljänneksi lasketaan kuinka suuri vahinko kustakin uhasta voi syntyä mihinkin kohteeseen.
5. Lopuksi määritellään, valitaan ja asetetaan sopivat kontrollit, eli hallintakeinot. Tässä vaiheessa otetaan myös huomioon taloudelliset mahdollisuudet, tehokkuudet ja kontrollien mahdolliset negatiiviset vaikutukset toimintaan.

Resurssien lisäksi turvallisuudessa tulisi ottaa huomioon myös lait ja etiikka. Esimerkiksi kysymykset yksittäisen ihmisen toiminnan valvomisesta ja sananvapaudesta voivat olla vaikeita ja rajata mahdollisia suojauskeinoja. Tässä luvussa mainitut tärkeimmät riskienhallintakeinot voi vielä katsoa alla olevasta kuviosta. (Turban ym. 2012, 533 - 535.)



Kuvio 3 – Tietoteknisten riskien hallintakeinot (Turban ym. 2012)

4.3 Sähköisen ja digitaalisen taloushallinnon kontrollit

Kontrollit ovat tärkeä osa riskienhallintaa yrityksessä. Kontrolleja on yrityksen sisäisiä ja ulkoisia, kuten esimerkiksi tilintarkastajat ja oma taloushallinto. Johto asettaa kontrolleille tavoitteita, ja on muutenkin niistä vastuussa. Kontrollien päätehtävät ovat raportoinnin luotettavuuden, toimintojen tehokkuuden ja lakien noudattamisen tarkistaminen ja varmistaminen. Ne voidaankin jakaa paljastaviin ja ehkäiseviin kontrolleihin. Kontrolloinnissa keskitytään eniten painoarvoltaan merkittäviin osiin ja prosesseihin, koska niissä olevat virheet voivat johtaa lisäkuluihin tai vääristyneisiin raportteihin. Digitaalisessa taloushallinnossa järjestelmät ja ohjelmat auttavat kontrolleja muun muassa reaaliaikaisuudella ja läpinäkyvyydellä. Kontrollit voivat määrittää asetusten kautta mitä järjestelmä automaattisesti tarkkailee ja esimerkiksi mistä lukujen suhteista ja virheistä järjestelmä tekee automaattisen hälytyksen. Myös erilaiset järjestelmien ominaisuudet, kuten rajatut käyttöoikeudet, hyväksymiskierrot ja muut pakotteet, auttavat ehkäisevää kontrollointia. (Lahti & Salminen 2014, 188 - 190.)

Yleiset kontrollit varmistavat taloushallinnon raportoinnin oikeellisuuden. Näitä ovat esimerkiksi tehtävien jakaminen eri henkilöille vaarallisten työyhdistelmien estämiseksi, pakolliset kentät järjestelmään tai ohjelmaan jotka pitää täyttää jotta tosite lähtee eteenpäin, samojen tositteiden uudelleensyöttämisen estämistä esimerkiksi laskunumeron mukaan, euromääräinen raja syötettäville tiedoille ennen lisävarmennuksia tai määritelmät minkälaista tietoa mihinkin kenttään voi syöttää välttääkseen virheitä. Prosessikohtaiset kontrollit kohdistuvat nimensä mukaan tiettyyn prosessiin, eivätkä ole yleistettävissä muille prosesseille sellaisinaan. Ne voidaan jakaa järjestelmän sisäisiin ja ulkoisiin kontrolleihin, joista sisäiset ovat automatisoituja suurimmaksi osaksi. Järjestelmän sisäisiä kontrolleja ovat esimerkiksi ostolaskutuksessa muun muassa toimittajatietojen muuttamisen oikeuksien rajaus henkilöille jotka eivät voi syöttää tai maksaa laskuja, lokitiedot toimittajarekisteriin tehdyistä muutoksista ja niiden tekijöistä, samannumeroisen laskun esto samalla toimittajalla jotta vältetään tuplalaskut, vastaanotetut tilaukset verrataan ostotilaukseen ja toimittajan antamiin tietoihin, pakotetut ennalta määritelleet kiinteät hyväksymiskierrot ostolaskuille ja euromääräiset hyväksymisrajat henkilöittäin. Järjestelmän ulkopuoliset kontrollit ovat yleisemmin manuaalista työtä enemmän vaativia toimenpiteitä. Näitä puolestaan ovat ostolaskutuksen kohdalla esimerkiksi hyväksymismenettely uuden toimittajan avaukselle jotta voidaan rajata ketkä voivat pyytää uusia toimittajia järjestelmään, toimittajien seuranta mahdollisten duplikaatioiden, eli kopioiden, varalta ettei järjestelmässä ole sama toimittaja moneen kertaan, ostolaskujen hyväksyntämenettely, ostoreskontran ostovelkojen ja toimittajien antamien ostovelkatietojen täsmäytys virheiden varalta tai selvitykset

vanhoiksi jääneistä ostolaskuista maksukiellossa olevien laskujen ja vanhojen hyvityslaskujen aiheellisuudesta. (Lahti & Salminen 2014, 190 - 195.)

Edellisessä kappaleessa lueteltiin sisäisiä ja ulkoisia kontrolleja ostolaskutuksen näkökulmasta. Prosessikohtaisia sisäisiä ja ulkoisia kontrolleja on tämän lisäksi ainakin maksatuksessa, matkalaskujen käsittelyssä, myyntilaskutuksessa, kassanhallinnassa, maksuliikenteessä ja pääkirjanpidossa. Myyntilaskutuksen kontrollit pyrkivät varmistamaan, että kaikista palveluista ja tavaroista laskutetaan asianmukaisesti ja myyntisaatavat maksetaan. Mahdollisia kontrolleja järjestelmään tähän liittyen ovat esimerkiksi automaattinen tilauksen tai lähetyksen estäminen myyntikiellon omaaville asiakkaille ja automatisoitu maksukehotusten lähetys ja tietyn ajan erääntyneiden myyntilaskujen siirtäminen perintätoimistolle. Ulkopuolisia kontrolleja myyntilaskutusprosessiin ovat esimerkiksi luottotietojen tarkastaminen ennen asiakkaan tallentamista järjestelmään tai ohjelmaan ja avoimen saldon tarkastaminen vastaanotetulta tiliotteelta. (Lahti & Salminen 2014, 197 - 198.)

Matkalaskujen käsittelyssä ja maksatuksessa kontrollit pyrkivät estämään ja havaitsemaan yritykselle kuulumattomat maksut ja sääntöjen, kuten matkustussääntöjen, rikkomiset näissä prosesseissa. Järjestelmään voi esimerkiksi automatisoida työntekijärekisterin ylläpidon henkilöstöhallinnon tai palkkajärjestelmän mukaan, jolloin se pysyy aina ajan tasalla nykyisistä työsuhteista, tai asettaa maksuaineiston automaattisen luonnin perustumaan esimiehen aikaisemmin hyväksyttyihin matkalaskutapahtumiin, jolloin

”…on hyvin epätodennäköistä, että maksuun menee prosessin ohi hyväksymättömiä tapahtumia väärälle pankkitilille”. (Lahti & Salminen 2014, 196)

Muita kuin järjestelmän sisäisiä kontrolleja maksatukseen ja matkalaskujen käsittelyyn ovat esimerkiksi matka- ja kululaskujen tietojen ja selitteiden vertailu niihin liitettyihin kuitteihin, näiden laskujen hyväksyminen ennen matkan aloittamista tekemällä matkasuunnitelman ja laskujen aiheellisuuden varmentaminen tehdyn matkasuunnitelman avulla. Maksuliikenteen ja kassanhallinnan kontrollit puolestaan pääsääntöisesti jakavat prosessin eri vaiheet eri työntekijöille, jotta ei synny vaarallisia työkombinaatioita ja riskit saadaan minimiin. Järjestelmän sisäisiä kontrolleja on tähän esimerkiksi enemmän kuin yhden hyväksynnän vaatiminen, oikeuksien rajaaminen prosessin eri vaiheiden mukaan eri henkilöille, kuten pankkitietojen syöttämisen ja laskujen hyväksymisen, ja tiedon automaattinen siirtäminen kassajärjestelmästä kirjanpitoon. Tärkein taloushallinnon järjestelmän ulkopuolinen kontrolli maksuliikenteeseen liittyen, on eri reskontrista lähetetyistä maksuista kerätyn selvittelytilin ja pankkitililtä lähteneiden maksujen täsmäytys toisiinsa,

jotta huomataan tuplamaksut, ylimääräiset maksut ja muut mahdolliset virheet. (Lahti & Salminen 2014, 195 - 198.)

Pääkirjanpito vaatii myös omat kontrollinsa, joiden tehtävänä on tulos- ja taseraportoinnin oikeellisuuden varmistaminen. Kirjanpidon järjestelmän kontrolleja ovat esimerkiksi avoimien ja selvitettyjen tase-erien tilan merkitseminen järjestelmään, jotta ajolla saadaan automaattisesti avoimet tase-erät dokumentointia ja tarkistamista varten. Muita järjestelmän sisäisiä kontrolleja ovat reskontrien ja pääkirjanpidon tietojen täsmäytysraportit ja kauden sulkeminen kirjausten ollessa valmiita, jotta raportoituun kauteen ei voi enää tehdä lisää kirjauksia. Yksi järjestelmän ulkopuolella tehtävistä kontrolleista pääkirjanpitoon liittyen on taseen avoimien erien läpikäynti. Vanhat toteutuneisiin tapahtumiin liittyvät varaukset ja jaksotukset pitää purkaa tuloslaskelmaan, jotta ne eivät ole kirjanpidossa kahteen kertaan. (Lahti & Salminen 2014, 199.)

5 Empiirisen tutkimuksen toteutus

Teknologian kehitys on tuonut taloushallinnolle paljon hyödyllisiä ja tehokkuutta lisääviä ratkaisuja. Taloushallinnon digitalisoituminen mahdollistaa kuitenkin myös uusia riskejä, joista voi olla vaikea pysyä perillä nopeiden muutoksien tapahtuessa. Tämän opinnäytetyön tarkoitus on tutkia mitä tämänlaisia riskejä on, ja miten niitä hallitaan taloushallinnon työntekijän näkökulmasta. Tutkimuksen aiheena on siis: Taloushallinnon digitalisoitumisen tuomat riskit ja niiden hallinta taloushallinnon työntekijän näkökulmasta. Tutkimuksen on tarkoitus auttaa taloushallinnon alalla työtä tekevää henkilöä tuntemaan taloushallinnon sähköistymisen ja digitalisoitumisen tuomista riskejä ja oppimaan niiden hallinnan tavoista.

