Sini Fröblom

Ohjelmistorobotiikan asettamat vaatimukset organisaation kontrolliympäristölle

Laskentatoimen ja rahoituksen akateeminen yksikkö
Laskentatoimen pro gradu -tutkielma
Laskentatoimi ja tilintarkastus

Vaasa 2021

VAASAN YLIOPISTO
Kauppatieteiden akateeminen yksikkö
Tekijä: Sini Fröblom
Tutkielman nimi: Ohjelmistorobotiikan asettamat vaatimukset organisaation kontrolliympäristölle
Tutkinto: Kauppatieteiden maisteri
Oppiaine: Laskentatoimi ja tilintarkastus
Työn ohjaaja: Mikko Ranta
Valmistumisvuosi: 2021 **Sivumäärä:** 112

TIIVISTELMÄ:
Organisaatiot pyrkivät parantamaan kilpailukykyään erilaisilla toiminnan tehostamisen keinoilla. Viime vuosien trendi on ollut tehostaa liiketoimintaprosesseja prosessiautomaation avulla. Prosessiautomaation tavoitteena on suorittaa aiemmin ihmisen manuaalisesti suorittama prosessi automatisoidusti ohjelmistorobotiikan avulla. Teknologisen kehityksen myötä ohjelmistorobotiikan käyttö on yleistynyt. Siten tarve niiden hallinnalle kasvaa. Samaan aikaan prosessiautomaatioratkaisut monimutkaistuvat, mikä edelleen lisää hallinnan tarvetta. Yhä useammissa organisaatioissa siirrytään nyt tai lähitulevaisuudessa prosessiautomaation osalta kokeiluvaiheesta yhä systemaattisempaan käyttöön, jolloin toimintaan liittyvät riskitkin kasvavat. Näin tarve ohjelmistorobottien tehokkaan kontrolloinnin tutkimukselle kasvaa.

Tutkielmassa haastateltiin eri alojen asiantuntijoita ohjelmistorobotiikkaan liittyvistä riskeistä ja niiden hallinnasta. Tavoitteena on tarkastella ohjelmistorobotiikka-trendiä riskienhallinnan näkökulmasta ja arvioida millaisia vaatimuksia teknologian yleistyminen asettaa organisaation kontrolliympäristölle. Tarkoituksena on selvittää mitä erityispiirteitä ohjelmistorobotiikkaan liittyy, ja mitkä ovat tehokkaimmat valvontatoimenpiteet nämä erityispiirteet huomioon ottaen. Tutkimusaineiston analyysimenetelmänä on käytetty teoriaohjaavaa aineistoanalyysiä.

Tutkimus toteutettiin teemahaastatteluin ohjelmistorobottien parissa työskennelleille eri alojen asiantuntijoille. Tutkimuksessa korostui toiminnan prosessikohtaisuus, ja keskitetyn hallintamallin merkitys yksittäisten automaatioprosessien johtamisen ja valvonnan apuna. Haasteeksi ohjelmistorobotiikan valvonnan osalta osoittautui ristiriita keskitetyn hallintamallin ja prosessikohtaisesti kehitettävän ohjelmistorobotiikan välillä. Yleispäteviä yksittäisiä kontrolleja ohjelmistorobottien hallintaan on vaikea määritellä, koska kontrolloinnin tarve ja tehokkaat kontrollit vaihtelevat aina prosessikohtaisesti. Koska ohjelmistorobotiikan käyttö alkaa organisaatiossa yksittäisten prosessien automatisoinnista usein kokeilun kautta, keskitetylle hallintamallille ei alkuun ole tarvetta. Tämä ristiriita on tiedostettava, kun organisaatiossa lähdetään edistämään laajamittaista ohjelmistorobotiikan käyttöönottoa.

AVAINSANAT: Sisäinen valvonta, Ohjelmistorobotiikka, Robotic Process Automation, RPA, Kontrollit, Hyvä tiedonhallintatapa, IT Governance

Sisällys

Kuviot

Taulukot

1 Johdanto

Digitalisaation mahdollistamana, organisaatioiden johto ja päättäjät etsivät uusia tapoja tehostaa liiketoimintaa ja sen tukitoimintoja. Tämän kehityksen myötä taloushallinnon ja raportoinnin on pystyttävä vastaamaan jatkuvasti kasvaviin tehostamisvaatimuksiin. Tehostamispyrkimykset ovat johtaneet liiketoimintaprosessien virtaviivaistamiseen ja standardisoimiseen. (Seasongood, S 2016). Samalla teknologia ja sen luomat mahdollisuudet tunnistetaan kriittiseksi kilpailuetua luovaksi liiketoimintatekijäksi (Bendoly, Rosenzweig, Stratman 2009; Ojiako 2012). Standardisoidut liiketoimintaprosessit, uudet teknologiset innovaatiot ja tarve prosessien tehostamiselle on lisännyt kysyntää prosessien automatisoinnille. Uuden tyyppisiä automaatioratkaisuja, esimerkiksi robotiikkaa ja tekoälyä, kehitellään ja käyttöönotetaan jatkuvasti organisaatioiden tehostamisvaatimuksien saavuttamiseksi (King, Hammond ja Harrington 2017).

Teknisen kehityksen myötä, liiketoimintaympäristö muuttuu jatkuvasti. Liiketoimintaympäristön muuttuessa, muuttuvat myös liiketoimintaa uhkaavat riskit. Organisaatioissa onkin huutava tarve laadukkaille sisäisen valvonnan ja riskienhallinnan järjestelmille, jotka auttavat hallitsemaan liiketoimintatavoitteiden toteutumisen esteenä olevia riskejä (COSO, 2013). Viimevuosien kirjanpitoskandaalit ja globaalit finanssikriisit ovat osoittaneet sisäisen valvonnan ja riskienhallinnan merkityksen. Kriittiset tapahtumat ovat korostaneet erilaisten valvontatoimenpiteiden strategista roolia ja havainnollistaneet sisäisen valvonnan merkitystä menestyksekkään liiketoiminnan ja tehokkaan riskienhallinnan edesauttajana (Collier, Berry ja Burke 2007; Fraser ja Simkins 2010).

Ohjelmistorobotiikan ja sisäisen valvonnan yhdistäminen tutkimuksessa on mielekästä, koska ohjelmistorobotiikan käyttö yleistyy ja automatisoitujen prosessien määrä organisaatiossa kasvaa, jolloin myös valvonnan ja hallinnan tarve lisääntyy. Ohjelmistorobotiikka suorittaa tiettyä prosessia ihmisen tapaan, mutta se on ohjelmisto. Toisaalta ohjelmistorobotiikka ei perinteisten tietojärjestelmien tapaan pyri luomaan uutta ohjelmistoa tietyn prosessin suorittamiseksi, vaan operoi jo olemassa olevien tietojärjestelmien päällä. (Aalst, Bichler ja Heinzl 2018.) Tämän tutkielman tavoitteena on selvittää,

millaiset asiat on otettava huomioon robottien kontrolloinnissa, suhteessa ihmisten tai perinteisten tietojärjestelmien kontrollointiin.

Ohjelmistorobotiikkaa ei ole vielä tutkittu kovin kattavasti (Moffitt, Rozario ja Vasarhelyi 2018). Ohjelmistorobotiikan tutkimus on nojannut vahvasti tekniseen puoleen ja siihen, millaiset prosessit soveltuvat parhaiten automatisoitaviksi (Aalst, Bichler ja Heinzl 2018; Fung 2014). Teknologia kuitenkin jatkuvasti kehittyy ja automatisoitavat prosessit monimutkaistuvat, joten tutkimustarve ohjelmistorobottien hallinnalle kasvaa. Ohjelmistorobottien hallinnasta on jonkin verran aiempaa kirjallisuutta. Esimerkiksi Jiles (2020) kuvasi artikkelissaan ohjelmistorobottien hallinnan merkitystä ja erilaisia hallinnan malleja. Asatiani, Kämäräinen ja Penttinen (2019) tutkivat erästä ohjelmistorobotiikan hallinnan mallia, ja siihen liittyviä käytännön ongelmia. Laajempaa tutkimusta erilaisista hallinnan malleista ja erilaisista niihin liittyvistä valvontatoimenpiteistä tarvitaan, jotta organisaatioissa voidaan paremmin räätälöidä heidän tarpeisiinsa sopivat ohjelmistorobotiikan hallinnan ja valvonnan mallit.

Tämä tutkielma koostuu kahdesta osasta. Ensin avataan aiempaan tutkimukseen ja kirjallisuuteen peilaten sisäisen valvonnan, kontrolliympäristön, IT-kontrollien ja ohjelmistorobotiikan käsitteitä. Tavoitteena on auttaa lukijaa ymmärtämään näiden käsitteiden välisiä yhteyksiä. Lukijan tulisi ymmärtää, miksi organisaation kontrolliympäristön laatuun tulisi panostaa, ja miten IT-kontrollit tätä edistävät. Lisäksi tulisi käsittää, miten ohjelmistorobotit voivat edistää organisaation liiketoimintatavoitteiden saavuttamisessa, ja millaiset riskit näiden tavoitteiden saavuttamisen voisi estää. Tutkielman empiirisessä osassa pyritään asiantuntijahaastattelujen avulla selvittämään, mitkä ovat kaikkein kriittisimmät ohjelmistorobotiikkaan liittyvät riskit organisaation liiketoimintatavoitteiden toteutumisen kannalta, ja millaisia vaatimuksia se asettaa organisaation kontrolliympäristölle. Lisäksi selvitetään, millaiset käytännön IT-kontrollit soveltuvat parhaiten edellä mainittujen riskien hallitsemiseen, ja kontrolliympäristön laadun varmistamiseen.

2 Organisaation kontrolliympäristö

Tämän kappaleen tavoitteena on avata organisaation kontrolliympäristön käsitettä, sisäisen valvonnan toimintaympäristönä. Lukijan tulisi ymmärtää millaisista tekijöistä kontrolliympäristö koostuu, ja miten nämä tekijät vaikuttavat kontrolliympäristön laatuun ja tehokkuuteen. Näillä tekijöillä viitataan erilaisiin kontrolleihin, joita esitellään tarkemmin myöhemmin tässä kappaleessa. Tässä tutkielmassa sisäinen valvonta nähdään toimintona, jota toteutetaan kontrolliympäristössä erilaisten käytännön kontrollien avulla. Sisäisen valvonnan, kontrolliympäristön ja kontrollien käsitteet ovat osittain päällekkäisiä ja niiden merkitys saattaa vaihdella käytettävän kontekstin mukaan. Tämän vuoksi, tässä kappaleessa kuvataan tämän tutkielman pohjana käytetyt käsitteiden määrittelyt ja niiden väliset vuorovaikutussuhteet. Näin lukija saa paremman käsityksen tutkielman pohjana käytetystä teoreettisesta viitekehyksestä.

Käsitteiden selkeyttämiseksi, määrittelyn apuna käytettiin jo olemassa olevia sisäisen valvonnan ja tiedonhallinnan viitekehyksiä ja niiden mukaisia määritelmiä käytetyille käsitteille. Alkuun sisäisen valvonnan, kontrolliympäristön ja kontrollien käsitteitä avataan yleisellä tasolla sisäisen valvonnan viitekehykseen peilaten. Tämän jälkeen tarkasteluun otetaan tietotekninen näkökulma ja tarkastelua tehdään tiedonhallinnan viitekehyksen kautta. Kuvailuun otetaan mukaan IT-kontrolliympäristön käsite, sekä esitellään muutamia käytännön IT-kontrolleja.

2.1 Sisäinen valvonta ja kontrolliympäristö

Toimiva kontrolliympäristö on tehokkaan sisäisen valvonnan ja riskienhallinnan kannalta kriittinen tekijä. Koko sisäisen valvonnan järjestelmä lepää kontrolliympäristön varassa. Toisin sanoen kontrolliympäristö toimii pohjana, jossa sisäinen valvonta toimii. (Rubino, Vitolla ja Garzoni 2017.) Kontrolliympäristö tarjoaa perustan, jonka pohjalta organisaatio suunnittelee ja toteuttaa sisäistä valvontaa. Kontrolliympäristön laatu vaikuttaa kaikkiin sisäisen valvonnan kolmesta tavoitteesta. Sisäisen valvonnan tavoitteita on varmistaa

toiminnan tehokkuus, tuloksellisuus ja taloudellisen raportoinnin luotettavuus, sekä lakien ja säännösten noudattaminen. (COSO, 2013; Shelleman 1995; Simons 1996.)

Sisäisen valvonnan suoria hyötyjä on hankalaa mitata, koska se on luonteeltaan riskienhallintaa. Konkreettisia rahassa mitattuja lukuja, kuten takaisinmaksuaikoja on hankala laskea, koska oikein toimiessaan sisäinen valvonta ehkäisee tavoitteiden saavuttamisen esteenä olevia riskejä. Tehokkaan sisäisen valvonnan hyödyt kohdistuvat yritykselle, sidosryhmille ja omistajille epäsuorasti. Realisoitumattomien riskien kustannusvaikutuksia on hankala mitata. Huonosti järjestetyllä sisäisellä valvonnalla on kuitenkin kova hinta. (Sihvonen 2019 s. 70).

Kontrolliympäristön laadun arviointi vaatii perusteellista ymmärrystä organisaation toiminnasta ja liiketoimintatavoitteista. Lisäksi liiketoimintatavoitteita uhkaavat riskit ja riskejä hallitsevat valvontatoimenpiteet on tunnistettava. Tämä vaatii ymmärrystä liiketoimintaprosesseista, organisaation resursseista, organisaatiorakenteista, rooleista ja vastusta. (Rubino ja muut 2017.) Sisäisen valvonnan laadun kannalta on tärkeää tehdä asianmukainen kartoitus ja kuvaus kontrolliympäristön osatekijöistä. Näin pystytään paremmin arvioimaan ovatko nämä tekijät riittäviä koko organisaation valvonta- ja ohjaustarpeisiin. (Zack 2013.)