Tutkimusongelman mukaan haettava tieto on laadullista, koska tarkoitus on saada kuvaavaa tietoa riskeistä ja niiden hallinnasta. Tehty tutkimus oli tästä syystä luonteeltaan myös laadullinen, eli kvalitatiivinen, tutkimus. Laadullisen tutkimuksen tarkoituksena on pyrkiä ymmärtämään, tulkitsemaan ja jopa mallintamaan tutkittavaa asiaa. Se on myös ainutkertaista ja tilannesidonnaista. Tämä johtuu siitä, että laadullisella tutkimuksella saatu tieto on aina esimerkiksi ajankohtaan, yhteyksiin ja ympäristötekijöihin liittyvää. Kvalitatiivisessa tutkimuksessa teoria, aineisto ja käsitteistö ovat vuorovaikutuksessa, eikä teorian muotoilu ole sen pää painopiste. (Pitkäranta 2014, 27 – 30.)

Tutkimuksen oli tarkoitus olla hyödyksi taloushallinnon alalla työskenteleville henkilöille, joten myös tutkimuskohteena olivat taloushallinnon alalla työskentelevät henkilöt. Tutkimus tehtiin Suomessa ja siihen osallistuvat henkilöt valittiin rajallisten resurssien ja ajan puitteissa minulle jollain tavalla tutuista ihmisistä, joilla olisi suuri todennäköisyys osallistua ja vastata tutkimukseen. Tutkimustavaksi valittiin sähköpostin välityksellä lähetettävä avoin kyselylomake, koska se oli vastaajille kätevin tapa osallistua tutkimukseen. Tällöin vastaajat pystyivät itse vastaamaan silloin kuin heillä oli aikaa, he pystyivät vastaamaan myös ollessaan kaukana ja he pystyivät pohtimaan vastauksiaan rauhassa ja mahdollisesti myös pienissä erissä. Tutkimuksen kannalta oli hyvä valita vastaajille paras menetelmä, koska siten pystyin varmistamaan mahdollisimman kattavat vastaukset ja suuremman osallistumisprosentin.

5.1 Kyselyyn vastanneet

Kyselyyn osallistui neljä talousalalla tällä hetkellä tai aikaisemmin työskennellyttä henkilöä, jotka halusivat pysyä nimettöminä. Vastanneilla on eri määrä kokemusta taloushallin-

non alan töistä ja myös eri tasoilla. Vastausten mahdollista erittelyä varten jaan vastanneet vastaajiin A, B, C ja D.

Taulukko 1 – Kyselyyn vastanneiden taustatietoja

Vastaaja	Ikä	Kokemus (vuosia noin töissä taloushallinnossa)	Käytetyn taloushallinnon kehityksen taso (arviolta parhaimmillaan)
Vastaaja A	49	25	sähköistynyt 100 %, digitalisoitunut 80 %
Vastaaja B	30	6	sähköistynyt 100 % digitalisoitunut 65 %
Vastaaja C	62	16	sähköistynyt 100 % digitalisoitunut 65 %
Vastaaja D	66	40	sähköistynyt 80 % digitalisoitunut 50 %

Kuten taulukko yhdestä voi nähdä, vastaaja B:llä on suhteessa vähemmän kokemusta taloushallinnon tehtävistä ja on vastanneista nuorin, kun taas D:llä on kaikista vastanneista eniten kokemusta taloushallinnon asiantuntijatehtävistä. A:lla ja C:llä on molemmilla paljon kokemusta alalta. Kaikkien vastanneiden taloushallinto oli vähintään sähköistynyt, mutta vastaaja A:n taloushallinnosta oli hänen arvionsa mukaan jopa *"…70 – 80 % automatisoitua viimeisen kymmenen vuoden aikana*", tehden siitä kaikista vastanneista digitalisoituneimman taloushallinnon. Vastaaja B:llä ei ole kokemusta muusta kuin sähköisestä ja digitalisoituneesta taloushallinnosta: *"Kirjanpito on aina minun työssäni tapahtunut tietokoneella. Viime vuosina olen tehnyt kirjanpitoa yrityksille, joilla kaikki kirjanpitomateriaali säilytetään sähköisessä muodossa."* Vastaaja C:llä on enemmän kokemusta sähköistyneestä taloushallinnosta ja jonkin verran kokemusta digitalisoituneemmasta taloushallinnosta. *"Meillä tapahtui kaikki laskutus, työajankäyttörekisteröinnit, matkalaskujen laatiminen ja kirjaukset kirjanpitoon omista henkilökohtaisista kannettavista."* Vastaaja D:n käytetyn taloushallinnon kehityksen taso ei ole sähköistyneisyyden osalta koskaan ollut 100 %, koska hänen työpaikallaan on aina käytetty myös merkittävässä määrin paperista taloushallintoa. Vastaajista A, C ja D ovat enimmäkseen työskennelleet suurissa yrityksissä, kun taas vastaaja B on enimmäkseen tehnyt töitä pienemmissä yrityksissä.

Viimeiseksi jää vastaaja D:n käyttämän taloushallinnon kehittyneisyyden arviointi. Hänellä on kokemusta ainakin sähköistyneestä taloushallinnosta, mutta myös hieman vanhem-

masta digitalisoituneemmasta taloushallinnosta. Tästä syystä taulukossa 1 vastaaja D:n taloushallinnon digitalisoituminen parhaimmillaan on arvioitu olevan noin 50 %. Esimerkiksi hänen käyttämänsä järjestelmä oli yhtenäinen ja kattoi monia osaprosesseja: *"Järjestelmästä oli liittymiä moniin muihin järjestelmiin sekä taloushallinnossa että muualla organisaatiossa."* Kaikilla vastanneilla on siis kokemusta sekä sähköisestä, että digitalisoituneesta, taloushallinnosta. Kaikkien vastaajien työpaikoilla on tämän lisäksi lähivuosina uudistettu ja automatisoitu järjestelmiä, joten heiltä saatu tieto on tässä mielessä ajankohtaista. Kaikki vastaajat ovat tehneet sähköisesti tai digitaalisesti etätöitä, ja kaikki paitsi vastaaja D ovat käyttäneet paljon pilvipalveluita.

5.2 Tutkimuksessa käytetyt kysymykset

Avoimessa kyselyssä oli yhteensä yksitoista kysymystä. Ensimmäinen kysymys kysyi tarkemmin taustoista. Sen jälkeen tulevat yhdeksän pääkysymystä liittyi suoraan työn aiheeseen. Viimeinen, eli yhdestoista, kysymys mahdollisti kommentteja ja pohdintoja. Tarkemmin ottaen ensimmäinen kysymys tarkensi vastaajan kokemusta sähköisen ja digitaalisen taloushallinnon käytöstä, eli mitä aiheeseen liittyviä digitalisoituneen taloushallinnon teknologisia osia vastaaja on käyttänyt. Yhdeksän pääkysymystä voidaan jakaa kahteen eri aiheeseen: riskeihin ja riskienhallintaan. Viisi kysymyksistä, eli kysymykset 3, 4, 8, 9 ja 10 kysyvät eri tavoin riskeistä, joita digitaalinen taloushallinto mahdollistaa. Kysymykset 2, 5, 6 ja 7 kysyvät kokemuksista näiden riskien hallinnasta eri muodoissa. Seuraavasta taulukosta voi nähdä kaikki haastattelukysymykset lyhennetyssä muodossa.

Taulukko 2 – Haastattelukysymykset lyhennetyssä muodossa

1. Käytätkö nykyään/käytitkö ennen paljon työnteossa taloushallintoon liittyvää teknologiaa, laitteita, ohjelmia tai järjestelmiä?
2. Mitä olet huomioinut teknologian käytön koulutuksesta työpaikalla/työpaikoilla taloushallintoon liittyen?
3. Oletko kokenut töissä taloushallinnon toimintaa, tai yrityksen muuta toimintaa, haittaavia hyökkäyksiä, jotka ovat tulleet internetin avulla/välityksellä?
4. Oletko kokenut merkittäviä tai pienempiä ei-tahallisia sähköisen taloushallinnon häiriöitä, virheitä, vahinkoja?
5. Seurataanko mielestäsi työpaikalla annettuja ohjeita ja säädöksiä taloushallintoon liittyen tarpeeksi tarkkaan ja luetaanko ne tarpeeksi huolellisesti?
6. Otetaanko teknologian kehityksen myötä tulevat riskit töissäsi mielestäsi tarpeeksi huomioon vaikka se onkin kallista ja aikaa vievää?
7. Miten vertailisit nykyistä sähköistä/digitalisoitunutta taloushallintoa vanhempaan paperiseen taloushallintoon?
8. Onko pilvipalvelu mielestäsi turvallinen?
9. Lisääkö etätöiden teko mielestäsi riskien määrää?
10. Oletko huomannut tai kokenut, että kilpaileva yritys tai jokin sidosryhmä olisi yrittänyt saada työpaikaltasi jotain salaista tietoa sähköisesti?
11. Herääkö omia ajatuksia, mielenkiintoisia pointteja, tai muuta kommentoitavaa, jota haluaisi aiheeseen liittyen esittää?

Sähköpostilla lähetetty avoin kyselylomake näkyy alkuperäisessä muodossaan liitteenä (liite 1). Kysymysten asettelu oli osittain tarkoituksenmukaisesti melko avointa, jotta vastauksiin saataisiin mahdollisimman paljon hyödyllistä tietoa ja kokemuksia. Erottelin kysymykset kuitenkin aiheiden sisällä sen mukaan, että saisin vastaajilta tietoa erityisesti tietyistä alan kirjallisuudesta löytyneistä aihealueista. Kahden pääaiheen, riskien ja niiden hallinnan, jakaminen yhteensä yhdeksään eri kysymykseen auttoi myös vastaajia muistamaan mitkä asiat aiheeseen liittyvät. Yhdennentoista kysymyksen, jossa kysyttiin aiheesta muita mahdollisia mielipiteitä ja kokemuksia, oli tarkoitus mahdollistaa vastaajien kertoa kysymysten ulkopuolelta aiheeseen liittyviä näkökulmia, joita kysymysten asettelussa en osannut ottaa huomioon.

Riskeihin liittyvistä kysymyksistä asetin kysymykset 3 ja 4 avoimelle kyselylomakkeelle tärkeämmiksi, ja kysymykset 8, 9 ja 10 ei-tärkeiksi tarkentaviksi lisäkysymyksiksi. Riskeihin liittyvistä tärkeämmistä kysymyksistä kysymys 3 hakee tietoa ulkopuolelta tulevista tahallisista uhista ja kysymys 4 hakee tietoa tahattomista, sekä sisäisistä että ulkoisista, riskeistä. En tässä tutkimuksessa kysynyt yrityksen sisäisistä tahallisista uhista, koska nämä ovat yrityksille ja työntekijöille henkilökohtaista ja arkaluontoista tietoa. Edellä mainitut kysymykset keskittyvät toteutuneisiin riskeihin, minkä tarkoituksena on kysyä taloushallinnon työntekijöiden kokemuksia. Toteutuneet riskit ovat siinä mielessä olennaisia, että ne ovat ainakin näillä vastanneilla pitkien urien aikana tapahtuneet, eivätkä jääneet vain teorian tasolle. Kysymykset 8, 9 ja 10 kysyvät vielä erikseen pilvipalveluiden, etätöiden ja tietoturvan riskeistä, sillä nämä kaikki ovat olennaisia osia kehittynyttä sähköistä tai digitalisoitunutta taloushallintoa.

Riskien hallintaan liittyvät kysymykset 2, 5, 6 ja 7 kysyvät eri kautta taloushallinnon sähköistymisen ja digitalisoitumisen kannalta riskienhallinnasta. Nekin hakevat tietoa erityisesti taloushallinnossa työskentelevän henkilön näkökulmasta, mistä syystä keskityin kokemuksiin koulutuksesta, työpaikalla olevista säännöistä ja ohjeista, niiden noudattamisesta ja hallintaan käytettyjen resurssien riittävyydestä. Seitsemäs kysymys osittain liittyy molempiin riskeihin ja niiden hallintaan, mutta sen ajatuksena oli antaa vapaasti mahdollisuus tuoda esille muita riskienhallintaan liittyviä kokemuksia.

6 Tutkimuksen tulokset

Käyn tulokset läpi aiheittain ensin keskittyen itse riskeihin, ja myöhemmin niiden hallintaan. Riskeistä käydään ensin läpi toteutuneet tahalliset ulkopuolelta tulevat riskit, ja sitten tahattomat ulko- ja sisäpuolelta tulevat riskit. Tämän jälkeen esitän vastaajien mielestä tärkeimmät riskit, jotka eivät ole kuitenkaan toteutuneet heidän uriensa aikana. Riskien jälkeen siirrymme riskien hallintaan, josta käydään ensin läpi yleisiä asioita, ja sitten aihekohtaisia osia, kuten koulutus ja työpaikalla annettujen ohjeiden noudattaminen.

6.1 Vastanneiden kohtaamat toteutuneet riskit sähköisessä ja digitaalisessa taloushallinnossa

Sähköisen ja digitaalisen taloushallinnon ulkopuolelta tulevista riskeistä on kaikilla vastanneilla kokemusta. Vastaaja A:lle on erityisesti tullut vastaan tietopyyntöhuijauksia ja rahansiirtohuijauksia, mutta nämä ovat hänen mielestään helppoja tunnistaa huijauksiksi. Hänelle ne tulevat yleensä sähköpostin välityksellä. Vaikka huijausviestit eivät itsessään ole kovinkaan teknisiä, ne hyödyntävät digitaalisen taloushallinnon tiedonvälitystä ja sen heikkouksia ja ovat yksi sosiaalisen manipuloinnin tavoista. Myös vastaaja B on kohdannut paljon huijausviestejä, mutta ne eivät ole aiheuttaneet hänelle ongelmia ja ovat olleet helppoja tunnistaa. Vastaaja D puolestaan muistelee saaneensa jopa miljoonia haitallisia tai turhia viestejä uransa aikana, ja monia viestejä jotka sähköpostiohjelma itse luokitteli haitalliseksi ja mahdollisesti vaaralliseksi roskapostiksi.

Muita ulkoisia tahallisia uhkia ovat olleet sähköpostin mukana tulleet virukset ja internetin kautta tulevat madot ja haittaohjelmat. Nämä virukset ovat vastaaja C:n työpaikalla lamauttaneet koneita, ja joskus jopa kokonaisia järjestelmiä. Vastaaja C:n työpaikalta on myös varastettu digitaalisessa taloushallinnossa käytettäviä koneita ja laitteita tiukoista turvatoimista huolimatta. Hänen mukaansa erityisesti kannettavia tietokoneita on varastettu, ja ne ovat voineet sisältää yrityksen kannalta salaista ja arvokasta tietoa. Hän ei ole silti kuullut, että tätä informaatiota olisi pystytty käyttämään väärin ainakaan merkittävällä tasolla. Kaikille vastanneille merkittävät ulkoiset uhat ovat olleet melko harvinaisia. Esimerkiksi vastaaja B ei ole koskaan kohdannut aggressiivisia hyökkäyksiä käyttämiinsä järjestelmiin tai internetpalveluihin.

Vastanneet ovat kokeneet sähköistä ja digitaalista taloushallintoa kohtaan paljon enemmän tahattomia uhkia kuin tahallisia. Näitä tahattomia riskejä ovat erityisesti olleet internetyhteyteen liittyvät ongelmat, mutta muita toteutuneita riskejä ovat olleet esimerkiksi ongelmat ohjelmien, pilvipalveluiden ja järjestelmien kanssa. Harvinaisempia toteutuneita

riskejä ovat olleet sähkökatkokset, työpaikan ulkopuolisten tiedonsiirtokaapelien vaurioitumiset ja pankin tietojenkäsittelyn häiriöt.

Kaikilla vastaajilla on ollut monia erilaisia internetyhteyteen liittyviä ongelmia. Vastaajilla A ja B internetyhteys usein katkeilee, mikä täysin estää sinä aikana työn tekemisen pilvessä toimivilla järjestelmillä. Vastaaja B on kokenut internetin olevan ulkomailla työskennellessään usein paljon epävakaampi ja hitaampi. Internet on joskus katkennut B:llä pelkästään itse pilviverkon ja työpaikan välillä palveluntarjoajan puolen häiriöiden takia. Vastaaja D:llä internet ei ole välillä toiminut liittymäntoimittajan ongelmien vuoksi. Internetyhteyteen liittyvät ongelmat voivat olla sähköisessä ja digitaalisessa taloudessa hyvinkin merkittäviä. Ne voivat pahimmillaan pysäyttää kaiken työnteon pilvessä olevalla taloushallinnon järjestelmällä, mikä esimerkiksi vastaaja B:llä sisälsi maksatuksen, laskutuksen ja palkkatoiminnot. Internetyhteyden katkeamisen hän kertoi voivan olla kriittistä erityisesti maksatuksen tärkeyden takia. Vastaaja B:n tapaan vastaaja C:kin painotti maksujärjestelmän täsmällisen toiminnan tärkeyttä: *”Maksun viivästyminen yhdelläkin päivällä oli valtakunnan tason uutinen ja aiheutti yrityksen asiakkaiden puhelinpalveluun suunnattomat jonot, kun asiakkaat kyselivät miksi maksu ei ole vielä tullut tilille.”* Vastaajat A, C ja D eivät kuitenkaan muista yhteysvikojen olleen koskaan kriittisiä taloushallinnon pitkäaikaisen toiminnan kannalta, kunhan niihin on asianmukaisesti varauduttu.

Seuraavaksi eniten kohdattuja tahattomia uhkia ovat olleet järjestelmiin, ohjelmiin ja pilvipalveluihin liittyvät kaatumiset, kehitysviat ja ongelmat. Vastaaja C:n työpaikalla koko suuren yrityksen kattava järjestelmä on kaatunut järjestelmävikojen takia kokonaan välillä tunneiksi tai jopa kokonaisiksi päiviksi. Järjestelmän kaatumiset aiheuttivat esimerkiksi työajan menetyksiä ja toiminnan myöhästymistä aikataulusta. Järjestelmä ei välttämättä myöskään toiminut oikein uusien päivitysten myötä, ja niitä jouduttiin välillä korjaamaan. Yksi järjestelmävirheistä mahdollisti vahingossa vastaaja C:n työpaikalla satunnaisten tärkeiden tietojen leviämisen vääriin järjestelmän osiin, minkä korjaaminen vaati paljon aikaa ja aiheutti kuluja. Vastaaja D:n asiakkaiden käyttämässä ohjelmassa oli esiintynyt virhe, jossa ohjelma ei tallentanut kirjattuja luottotappioita ollenkaan. Virhe oli huomattu vasta vuoden päästä sen alkamisesta. Vastaaja B on myös kokenut ongelmia ohjelmien käytössä, kun esimerkiksi uusi päivitys on huonontanut ohjelman käyttökokemusta ja hidastanut nopeutta merkittävästi. Hän on myös kohdannut ongelmia pilvipalveluiden kohdalla, sillä välillä niihin ei ole saanut yhteyttä, vaikka internetyhteydessä ei ole ollut samaan aikaan mitään vikoja. Tietomurtoihin liittyen ainoastaan yksi vastanneista oli uransa aikana saanut tietoonsa, että jokin sidosryhmä olisi yrittänyt hyökkäyksellä pelkästään varastaa heiltä arvokasta tietoa. Vastaaja C:n työpaikan tietoihin oli yritetty murtautua ”…*parikin kertaa…*”, ja hyökkäyksen tekijä oli tuntematon taho. Hyökkäykset jäivät kuitenkin

vain yrityksiksi, eikä tietoverkkoihin päästy koskaan käsiksi. Kaikki tärkeimmät vastaajille toteutuneet riskit on vielä erikseen koottuna seuraavalla sivulla kuviossa neljä.