Seuraavaksi sisäisen valvonnan tavoitteita ja kontrolliympäristön laatuun vaikuttavia tekijöitä havainnollistetaan sisäisen valvonnan viitekehyksen avulla. Sisäisen valvonnan käsite on monitasoinen ja laaja. Kontrolliympäristön käsite on taas verrattain abstrakti ja sen määritelmä saattaa vaihdella lähteen mukaan. Siispä käsitteiden ymmärtämisen edesauttamiseksi ja niiden välisen vuorovaikutuksen esittämiseksi hyödynnetään yleisesti hyväksyttyä viitekehystä. Tämä viitekehys esittää yksityiskohtaisesti koko sisäisen valvonnan prosessia ja sen eri osia (COSO 2013). Tässä tutkielmassa on kuitenkin näkökulmana kontrolliympäristö, joten seuraava kappale keskittyy yksityiskohtaisemmin kontrolliympäristön kannalta merkityksellisimpiin osatekijöihin.

2.2 COSO-viitekehys

Coso-viitekehys on Committee of sponsoring the Organizations of the Treadway Commision (COSO) julkaisema sisäisen valvonnan viitekehys. COSO on riippumaton organisaatio, jonka tavoitteena on edistää johtajuutta ja edelläkävijyyttä julkaisemalla viitekehyksiä riskienhallintaan, sisäiseen valvontaan ja väärinkäytösten ehkäisemiseen liittyen. COSO:n taustalla vaikuttaa laskentatoimen, tilintarkastuksen ja sisäisen tarkastuksen ammattilaisia sekä sijoittajien ja pörssin edustajia. COSO Internal Control – Integrated Framework -viitekehystä (COSO-viitekehys) käytetään mallina sisäisen valvonnan järjestämiseksi, ja sen eri osa-alueiden havainnollistamiseksi. Soveltamisohjeiden ja esimerkkien kautta se auttaa organisaatioita luomaan heidän tarpeidensa näkökulmasta tehokkaan sisäisen valvonnan järjestelmän. (Sihvonen 2019 s. 80). Suurin osa yrityksistä käyttääkin COSO:n sisäisen valvonnan viitekehystä organisaationsa sisäisen valvonnan sekä kontrolliympäristön laadun arvioinnissa. Viitekehys auttaa yrityksiä havaitsemaan ja ehkäisemään virheitä sisäisen valvonnan prosesseissa ja kontrolleissa. (D'Aquila 2014; Rubino ja Vitolla 2014c.)

COSO-viitekehyksestä puhuttaessa käytetään usein viitekehyksen kuvaamisen apuna kolmiulotteista kuutiota (kts. Kuvio 1). Etummaisella sivulla on Sisäisen valvonnan viisi osatekijää: valvontaympäristö, riskienarviointi, valvontatoimenpiteet, informaatio ja kommunikointi, sekä seuranta. Sisäinen valvonta koostuu näistä viidestä komponentista. Kuution yläosa kuvastaa sisäisen valvonnan tavoitteita: toiminnot, raportointi ja vaatimustenmukaisuus (lait ja säädökset) (COSO 2004; Sihvonen 2019 s. 80-82). Tavoitekategoriat muodostavat sisäisen valvonnan määritelmän, joka kuuluu COSO:n mukaan seuraavasti:

> *"Sisäinen valvonta on prosessi, johon vaikuttavat yhtiön hallitus, johto ja muu henkilöstö, joka on suunniteltu tuottamaan kohtalaista varmuutta siitä, että yhtiö saavuttaa toimintaan, raportointiin ja vaatimustenmukaisuuteen liittyvät tavoitteensa."* (COSO 2004)

Kolmas ulottuvuus kattaa koko organisaatiorakenteen, jolle sisäinen valvonta tulee ulottaa. Tavoitteena on määritellä omat sisäisen valvonnan roolit liiketoiminnalle, tukitoiminnoille ja sisäiselle tarkastukselle. Lisäksi jokaista COSO-viitekehyksen osatekijää kohden on kuvattu yhteensä 17 periaatetta. Periaatteisiin liittyy tarkentavia ohjeistuksia, joilla pyritään auttamaan periaatteiden ymmärtämistä käytännössä. COSO:n mukaan tehokas sisäinen valvonta tarkoittaa sitä, että kaikki COSO-mallin 5 komponenttia ja 17 periaatetta on otettu käyttöön. Käyttöönoton toteutus on vapaa, kunhan periaatteissa määritellyt kontrollit on implementoitu organisaation prosesseihin ja jokapäiväiseen toimintaan. (Sihvonen 2019 s. 80-82).

Kuvio 1 COSO Sisäisen valvonnan viitekehys (COSO 2004).

Tämä tutkielma keskittyy kontrolliympäristöön ja organisaation kontrolleihin. Siispä esittelemme nyt viidestä sisäisen valvonnan komponentista tarkemmin näihin liittyvät perusperiaatteet.

2.2.1 COSO määritelmä kontrolliympäristölle

Kontrolliympäristöllä viitataan organisaatiotason valvontatoimenpiteisiin. Näitä kontrolleja ovat esimerkiksi organisaation toimintaohjeet, kuvatut prosessit, controlling- ja sisäisen tarkastuksen toiminnot sekä määritellyt laskentaperiaatteet. (Lahti ja Salminen 2014). Kontrolliympäristöön lukeutuu myös organisaation eettiset periaatteet ja niiden soveltaminen, organisaatiorakenne, vallan ja vastuun eriyttäminen, sekä johtamisen menetelmät, esimerkiksi henkilöstön kehittäminen ja palkitseminen. Lisäksi se kattaa paljon muita sisäisen valvonnan laatuun vaikuttavia muuttujia, kuten toimivallan ja vastuiden jakaminen. (Graham 2015.) Kaiken tämän muodostama kontrolliympäristö luo pohjan tehokkaalle sisäiselle valvonnalle. (Sihvonen 2019 s. 83). Kontrolliympäristön viisi periaatetta ovat:

1. Organisaatio osoittaa sitoutumisen rehellisyyteen ja eettisiin arvoihin
2. Hallitus on riippumaton toimivasta johdosta ja toteuttaa valvontarooliaan sisäisen valvonnan kehittämiseen ja toteuttamiseen liittyen
3. Toimiva johto luo hallituksen valvomana rakenteet, raportointisuhteet ja riittävät valtuudet ja vastuut tavoitteiden saavuttamiseksi
4. Organisaatio osoittaa sitoutumisensa houkutellakseen, kehittääkseen ja ylläpitääkseen kyvykkäitä henkilöitä tavoitteidensa mukaisesti
5. Organisaatio vastuullista yksilöitä heidän sisäiseen valvontaansa liittyvistä velvoitteistaan tavoitteiden saavuttamiseksi. (D'Aquila 2013; Sihvonen 2019 s. 83).

Kontrolliympäristö luo siis pohjan, jonka perusteella organisaation johto päättää sisäisen valvonnan järjestämisestä. Kontrolliympäristö siis vaikuttaa kaikkiin sisäisen valvonnan tavoitteisiin ja sen toimintoihin. (COSO 1992; COSO 2013; Moeller 2011.)

2.2.2 COSO määritelmä valvontatoimenpiteille eli kontrolleille

Valvontatoimenpiteet eli kontrollit ovat COSO-mallin komponentti, joka pitää sisällään määrittelyt menetelmät ja toimintatavat, joiden avulla varmistetaan, että johdon ohjeistusta sisäiseen valvontaan ja riskienhallintaan liittyen noudatetaan (D'Aquila 2013). Kontrolleja suoritetaan kaikilla organisaatiotasoilla, liiketoimintaprosesseissa ja tietojärjestelmissä. (Sihvonen 2019 s. 91). Kontrolleihin liittyvät kolme perusperiaatetta ovat:

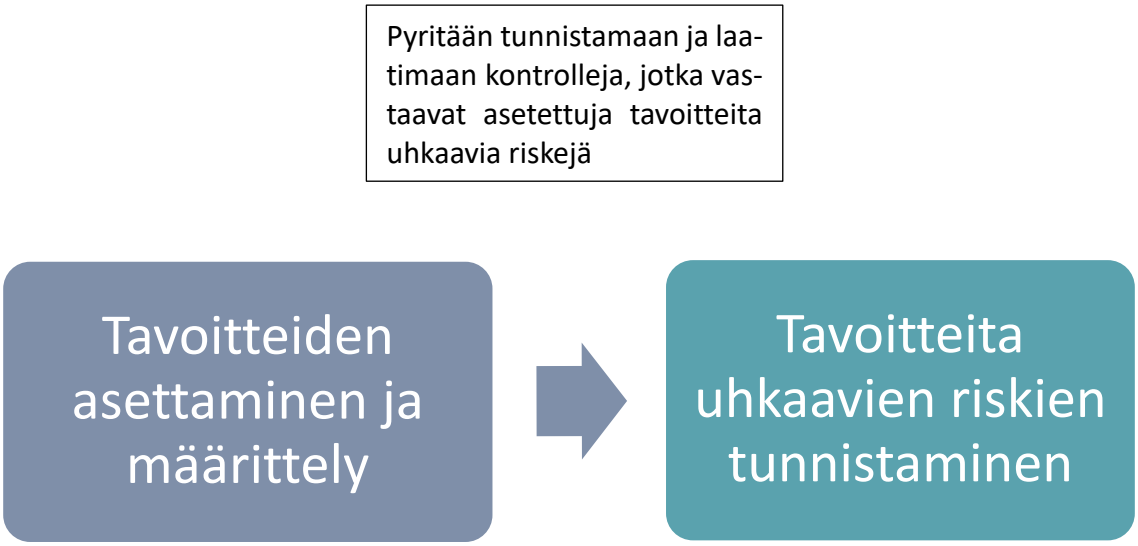
1. Organisaatio valitsee ja kehittää kontrolleja, jotka edesauttavat tavoitteiden saavuttamiseen liittyvien riskien vähentämistä hyväksyttävälle tasolle
2. Organisaatio valitsee ja kehittää teknologiaan liittyviä yleisiä kontrolleja tavoitteiden saavuttamisen tueksi
3. Organisaatio käyttöönottaa kontrolleja sellaisina toimintatapoina, joiden perusteella organisaation odotukset ovat selvät, sekä menettelyillä, joiden perusteella toimintatavat toteutetaan käytännössä. (D'Aquila 2013; Sihvonen 2019 s. 91-92).

Perusperiaatteissa korostuu riskilähtöisyys. Kontrollien suunnittelemisen ja asettamisen perustana tulisi aina olla havaittujen riskien pohjalta tehty arviointi (D'Aquila 2013). Tyypillinen virhe on kehittää kontrolliympäristöä kontrollilähtöisesti. Kontrollien tapauksessa määrä ei korvaa laatua ja kontrollien määrä saattaa helposti kasvaa hallitsemattomasti. (Sihvonen 2019 s. 92). Kontrollien käyttöönoton taustalla pitäisi siis olla lähtökohtaisesti organisaation tavoitteet.

2.3 Kontrollit

Kontrollit eli valvontatoimenpiteet varmentavat organisaation tavoitteiden mukaista toimintaa ja hallitsevat tavoitteiden toteutumisen esteenä olevia riskejä. Riskejä hallitaan poistamalla niitä, pienentämällä niiden tapahtumisen todennäköisyyttä, tai minimoimalla niiden vaikutuksia. Riskienhallintaa suoritetaan kontrolleilla. (Lahti ja Salminen 2014.) Kontrollien suunnittelu alkaa tavoitteiden selkeästä määrittelystä. Tämän jälkeen

on tunnistettava ja analysoitava näitä tavoitteita uhkaavat riskit. Lopuksi arvioidaan ja määritellään näihin riskeihin parhaiten vastaavat kontrollit. (Sihvonen 2019 s. 89).



Kuvio 2. Kontrollien asettaminen (Sihvonen 2019 s. 89).

Kontrolliympäristö muodostuu estävistä, havaitsevista ja korjaavista kontrolleista. Eri prosessien toiminnan ja laadun valvonta tulisi toteuttaa siten, että eri prosessin vaiheissa suoritetut kontrollit tukevat toisiaan. (Lahti ja Salminen 2014). Tehokkuuden kannalta ei ole asianmukaista suorittaa päällekkäisiä kontrolleja useissa prosessin eri vaiheessa. Sisäisen valvonnan ja kontrolliympäristön suunnittelun merkitys korostuu tässäkin. Koko prosessi ja sen eri vaiheiden ainutlaatuiset ominaisuudet on tunnettava, jotta osataan asettaa tietyt kontrollit prosessin oikeisiin vaiheisiin. Kontrollit tulisi kohdistaa prosessissa sinne, missä ne ovat riskienhallinnan näkökulmasta kaikkein tehokkaimmat. Prosessin alkuvaiheen kontrollit liittyvät usein esimerkiksi tietojärjestelmään syötettyjen tietojen varmentamiseen. Kun tiedot on todettu heti järjestelmään syötettäessä oikeiksi, niitä ei ole välttämätöntä tarkistaa erikseen prosessin joka vaiheessa. Tietenkin olettaen, että muutoin automatisoidut prosessit ja kontrollit on todettu asianmukaisiksi, jolloin oikein syötetty tieto ei muutu prosessin myöhemmissä vaiheissa. (Sihvonen 2019 s. 89; Lahti ja Salminen 2014).

Kontrollien tulisi ensisijaisesti ehkäistä riskejä ja virheitä. Lisäksi kontrolliympäristön tulisi sisältää automaattisten kontrollien lisäksi manuaalisia kontrolleja. Manuaaliset kontrollit tukevat automaattisia kontrolleja, koska niiden avulla voidaan hallita riskejä, joita ei voida riittävästi hallita automaattisin kontrollein. Manuaaliset kontrollit soveltuvat erinomaisesti suuriin, kertaluonteisiin tai epätavanomaisiin tapahtumiin, joiden analysoimiseen vaaditaan inhimillistä harkintaa. Lisäksi manuaaliset kontrollit soveltuvat vaikeasti määriteltävien, ennakoitavien ja ennustettavien riskien hallintaan. Koska manuaalisia kontrolleja suorittavat järjestelmien sijaan ihmiset, niitä on keskimäärin helpompi kiertää ja jättää huomiotta. Lisäksi ne ovat alttiita inhimillisille virheille, erehdyksille ja epäjohdonmukaiselle suorittamiselle. (Lahti ja Salminen 2014 s.189-190).