Kuvio 4 – Avoimeen kyselyyn vastanneiden kohtaamat digitaalisen taloushallinnon riskit

6.2 Vastaajien mielestä merkittävimmät ei-toteutuneet riskit

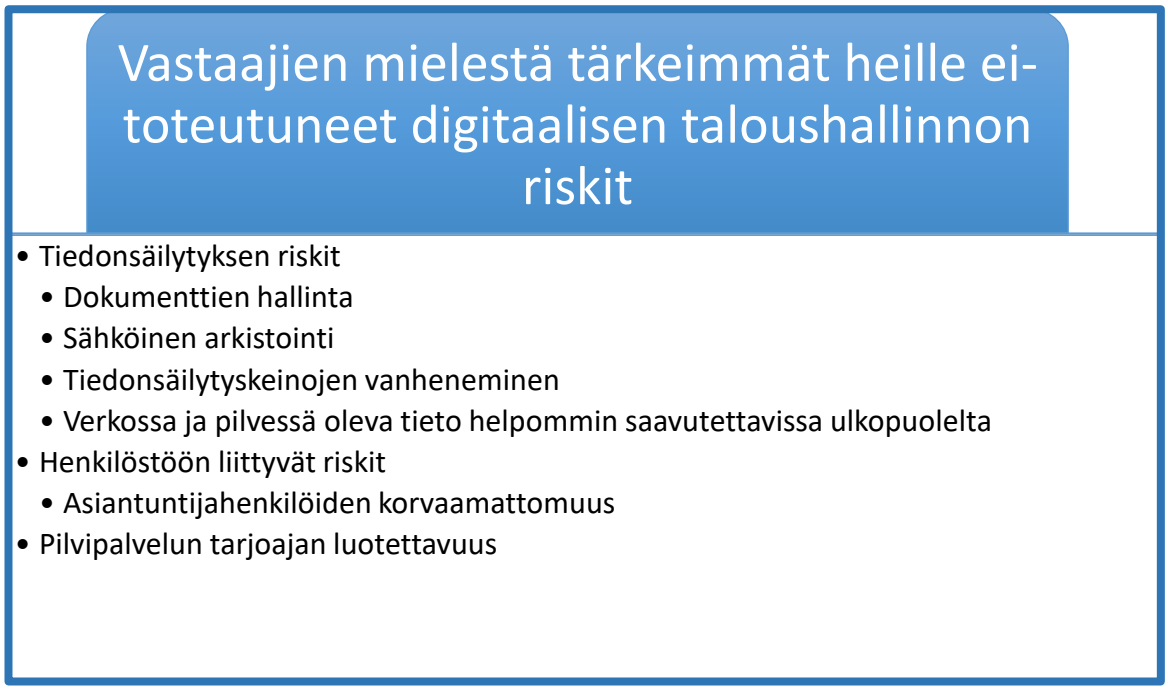
Vastaajat B, C ja D olivat vahvasti sitä mieltä, että erityisesti tiedonsäilytykseen liittyvät riskit sähköisessä ja digitaalisessa taloushallinnossa vaativat enemmän huomiota kuin ne yleisesti ottaen saavat. Vastaaja B:n mukaan dokumenttien hallinta ja sähköinen arkistointi mahdollistaa uusia riskejä, kun ne molemmat siirretään erilliseen pilvipalveluun omien serverien sijasta. Vastaaja D painottaisi tietojen säilyttämiseen liittyviä riskejä enemmän. Hän halusi muistuttaa, että sähköisessä ympäristössä tietoja on säilytettävä kirjanpitolain mukaan kahdella välineellä ja niiden toimivuus ja luettavuus on varmistettava tietyin aikavälein. Vastaaja D:n mukaan laitehankintojen yhteydessä voikin unohtua, että uudet laitteet eivät mahdollisesti luekaan vanhoja säilytysvälineitä. Myös vastaaja C on huolissaan tietovälineiden ja tietojen tallennusmuotojen muutoksista. Hänkin korostaa sitä, pystytäänkö tietoja hakemaan vanhoilta välineiltä, joille tieto on jopa kymmeniä vuosia sitten tallennettu. Hänen mielestään tiedonsäilytykseen liittyvät riskit voivat olla vaikeampia pienemmillä yrityksillä.

Vastaaja C esitti yhtenä riskinä vielä omaan henkilöstön määrään liittyvät tahattomat riskit. Tästä hän antoi esimerkkinä tilanteen, jossa järjestelmän teknistä ylläpitoa hallitsee vain yksi henkilö. Yksi henkilö ei ehdi virhetilanteissa ja ongelmatilanteissa korjaamaan järjestelmää riittävän nopeasti, mikä voi aiheuttaa pitempiaikaisempia katkoksia. Toisena esi-

merkkinä hän antoi erityisasiantuntijoiden tärkeyden olevan vielä merkittävämpi sähköisessä ja digitaalisessa taloushallinnossa, jolloin heidän lähteminen tai siirtyminen kilpailijoille voi olla suurempi riski.

Yleisesti ottaen sähköisen ja digitaalisen taloushallinnon riskialttiutta pidettiin vastaajien mielestä korkeampana kuin paperisen taloushallinnon. Kehittyneemmän taloushallinnon riskialttiita puolia esitettiin olevan erityisesti tiedon ja järjestelmien sijaitseminen internetissä ja pilvipalveluissa, jolloin ulkopuolisen on helpompi päästä siihen käsiksi paperiseen taloushallintoon verrattuna. Esimerkiksi vastaaja D:n mukaan tiedon sähköistyminen mahdollistaa siihen paikasta ja ajasta riippumattoman pääsyn, mutta taloushallinnon tiedot eivät kuitenkaan yleisesti ottaen ole erityisen houkuttelevia rikollisille. Vastaaja A oli kuitenkin sitä mieltä, että sähköisen ja digitaalisen taloushallinnon myötä riskit ovat vähentyneet, koska automatisointi ja muut järjestelmien ominaisuudet vähentävät merkittävässä määrin inhimillisiä virheitä. Esimerkiksi ohjelmien tarkastusominaisuudet ovat hänen mielestään lisääntyneet ja kehittyneet. Vastaaja D taas on eri mieltä, koska hänen mukaansa sähköisessä ja digitaalisessa taloushallinnossa lähes kaikki työntekijät tuottavat tietoa suoraan taloushallinnon järjestelmiin, mikä puolestaan lisää tahattomien virheiden määrää. Hänen mielestään aikaisempi tapa, jossa vähemmän kokeneet työntekijät tekivät muutoksia vain alajärjestelmiin ja kokeneet työntekijät tekivät kirjanpitoon asti menevät kirjaukset, oli vähemmän riskialtis. Kaikki vastaajat olivat kuitenkin siitä samaa mieltä, että taloushallinnon kehitys on nopeuttanut, automatisoinut ja tehostanut työntekoa niin merkittävästi, että lisääntynyt riskien määrä on sen arvoista.

Kysyin avoimessa kyselyssä myös erikseen vastaajien mielipiteitä pilvipalvelun ja sähköisesti tehtyjen etätöiden riskeistä. Vastaajien mielestä pilvipalvelun riskejä ovat muun muassa sen tarjoajan luotettavuus ja tiedon säilytyksen luotettavuus pilvessä. Vastaaja A on kuitenkin sitä mieltä, että pilvipalveluiden suojaukset ovat usein paremmat kuin omien palvelimien, ja varmuuskopiointi on varmempaa ja helpompaa pilvipalvelun avulla. Etätöiden teko sähköisissä ja digitaalisissa taloushallinnoissa on vastaajien mielestä melko turvallista, mutta riskejä löytyy ainakin tiedonsiirtoyhteyksistä ja omien huonommin suojattujen koneiden käytöstä. Vastaajat A ja C ovat vakuuttuneita siitä, että hyvällä riskienhallinnalla etätöiden teko ei ole merkittävästi riskeille alttiimpaa kuin itse työpaikalla työskentely. Seuraavalla sivulla on vielä koottuna erikseen kaikki vastaajien mielestä tärkeimmät heille ei-toteutuneet riskit kuviossa 5.



Kuvio 5 – Avoimeen kyselyyn vastanneiden mielestä tärkeimmät heille toteutumattomat digitaalisen taloushallinnon riskit

6.3 Sähköisen ja digitaalisen taloushallinnon riskienhallinta vastaajien näkökulmasta

Tietoperustan lähteiden mukaan johto yleensä päättää siitä, paljonko käytetään rahaa ja huomiota riskienhallintaa kohtaan, ja esimerkiksi ATK – alan ammattilaiset voivat tuntea tarkemmin virustorjuntojen, palomuurien, järjestelmien suojaussysteemien ynnä muiden tietoteknisten hallintakeinojen erot ja yksityiskohdat. Taloushallinnon työntekijän näkökulmasta riskienhallinta liittyy paljon esimerkiksi koulutukseen, ohjeiden noudattamiseen ja yleiseen riskienhallinnan tasoon. Käymme seuraavaksi läpi vastaajien työpaikkojen riskienhallinnan yleisen tason arviointia ja tärkeimpiä hallintatapoja, jonka jälkeen keskitymme taloushallinnon työntekijän näkökulmasta tarkempiin riskienhallinnan osiin sähköisessä ja digitaalisessa taloushallinnossa.

Koska sähköisessä ja digitaalisessa taloushallinnossa on vastaajien B, C ja D mielestä enemmän riskejä, vaatii se myös enemmän riskienhallintaa kuin paperinen taloushallinto. Vastaaja A:n mielestä tosin automatisointi ja robotiikka auttavat riskienhallintaa, mikä voisi jopa vähentää tarvittavaa riskienhallintaa paperiseen taloushallintoon verrattuna. Vastaaja C piti kehittyneen taloushallinnon riskienhallintaa vaikeampana pienemmissä yrityksissä, koska niillä ei ole välttämättä mahdollisuuksia tai resursseja panostaa yhtä paljon tietoturvallisuuteen.

Vastaajista C kirjoitti toteutuneiden riskien osuuden aikana eniten siitä, kuinka hyvin hänen työpaikallaan riskienhallinta pystyi torjumaan ja korjaamaan toteutuneita uhkia. Hän erityisesti kehui järjestelmien karanteeniominaisuuksia ja varmuuskopioita, joiden ansiosta maksut eivät kertaakaan jääneet lähtemättä yrityksen tai ohjelmistotoimittajasta aiheutuneen vian vuoksi. Karanteenissa tietyt järjestelmän vähemmän tärkeät osat lukitaan pois katkaisemalla niiden yhteydet muihin järjestelmiin ja niiden osiin, jotta niihin päässeet virukset eivät pääse leviämään pidemmälle. Hänen työpaikallaan myös esimerkiksi järjestelmäviat korjattiin nopeasti kokeneen asiantuntijan ansiosta ja tietomurtoyritykset eivät päässeet tietokantoihin sisälle monitasoisen turvallisuussysteemin takia. Tietoturvallisuus oli vastaaja C:n työpaikalla yksi tärkeimmistä kriteereistä järjestelmien rakentamisessa ja valmisohjelmien valinnassa. Tärkeitä riskienhallintakeinoja vastaaja C kirjoitti olevan esimerkiksi salassapitovelvollisuuden vaatimisen järjestelmän toimittajilta ja muilta siihen liittyviltä henkilöiltä sekä keinohenkilötunnusten käytön. Keinohenkilötunnukset ovat henkilötunnuksia, jotka eivät mene virallisen henkilötunnusmallin mukaan. Tästä syystä niitä voidaan käyttää turvallisesti sähköpostin ja turvattomien tiedonsiirtolinjojen kanssa.