Kontrolliympäristön laadun varmistamiseksi, havaitut riskit ja niihin vastaavat kontrollit tulisi pystyä kuvaamaan asianmukaisesti. Lisäksi asetettuja tavoitteita ja havaittuja riskejä näiden tavoitteiden esteenä olisi hyvä aika-ajoin kyseenalaistaa. Näin käytössä olevien kontrollien ja koko kontrolliympäristön laatua ja asianmukaisuutta voidaan arvioida ja tarvittaessa tehostaa. Kontrolliympäristön, sisäisen valvonnan ja riskienhallinnan riittävyyttä tulisi varmistaa säännöllisellä arvioinnilla ja seurannalla. (Lahti ja Salminen 2014 s.188-190).

2.3.1 Kontrollien tehokkuus

Jotta sisäinen valvonta ja kontrolliympäristö voidaan määritellä tehokkaaksi, on tehokkuutta pystyttävä mittaamaan. Hyvin suunnitellut prosessit ja kontrollit eivät aina ole tehokkaita. Johdon on pystyttävä varmentamaan, että kontrollit ovat asianmukaisesti käyttöönotetut ja toimivat suunnitellusti. (Sihvonen 2019 s. 110). Tietojärjestelmät ja erilaiset raportointityökalut, ovat erinomainen tapa seurata kontrollien tehokkuutta. Niiden avulla voidaan reaaliaikaisesti valvoa yrityksen prosesseja. Tallaisten reaaliaikaisten seurantakontrollien hyötynä on se, että poikkeamiin voidaan reagoida välittömästi. Haittapuolena taas on reaaliaikaisten seurantakontrollien vaatimat investoinnit. Reaaliaikaisen

seurantakontrollien lisäksi tai sijasta voidaan käyttää erilaisia analytiikka- ja visualisointityökaluja. Näiden käyttö tosin vaatii useimmiten myös ihmistyövoimaa. (Sihvonen 2019 s. 118).

Esimerkiksi myynnin hyvityslaskujen seurantaa voidaan suorittaa reaaliaikaisilla seurantakontrolleilla asettamalla järjestelmään raja-arvoja poikkeuksellisen suurille laskuille, tai poikkeuksen suurelle määrälle tehtyjä hyvityksiä asiakas- tai toimintayksikkötasolla. Ennalta ohjelmoitujen raja-arvojen ylittyessä, järjestelmä esimerkiksi antaa varoituksen, vaatii ylimääräistä hyväksyntää tai lähettää tiedon kolmannelle osapuolelle reaaliaikaisesti hyvityslaskun luonnin yhteydessä. Analytiikka ja visualisointityökaluilla voidaan jälkikäteen analysoida tehtyjä hyvityslaskuja, ja sen perusteella näiden samaisten raja-arvojen perusteella poimia poikkeukselliset anomaliat massasta, ja tehdä tarkempaa selvitystä niiden oikeellisuudesta. Ohjelmistorobotiikka on mahdollistanut sen, että reaaliaikaisia seurantakontrolleja voidaan asentaa prosessien taustalle reagoimaan ennalta ohjelmoitujen raja-arvojen ylittyessä tai muiden poikkeavien tilanteiden tapahtuessa. Näin reaaliaikaisia seurantakontrolleja voidaan rakentaa myös erillisten prosessien ja ohjelmien yhteyteen. (Sihvonen 2019 s. 118-119).

2.4 Tiedonhallinta ja IT-kontrolliympäristö

Laskentatoimen näkökulmasta tietotekniikan merkitys korostuu kaikilla sen osa-alueilla. Jatkuvasti kasvava osa taloudellisesta raportoinnista, johdon laskentatoimesta, tilintarkastuksesta ja verotuksesta hoidetaan automatisoidusti erilaisissa tietojärjestelmissä. Uudet tietotekniset ratkaisut asettavat uudenlaisia kontrollivaatimuksia, jotta niihin liittyvä riski saadaan laskettua hyväksyttävälle tasolle (Janvir, Payne, Byrnes, Schneider ja Curtis 2012). Aiemmassa tutkimuksessa korostetaan tietotekniikan strategista (Henderson ja muut 2010; Nicolaou ja muut 2011; Piccoli and Ivés 2005; Premkumar ja muut 2004) ja operatiivista (Dehning ja muut 2007; Hunton 2002; Hunton ja muut 2008) roolia kilpailuedun ja menestyksekkään liiketoiminnan näkökulmasta. Jotta tietotekniikka luo kilpailuetua, on sitä ensin pystyttävä valvomaan ja hallitsemaan. Mitä enemmän ja mitä

monimutkaisempaa tietotekniikkaa käyttöönotetaan, sitä monimutkaisemmaksi sen hallinta muuttuu. (Janvir ja muut 2012.)

Ottaen huomioon, että suurin osa taloushallinnon järjestelmistä on koneistettu, kirjanpitäjien ja muiden taloushallinnon tehtävissä työskentelevien tulisi pystyä luottamaan näiden järjestelmien suorittamiin prosesseihin ja siihen, että ne tuottavat heidän päätöksentekonsa tueksi asianmukaista taloudellista tietoa. (Rubino ja Vitola 2017). Tietoteknisen kehityksen vuoksi, taloudellisen tiedon raportointijärjestelmät sekä niiden kontrollit ovat merkittävästi monimutkaistuneet. Myös taloudellisen tiedon varmentamisen näkökulmasta, ”olennaisen evidenssin” määritelmä on muuttunut. (Tucker 2018.) Erilaiset tietojärjestelmät, esimerkiksi toiminnanohjausjärjestelmät, vaativat luotettavan toiminnan varmistamiseksi järjestelmäkohtaisia sisäänrakennettuja kontrolleja (Grabski and Leech 2007; Morris 2011). Myös jatkuvasti korostuva järjestelmäriippuvuus asettaa uudenlaisia kontrollivaatimuksia toiminnan jatkuvuuden varmistamiseksi (Grabski ja muut 2011). Onkin hyvä pohtia, millaisia velvoitteita tietotekninen kehitys asettaa kontrolliympäristölle, jonka tehtävänä on varmistaa taloudellisen tiedon laatu.

Tietoteknisen kehityksen korostunut merkitys osana organisaation sisäistä valvontaa näkyy selvästi myös ammattikirjallisuudessa, ohjeistuksissa sekä sääntelyssä (Rubino ja muut 2017). Esimerkiksi edellä esiteltyä COSO-viitekehystä päivitettiin vuonna 2013 vastaamaan nykyajan sisäisen valvonnan haasteisiin ja uudenlaiseen toimintaympäristöön, sekä palvelemaan uusia sisäisen valvonnan tarpeita yhä kokonaisvaltaisemmin (Janvrin ja muut 2012). Toimintaympäristöä on merkittävästi muovannut juuri tietotekninen kehitys. Tämän kehityksen myötä liiketoiminta, riskit ja vaatimukset sisäiselle valvonnalle ovat muuttuneet (D’Aquila ja muut 2014). Taloudellisen raportoinnin luotettavuuden varmistaminen on yksi COSO-mallin päätavoitteesta, ja se on yksi sisäisen valvonnan peruspilareista (Altamuro ja Beatty, 2010). Päivitetyn COSO-viitekehyksen myötä tarkasteluun otettiin mukaan teknologisen kehityksen tuomat vaatimukset sisäiselle valvonnalle. Näihin vaatimuksiin kuuluu esimerkiksi, tiedon omistajuus ja hallinta, kyberturvallisuus, tekoälyn rooli ja lisääntynyt automaatio (Tucker 2018).

Seuraavissa kappaleissa keskitytään sisäiseen valvontaan erityisesti tietojärjestelmien hallinnan näkökulmasta.

2.4.1 Hyvä tiedonhallintatapa ja COBIT-viitekehys

Yhä tietoteknisempi toimintaympäristö asettaa sisäiselle valvonnalle ja organisaation kontrolliympäristölle uudenlaisia vaatimuksia. Nykyaikainen sisäisen valvonnan järjestelmä edellyttää yhä enemmän integroitujen ratkaisujen käyttöä. Perinteisten viitekehysten ja toiminnanohjausmenetelmien lisäksi tarvitaan uudenlaisia tiedonhallinnan viitekehyksiä ja niiden pohjalta rakennettuja hallintamalleja (Rubino ja Vitola 2014b). Hyvä tiedonhallintatapa eli IT-Governance kuvaa hyviä IT:n johtamisen menetelmiä. IT:n johtamiseen tarvitaan strukturoituja ja systemaattisia toimintamalleja, jotka ohjaavat ICT-osaston toimintaa ja päätöksentekoa. Uusien lakien ja säädösten sekä teknologisen kehityksen ja toiminnan monimutkaistumisen myötä, vaatimukset sisäiselle valvonnalle ja riskienhallinnalle korostuu. Näiden toimintatapojen, ohjeistuksien ja prosessien kokonaisuutta kutsutaan IT-governanceksi eli hyväksi tiedonhallintatavaksi (SandrinoArndt 2008).

Vaikka aiemmin esiteltyä COSO-viitekehystä käytetään laajamittaisesti kontrolliympäristön laadun ja tehokkuuden arvioinnin pohjana, sillä on omat rajoitteensa. COSO-viitekehys ei varsinaisesti ota huomioon sisäistä valvontaa ja kontrolleja tietoteknisestä näkökulmasta. (Rubino ja Vitola 2014). Tietotekniikalla on tärkeä rooli kilpailuedun sekä strategisen tehokkuuden näkökulmasta. Lisäksi tietotekniikkaa on laajamittaisesti käytössä organisaatioiden useimmissa prosesseissa, mikä lisää sen merkitystä osana sisäisen valvonnan kontrolliympäristöä. (Rubino ja Vitola 2017; Ratsula 2016 s. 240). Kun tietojärjestelmien merkitys osana liiketoimintaa koko ajan korostuu ja kokonaisia liiketoimintaprosesseja automatisoidaan osittain tai kokonaan tietojärjestelmien suoritettavaksi, on tärkeää huomioida tämän vaikutus myös sisäisen valvonnan näkökulmasta. COSO-viitekehyksen rajoitteita voidaan hallita ottamalla käyttöön muun tyyppisiä viitekehyksiä (Rubino ja muut 2014).

IT Governance Institute (ITGI) on vuonna 1998 perustettu voittoa tavoittelematon organisaatio, jonka tavoitteena on lisätä organisaatioiden tietoisuutta hyvästä tiedonhallintatavasta ja tarjota parhaita käytäntöjä tiedonhallintaan (Moeller 2013). Myös toinen voittoa tavoittelematon organisaatio ISACA (Information systems Audit and Control Association) on ottanut vahvasti kantaa hyvään tiedonhallintatapaan ja sen merkitykseen osana organisaatioiden tietojärjestelmien hallintaa. ISACA määrittelee hyvän tiedonhallintatavan organisaatiosuhteiden ja prosessien rakennelmana, joka ohjaa ja valvoo organisaation toimintaa suhteessa sen tavoitteisiin. Hyvä tiedonhallintatapa ohjaa ja valvoo organisaation tietojärjestelmiä ja IT-prosesseja tavoitteena esimerkiksi hallita toimintaan liittyviä riskejä (Brand ja Boonen 2010). Vuonna 2008 julkaistiin myös hyvän tiedonhallintatavan käsitteistö ISO 38500 standardissa nimeltään ”Corporate Governance of IT”. (ISO 38500 2008.)

Hallintamallin implementoinnissa on ongelmana, että organisaatiot ovat hyvin erilaisia ja niiden tietojärjestelmät ja prosessit vaihtelevat suuresti. Siten kaiken kattavaa kokonaisuutta on hankalaa määritellä (Ayat, Masrom, Sahibuddin ja Sharifi 2011). Erilaiset viitekehykset auttavat organisaatioita ymmärtämään hyvän tiedonhallintatavan periaatteita ja räätälöimään oman organisaation tarpeisiin soveltuvan hallintamallin. COBIT (Control Objectives of Information and Related Technology) on ISACA:n ja ITGI:n julkaisema viitekehys hyvään tiedonhallintatapaan. Siinä liitetään loogisella tavalla yhteen hyvä tietohallintotapa, teknologia, prosessit sekä liiketoiminnan tavoitteet. (Moeller 2013; Ratsula 2016 s. 65). Tämän lähestymistapa tarjoaa organisaation johdolle uusia työkaluja sisäisen valvonnan toteuttamiseen ja kontrolliympäristön laadun arvioimiseen. (Rubino ja Vitola 2014b). Mallin tavoitteena on esittää IT-kontrollien tavoitteet siten, että ne ovat kaikille asianomaisille selkeästi ymmärrettävissä. COBIT-viitekehys lähtee COSO-viitekehyksen tapaan liikkeelle sidosryhmien tarpeista. Niiden pohjalta määritellään liiketoiminnan tavoitteet ja edelleen IT-tavoitteet, joiden pohjalta määritellään tarpeelliset IT-prosessit. (Moeller 2013; Ratsula 2016 s. 65).

COBIT 5 rakentuu seuraavista viidestä perusperiaatteesta (Ratsula 2016 s. 65):

- Sidosryhmien vaatimukset tulee täyttää
- Organisaation kaikki toiminnot tulee kattaa
- Yksi viitekehys riittää kattamaan kaiken
- Kokonaisuuteen keskittyvä toimintatapa
- Johtaminen ja hallinnointi eriytetään toisistaan

COBIT:in vahvuus on sen liiketoimintalähtöisyys. Sen avulla voidaan havainnollistaa yhteyttä liiketoimintatavoitteiden ja IT:n välillä. COBIT-viitekehys mielletään usein ylätason tiedonhallinnan työvälineeksi, ja siten strategisen tason viitekehykseksi. Sitä hyödynnetään usein strategisessa tiedonhallinnassa sekä sisäisissä ja ulkoisissa auditoinneissa, joissa näkökulmana on liiketoiminnan IT-riippuvuuksien hallinta. Operatiivisella tasolla tarvitaan usein COBIT-viitekehyksen lisäksi käytännönläheisempiä malleja. (Ratsula 2016 s. 65-66). Lisäksi COBIT-viitekehyksessä on perinteinen sisäisen valvonnan näkökulma. Se soveltuu hyvin esimerkiksi tietojärjestelmien omistajille ja IT-tarkastajille, ja tarjoaa laajan valikoiman työkaluja tiedonhallintaan ja valvontatoimenpiteiden kehittämiseen. (Rubino ja Vitolla 2014b.)

Organisaation kontrolliympäristön laadun näkökulmasta, COBIT-viitekehys auttaa havainnollistamaan yksityiskohtaisesti kontrolliympäristön eri komponentteja. Näin eri komponentit on helpompi ottaa huomioon erilaisia tietojärjestelmäprosesseja implementoitaessa (Moeller 2013; Rubino ja Vitola 2017). Lisäksi COBIT-viitekehyksessä korostuu liiketoimintalähtöisyys, mikä auttaa varmistamaan, että erilaiset implementoitavat prosessit tukevat organisaation liiketoimintatavoitteiden saavuttamista. COBIT-viitekehys auttaa yrityksiä paremmin integroimaan, kohdistamaan ja linkittämään prosessinsa organisaation asettamiin päämääriin ja tavoitteisiin. Lisäksi COBIT-viitekehys auttaa työntekijöiden osallistamisessa ja voimaantumisessa, sekä heidän vastuiden ja tehtävien selventämisessä. Viitekehyksen perusidea on se, että laadukkaan IT-kontrollin kannalta on välttämätöntä pohtia, millainen tieto on organisaation tavoitteiden toteutumisen kannalta olennaista. (Moeller 2013; Rubino ja Vitola 2017.)

Käytettiin apuna viitekehystä tai ei, jokaisessa organisaatiossa tulisi tiedostaa tarve tehokkaalle tiedonhallintamallille. Hallintamallin tulisi edesauttaa asianmukaista tiedonhallintaa ja IT-toimintojen johtamista. Hallintamallin tulisi myös valvoa kontrollivaatimusten täyttymistä kaikkien organisaatiossa toimivien tietojärjestelmien osalta. (Weill ja Ross 2004; Haislip, Masli, Richardson ja Watson 2015.) Kun otetaan huomion tietotekniikan laajamittainen käyttö useimmissa organisaatioissa, tarvitaan niiden valvontaankin koko organisaation kattavia kontrolleja. Hallintamalli toimii tämänlaisena organisaatiotason kontrollina. (Rubino ja Vitolla 2017.) Organisaatiotason kontrollien lisäksi Rubino ja Vitolla (2017) korostivat myös prosessitason IT-kontrollien merkitystä. Seuraavaksi esitellään tarkemmin sekä organisaatiotason että prosessitason IT-kontrolleja.

2.4.2 IT-Kontrollit

Usein tietojärjestelmät linkittyvät organisaation kaikkien prosessien, toimintojen ja yksiköiden läpi. Ne vastaavat myös merkittäviltä osin taloudellisen informaation tuottamisesta. Tietojärjestelmäkenttään kuuluu esimerkiksi myynti-, osto-, varastointi, kirjanpito-, ja henkilöstöhallinnon järjestelmät. Tietojärjestelmätoiminnot kattavat palvelintilat, tietoturvallisuuden, jatkuvuuden ja toipumisvalmiuden, virustorjuntaohjelmistot, sovellukset ja niiden kehityksen, projektityöskentelyn, tietoliikenteen sekä niihin liittyvät sopimukset. Koska tietojärjestelmät ovat levinneet laajalti koko organisaatioon, niiden hallinta luo oman haasteensa sisäiselle valvonnalle. (Benaroch, Chernobai ja Goldstein 2012; Ratsula 2016.s. 240). Tietojärjestelmien valvonnan apuna toimivat IT-kontrollit, jotka ovat yksi kontrolliympäristön osa. Koska tietojärjestelmien merkitys osana organisaation toimintaa jatkuvasti korostuu, voidaan ajatella IT-kontrollien merkityksen osana kontrolliympäristöä myöskin korostuvan (COSO, 2013; Masli, Richardson, Sanchez ja Smith 2011; Li, Peters, Richardson ja Watson, 2012).

Tietojärjestelmien korostuneen roolin vuoksi, jokainen organisaatio tarvitsee IT kontrolleja varmistamaan, että tiedonhallinta on tehokasta ja tuottaa asianmukaista tietoa organisaation käyttöön (Rubino ja muut 2017). Organisaatio tuottaa tietoa esimerkiksi

päätöksenteon tueksi, joten tietojärjestelmillä on tärkeä rooli tiedon oikea-aikaisuuden, luotettavuuden ja tarkkuuden varmistamisessa. Li ja muut (2012) totesivat tutkimuksessaan IT-kontrollien vaikuttavan positiivisesti tietojärjestelmien tuottaman tiedon laatuun. Lisäksi on huomioitava, että yritystoiminnan ollessa yhä kriittisemmin riippuvainen tietojärjestelmistä, niiden valvonnan ja kontrolloinnin merkitys korostuu. Tietotekniikalla ja tietojärjestelmillä on siis suuri vaikutus kontrolliympäristön komponentteihin. (Rubino ja muut 2017.)

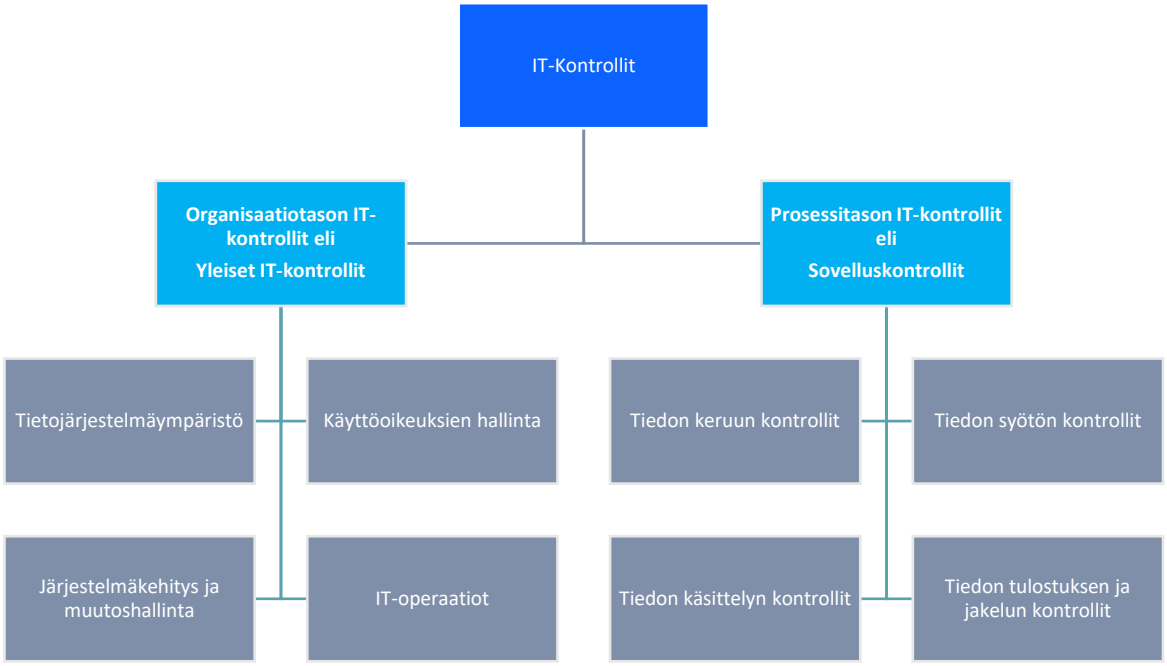
IT-kontrolleilla on esimerkiksi seuraavanlaisia tavoitteita (Ratsula 2016.s. 240-241):

- Tehokas IT-ympäristö
  - IT-strategia sekä henkilöstön roolien ja vastuiden selkeä määrittely
- Selkeä käyttöoikeuksien hallinnan prosessi
  - Käyttöoikeuksia valvotaan ja seurataan
- Turvatut IT-järjestelmät ja valvotut käyttöoikeudet
  - Estetään vaarallisten työyhdistelmien syntyminen ja käyttöoikeuksien väärinkäytökset
- IT-järjestelmämuutokset tehdään hyväksyttyjen käytäntöjen mukaisesti
  - Muutoshallinta epätoivottujen muutoksien ehkäisemiseksi
- Tietoturvan edistäminen
  - Asianmukaiset virustentorjuntaohjelmistot, varmuuskopiointijärjestelmät sekä fyysiset turvallisuustoimet.

Edellä mainittuja tavoitteita toteutetaan käytännössä IT-kontrollien avulla. Ne edustavat erillistä tietojärjestelmiin liittyvää sisäisen valvonnan luokkaa. IT-kontrollit jaetaan yleisiin IT-kontrolleihin ja Sovelluskontrolleihin (Ratsula 2016.s. 240-241). Yleiset IT-kontrollit liittyvät tietojenkäsittelytoimintaan ja hyvään tietohallintotapaan. Ne keskittyvät organisaatiotason käytäntöihin ja menetelmiin, joiden avulla pyritään hallitsemaan kaikkien organisaation sovellusten toimintaa. Yleensä yleisillä IT-kontrolleilla viitataan kontrolleihin, joilla varmistetaan, että kontrolliympäristö on asianmukainen ja ulottuu kaiken kokoisiin järjestelmiin. Nämä kontrollit valvovat suurtietokone- (mainframe), palvelin- ja

loppukäyttäjäympäristöjä. (Ratsula 2016 s. 245; Rubino ja muut 2017.) Sovelluskontrollit taas liittyvät tiettyihin tietokoneohjelmointisovelluksiin tai prosesseihin. (Ratsula 2016.s. 240-241; Rubino ja muut 2017). Ne ovat tiedon keruuseen, syöttämiseen, käsittelemiseen, tulostukseen ja jakelemiseen liittyviä toimenpiteitä. Niiden avulla pyritään varmistamaan tiedon olevan täydellistä, tarkkaa, asianmukaisten henkilöiden käsittelemää ja yhtenäistä. Sovelluskontrollit rakentuvat yleisten IT-kontrollien päälle. (Ratsula 2016 s.245; Rubino ja Vitolla 2014.) Näiden IT-kontrollien toiminta vaikuttaa organisaation IT-kontrolliympäristön toimintaan ja sen laatuun. Rubino ja Vitolla (2017) käyttivät tutkimuksessaan termejä organisaatiotason IT-kontrollit ja prosessitason IT-kontrollit. Tässä tutkielmassa käytämme jatkossa yleisten IT-kontrollien ja sovelluskontrollien sijaan termejä organisaatiotason ja prosessitason IT-kontrollit. Näin pyritään korostamaan tarkasteltavaa hallinnan tasoa.

Organisaatiotason IT-kontrollit siis valvovat kokonaisvaltaisesti kaikkien tietojärjestelmien toimintaa, infrastruktuuria ja useita erilaisia sovelluksia. Strategisella tasolla operoivat organisaatiotason IT-kontrollit tukevat prosessitason IT-kontrollien toimintaa, jotka voidaan nähdä operoivan enemmän operatiivisella tasolla. Yhdessä nämä erityyppiset kontrollit varmistavat organisaation tietojärjestelmien sujuvan toiminnan. (Ratsula 2016 s. 241-245; Rubino ja muut 2017.) Seuraavissa kappaleissa eritellään tarkemmin näitä kahta kontrollityyppiä ja esitellään käytännön kontrolleja molemmista kategorioista. Nämä eri kontrollityypit ja niihin kuuluvat kontrollit on esitelty alla Kuvio 5:ssä.



Kuvio 3 Erilaiset IT-kontrollit (Ratsula 2016).

2.4.3 Organisaatiotason IT-kontrollit

Tietojärjestelmät ovat jatkuvasti yhä kriittisempi liiketoimintatekijä. Ne kulkevat usean organisaatioyksikön läpi ja monet liiketoimintaprosessit ovat tiivisti sidoksissa tietojärjestelmien toimivuuteen. Tietojärjestelmien kriittinen asema ja laaja ulottuvuus huomioiden, on sisäisen valvonnan ja tiedonhallinnan tutkimuksen perusteella selvää, että organisaatioiden on otettava käyttöön erilaisia organisaatiotason kontrolleja tietojärjestelmien hallintaan. (Davenport, 2013; Rubino ja Vitolla 2017).

Organisaatiotason IT-kontrollien määritelmä saattaa vaihdella tutkimuksen ja tarkasteltavan näkökulman mukaan. Rubino ja Vitolla (2017) käyttivät nimitystä organisaatiotason IT-kontrollit, kun taas Ratsula (2016) käytti nimitystä yleiset IT-kontrollit. Davenport (2013) määritteli IT-kontrolliympäristön organisaatiotasolla operoiviksi kontrolleiksi, jotka pyrkivät varmistamaan, että organisaatiorakenne ja tehdyt organisaatiokonfiguroinnit ovat linjassa asetettujen liiketoimintatavoitteiden kanssa. Yksinkertaisuuden

vuoksi, tässä tutkielmassa käytetään kuitenkin organisaatiotason IT-kontrollien termiä erottamaan organisaatiotason ja prosessitason valvonta.

Organisaatiotason IT-kontrollit pyrkivät hallitsemaan riskejä liittyen organisaation henkilöstöön, tietoturvallisuuteen, IT-sovelluksiin ja ulkopuolisiin palveluntarjoajiin. (Ratsula s. 242.) Eräs organisaatiotason IT-kontrolli on tietojärjestelmäympäristö, joka koostuu organisaatiossa käyttöönotetuista toimintaperiaatteista ja menettelytavoista, tietojärjestelmäinfrastruktuurista ja sovelluksista. Näiden avulla toteutetaan liiketoimintastrategiaa ja pyritään edistämään liiketoimintatavoitteiden saavuttamista. (Ratsula 2016 s. 242-244.) Tätä kutsutaan myös hyväksi tiedonhallintatavaksi, jota käsiteltiin laajemmin COBIT-viitekehyksen yhteydessä kappaleessa 2.4.1. Hyvä tiedonhallintatapa ja COBIT-viitekehys.

Tehokkaan kontrolliympäristön kannalta tärkeimpiä kontrolleja ovat työtehtävien eriyttäminen ja käyttövaltuushallinta. Kriittiset ja riskiset työtehtävät yhdistettynä laajoihin käyttöoikeuksiin ovat vaarallinen yhdistelmä, joka johtaa kokonaisuuden kannalta tehottomaan lopputulokseen. Tämä johtuu siitä, että prosessissa aiemmin suoritettuihin kontrolleihin ei voida enää luottaa, koska ne on mahdollista kiertää. (Lahti ja Salminen 2014). Käyttövaltuushallinta korostuu, kun organisaatioiden tietojärjestelmäkenttä monimutkaistuu ja siten käytössä olevien järjestelmäkäyttöoikeuksien määrä kasvaa.