Vastaajien A, B ja D työpaikoilla on myös annettu paljon huomiota ja käytetty resursseja sähköiseen ja digitaaliseen taloushallintoon liittyvään riskienhallintaan. Vastaaja A kirjoitti, että riskien huomiotta jättäminen tulisi paljon kalliimmaksi, kuin niiden huolellinen hallinta. Vastaaja B:n mukaan koulutus, virustorjunnat, tarkat ohjeet ja yleinen tietoturva ovat tärkeimpiä riskienhallinnan keinoja kehittyneessä taloushallinnossa. Vastaaja D:n mielestä turvallisuuden varmistaminen väistämättä vie aikaa ja vähentää työn joustavuutta, ja hänestä se tuntui välillä liiankin tarkalta. Hänen työpaikallaan oli oma internetturvallisuusosasto. Myös vastaaja B mainitsi riskienhallinnan vievän paljon aikaa, jonka takia hyvin kiireisillä työpaikoilla se saattaa jäädä vähemmälle huomiolle. Hänen mukaansa sähköisen ja digitaalisen taloushallinnon riskienhallinta ei välttämättä olekaan oikeastaan rahallinen kysymys, vaan sen hoitaminen riippuu paljon enemmän käytettävissä olevasta ajasta.

6.4 Vastaajien näkemykset koulutuksesta liittyen sähköisen ja digitaalisen taloushallinnon riskienhallintaan

Vastaajien B, C ja D mielestä koulutus on erittäin tärkeä osa kehittyneen taloushallinnon riskienhallintaa. Vastaaja A kuitenkin kirjoitti, että jokaisella tulisi jo henkilökohtaisen tietoturvan kannalta olla selvillä monia perusasioita riskeihin liittyen ennen koulutusta. Myös vastaaja D piti koulutuksessa tärkeänä koulutettavaa henkilöä ja hänen vastaanottokykyään. A:n mainitseman tietoteknisten taitojen lisäksi vastaaja D luetteli koulutettavan tärkeitä ominaisuuksia olevan ikä, motivaatio ja aiempi työkokemus.

Työpaikkojen koulutuksessa sähköiseen ja digitaaliseen taloushallinnon riskienhallintaan liittyen voi olla työpaikkakohtaisesti heikkouksia ja vahvuuksia. Vastaaja B:n mukaan tietoturva-aiheet ja järjestelmien käyttöturvallisuus ovat jääneet hänen saamassaan koulutuksessa liian vähälle huomiolle. Hän on myös huomannut työpaikoillaan, että erityisesti tiedonsäilytyksen riskeistä digitaalisessa taloushallinnossa ei hänelle ole koulutettu tai edes mainittu oikeastaan mitään. Vastaaja C:n työpaikalla koulutus oli erityisen laajamittaista ja onnistunutta tietoturvallisuuden, riskien ja laitteiden osalta. Heidän koulutuksessaan painotettiin muun muassa järjestelmien, puhelimien, salasanojen, laitteiden ja suojattujen yhteyksien riskienhallintaan liittyviä käytäntöjä. Samalla työpaikalla oli myös tarkkaa kouluttaa mitä tietoa sai jakaa ulkoisten sidosryhmien kanssa ja miten esimerkiksi saapuneiden vieraiden kanssa työpaikalla toimittiin. Hänen työpaikallaan kaikkien kokouksiin osallistuneiden vieraiden piti allekirjoittaa salassapitosopimus. Koulutusta auttoivat työpaikan sisäisillä nettisivuilla olevat ohjeet ja ajankohtaiset muistutukset. Vastaaja C:n mukaan kaikkien työtehtävien aikataulut olivat kuitenkin niin kierät, että uusista järjestelmistä ja muuttuneista ratkaisuista ei ehditty kouluttaa tarpeeksi jatkuvien muutoksien keskellä. Uusien työntekijöiden tullessa töihin heillä oli niin paljon opittavaa kerralla, että esimerkiksi kaikkien tietoturva-asioiden muistamisessa oli alussa paljon vaikeuksia.

Vastaaja D:n mukaan järjestelmän koulutuksen voi mahdollisesti tehdä myös järjestelmätoimittaja itse. Tällöin koulutuksen laatuun vaikuttaa tarjoajien välinen kilpailutilanne. Järjestelmätoimittajat voivat myös antaa jatkuvaa neuvontapalvelua sopimuksen mukaan. Vastaaja D kuitenkin myös muistuttaa, että järjestelmän vaihdon ollen jo meneillään ei sitä voi pelkästään koulutuksen laadun takia vaihtaa, mutta tämän voi korjata ostamalla lisäkoulutusta lisäkuluilla. Hänen omalla työpaikallaan koulutus tapahtui oman henkilökunnan voimin. Siitä vastasi tarkemmin ottaen tietotekniikkaosasto, joka sisälsi helpdeskin. Helpdesk oli vastaaja D:llä talon sisäinen tietoteknisissä ongelmissa auttava palveluryhmä. Kuten muutkin vastaajat mainitsivat, myös vastaaja D:n mukaan koulutuksen suurimpiin ongelmiin kuului ajanpuute ja koulutuksen vastaanottajan kärsimättömyys. Välillä koulutus oli myös kokonaan työn jälkeen omalla ajalla tehtävää opettelua, mikä teki siitä edelleen vaikeampaa.

6.5 Vastaajien näkemykset työpaikalla annettuihin sääntöihin ja ohjeisiin liittyen sähköisen ja digitaalisen taloushallinnon riskienhallintaan

Tietoperustan lähteiden mukaan johdon ja tietotekniikan asiantuntijoiden tekemät riskienhallinnan strategiat toteutuvat käytännössä hankintojen lisäksi annettujen sääntöjen ja ohjeiden noudattamisella. Taloushallinnossa työskentelevien henkilöiden on siis tärkeää

osata ja noudattaa heille annettuja sääntöjä ja ohjeita, jotta riskienhallinnan strategia toteutuisi. Annettavien ohjeiden määrä on esimerkiksi uusien tietoturvariskien johdosta kasvanut ajan myötä.

Vastaaja C:n työpaikalla ei sähköistymisen alkuvaiheilla annettu paljoakaan ohjeita järjestelmien ja internetin turvalliseen käyttöön liittyen, vaan järjestelmän turvallisuuden nähtiin olevan aluksi enimmäkseen sen tarjoajan ja tietohallinnon vastuulla. Sähköistymisen ja digitaalisen taloushallinnon kehityttyä on sääntöjä ja ohjeita annettu jatkuvasti enemmän esimerkiksi järjestelmien, salasanojen tai suojattujen yhteyksien käytöstä. Internetin käytölle määriteltiin hyvin tarkat säännöt työntekijöille, sähköpostin käytölle tehtiin tarkat ohjeet ja varmuuskopiointikäytännöt vakiintuivat. Vastaaja C:n työpaikalla ohjeita oli annettu uusista järjestelmistä lähivuosina niin paljon, ettei niihin kaikkiin ollut työntekijöillä aikaa kunnolla perehtyä.

Vastaaja A:n mukaan mitä paremmin ohjeet ja säännöt on laadittu ja päivitetty, sitä tarkemmin työntekijät yleensä seuraavat niitä. Hän korostaisi sääntöihin liittyen ohjelmissa ja järjestelmissä olevia käyttörajoituksia, jotka pakottavat tiettyjen sääntöjen noudattamisen. Käyttörajoituksia voivat olla esimerkiksi vain tietynlaisen tiedon hyväksyminen tiettyihin kohtiin ja pääsyrajoitukset tiettyihin ohjelman ominaisuuksiin. Vastaaja B on huomannut työpaikoillaan, että annettuja ohjeita ja sääntöjä on seurattu yleisesti ottaen hyvin. Hänen mukaansa ongelmia sääntöihin on liittynyt enemmänkin niiden tekemisvaiheen puutteellisuudet pienemmissä yrityksissä ja ajan riittämättömyys kiireisinä aikoina. Pienemmillä yrityksillä ei vastaaja B:n kokemuksesta ole aina sähköisen ja digitaalisen taloushallinnon riskienhallintaa tuntevaa tai kokemusta omaavaa henkilöä. Tällöin myös ohjeiden ja sääntöjen määrä ja laatu voi olla paljon heikompaa. Pienissä yrityksissä monet asiat saatetaan pitää myös itsestään selvyyksinä, joten niistä ei ohjeisteta tai niille ei aseteta ollenkaan virallisia sääntöjä. Vastaaja B kirjoitti esimerkin, jossa yksi työntekijöistä oli tehnyt puoli vuotta töitä koneella, jolle hän ei ollut koko aikana asentanut minkäänlaista virustorjuntaa. Hän kirjoitti edelleen, että vaikka ohjeiden ja sääntöjen tarve kehittyneen taloushallinnon turvallisuuteen liittyen riippuu paljon vastaanottavasta henkilöstä ja hänen kokemuksestaan, pitäisi kaikissa yrityksissä olla esimerkiksi tietoturvaohjeita ja – sääntöjä työntekijöiden iästä, kokemuksesta ja osaamisesta huolimatta.

Jos vastaaja D:n työpaikalla ei noudattanut ohjeita tai sääntöjä, sai siitä heti huomautuksen. Hänen työpaikallaan oli tarkkaan ohjeistettu kenelle sai lähettää mitä tietoa ja mitä kautta. Asiakkaiden kanssa tehtyihin kirjallisiin sopimuksiin lisättiin oma kohta tietoturvallisuuteen liittyviin sääntöihin. Asiakkaat eivät kuitenkaan aina noudattaneet näitä sääntöjä, mutta nämä tapaukset aina osoittautuivat tahattomiksi. Sivulla 41 on vielä koottuna kuvi-

ossa 6 yhdistettynä vastaajien työkokemukseen perustuvat sähköisen ja digitaalisen riskienhallinnan tavat ja oleelliset näkökannat riskienhallintaan liittyen.