Käyttöoikeuksien hallinta viittaa menettelyihin, joilla rajoitetaan pääsyä organisaation tietojärjestelmiin ja dataan. Tallaisilla kontrolleilla hallitaan riskiä siitä, että oikeudettomasti tai valtuudettomasti päästään käsiksi dataan, tehdään kirjauksia tai muutoksia, käytetään ohjelmistoja tai ylipäätänsä otetaan käyttöön hyväksymätön ohjelma. Periaatteessa henkilöllä pitäisi olla pääsy vain niihin järjestelmiin, joita hänen työtehtäviensä suorittaminen vaatii. Liian laajat käyttöoikeudet lisäävät esimerkiksi väärinkäytösten riskiä. Tietoihin pääsyä kontrolloidaan käyttäjien tunnistamisella ja käyttäjien valtuuttamisella. Tunnistaminen hoituu käytännössä esimerkiksi salasanoilla, avainkorteilla ja biometrisillä tiedoilla. Valtuuttaminen tapahtuu säännöillä, joissa määritellään mihin

tietojärjestelmäresursseihin tunnistetulla käyttäjällä on pääsy. (Ratsula 2016 s. 242.) Käyttöoikeuksiin liittyvät kontrollit, olisi tehokkainta suorittaa käyttövaltuushallintaprosessin alkuvaiheessa, käyttöoikeuksien perustamisen ja muuttamisen yhteydessä. Järjestelmässä olisi esimerkiksi hyvä tehdä mahdottomaksi avata käyttöoikeuksia tietyissä tehtävissä työskenteleville henkilöille, vaarallisilta työyhdistelmiltä välttymiseksi. (Lahti ja Salminen 2014).

Järjestelmäkehitys ja muutoshallinta vastaa riskeihin, jotka liittyvät tietojärjestelmien suunnitteluun, kehittämiseen ja muutoshallintaan. Esimerkiksi tietoturva- tai muut liiketoimintariskit. Puutteelliset kontrollit voivat aiheuttaa sen, ettei käyttöönotettu tai päivitetty tietojärjestelmä vastaa odotuksia ja täytä organisaation tarpeita, jolloin liiketoiminnalliset tavoitteet jäävät saavuttamatta. Uusien tietojärjestelmien implementointi tai vanhojen muokkaaminen, tulisi aina järjestää liiketoimintaprosesseja vaarantamatta. Varsinaisena kontrollina toimii esimerkiksi järjestelmien testaaminen. Kaikki uudet päivitykset tulisi testata testiympäristössä, ennen kuin ne viedään tuotantoon ja otetaan käyttöön. (Ratsula 2016 s. 242-244.)

IT-operaatioiden avulla pyritään hallitsemaan riskejä niiden toteutumisen jälkeen. Niiden tulisi ongelmatilanteen sattuessa toimia välittömästi, jotta liiketoiminnan jatkuvuus turvataan. Esimerkiksi relevantin datan palautettavuus, virustorjuntaohjelmat ja turvalliset aineistonsiirtomenetelmät, datakeskusten ja servereiden fyysinen turvallisuus. Riskejä kontrolloidaan varmistamalla, että ennalta suunnitellaan havaittuja riskejä vastaavat toimintaohjeet, roolit ja vastuut, sekä ohjelmoidaan esimerkiksi järjestelmiin ennalta toimintaohjeet poikkeustilanteiden varalle. (Ratsula 2016 s. 244-245.)

Aiemmassa sisäisen valvonnan tutkimuksessa korostetaan myös organisaation henkilöstön merkitystä kontrolliympäristöön vaikuttavana tekijänä. Aiempi tutkimus nojaa esimerkiksi työvoiman jakautumiseen ja työntekijöiden ja liiketoimintayksiköiden välisiin suhteisiin. (Jajodia, List ja McGregor, 1997; Jajodia ja Strous 2004). Myöskin IT-kontrolliympäristön näkökulmasta on olennaista tarkastella ihmisten ja tietojärjestelmien

välistä vuorovaikutusta ja riippuvuussuhteita. Ihmisethän tietojärjestelmiä pääasiallisesti käyttävät. Yksi IT-kontrolliympäristön tavoitteista on varmistaa, että organisaatiorakenne ja henkilöstö mahdollistavat tavoitteiden mukaisen tietojärjestelmien kehittämisen ja käytön (Davenport, 2013; Rubino ja Vitolla 2017).

Rubino ja Vitolla (2017) kuvaavat organisaatiotason IT-kontrolleja organisaatiorakenteen kautta erityisesti henkilöstön ja organisaatiorakenteiden näkökulmasta. He ovat listanneet ensin organisaatiorakenteelle asetettuja vaatimuksia ja sitten organisaatiotason IT-kontrolleja, joilla näiden vaatimusten saavuttamista voidaan edistää (Rubino ja Vitolla 2017). Tätä prosessia on esitelty alla Kuviossa 3:

Kuvio 4 Organisaatiotason IT-kontrollit (Rubino ja Vitolla 2017).

Organisaatiotason IT-kontrollien tavoitteena on siis asianmukaisten sääntöjen ja menettelyjen laadinta, vastuiden määrittely, ja niiden noudattamisen varmistaminen, sekä työtehtävien riittävä eriyttäminen. (Janvir ja muut 2012; Rubino ja Vitolla 2017.) Nämä kontrollit ovat erityisen kriittisiä etenkin väärinkäytösriskien hallinnassa (Power 2013). Organisaatiotason IT-kontrollien avulla pyritään estämään tilanteet, joissa yhdelle henkilölle tarjoutuu mahdollisuus ohittaa sisäisen valvonnan kontrollit, ja tahallaan tai vahingossa

toimia organisaation liiketoimintatavoitteiden vastaisesti (Agoglia, Brown ja Hanno 2003).

2.4.4 Prosessitason IT-kontrollit

Ylätason hallintamallin ja muiden organisaatiotason kontrollien lisäksi tietojärjestelmät vaativat prosessitason IT-kontrolleja. Prosessitason IT-kontrolleista käytetään myös nimitystä sovelluskontrollit (Ratsula 2016). Eri liiketoimintaprosessit ovat erilaisia ja niihin liittyy erityyppisiä prosessikohtaisia riskejä. Näin riskienhallintaa ja sisäistä valvontaa tulisi harjoittaa myös prosessitasolla. Tehokas kontrolliympäristö vaatii asianmukaista integraatiota organisaatiorakenteiden ja liiketoimintaprosessien välillä. IT-prosessikontrollit valvovat tietojärjestelmien toimintaa liiketoimintaprosessitasolla. Ne toimivat yhdessä organisaatiotason IT-kontrollien kanssa varmistaakseen koko organisaation saumattoman toiminnan. (Rubino ja Vitolla 2017.)

Prosessienhallinta on kiinteässä yhteydessä tietojärjestelmäkehityksen kanssa, koska tietotekniikka tarjoaa laajasti prosessikehitykseen toimivia työkaluja. Näin prosessikontrollit ovat myös tiiviissä yhteydessä tietojärjestelmähallinnan kanssa (Laudon ja Laudon 2004). Koko organisaaton toiminta voidaan nähdä koostuvat yhteen nivoutuvista prosesseista. IT-prosessikontrollit pyrkivät määrittelemään ja hallitsemaan prosesseissa kulkevia tietovirtoja. Niiden avulla valvotaan organisaation tiedonvälitysprosesseja, sekä liiketoimien valtuuttamista ja hyväksymistä. (Rubino ja Vitolla 2017.)

Liiketoiminatavoitteiden toteutumisen kannalta ei riitä, että organisaatiossa määritellään tavoitteiden toteutumisen kannalta tarpeelliset säännöt, toimintaohjeet ja menettelytavat. Niiden lisäksi on selvitettävä, millaista tietoa organisaation prosesseissa liikkuu ja miten tätä tiedonkulkua hallitaan. Tiedonhallinta mahdollistaa liiketoimintatavoitteiden saavuttamisen, suoritettujen toimintojen onnistumisen seurannan sekä tarvittavien muutosten toimeenpanon. (Rubino ja Vitolla 2017.) Käytännössä tämä tarkoittaa sitä, että määrittelemällä millaista tietoa eri prosesseissa kulkee, on helpompi määritellä

tiedon laadun kannalta olennaiset riskit ja asettaa laadunvarmistuksen kannalta tehokkaat kontrollit.

IT-prosessikontrollit varmistavat, että päätöksenteon ja liiketoiminnan tukena käytettävä tieto on laadukasta ja eheää. Lisäksi ne varmistavat asianmukaisen tiedonkulun eri liiketoimintayksiköiden ja organisaatiotasojen välillä. (Rubino ja Vitolla 2017.) Saatavilla oleva, tarkka ja oikea-aikainen tieto edistää liiketoimintatavoitteiden ja sisäisen valvonnan tavoitteiden saavuttamista (Romney, Steinbart, Zhang ja Xu 2006). Tieto- ja tiedonvälitysprosessien sekä niistä saatavan tuotoksen laadunvarmistuksen merkitystä korostetaan useissa IT-viitekehyksissä. Esimerkiksi COBIT-viitekehyksessä organisaation IT-resursseja tarkastellaan erilaisina prosesseina. Erilaisten valvontakriteerien tulisi täyttyä jokaisen prosessin osalta. Näitä valvontakriteereitä ovat esimerkiksi toimivuus, tehokkuus, luottamuksellisuus, eheys, saatavuus, vaatimustenmukaisuus ja luotettavuus. (Rubino ja muut 2014b.) Tietotekniikkaa hyödynnetään etenkin prosesseissa, joissa kerätään, tunnistetaan tai muokataan eri lähteistä saatavaa tietoa ja varmistetaan sen asianmukainen toimittaminen (Dewett ja Jones 2004). Siten prosessitason IT-kontrollitkin usein valvovat näiden tehtävien toteutumista.

Tiedon keruun kontrollit pyrkivät verifioimaan tiedon lähteen ennen tietojen syöttämistä. Tunnistaminen voi tapahtua esimerkiksi allekirjoituksen avulla, mutta kontrollit on usein automatisoitu tietojärjestelmiin koneellisesti luettavin keinoin. Tiedon syötön kontrollit varmentavat syötettävän tiedon oikeellisuutta ja laatua. Varsinaisia kontrolleja ovat esimerkiksi juokseva numerointi, päivämäärätarkistukset, raja-arvotarkistukset, pakolliset syöttökentät, tuplasyötön estot ja limiittien tarkastukset. (Ratsula 2016 s. 245-249; Rubino ja Vitolla 2017.)

Tiedon käsittelyn kontrolleilla valvotaan syötetyn tiedon kulkua läpi prosessin. Ne varmistavat, että tiedon kulku sujuu aiotulla tavalla. Varsinaista tarkastusta ja kontrollointia voidaan toteuttaa esimerkiksi vertailemalla kontrollisummia ajovaiheiden välillä, tarkastamalla laskentaedellytysten täyttymistä, luomalla tiedon oikeellisuus- ja

rajatarkastuksia, sekä suorittamalla satunnaistarkastuksia kriittisiin tietoihin. (Ratsula 2016 s. 245-249; Rubino ja Vitolla 2017.)

Tiedon tulostuksen ja jakelun kontrollit varmistavat, että järjestelmien tuottama tulostus on asianmukaista ja oikeaa. Lisäksi niillä pyritään varmistamaan, että nämä tulosteet tulevat oikeaan käyttöön. Tulosteet eivät tässä asiayhteydessä tarkoita pelkästään fyysisiä paperitulosteita, vaan myös digitaalisessa muodossa ladattua ja jaettua tietoa. Varsinaisia kontrolleja ovat esimerkiksi päiväys ja kellonaika, sovelluksen nimi tai tunnus, tulosteen nimi, tilannepäivämäärä, sarakeotsikot, sivunumerointi sekä lukumäärä ja lopun yhteissumma. Erityishuomiota on kiinnitettävä tulostuksessa käytettäviin laitteisiin, niiden käyttöoikeuksiin ja tulosteiden suojaamiseen. (Ratsula 2016 s. 245-249; Rubino ja Vitolla 2017.)

Edellä mainitun IT-kontrollien kaksin jaottelun avulla voidaan havainnollistaa sitä, miten IT-kontrollien käyttöönotto ja kehittäminen käytännössä auttaa varmistamaan tietojärjestelmien asianmukaisen toiminnan ja miten ne käytännössä parantavat organisaation kontrolliympäristön laatua. Ensinnäkin asianmukaisilla IT-kontrolleilla tulisi olla positiivinen vaikutus organisaation tietojärjestelmien suunnitteluun, kehittämiseen, käyttöönottoon, tukemiseen ja hallintaan. Pääsääntöisesti organisaatiotason IT-kontrollit vaikuttavat positiivisesti tietojärjestelmiin liittyvien IT-infrastruktuurien hallintaan ja kehittämiseen, ja siten ne aktiivisesti vaikuttavat organisaatiorakenteen uudistamiseen ja siihen liittyvien roolien tunnistamiseen ja vastuiden asianmukaiseen jakamiseen. Prosessitason IT-kontrollit taas parantavat kontrolliympäristön laatua pääasiallisesti sisäisten ja ulkoisten raportointijärjestelmien kautta, parantamalla niiden tuottaman tiedon paikkansapitävyyttä, oikeellisuutta ja täydellisyyttä. (Rubino ja Vitolla 2017.)

3 Ohjelmistorobotiikka ja prosessiautomaatio

Tuotantoteollisuudessa on jo vuosia menestyksekkäästi käytetty teollisuusrobotteja erilaisten rutiininomaisten tuotantotehtävien automatisoinnissa. Nyt toimistotyö on samanlaisen murroksen keskellä. Vedder ja Guynes (2016) kutsuivat tätä murrosta botsourcingiksi. Nykypäivänä toimistotyöntekijän suorittamat rutiinityöt tapahtuvat liikuttamalla hiiren kursoria erilaisten ohjelmistojen välillä. Kun työtehtävät suoritetaan tuotantolinjojen sijaan tietokoneiden välityksellä ohjelmistoissa, siirtyvät tehtäviä automatisoivat robotitkin sinne. Tässä kappaleessa pyritään avaamaan tätä uutta automatisaation aaltoa ja esittelemään tarkemmin sen taustalla toimivaa teknologiaa. Ensin tutustutaan ohjelmistorobotiikan käyttöön ja teknologian leviämiseen organisaatioissa. Seuraavaksi käsitellään ohjelmistorobotiikkaan liittyviä riskejä ja hyötyjä omissa kappaleissaan. Lopuksi esitellään vielä ohjelmistorobotiikantutkimuksessa esille nousseita riskejä vastaavia kontrolleja.

Tietokoneohjelmistoissa suoritettavien tehtävien automatisointia robottien avulla kutsutaan ohjelmistorobotiikaksi (Robotic Process Automation, RPA). Ohjelmistorobotiikka mahdollistaa useiden säännönmukaisten tehtävien automatisoinnin jo olemassa olevissa tietojärjestelmissä. Robotti pystyy jäljittelemään ihmisen toimintaa ja voi siirtyä järjestelmästä toiseen ihmisen tavoin. (Denver 2020; IRPAAI 2018.) RPA toimii ratkaisuna niiden tehtävien automatisointiin, joita ei ole taloudellisesti järkevää automatisoida perinteisiä järjestelmiä käyttäen (Kaarlejärvi ja Salminen 2018 s. 53). Aivan kuten fyysiset tuotantolinjarobotit, ohjelmistorobotitkin automatisoivat rutiininomaisia tehtäviä, mutta tuotantolinjojen sijaan niiden toimintaympäristönä toimii eri ohjelmistoalustat. Se siis käyttää toista ohjelmistoa, kuten kirjanpitojärjestelmää, pääosin käyttöliittymän välityksellä, aivan kuten ihmisetkin (Salminen ja muut s. 53).

Ohjelmistorobotin tehtävänä on toistaa aiemmin ihmisvoimin suoritettu toiminto ennalta ohjelmoitujen ohjeiden mukaisesti (Salminen ja muut s. 53). Tallaisia toimintoja ovat esimerkiksi tiedon haku, siirto ja muokkaaminen (Lacity, Willcocks ja Graig 2015). Robotit eivät ole älykkäitä, ja toisin kuin tekoäly, ne pystyvät suorittamaan tietyn

tehtävän vain ennalta ohjelmoitujen ohjeiden mukaisesti (Denver 2020; Lacity, Willcocks ja Graig 2015). Ohjelmistorobotti täydentää perinteisten tietojärjestelmien automaatiota, esimerkiksi siirtämällä tietoa järjestelmien välillä, tehden täsmäytyksiä useiden tietolähteiden välillä, käynnistäen ajoja tai hoitaen prosesseja järjestelmän sisällä (Salminen ja muut s. 53).

3.1 Ohjelmistorobotiikan käyttö organisaatiossa

Ohjelmistorobotiikan yleistyessä on sitä käsittelevässä tutkimuksessa kiinnitetty huomiota teknologian leviämiseen ja siihen liittyviin kysymyksiin. Tässä kappaleessa esitellään ohjelmistorobotiikalle tyypillistä leviämistä käyttöönottavassa organisaatiossa, ja millaiset tekijät vaikuttavat tämän teknologian onnistuneeseen käyttöönottoon ja leviämiseen. Ohjelmistorobotiikan käyttö etenee usein kokeilun kautta. Useimmiten tämä toteutuu siten, että organisaatiossa toteutetaan ensin niin sanottu ”Proof of Concept”, eli pilotoidaan kokeilumielessä muutama prosessiautomaatio. Onnistuneiden kokeilujen kautta luottamus uutta teknologiaa kohtaan kasvaa ja ohjelmistorobotiikan käyttöä lisätään. Käytön lisääntyessä tarve ohjelmistorobotiikan hallinnalle ja keskitetylle ohjelmistorobotiikkaohjelmalle kasvaa. (Anagnoste 2018.) Mancher, Huff, Grabowski ja Thomas (2018) kehottavat käyttöönottavaa organisaatiota kiinnittämään alkuun huomiota palveluntarjoajan valintaan, henkilöstön kouluttamiseen, käyttöönottostrategiaan ja sidosryhmien sitouttamiseen. Nämä tekijät lisäävät onnistuneen ohjelmistorobotiikan pilotoinnin todennäköisyyttä.

Ensimmäisten robotiikkakokeilujen kannalta on tärkeää tunnistaa millaiset prosessit soveltuvat parhaiten automatisoitaviksi. Prosessiautomaatio kannattaa alkuun aloittaa mahdollisimman helppojen ja yksinkertaisten prosessien automatisoinnilla. Näin saadaan alkuun muutama onnistunut kokeilu, joiden perusteella ohjelmistorobotiikkaohjelman toimintaa voidaan edelleen kehittää. (Mancher ja muut 2018.) Tämän tyyppinen ”Proof of concept” mahdollistaa organisaatiokyvykkyyden testaamisen ennen kuin lähdetään investoimaan koko organisaationlaajuiseen ohjelmistorobotiikkaohjelmaan.

Aiemmassa tutkimuksessa on kiinnitetty paljon huomiota siihen, millaisia ominaisuuksia prosessiautomaatiolle soveltuvalta prosessilta vaaditaan. Taulukossa 1 on kerättynä erilaisista ohjelmistorobotiikantutkimuksista vaatimuksia ohjelmistorobotiikalla automatisoitavalle prosessille. Kokeiluvaiheessa automatisoitavien prosessien tulisi täyttää mahdollisimman monta Taulukon 1 vaatimuksista, jolloin onnistuneen pilotoinnin todennäköisyys kasvaa.

Vaatimukset ohjelmistorobotiikalla automatisoitavalta prosessilta	
Transaktioiden suuri määrä	Suurimääräiset ja jatkuvasti samanlaisena toistuvien transaktioiden automatisoiminen on helposti perusteltavissa (Slaby, 2012).
Riittävästi arvoa tuottavat transaktiot	Vaikka yksittäisten transaktioiden määrä ei olisikaan suuri, automatisaation ajurina voi toimia myös tietyn yksittäisen prosessin merkityksellisyys arvonluonnissa. Esimerkiksi erilaisissa 24/7 palveluissa, automatisoinnilla voidaan saavuttaa merkittäviä kustannussäästöjä (Sutherland, 2013). Automatisaation ajurina toimii näin yö-lisien takia suuret kustannussäästöt, eikä niinkään itse prosessin toistuvuus.
Useaan järjestelmään tapahtuva toistuva pääsy	Useiden järjestelmien välillä tapahtuvat prosessit vaativat usein erillisiä kirjautumisia ja mahdollisesti tietojen kopiointia järjestelmästä toiseen. Suorituskyky paranee, kun kirjautumiset ja tietojen kopioinnit on automatisoitu (Sutherland, 2013).
Vakaa ympäristö	Ennalta ohjelmoitava automatisointi vaatii stabiilin toimintaympäristön, jotta mahdollisia huomioon otettavia muutoksia on mahdollisimman vähän. (Asatiane ja Penttinen 2016; Slaby, 2012)
Vähäinen tarve inhimilliselle ajattelulle	Inhimillisen ajattelun tarve on usein esteenä prosessin automatisoinnille, ellei tarvittavaa subjektiivisuutta ja inhimillistä harkintaa pystytä toteuttamaan esimerkiksi tekoälyn avulla (Asatiane ja Penttinen 2016; Sutherland 2013).
Vähäinen tarve poikkeuksien käsittelylle	Automatisoitavassa prosessissa tulisi olla mahdollisimman pieni poikkeusmarginaali, koska poikkeuksien käsittely tulisi myös olla automatisoitavissa (Slaby 2012).

Manuaaliset ja inhimillisille virheille alttiit IT-prosessit	Inhimillisten virheiden poistaminen, on yksi automatisaation motivaattori. Mitä useampia muuttujia ja vaiheita manuaalisesti suoritettavissa prosesseissa on, ja mitä useamman järjestelmän välillä sitä suoritetaan, sitä useampi mahdollisuus inhimilliselle virheelle löytyy (Sutherland, 2013).
Helposti IT-prosesseiksi pilkottavat prosessit	Mitä pidemmästä ja monimutkaisemmasta prosessista on kyse, sitä vaikeammaksi automatisointi muuttuu. Mikäli prosessi voidaan pilkkoa selkeisiin ja yksiselitteisiin alaprosesseihin, automatisoitavia työtehtäviä on helpompi löytää (Slaby 2012).
Nykyisten manuaalisten kustannusten tarkka kartoittaminen	Asiaan perehtymättömien päättäjien, on helpompi tehdä päätöksiä prosessien automatisoinnista vertailemalla manuaalisia käyttökustannuksia ja sijoitetun pääoman tuottolukuja (Sutherland, 2013).

Taulukko 1. Vaatimukset automatisoitavalle prosessille (Fung, 2014; Slaby 2012).

Heti ensimmäisten ohjelmistorobottien käyttöönoton jälkeen on organisaation ryhdyttävä järjestämään ohjelmistorobotiikkaohjelman hallintamallia. Hallintamallin merkitystä tulisi korostaa jo heti ohjelmistorobotiikkatoimintaa käynnistettäessä, vaikka varsinaista tarvetta ei vielä muutaman robotin hallitsemiseksi ole. Myöhemmin kun ohjelmistorobotiikkaohjelman toiminta on levinnyt laajamittaisesti ympäri organisaatiota, tarve valmiille hallintamallille on jo huutava. (Mancher ja muut 2018.)

Organisaation johdon tulisi harkita jo varhaisessa vaiheessa, miten ohjelmistorobotiikkaohjelman toiminta järjestetään. Asianmukaisen hallintamallin järjestäminen ja ohjelmistorobotiikkastrategian luominen vaativat sen, että tiedetään, miten toimintaa ohjataan. Ohjelmistorobotiikkaohjelman kannalta on esimerkiksi kriittistä pohtia, miten robotiikkapalveluita tarjotaan liiketoimintayksiköille. Halutaanko ohjelmistorobotiikkaohjelman toiminta järjestää keskitetysti palvelukeskustyyppisesti vai halutaanko toiminta järjestää hajautetummin ympäri organisaatiota. (Mancher ja muut 2018; Asatiani ja muut 2019.)

3.2 Ohjelmistorobotiikan hyödyt

Ohjelmistorobotiikan hyödyt ovat pitkälti linjassa yleisesti automatisaatiolla tavoiteltujen hyötyjen kanssa. Tässä kappaleessa esitellään ohjelmistorobotiikkaa käsittelevässä kirjallisuudessa sekä tutkimuksessa esiin nousseita hyötyjä. Tavoiteltavat hyödyt ovat useimmiten liiketoimintaprosessien tehostamista sekä arvoa luomattomien ja pitkäveteisten prosessien eliminointia (Türkyılmaz ja Birol 2019). Tällä tarkoitetaan esimerkiksi asiantuntijatyön siirtämisellä manuaalisista työtehtävistä vaativampiin ja innovoivampiin inhimillistä ajattelua vaativiin tehtäviin. Lisäksi ohjelmistoroboteilla tavoitellaan usein toimintojen laadun parantumista kustannustehokkuuden, täsmällisyyden ja tuottavuuden kautta (Denver 2020).

Esimerkiksi talous ja kirjanpitotehtäviä hoitavat henkilöt joutuvat usein suorittamaan suuren määrän samankaltaisena toistuvia rutiinitehtäviä, jotka ovat omiaan automatisoitaviksi (Seasongood 2016; Vedder Guynes 2016). Robottien avulla voidaan eliminoida manuaalisia prosesseja, mikä säästää aikaa ja resursseja. Näin saadaan merkittäviä kustannushyötyjä ja mahdollistetaan organisaation tuottavuuden paraneminen. Robotit työskentelevät kellon ympäri vuoden jokaisena päivänä tauotta. Robotit eivät myöskään tee inhimillisiä virheitä eivätkä vaadi jatkuvaa kouluttamista. Tämä pienentää riskejä ja säästää aikaa. (Salminen ym s. 53; Seasongood, S 2016). Robottien arvioidaan muokkaavan organisaation henkilöstörakennetta siten, että yhä useampi prosessi, joka ei ole liiketoiminnan kannalta kriittinen eikä vaadi inhimillistä ajattelua, suoritetaan ihmisen sijaan ohjelmistorobotin toimesta (Moffitt, Rozario ja Vasarhelyi 2018).

Työvoimakustannukset ovat yrityksille usein yksi suurimmista kustannuseristä. Suuret työvoimakustannukset usein ajavat yrityksiä harkitsemaan eri toimintojen ulkoistamista halvemman työvoiman maihin, mikä on suuri ja riskinen investointi. Ohjelmistorobotiikan avulla on mahdollista alentaa tehokkaasti työvoimakustannuksia, erityisesti palkkoihin, ylitöihin, työetuihin sekä yleiskustannuksiin liittyen. Robotin lisensiointikustannus on usein halvempaa kuin kokopäiväisen työntekijän palkkaaminen (Seasongood 2016).

Robotit voivat toimia joko yhdessä ihmisten kanssa tai yksinään. Niiden avulla voidaan automatisoida kokonaisia prosesseja tai niiden osia. Prosessiautomaatio mahdollistaa työntekijöiden ajan ja voimavarojen siirtämisen yhä vaativampiin ja strategisesti merkittävämpiin työtehtäviin (Seasongood 2016). Käsiteltävien datamassojen kasvaessa ja laatustandardien noustessa toiminnan tehostaminen on välttämätöntä. Vaikka automatisaation usein pelätään johtavat irtisanomisiin ja työpaikkojen vähenemiseen, ohjelmistorobotiikan voidaan ennemminkin nähdä auttavan työntekijöitä suoriutumaan työtehtävistään tehokkaammin ja laadukkaammin (Lacity, Willcocks ja Craig, 2015). Manuaaliset työtehtävät ovat tekijöilleen usein ikävystyttäviä, joten näiden tehtävien automatisoinnilla on positiivinen vaikutus työn mielekkyyteen ja työhyvinvointiin. Lisäksi manuaalisten työtehtävien automatisoinnilla voidaan parantaa innovatiivisuutta, kun manuaalisten tehtävien sijaan voidaan keskittyä edellä mainittuihin inhimillistä ajattelua vaativiin strategisiin tehtäviin. (Seasongood 2016.)