Kuvio 6 – Avoimeen kyselyyn vastanneiden oleellisimmat kokemukset ja mielipiteet koottuna

7 Pohdinta

Opinnäytetyön aiheesta, eli sähköisen ja digitaalisen taloushallinnon tuomista riskeistä ja riskienhallinnasta, en löytänyt yhtäkään suoraan tässä kohderajauksessa olevaa kirjallisuuden teosta, teoksen osaa tai tutkimusta. Oletan siis, että tarkemmin ottaen taloushallinnon työntekijän näkökulmasta ei asiaa ole todennäköisesti kovinkaan paljon vielä tutkittu, tai näitä tutkimuksia ei ole julkaistu kaikille luettaviksi. Tutkimuksesta saatuja tuloksia voi kuitenkin verrata suurempiin kokonaisuuksiin, kuten tietotekniseen tietoturvaan ja digitaalisesta taloushallinnosta saataviin tietoihin. Vertailen tuloksia samassa järjestyksessä kuin ne on tässä työssä esitetty.

7.1 Tulosten pohdinnat riskeistä

Tuloksista ensimmäinen mielenkiintoinen seikka oli kuinka vähän erilaisia toteutuneita ulkoisia riskejä vastaajat olivat kohdanneet sähköisessä ja digitaalisessa taloushallinnossa. Tietoperustassa olevia matoja, sosiaalisia huijauksia, viruksia, Troijan hevosia ynnä muita tietoteknisiä uhkia oli kohdattu melko vähän, ja ainoastaan haitallisia sähköposteja oli vastaanotettu paljon. Kaikista vastaajien työpaikoista pelkästään vastaaja C:n työpaikalla oli kohdattu muutamaan otteeseen merkittäviä viruksia, jotka olivatkin päässeet leviämään laajemmin järjestelmiin. Tahallisten riskien sijasta tahattomia riskejä oli kohdattu useammin, ja niillä oli ollut merkittävämpiä vaikutuksia vastaajien taloushallintoa kohtaan. Erityisesti internetyhteyteen, järjestelmiin ja pilvipalveluun liittyviä ongelmia oli eniten, ja niiden vaikutukset olivat paljon merkittävämpiä kuin tahallisten riskien. Tahattomat riskit johtivat pitkiin ylitöihin, korjaustoimenpiteisiin, varakopioiden käyttöön ja hyvin tärkeät maksatukset eivät melkein ehtineet lähteä ajoissa. Tietoperustassa ja siinä käytetyissä lähteissä tahalliseen rikolliseen toimintaan liittyviä riskejä painotettiin paljon enemmän, mutta näyttäisi siltä että vastaajilla tahattomat riskit olivat toteutuneet vaarallisempina. Täytyy kuitenkin muistaa, että tässä tutkimuksessa ei kysytty tahallisia työpaikan sisältä tulleita riskejä. Näitä riskejä pidettiin tietoperustan lähteissä vähintäänkin yhtä tärkeinä kuin muita riskejä.

Tietoteknisen tietoturvallisuuden kannalta tiedon varastamista ja urkintaa oli painotettu todennäköisenä ja yleistyvänä riskinä tietoperustan lähteissä. Vastaajat eivät olleet kohdanneet paljoakaan tietojen vakoiluun tai varastamiseen liittyviä toteutuneita uhkia. Ainoastaan vastaaja C:n työpaikalla oli vakoiluohjelma yrittänyt muutamia kertoja murtautua tietojärjestelmään, mutta yksikään murtautumisista ei onnistunut. Vaikka vastaaja C:n työpaikalta oli myös varastettu kannettavia tietokoneita kokoushuoneista, ei varkauksien

motiivia nähty olevan niiden sisältämä tieto vaan tietokoneen myyntiarvo. Kukaan vastaajista ei siis ole kokenut työpaikoillaan ulkoisesta lähteestä tulevaa tiedon varastamis- tai urkintayritystä, joka olisi onnistunut. Vastaaja D mainitsikin, että taloushallinnon tiedot eivät välttämättä ole niin houkuttelevia rikollisille.

Vastaajien mielestä heille merkittävimmät toteutumattomat riskit sähköisessä ja digitaalisessa taloushallinnossa olivat tiedonsäilytykseen liittyvät riskit. Monet vastaajista olivat huolissaan tiedon tallennusmuotojen vanhentumisesta, jolloin niiden lukeminen on hankalaa uusilla tietokoneilla ja ohjelmilla. Tietoperustan digitaalisen taloushallinnon arkistointikohdassa lukeekin, että sähköiseen muotoon tallennettu tieto pitää olla luettavissa jollain ohjelmalla tai järjestelmällä sen laissa määrätyn säilytysajan. Jos vastaajien työpaikoilla tämä tieto on unohtunut, olen heidän kanssa samaa mieltä sen huomiontarpeesta, jotta tallennetut taloushallinnon tiedot pysyvät lukukelpoisina tarvittavan ajan. Taloushallinnon tietojen säilytyksestä järjestelmissä ja pilvipalveluissa oltiin myös huolissaan, mikä puolestaan liittyy enemmän tietoturvaan, yhteyksien vakauteen ja palveluntarjoajien luotettavuuteen. Tietoperustan lähteissä sanottiin tähän liittyen ainakin se, että taloushallintoon liittyvä tieto pitää olla tallennettuna vähintään kahdessa eri kohteessa. Jos vastaajilla A ja B taloushallinnon tiedot olivat tallennettuna pelkästään yhdessä sijainnissa, kaipaa tämäkin asia kenties enemmän huomiota. Vastaaja C oli kuitenkin erittäin tyytyväinen hänen työpaikkansa varakopioinnin onnistumiseen.

Yleisesti ottaen vaikka vastaajat B, C ja D pitivät sähköistä ja digitaalista taloushallintoa paljon riskialttiimpana verrattuna paperiseen taloushallintoon, ei heidän työpaikoillaan vastauksien mukaan toiminta ole ollut kovinkaan uhattuna toteutuneiden riskien johdosta. Eniten huolenaihetta on herättänyt maksatuksen maksujen ajoissa eteneminen vastaaja B:llä ja C:llä, mutta tätä oli esimerkiksi vastaaja C:n mukaan ulkoiset tahattomat riskit haitannut enemmän. Se, että toteutuneet riskit eivät ole onnistuneet uhkaamaan vastaajien työpaikkojen toimintaa, ei kuitenkaan tarkoita, etteivät nämä riskit voisi olla myös hyvin vaarallisia toiminnan kannalta. Tästä pääsemmekin pohdinnan seuraavaan osaan, eli riskienhallintaan.

7.2 Tulosten pohdinnat riskienhallinnasta

Riskienhallinnasta ilmeni myös monia mielenkiintoisia asioita. Ensinäkin vastaajien B, C ja D mielestä pienemmillä yrityksillä riskienhallinta sähköiseen ja digitaaliseen taloushallintoon liittyen on vaikeampaa. Syiksi tähän annettiin esimerkiksi resurssien vähempi määrä ja tästä johtava pienempi valikoima erilaisia vaihtoehtoja. Vastaaja B, joka on vastaajista eniten työskennellyt pienemmissä yrityksissä, kuitenkin kirjoitti, että suurin ongelma ris-

kienhallinnan kanssa hänen työpaikoillaan oli kokeneiden ja osaavien ammattilaisten puute tämän aihealueen osalta. Jos pienessä työpaikassa ei ollut tietoturvasta tai järjestelmien turvallisuudesta aiempaa kokemusta omaavaa työntekijää, kärsi riskienhallinta tämän osalta tämän takia eniten. Vastaaja C:nkin työpaikalla, mikä on verrattuna vastaaja B:n työpaikkoja paljon isompi, tietoturvasta ja joistain kehittyneen taloushallinnon riskienhallinnan osista saattoi olla vastuussa pelkästään yksi kokenut henkilö. Jos tämä työntekijä päätti lähteä tai meni eläkkeelle, saattoi olla hyvinkin vaikeaa löytää samanlaista kokemusta omaava uusi henkilö tilalle. Tähän liittyen vastauksista ilmeni toinen mielenkiintoinen seikka: sähköiseen ja digitaaliseen taloushallintoon liittyvää riskienhallintaa ei vastaajien työpaikoilla koettu rahallisena ongelmana. Vaikka tietoperustan lähdemateriaalissa korostettiin muiden asioiden ohella riskienhallinnan mahdollisesti erittäinkin kovia kustannuksia, eivät vastaajat olleen kokeneet asiaa välttämättä ihan samalla tavalla. Kustannuksien sijasta kaikki vastaajat pitivät riskienhallintaa paljon enemmän ajallisena ongelmana. Jopa pienemmissä yrityksissä työskennellyt vastaaja B korosti erityisesti kehittyneen taloushallinnon riskienhallintaan liittyvää ajan tarvetta. Pahimmillaan tämä oli johtanut vastaajien työpaikoilla ylitöihin, kotona tehtävään itseopiskeluun tai jopa riskienhallinnan laiminlyöntiin suunnitteluvaiheesta lähtien.

Kaikkien vastaajien työpaikoilla sähköisen ja digitaalisen taloushallinnon riskienhallintaa pidettiin hyvin tärkeänä. Vastaaja C:n mukaan uutta järjestelmää valitessa tärkein valintakriteeri oli turvallisuus, ja vastaaja D:n työpaikalla riskienhallintaa pidettiin hänen mielestään jopa melkein liiankin kireänä. Näin ei kuitenkaan aina ollut vastaaja C:n työpaikalla, vaan tietoteknisen tietoturvan oleellisuuteen oli herätty vasta sähköistymisen jo ollessa pitkällä. Tästä voisi mahdollisesti spekuloida, että myös digitaalisen taloushallinnon tuomista uusista riskeistä voi olla hyvä olla ajan tasalla riskienhallinnan kannalta mahdollisimman nopeasti. Yksikään vastaajista tai heidän työpaikoistaan ei ollut pitänyt riskienhallinnan tärkeyttä liioiteltuna. Esimerkiksi vastaaja A:n mukaan hyvin hoidettu kehittyneen taloushallinnon riskienhallinta tulee paljon halvemmaksi kuin huonosti hoidettu.