Robottien käyttöönotto tukee myös hyvin palvelukeskusten toimintaa. Robotit toimivat samalla periaatteella ohjelmistojen ja systeemien kanssa, kuin työntekijät palvelukeskuksissa. Palvelukeskuksien menestyksellinen käyttöönotto vaatii toimintaprosessien ja toimintojen yhtenäistämistä, jotta ne voidaan keskitetysti suorittaa (Partanen 2005). Tallainen standardisointi luo otollisen ympäristön ohjelmistorobotiikan käyttöönotolle, sillä suurimmat hyödyt saadaan juuri toistuvia ja standardisoituja prosesseja automatisoimalla. Näin robottien avulla voidaan vähentää tai jopa poistaa riippuvaisuutta palvelukeskuksista. Myöskin aikaeroihin liittyvät haitat, jotka ovat ulkoisten palvelukeskusten yleinen ongelma, vähenevät merkittävästi robottien seurauksena. (Seasongood 2016; Lacity ja muut 2016).

Myös sisäisten asiakkaiden palvelukokemus paranee, kun tehtäviä, jotka aiemmin vaativat satoja ihmistyötunteja, voidaan nyt suorittaa merkittävästi nopeammin. Etenkin taloushallintoon liittyy paljon työtehtäviä, jotka voitaisiin delegoida robottien suoritettavaksi. Ohjelmistorobotit on suunniteltu toimimaan saumattomassa vuorovaikutuksessa jo olemassa olevien järjestelmien kanssa eivätkä ne vaadi tuekseen laaja-alaista IT-

tukiverkkoa. Näin ne ovat taloushallinnon henkilöstölle suhteellisen helposti omaksuttavissa osaksi päivittäistä toimintaa. (Seasongood, S 2016). Kun taloushallinnon prosessit tehostuvat, pystytään jatkuvasti kasvavaa datamassaa käsitellä samoilla panoksilla yhä nopeammin. Näin sisäiset asiakkaat saavat yhä parempaa palvelua, mikä hyödyttää koko organisaatiota.

Lisäksi on hyvä huomata, että ohjelmistorobotiikka vaatii käyttöönottavalta organisaatiolta vähemmän IT-asiantuntemusta ja perinteistä järjestelmäkehitystä. Tämän vuoksi ohjelmistorobotiikkaa voidaankin kuvata niin sanotuksi kevyt IT:ksi. Näin automatisaatiota on mahdollista toteuttaa liiketoimintalähtöisesti ja perinteistä IT-järjestelmäkehitystä kevyemmin. (Willocks, Lacity ja Craig, 2015.)

3.3 Ohjelmistorobotiikan riskit

Kun prosesseja suorittaa ihmisten sijaan ohjelmistorobotti muuttuvat myös niihin liittyvät riskit. Nämä uudenlaiset riskit on kartoitettava jo robottien käyttöönoton suunnitteluvaiheessa, jotta riskejä vastaavat valvontatoimenpiteet voidaan suunnitella ja käyttöönottaa ajoissa. Jos robotti jostain syystä toimii virheellisesti ilman toimivaa kontrollia, virheellinen toiminta saattaa jatkua pitkään. Tällä voi olla katastrofaaliset seuraukset. (Aalst, Bichler ja Heinzl 2018.)

Laajamittaiset riskit liittyvät usein hallitsemattomaan ohjelmistorobotiikan käyttöön ja leviämiseen organisaatiossa. Ohjelmistorobotiikan käyttöönotto ei varsinaisesti tarvitse tuekseen IT-osastoa, vaan sitä voidaan kehittää liiketoimintayksikkövetoisesti (Asatiani ja muut 2019; Willcocks ja muut 2015). Toisaalta ohjelmistorobotiikka on hyvin prosessikohtaista ja substanssiasiantuntijoiden prosessituntemus korostuu. Tämän vuoksi ohjelmistorobottien hallinta ja soveltuvan hallintamallin käyttöönotto on haastavaa. (Asatiani ja muut 2019.) Asatiani, Kämäräinen ja Penttinen (2019) havaitsivat tutkimuksessaan useita ohjelmistorobottien hallintaan liittyviä riskejä ja haasteita. Esimerkiksi

puutteellinen johtaminen automatisoitavien prosessien suhteen tai puutteellinen ohjelmistorobottien valvonta (Asatiani ja muut 2019).

Ohjelmistorobotteihin ei sinällään päde samanlaiset petos- ja väärinkäytösriskit kuin ihmisten suorittamiin prosesseihin liittyy. On kuitenkin huomioitava, että teknologian hyvin tunteva henkilö voi halutessaan ja olosuhteiden niin salliessa käyttää hyväkseen tilannetta, jossa robotti voi rajoituksetta toimia organisaation järjestelmissä. Ohjelmistorobotteihin liittyviä riskejä arvioitaessa on heti alkuun huomioitava käyttöoikeuksiin liittyvät riskit ja niiden hallinta. Ohjelmistorobotti toimii organisaation tietojärjestelmissä käyttäen samanlaisia käyttäjätunnuksia kuin ihmiset. Toisin kuin ihminen, ohjelmistorobotti on kuitenkin hakkeroitavissa. Vaikka robotti ei ymmärräkään väärinkäytöksen käsitettä, on erittäin riskistä olettaa, ettei robottien käyttöönoton jälkeen väärinkäytöksen mahdollisuutta enää ole. (Denver 2020). Organisaation on varmistettava, että heillä on tarpeeksi ohjelmistorobotiikkaan liittyvän teknologian tuntevia henkilöitä. Puutteellinen ohjelmistorobotiikkaosaamisen taso kasvattaa riskiä sille, ettei organisaatiossa pystytä tarpeeksi tehokkaasti kehittämään ja johtamaan ohjelmistorobotiikkaa ja automatisoituja prosesseja. (Denver 2020.) Jos esimerkiksi organisaatiossa on vain yksi teknologian tunteva henkilö, riski väärinkäytöksille ja aseman väärinkäytölle kasvaa. Robottien asianmukainen valvonta vaatii riittävän monipuolisesti asiantuntemusta robottien toiminnasta.

Ohjelmistorobotit voivat myös hidastaa ja vaikeuttaa innovointia. Robotit ohjelmoidaan toimimaan yhdessä selainpohjaisten sovellusten kanssa. Siten ne ovat riippuvaisia kaikista muutoksista näissä sovelluksissa. Jos IT-osaston on otettava käyttöön jokin uusi päivitys, korjaustiedosto tai lisälaite, on aina pohdittava miten tämä vaikuttaa järjestelmän kanssa toimiviin robotteihin. (DeBrusk, 2017). Robotit vaativat toimiakseen riittävän stabiilin toimintaympäristön. Toimintaympäristön tulisi pysyä suhteellisen muuttumattomana vähintään vuoden, jotta robotiikan käyttöönoton voidaan ajatella olevan kannattavaa (Slaby 2012). Tämän stabiilin toimintaympäristön ylläpitäminen ei luo optimaalista ympäristöä innovatiivisuudelle. Mikäli robotin merkitys osana tiettyä prosessia on suuri,

uusien potentiaalisten innovaatioiden kehittäminen ja käyttöönotto saattaa vesittyä robotin yhteistyökyvyttömyyteen. Lisäksi robottien osallisuus luo ohjelmistokehittäjille lisävaivaa, kun he joutuvat pohtimaan miten robotit reagoivat mihinkin muutokseen. Tämä hidastaa kehitystyötä.

Samaan aikaan on muistettava, etteivät robotit poista ydinalustojen uudelleenarvioinnin ja kehittämisen tarvetta. Kun robottien implementointistrategioiden vauhtiin päästään, helposti ne mielletään matalan kynnyksen ratkaisuna kaikkiin tehostamisongelmiin. Robotit kyllä mahdollistavat tuottavuuden parantamisen manuaalisten prosessien automatisoinnin kautta. Tietyissä tapauksissa muilla työkaluilla päästään kuitenkin parempaan tuottavuuteen ja kustannustehokkuuteen. Esimerkkeinä tämän tyyppisistä työkaluista on kokonaisvaltaiset prosessien digitalisoinnit, nopea prosessisuunnittelu, itsepalveluliittymät (Self-Service Interface, SSI) ja koneoppiminen. On tärkeää, että tehostustarpeisiin on käytössä useampia työkaluja, joiden soveltuvuutta pohditaan tapauskohtaisesti, jotta löydetään kuhunkin tilanteeseen parhaiten soveltuva ratkaisu. (Asatiani ja muut 2019; DeBrusk 2017.) Kun tarve automatisaatiolle herää, olisi hyvä pohtia useampia eri vaihtoehtoja, joista sitten valitaan kuhunkin tilanteeseen soveltuvin ratkaisu. Vaikka robottien implementointi olisi helpoin ratkaisu heränneeseen automatisaatiotarpeeseen, se ei automaattisesti tarkoita, että se olisi soveltuvin.

Monien yritysten IT-infrastruktuuri kärsii investointi- ja innovointivajeesta. Vaikka robottien avulla voidaan vapauttaa resursseja ja saavuttaa kustannussäästöjä, ne eivät poista organisaatioiden tarvetta kriittisesti tarkastella IT-resurssiensa kilpailukykyä ja nykyaikaisuutta. Onnistuneiden robotiikkainvestointien riskinä on se, että pienten roboteilla automatisoitujen prosessien avulla voidaan välttää laajamittaisten tietojärjestelmäinvestointialoitteiden kustannukset ja riskit. Tämä ei ole pitkällä aikavälillä menestyksellinen strategia. (DeBrusk 2017.) Toisaalta tutkimuksessaan Asatiani ja muut totesivat, että tallainen ajattelu voi myös estää ohjelmistorobotiikan käyttöä, kun se mielletään pelkäksi laastariksi varsinaisten IT-investointien tarpeeseen. Näin ohjelmistorobotteja saatetaan harkita vasta viimeisenä vaihtoehtona (Asatiani ja muut 2019).

Satunnaisten inhimillisten virheiden sijaan robottien tekemät virheet ovat järjestelmällisiä ja toistuvia. Robotit eivät reagoi positiivisesti pienimpiinkään käyttöliittymän muutoksiin, toisin kuin ihmiset, joita uudet ponnahdusikkunat tai pienet muutokset välilehden ulkoasussa eivät haittaa. Ongelmat robotin toiminnassa voivat aiheuttaa merkittävää tietojen vioittumista, koska virheen ilmeneminen on toistuvaa ja jatkuvaa. (DeBrusk 2017). Siten pieni pyöristysvirhekin voi kertaantuessaan muodostua isoksi ongelmaksi, ellei sitä huomata ja korjata ajoissa. Pienen virheen toistuminen potentiaalisesti useita kertoja sekunnissa, luo uniikin ja erityisesti ohjelmistoroboteille tyypillisen riskin, joka on syytä pitää mielessä teknologiaa hyödynnettäessä (Denver 2020).

Liian laajamittainen ja nopea ohjelmistorobottien käyttöönotto saattaa vaarantaa niillä tavoitellut hyödyt. Hallintamallin suunnittelu ja rakentaminen laajamittaisen käyttöönoton mahdollistamiseksi, saattaa syödä valtaosan käyttöönottobudjetista. Ellei ohjelmistorobotiikkaohjelman hallintaan riittävästi panosteta, ensimmäisistä automatisaatioprojekteista ei välttämättä saada tarpeeksi tehokkaita ja tuottavia. Näin robotiikkainvestointien menestykselle ei ole riittävää näyttöä, mikä voi vaarantaa koko automatisaatio-ohjelman. (DeBrusk 2017).

Lisäksi ohjelmistorobotit työskentelevät usein yhdessä ihmisten kanssa. Näin ohjelmistorobottien implementointiin liittyy muutosvastarinnan ja huonon muutosjohtamisen riski. Työntekijät voivat kokea etujensa mukaiseksi olla edistämättä robottien implementointia, koska niiden koetaan vaarantavan heidän työpaikkansa (Vedder ja muut 2016). Tämä on yleinen pelko, sillä automaatiosta usein seuraa ihmistyöntekijöiden tarpeen väheneminen, mikä pahimmillaan johtaa irtisanomisiin (Lacity ja muut 2016b). Tulevaisuudessa ihmisten ja robottien välinen kilpailu tulee todennäköisesti kiristymään. Ihmisten tekemä työ tulee muuttamaan muotoaan, kun robotit pystyvät suorittamaan yhä monimutkaisempia työtehtäviä. (King, Hammond ja Harrington 2017). Pelko ei siis ole täysin perusteeton. Ohjelmistorobottien tavoitteenahan on jäljitellä ihmisen tekemää työtä

(Aalst, Bichler ja Heinzl 2018). Tutkimuksessaan Drew (2015) havaitsi jatkuvan teknisen muutoksen aiheuttavan työntekijöissä stressireaktioita. Tämä lisää muutosvastarinnan riskiä yhä useampien työntekijöiden suunnalta.

Vaikka ohjelmistorobotit eivät varsinaisesti ole perinteinen itsenäisesti toimiva tietojärjestelmä, niiden käyttöön liittyy samanlaisia tietoturvallisuuskysymyksiä ja -riskejä, jotka on otettava huomioon ja arvioitava, jotta näitä riskejä voidaan hallita. Ohjelmistorobotiikkapalveluntarjoajilla on sekä pilvessä, että laitteistoissa (on premises) toimivia RPA-ratkaisuja. Molemmissa tapauksissa pätee näille eri vaihtoehdoille tyypilliset tietoturvariskit. Toisaalta itse ohjelmistorobotteihin harvemmin säilötään mitään kriittistä tietoa, mikä jo itsessään pienentää tietovuodon riskiä, vaikka robotti hakkeroitaisiinkin. (Denver 2020.) Tähän ei kuitenkaan pidä tuudittautua, vaan tietoturva-asiat on pidettävä mielessä, huomioiden alustat, joissa ohjelmistorobotti toimii ja tiedot, joita se käsittelee. Ohjelmistorobotteihin liittyviä riskejä arvioitaessa on arvioitava myös niiden järjestelmien turvallisuus, joissa robotti toimii (Denver 2020).