Vastaaja C mainitsi useita sähköisen ja digitaalisen taloushallinnon riskienhallinnan keinoja, joita tietoperustan lähdeaineistossa ei ollenkaan mainittu. Laajamittainen varmuuskopiointi, järjestelmien osien karanteeniin pistäminen, salassapitosopimukset ja keinohenkilötunnukset olivat kaikki lähdeaineistosta puuttuvia riskienhallinnan tarkennettuja keinoja. Vastauksista kuitenkin myös huomasi, että tietoteknisestä tietoturvasta vastaajien työpaikoilla vastasi melkein aina jokin aiheeseen perehtynyt ammattilainen, internetturvallisuusosasto tai muu taloushallinnosta erillinen työpaikan osasto. Ainoastaan vastaaja B:n pienemmissä työpaikoissa kehittyneen taloushallinnon riskienhallinta jäi käytännössä kaikkien työntekijöiden yhteiseksi tehtäväksi, eikä kenenkään asiantuntijatiimin hoidettavaksi.

Kuten lähdeaineistossa kerrottiin, myös vastaajien työpaikoilla taloushallinnon työntekijät eivät olleet kovin tietoisia erilaisista palomuureista, järjestelmistä tai muista tarkemmista sähköisen ja digitaalisen taloushallinnon teknologisista riskienhallintakeinoista, vaan heidän tehtäväksi jäi koulutuksesta oppiminen ja sääntöjen sekä ohjeiden noudattaminen.

Yleisen riskienhallinnan tavoin myös koulutuksessa ja ohjeiden noudattamisessa sähköiseen ja digitaaliseen taloushallintoon liittyen vastaajat erityisesti korostivat ajanhallinnan tärkeyttä. Aika resurssina oli kaikkien vastaajien työpaikoilla hyvin rajallinen jo pelkästään jokapäiväisten tehtävien suorittamisessa, mutta järjestelmien vaihtuessa, riskienhallinnan muuttuessa, koulutuksen ollessa käynnissä ja sääntöjen muuttuessa aikaa oli vielä normaaliakin vähemmän. Kaikki vastaajat vaikuttivatkin olevan sitä mieltä, että mitä enemmän työntekijöillä oli aikaa käytettävänä riskienhallinnan ohjeiden lukemiseen, koulutuksiin osallistumiseen ja muuhun oppimiseen, sitä paremmin nämä myös heidän osaltaan onnistuivat. Missään lähdeaineistoista aikaa ei pidetty riskienhallintaan liittyvänä mainitsemisenarvoisena resurssina, joten ehkä asiaan olisi hyvä keskittyä jatkossa myös ajankäytön näkökulmasta. Ajankäytön lisäksi vastauksissa korostettiin koulutuksen, ohjeiden ja sääntöjen vastaanottajan merkitystä. Vaikka monet asiat tietoturvaan liittyen voidaan olettaa olevan itsestään selvyyksiä, on opettaessa työntekijöitä vastaajien mielestä tärkeää tietää koulutettavan nykyinen taso ja tietämys, tai kokonaan olla olettamatta mitään ja tehdä ohjeita ja sääntöjä mahdollisimman monista tärkeistä asioista.

Vastaaja A:n vastaukset olivat omalla tapaa kaikista kiinnostavimpia, koska ne erosivat vahvasti muiden vastanneiden näkemyksistä ja mielipiteistä. Hänen mielestä automatisointi, jota digitaalisessa taloushallinnossa erityisesti korostetaan, vähentää merkittävästi inhimillisten virheiden, ja näin ollen riskien, määrää. Automaation lisäksi kehittyneet järjestelmät havaitsevat paremmin virheitä ja poikkeavaisuuksia, ja järjestelmillä voi pakottaa työntekijöitä noudattamaan tiettyjä sääntöjä esimerkiksi syöttökenttien vaatimuksilla. Näitä samantyyppisiä digitaalisen taloushallinnon kontrolleja lueteltiin tietoperustan lähdeaineistossa. Vastaaja A kirjoitti myös, että kehittyneen taloushallinnon riskienhallinnassa yksilön omat aiemmat kokemukset ja tietämys esimerkiksi tietoteknisen tietoturvan käytännöistä ovat erittäin tärkeitä. Tämän perusteella voisi muodostaa näkemyksen, jonka mukaan työntekijän itse kannattaa pitää itsensä aktiivisesti mahdollisimman tietoisena jatkuvasti kehittyvän taloushallinnon muutoksista, mukaan lukien uusista riskeistä ja niiden hallinnasta. Kukaan vastanneista ei kuitenkaan ollut havainnut työpaikoillaan, että ohjeiden noudattamisessa tai koulutuksen asioiden muistamisessa olisi koskaan esiintynyt tahallista laiminlyöntiä. Tietotekniseen tietoturvaan liittyvän tiedon määrä lisääntyykin teknologian kehityksen myötä koko ajan, joten työpaikoilla olisi todennäköisesti hyvä muistuttaa työn-

tekijöitä hyvistä käytänteistä vastaaja C:n työpaikan tavoin esimerkiksi intranetin ja sähköpostiviestien avulla.

7.3 Opinnäytetyön tutkimuksen tarkastelu

Opinnäytetyössä käytetty tutkimus oli kvalitatiivinen, eli laadullinen, tutkimus. Kvalitatiivisesta tutkimuksesta saatava tieto ei ole matemaattisesti vertailtavaa tai tarkkaa kvantitatiivisen tutkimuksen tuloksiin verrattuna. Työn tarkoituksena oli kuitenkin saada lisää tietoa aiheesta, josta en löytänyt monia erilaisia aikaisempia lähteitä. Tutkimukseni löytöjen perusteella voisikin esimerkiksi mahdollisesti rajata tarkemmin aiheesta tehtäviä seuraavia tutkimuksia. Taloushallinnon sähköistymisen ja digitalisoitumisen riskit ovatkin jatkuvasti lisääntymässä tietoperustan lähteiden mukaan.

Tuloksista löytyi mielestäni erilaisia näkökulmia kehittyneen taloushallinnon riskeihin ja riskienhallintaan, joista voi olla hyötyä sekä taloushallinnon työntekijöille, mutta myös esimerkiksi esimiehille ja pienyritysten johtajille, jotka ovat kiinnostuneita aiheesta taloushallinnon työntekijöiden näkökulmasta. Vastaajien määrä oli kuitenkin melko pieni, vain kaiken kaikkiaan neljä vastaajaa, joten vastauksia ei voi yleistää millään varmuudella suurempia oletuksia ilman lisätutkimuksia. Tulokset eivät suuruudeltaan myöskään olleet kovin pitkiä, joten jatkossa aiheen tutkimuksissa voisi olla hyvä hakea kyselyyn enemmän vastaajia. Mielestäni kuitenkin jos ottaa huomioon, että aiheeseen liittyen ei aikaisemmin ole tietääkseni tehty paljon ainakaan opinnäytetyötutkimuksia tai kirjoitettu kirjallisuutta, voi tuloksissa oleva tieto olla mahdollisesti myös arvokasta.

Tutkimuksen tulokset ovat mielestäni uskottavia, koska kaikilla vastaajilla on aiheeseen liittyvää kokemusta useampia vuosia, eikä kenelläkään vastaajista ole tavoiteltavaa omaa etua tuloksiin liittyen. Aina on kuitenkin mahdollista, että vastaaja jostain syystä esimerkiksi vähättelee, liioittelee tai muuten vääristää antamaansa tietoa vahingossa tai tahallaan.

Tuloksien luotettavuudessa täytyy muistaa, että kaikki vastaajat olivat minulle jossakin määrin tuttuja henkilöitä, ja avoimessa kyselylomakkeessa käytetyt kysymykset oli johdettu tietoperustan kirjallisuuden lähteistä minun omat mielenkiintoni eri aiheisiin vaikuttaen. Annoin vastaajien kuitenkin myös kirjoittaa anonyymisti mahdollisimman vapaasti mitä vain aiheeseen liittyvää haluamaansa tietoa, jota yritin painottaa myös avoimen kyselylomakkeen vastaamisohjeissa. Jouduin tekemään haastattelukysymykset tilanteen vaadittua haluamaani nopeammin, joten kysymysten pohtiminen ja niistä konsultointi aiheesta kokeneemmilta henkilöiltä kärsi tämän osalta.

7.4 Oma oppimiseni ja kehittymiseni opinnäytetyön aikana

Opin tämän opinnäytetyön aikana tekemään itsenäisesti tutkimuksen, jota tukemaan hain ja kirjoitin aiheeseen liittyvää tietoa. Työn suunnitteluvaihe meni osittain hyvin ja ajallaan, mutta lukuisat opinnäytetyön asiat muuttuivat suunnitelmasta tekovaiheessa. Koko työn kokonaisuuden hahmottelu olisi kannattanut tehdä jo alusta pitäen tarkemmin, jotta se ei vahingossa pääse rönsyilemään. Opin tässä mielestäni sen, että suunnitteluvaiheessa aiempi kokemus samantyyppisestä suunnittelusta voi olla hyvinkin tärkeää. Suunnitelmasta muuttuivat esimerkiksi opinnäytetyön tarkempi aihe, aikataulutus ja yksityiskohdat tutkimuksen toteutuksessa. Aikataulu voi olla hyvä rakentaa mahdollisimman realistisesti, mutta kaikkia niihin vaikuttavia tekijöitä ei voi koskaan täysin ennakoida. Itse työn tekeminen, eli lukeminen, tutkiminen ja kirjoittaminen, opin olevan hyvin tarkkaa ja mielenkiintoista. Tutkimuksen tekemiseen liittyvää tietoa on kuitenkin niin paljon, että jotkin kokonaisuuden kannalta hieman vähemmän tärkeät asiat voivat helpommin päästä unohtumaan. Opinnäytetyön tekemisessä taustatyön tekemistä ja taustatiedon etsimistä ei saa mielestäni missään nimessä vähätellä, vaan niihin pitää kiinnittää paljon huomiota. Olisin itse voinut tehdä nämä kaksi vaihetta varmasti paremminkin.

Kuten aiemmin pohdinnassa kirjoitinkin, tein tutkimuksen kysymykset haluamaani nopeammin vastaajien toivomien aikataulujen puitteissa. Tutkimuksessa käytetyt avoimen kyselylomakkeen kysymykset olisi kannattanut tarkemmin pohtia ja vertailla ennen niiden lähettämistä vastaajille. Tekemäni kysymykset olivatkin mielestäni kenties tämän työn heikoin puoli. Vastauksien yhdistäminen toisiinsa oli vaikeampaa kysymysten asettelujen vuoksi, joten jatkossa kysymysten suunnittelussa kannattaa ainakin ottaa huomioon miten vastaajat saadaan kertomaan mahdollisimman toisiinsa vertailtavaa tietoa. Työssä onnistui mielestäni parhaiten tietoperusta, koska löysin mahdollisimman lähelle aiheeseen liittyvää tietoa kuin käyttämistäni valikoimista löytyi. Käytin myös englanniksi kirjoitettua lähdemateriaalia, jonka käänsin tietoperustaan suomenkielelle. Tietoperustan yleinen taloushallinto -osio olisi voinut olla paljon laajempi, mutta aiheen laajuuden takia minun oli pakko myös rajata paljon tietoa pois. Halusin tietoperustassa keskittyä enemmän tarkempiin aiheisiin, eli digitaaliseen taloushallintoon, sen riskeihin ja näiden riksien hallintaan.

Olin itse erittäin kiinnostunut opinnäytetyön aiheesta, mistä syystä myös valitsin sen. Opin erittäin paljon aiheeseen liittyvistä tarkemmista ala-aiheista, ja opin myös isohkon tutkimusprosessin tekemisestä alusta loppuun. Olen tyytyväinen tekemääni työhön, vaikka parannettavan varaa myös löytyy. Työstä saatava tieto on minulle varmasti myös työelä-

mässä hyödynnettävää. Toivon että tieto auttaa myös kaikkia muita aiheesta kiinnostuneita heidän työelämässään, opinnäytetyötä tehdessään tai mahdollisesti jotenkin muutenkin.

Lähteet

Kirjalliset lähteet

Helanto, L., Kaisaniemi, T., Koskinen, K., Kuntola, K. & Siivola, M. 2013. Taloushallinto. Nyt. Tilitoimistoammattilaisen opas sähköiseen taloushallintoon. ProContor International Oy. Espoo.

Lassila, A. 2017. Virusuhan pelätään kasvavan. Helsingin Sanomat, 130, s. A23 – A24.

Ikäheimo, S., Malmi, T. & Walden, R. 2012. Yrityksen laskentatoimi. Viides uudistettu painos. Sanoma Pro Oy. Helsinki.

Jormakka, R, Koivusalo K, Lappalainen J. & Niskanen M. 2015. Laskentatoimi. Edita Publishing Oy. Helsinki.

Kinnunen, J., Laitinen, E., Laitinen, T., Leppiniemi, J. & Puttonen, V. 2006. Mitä on yrityksen taloushallinto? Kolmas painos. Otavan Kirjanpaino Oy. Keuruu.

Lahti, S. & Salminen, T. 2014. Digitaalinen taloushallinto. Sanoma Pro Oy. Helsinki.

Lahti, S. & Salminen, T. 2008. Kohti digitaalista taloushallintoa – sähköiset talouden prosessit käytännössä. WSOYpro. Helsinki.

Mäkinen, L. & Vuorio, B. 2002. Taloushallinnon nettivallankumous. Gummerus Kirjapaino Oy. Jyväskylä.

Pitkäranta A. 2014. Laadullinen tutkimus opinnäytetyönä – työkirja ammattikorkeakouluun. e-Oppi Oy. Suomi.

Tomperi, S. 2013. Kehittyvä kirjanpitotaito. 14. uudistettu painos. Bookwell Oy. Porvoo.

Turban E, King D, Lee J, Liang T-P. & Turban D. 2012. Electronic Commerce 2012 – A Managerial and social networks perspective 7th edition. Pearson Education Limited. United States.

Wood, F. & Robinson, S. 2009. Book-keeping and accounts 7th edition. Pearson Education Limited. Harlow.

Verkkolähteet

Elisa 2017. Ville Konkare. Luettavissa: https://yksityisille.hub.elisa.fi/mika-on-pilvipalvelu/. Luettu: 27.3.2017.

Yrittäjät 2014. Suomen Yrittäjät. Sähköinen taloushallinto. Luettavissa: https://www.yrittajat.fi/yrittajan-abc/taloushallinto-ja-maksut/taloushallinto/sahkoinen-taloushallinto-317818#. Luettu: 29.11.2016.

Liitteet

Liite 1. Avoin haastattelulomake

HAASTATTEULKYSYMYKSET OPINNÄYTETYÖHÖN

Taloushallinnon digitalisoitumisen riskit ja niiden hallinta (virallinen nimi saattaa muuttua)

Pauli Martinmaa

OHJEET VASTAAMISEEN:

- vastaa enemmän siihen mihin haluat, halutessaan kysymyksistä voi hypätä yli tai vastata hyvin lyhyesti, 7 ensimmäistä kysymystä tärkeämpiä
- kysymykset ovat vain aiheita, joten niihin voi vastata melko vapaasti
- jos haluat, voin käyttää vastauksia nimettömänä, jolloin voimme sopia miten viittaamme vastauksiisi (esimerkiksi ammattinimikkeen tai muun mukaan) (esim. itse olisin taloushallinnosta vähän kokemusta saanut ammattikorkeakouluopiskelija)
- en tule kirjoittamaan kokonaisina ihan kaikkia vastauksianne työhöni, vaan viittaan niihin osiin jotka saan sopimaan muuhun osuuteen
- kiitos erittäin paljon vastauksistanne!

Tietokoneet, ohjelmistot ja järjestelmät ovat kehittyneet viime vuosikymmeninä nopeasti ja samalla myös yritysten taloushallinnon sähköistäminen ja digitalisointi on edennyt melkein yhtä nopeasti. Näiden järjestelmien kehitys on tuonut jonkin verran muutoksia ja uusia asioita taloushallintoon, joista tämä opinnäytetyö tutkii erityisesti taloushallinnon digitalisoitumisen tuomia riskejä ja niiden hoitamista. (digitalisoituminen tarkoittaa käytännössä vaan sähköisestä vielä kehittyneempää ja automatisoidumpaa)

1. Työpaikoilla käytetään nykyään paljon yhä uudistuvia ja kehittyviä tietokoneita, ohjelmia, järjestelmiä ja esimerkiksi uusia kännyköitä. **Käytätkö nykyään/käytitkö ennen paljon työnteossa taloushallintoon liittyvää teknologiaa, laitteita, ohjelmia tai järjestelmiä? Jotain esimerkkejä?**

2. Työntekijät tarvitsevat yleensä koulutusta kun uusia ohjelmia ja laitteita otetaan käyttöön, mutta myös kun uusi työntekijä otetaan töihin eikä hänellä ole kyseisistä laitteista tai ohjelmista aiempaa kokemusta. Koulutusta voi myös antaa esimerkiksi erilaisista nettihuijauksista, viruksista ja siitä miten korjata syntyneitä ongelmia. **Mitä olet huomioinut teknologian käytön koulutuksesta työpaikalla/työpaikoilla (taloushallintoon liittyen)? Onko koulutus mielestäsi näiden osalta onnistunutta ja riittävää? Miksi, miksi ei?**

Teknologia on tuonut mukanaan uudenlaisia uhkia taloushallinnolle ja muutenkin yrityksille ja ihmisille.

3. **Oletko kokenut töissä taloushallinnon toimintaa, tai yrityksen muuta toimintaa, haittaavia hyökkäyksiä, jotka ovat tulleet internetin avulla/välityksellä? Minkälaisia?** Näitä ovat esimerkiksi haitalliset sähköpostiviestit jotka sisältävät huijauksia, viruksia tai tukkivat viestintää, tai vaikkapa yrityksiä tunkeutua järjestelmään ulkopuolelta.

4. **Oletko kokenut merkittäviä tai pienempiä ei-tahallisia sähköisen taloushallinnon häiriöitä, virheitä, vahinkoja? Ovatko häiriöt aiheuttaneet riskitilanteita esimerkiksi tiedonleviämisen tai maksutapahtumien kannalta tai muuten haitanneet toimintaa?** Näitä ovat esimerkiksi järjestelmäviat, luonnonkatastrofien aiheuttamat ongelmat (liittyen sähköiseen taloushallintoon kuten internet katkennut päiväksi myrskyn johdosta jne.), tai ohjelman kehitysvaiheessa tehty virhe joka huomataan myöhemmin.

5. **Seurataanko mielestäsi työpaikalla annettuja ohjeita ja säädöksiä (mieluiten ohjelmista ja laitteista taloushallintoon liittyen) tarpeeksi tarkkaan ja luetaanko ne tarpeeksi huolellisesti? Rikottiinko töissä usein ohjeita tietoisesti tai tietämättä?** Tarkoitan esimerkiksi käyttöohjeita, turvallisuusohjeita, huomautuksia. Esimerkiksi työasioita ei saisi yleensä tehdä omalla ostetulla tietokoneella, koska siinä ei ole vaadittuja turvatoimia ja voi sisältää helpommin viruksia.

6. Digitaalisen taloushallinnon uhkien torjuminen voi tulla hyvinkin kalliiksi. Virustorjunnat, koulutukset, laitteiden ja järjestelmien testaukset, vaaroista muistuttaminen ja ohjeistaminen, varmempien ja turvallisempien palveluiden ostaminen jne. **Otetaanko teknologian kehityksen myötä tulevat riskit töissäsi mielestäsi tarpeeksi huomioon vaikka se onkin kallista ja aikaa vievää? Kun valittiin järjestelmää, ostettiin palveluita, oliko työpaikallasi varaa ja aikaa kiinnittää huomiota myös tarpeeksi turvallisuuteen?**

7. **Miten vertailisit nykyistä sähköistä/digitalisoitunutta taloushallintoa vanhempaan paperiseen taloushallintoon? Onko riskien määrä mielestäsi muuttunut? Onko riskienhallinta pysynyt kehityksessä mukana?** Usein esimerkiksi hakkerit löytävät järjestelmistä ja uusista keksinnöistä tietoturva-aukkoja, joita vasta myöhemmin osataan korjata.

LOPPUUN PIENEMPIÄ KYSYMYKSIÄ JOTKA KOSKEVAT TARKEMPIA AIHEITA, NÄISTÄ VOI HYVIN JÄTTÄÄ NE VÄLIIN MITKÄ EIVÄT KIINNOSTA

8. **Oletko käyttänyt pilvipalveluita? Tunnetko ymmärtäväsi sen käytön? Onko pilvipalvelu mielestäsi turvallinen?**

9. **Oletko tehnyt etätöitä? Lisääkö etätöiden teko mielestäsi riskien määrää? Kokemuksia?**

10. **Oletko huomannut tai kokenut, että kilpaileva yritys tai jokin sidosryhmä olisi yrittänyt saada työpaikaltasi jotain salaista tietoa?** (sähköisesti, netin kautta jne.)

11. **Herääkö omia ajatuksia, mielenkiintoisia pointteja, tai muuta kommentoitavaa, jota haluaisi aiheeseen liittyen esittää?**