3.4 Ohjelmistorobotiikkaan liittyvien riskien hallinta

Kappaleessa 2 Organisaation kontrolliympäristö on esitelty erilaisia kontrolleja, joilla pyritään varmistamaan organisaation, prosessien, työtehtävien, ihmisten ja tietojärjestelmien asianmukainen toiminta. Ohjelmistorobottien suorittamiin prosesseihin liittyy samoja riskejä kuin ihmisten suorittamiin prosesseihin, mutta myös monia uusia riskejä. Tämä on otettava riskienhallinnassa huomioon. Onkin tärkeää tiedostaa ohjelmistorobottien ja niihin liittyvien riskien erityispiirteet ja se, miten niitä voidaan tehokkaimmin kontrolloida. Ohjelmistorobottien näkökulmasta sisäisen valvonnan perimmäinen tavoite on varmistua siitä, että ohjelmistorobotit saavuttavat niille asetetut liiketoimintatavoitteet (Denver 2020).

Ilman tehokasta kontrolliympäristöä, robotista voi olla enemmän haittaa kuin hyötyä. Tästä esimerkkinä Y2K nimeä kantava ohjelmistovirhe vuosituhannen vaihteessa.

Tietokoneiden muistia säästääkseen, organisaatioissa käytettiin vuosiluvuista kaksimerkkistä lyhennettä, esimerkiksi 95 1995 sijasta. Vuosituhannen vaihtuessa tämä osoittautui ongelmalliseksi, koska 00 saattoi tarkoittaa vuotta 1900 tai 2000. (Schiano ja Weiss 2006; Westland 2000). Y2K-ohjelmistovirheen syynä oli pitkälti puutteellinen kontrolliympäristö. Tietotekniikkasovellusten jatkuvasti monimutkaistuessa, valvontajärjestelmät, laadunvarmistus ja hallintamallit eivät pysyneet kehityksen mukana. Näin yritykset joutuivat käyttämään mittavat panokset jäljittääkseen virheiden lähteet ja eliminoidakseen ne kriittisistä toiminnoistaan. (DeBrusk 2017.)

Nykyisessä dynaamisessa tuotantoympäristössä tapahtuu yhä useammin erilaisia poikkeamia. Tätä varten organisaatiolla tulisi olla sisäänrakennettuna toipumismekanismit ja toimintaprosessit, joiden avulla hallitaan poikkeamista aiheutuvat riskit. (Merdan, Lepuschitz ja Axinia 2011.) Kun tietotekniikkaan luotetaan sokeasti eikä tarvittavia kontrolleja ole varmistamassa automatisoidun prosessin asianmukaista toimintaa, vaikutukset voivat olla mittavat (Aalst ja muut 2018). Ohjelmistorobottien suunnittelu- ja käyttöönottovaiheessa on huolehdittava riittävästä automatisoitavien prosessien standardisoinnista, sekä asianmukaisten prosessien ja standardien noudattamisesta, jotta vältytään Y2K tyyppisiltä ehkäistävissä olevilta virheiltä (DeBrusk 2017). Käytännössä sisäistä valvontaa toteutetaan valvontatoimenpiteiden eli kontrollien avulla. Robottien käyttöönoton myötä, tulee organisaatiossa ottaa käyttöön erilaisia valvontatoimenpiteitä.

Ohjelmistorobottien yleinen hallinta, johtaminen ja valvonta on hyvä suunnitella heti ensimmäisen ohjelmistorobotin käyttöönottoa suunnitellessa. Ohjelmistorobottien käyttöönotto harvemmin jää vain yksittäisen työtehtävän automatisointiin. Usein ohjelmistorobottien avulla pyritään tehostamaan useampia manuaalisia tehtäviä. (Anagnoste 2018). Laajamittainen käyttöönotto vaatii tarvittavat organisaatiotason kontrollit. Koko robotiikkaohjelman hallinta ja johtaminen on järjestettävä niin, että jokaiselle aktiiviselle robotille on määriteltynä sen toiminnasta ja hallinnasta vastuussa oleva taho (Denver 2020). Asatiani ja muut (2019) korostivat tutkimuksessaan, että ohjelmistorobottien hallintamallissa tulisi pystyä huomioimaan paikalliset liiketoimintayksikköjen tarpeet sekä

organisaatiotasolla asetetut politiikat ja säännöt. Robotiikkaohjelman hallinnan tavoitteet ovat pitkälti linjassa kappaleessa 2.4 Tiedonhallinta ja IT-kontrolliympäristö esiteltyjen organisaatiotason IT-kontrollien kanssa.

Ohjelmistorobotiikan johtamisessa auttaa selkeä toiminnanohjauksen strategia sekä toimintaa ohjaava hallintamalli. Lacity ja Willcocks (2016b) pohtivat tutkimuksessaan tehokkaan prosessiautomaation mahdollistavia tekijöitä. Tutkimuksessa korostettiin keskijohdon sitouttamista ohjelmistorobotiikkaohjelman vision mukaiseen toimintaan, sekä liiketoimintayksiköiden sitouttamista pelkän IT-osaston sijaan (Lacity ja muut 2016b). Sitouttamisen lisäksi prosessin automatisoinnissa on kriittistä kartoittaa prosessin kulku. Prosessia suorittavien avainhenkilöiden asiantuntemus on tarpeen, jotta automatisoitavasta prosessista saadaan mahdollisimman todenmukainen kuvaus. (DeBrusk 2017; Fung 2014.) Prosessien avainhenkilöt saattavat myös poistua organisaatiosta, jolloin he vievät mukanaan inhimillisen pääomansa. Tämän tyyppisissä tilanteissa on tärkeää, että prosessit on tarkasti kuvatut.

Ohjelmistorobotit ovat ohjelmistokoodia, ja niitä tulisi siis käsitellä sellaisina. Robottien toimintaa tulisi pystyä valvomaan asianmukaisilla IT-kontrolleilla. Ohjelmistorobottien suunnittelussa tulee keskittyä prosessien standardisoitavuuteen, toistuvuuteen ja sen osien eriyttämiseen, jotta ne voidaan asianmukaisesti kartoittaa ja versioida. Prosessien kartoittaminen ja versiointi on tärkeää asianmukaisten laadunvarmistusprosessien ja kontrollien luomiseksi. Lisäksi prosessin automatisoinnin yhteydessä tulee koordinoida aktiivisesti ja tarkasti palveluntarjoajien ja kolmansien osapuolten, esimerkiksi ulkopuoliset koodarien ja muiden ohjelmistokehittäjien, kanssa. (DeBrusk 2017)

Tärkeä kontrolli on myös se, että robotit otetaan tuotantoon samojen testausprosessienkautta kuin kaikki muutkin organisaation ohjelmistosovellukset. (DeBrusk 2017.) Implementoimalla ohjelmistorobotteja IT-infrastruktuuriinsa, yritykset luovat joukon riippuvuussuhteita, joita on pystyttävä dokumentoimaan asianmukaisesti. Mikäli riippuvuussuhteita ei ole dokumentoitu, on hankalaa sopeuttaa robotteja ohjelmistomuutoksiin tai

jäljittää havaittuja virheitä robottien toteuttamissa prosesseissa. Näin ydinjärjestelmien muokkaamista on pystyttävä kontrolloimaan, ja muokkaukset ja päivitykset on testattava ja tarkastettava. Näin varmistetaan, ettei robottien skriptejä rikota. (DeBrusk 2017.) Ilman asianmukaisia kontrolleja, kokonaisuutta on vaikeaa hallita. Esimerkiksi suoritettava ohjelmistopäivitys ei vaikuta pelkästään päivitettävän ohjelmiston toimintaan, vaan myös robotteihin, jotka ovat tekemisissä tämän ohjelmiston kanssa. Muutoshallinnan merkitys korostuu, jotta dokumentoiduista riippuvuussuhteet osataan ottaa huomioon ennen muutoksen toimeenpanoa. (Ratsula 2016 s. 242-244.)

Robotti toimii aina ennalta ohjelmoidusti, joten se ei ymmärrä toimivansa haitallisesti eikä osaa kysyä neuvoa tai lopettaa toimintaansa, ellei sitä niin ole ohjelmoitu tekemään. Osittain tätä riskiä voidaankin pienentää hyvällä ohjelmoinnilla, mutta se vaatii hyvää suunnittelua ja ennakointia, sekä asianmukaista riskien arviointia. (DeBrusk 2017.)

4 Tutkimusteemojen johtaminen ja teoreettinen viitekehys

Tässä kappaleessa esitellään tarkemmin tutkimuksen toteutustapaa ja metodologisia valintoja. Alakappaleissa esitetään tarkemmin tutkimuksessa sovellettuja tutkimus-, tiedonkeruu ja aineistonkeruumenetelmiä sekä perustellaan tehdyt menetelmävalinnat. Tarkoituksena on auttaa lukijaa ymmärtämään miten menetelmävalinnat tukevat tutkimustavoitetta. Tutkimuksen tavoitteena on tarkastella millaisia vaatimuksia ohjelmistorobotiikan käytön ja käyttöönoton yleistyminen asettaa organisaation kontrolliympäristölle. Toisin sanoen, tarkoituksena on saada syvempää ymmärrystä siitä, miten organisaation valvontatoimenpiteiden tulisi muuttua, kun työtehtäviä suorittaa ohjelmistorobotti ihmisen tai perinteisen tietojärjestelmän sijaan.

4.1 Tutkimusmenetelmä

Tutkimus on toteutettu laadullisena tutkimuksena. Laadullinen tutkimus on toinen tieteellisen tutkimuksen kahdesta pääasiallisesta suuntauksesta (Mack, Woodsong, MacQueen ja Guest 2005). Laadullisen tutkimuksen tavoitteena on antaa kattava katsaus tutkittavaan ilmiöön sen tavanomaisessa toimintaympäristössä (Hirsijärvi, Remes ja Sajavaara 2004, 152). Tarkastelussa korostuu inhimillinen näkökulma, koska tavoitteena on asiantuntijoiden havaintojen ja kertomusten kautta ymmärtää ja kuvata ilmiötä (Eskola ja Suoranta 1998, 61). Laadullinen tutkimusmenetelmä soveltuu hyvin kartoittavaksi tutkimukseksi aiheille, joista ei vielä ole toteutettu laajalti aiempaa tutkimusta (Eriksson ja Kovalainen 2008, 5). Laadullinen tutkimus soveltuu hyvin myös jo laajemmin tutkitun aihealueen uusien vielä tutkimattomien osien kartoittamiseen (Järvinen 2004, 66).

Laadullinen tutkimus on usein tapaustutkimusta, jossa tutkimuksen painopiste on toiminnan tai ilmiön merkityksen tulkinnassa (Järvinen ym 2004, 68). Tässäkin tutkimuksessa tutkimusstrategiana on käytetty tapaustutkimusta. Tällä tarkoitetaan empiiristä tutkimusta, jossa tutkimuksen kohteena on joku todellisen elämän tapahtuma tai ilmiö (Eskola ja Suoranta 1998, 65). Tapaustutkimus soveltuu hyvin sellaisiin tilanteisiin, joissa

pyritään etsimään vastauksia kysymyksiin *miksi* ja *miten* (Yin 1994). Tapaustutkimus soveltuu tilanteisiin, joissa tutkijalla ei ole merkittävästi tarvetta ohjata tutkimuksen kulkua, vaan tavoitteena on laadulliselle tutkimukselle tyypilliseen tapaan tarkastella ajankohtaisia ilmiöitä niiden luonnollisessa ympäristössä (Benbasat, Goldstein ja Mead, 1987). Näin tapaustutkimus soveltuu erinomaisesti tuoreiden ilmiöiden tarkasteluun, niin sanottuna kartoittavana tutkimuksena. Tällöin tavoitteena on saada uusia näkökulmia vielä suhteellisen tuntemattomasta aiheesta. (Hirsijärvi ja Hurme 2008: 11, 35; Hirsjärvi, Remes ja Sajavaaran 2014 s. 129). Ohjelmistorobotiikka on vielä suhteellisen tuore ilmiö, ja sen käyttö on vasta viimevuosien aikana yleistynyt, joten akateemista tutkimusta aiheesta on vasta suhteellisen vähän. Siten aiheen tutkimiselle tapaustutkimuksen kautta on otolliset olosuhteet.

Ilmiöiden tutkiminen niiden luonnollisessa ympäristössä mahdollistaa havainnoinnin kautta uusien teorioiden kehittämisen. Tämän tyyppinen havainnointi ei välttämättä vaadi tuekseen ilmiötä ennalta selittävää teoriaa. (Benbasat ja muut 1984). Ohjelmistorobotiikan valvontaan liittyvää tutkimusta on tehty vasta suhteellisen vähän. Tämän tyyppiset tutkimukset ovat vielä vahvasti kartoittavassa vaiheessa, eikä selkeää teoreettista viitekehystä ollut selkeästi käytettävissä. Tämän tutkimuksen teoreettinen viitekehys on yhdistelty erikseen ohjelmistorobotiikkaa ja sisäistä valvontaa käsittelevästä tutkimuksesta.

4.2 Tutkimuksen kohde

Tapaustutkimuksen kohteena on usein tietty prosessi, toiminto tai tapahtuma jossain tietyssä kohdeorganisaatiossa (Koskinen, Alasuutari, ja Peltonen, 2005, s. 157). Tutkimuksen kohteena on suomalainen asiantuntijaorganisaatio, joka tarjoaa esimerkiksi varmennus- ja asiantuntijapalveluita. Ohjelmistorobotiikkaan liittyvää asiantuntijuutta organisaatiosta löytyy sekä sisäisten kehitysprosessien kautta, että ulkoisille asiakkaille annettavien varmennus- ja asiantuntijapalvelluiden kautta.

Haastateltavilla on siis kokemusta, sisäisestä ohjelmistorobotiikan kehityksestä tai asiakasorganisaatioiden ohjelmistorobotiikkaratkaisuista. Haastateltavilla oli kokemusta joko UiPath tai BluePrism palveluntarjoajien ohjelmistorobotiikkasovelluksista ja järjestelmistä. Organisaatiossa ohjelmistorobotiikkaa ohjataan keskitetysti.

4.3 Aineistonkeruumenetelmä ja tutkimusmalli

Tutkimuksen kohteen ollessa uusi ilmiö, on teemahaastattelu yleisesti käytetty aineistonkeruun menetelmä. Menetelmän tavoitteena on saada syvää ymmärrystä tutkittavasta ilmiöstä ja sen vaikutuksista (Rubin ja Rubin 2005: 2-3). Kyselylomakkeella kerättävä aineistonkeruu tuottaa suoraviivaisia ja binäärisiä kyllä tai ei vastauksia, kun taas haastatteluiden perusteella voidaan pureutua syvemmälle syihin ja seurauksiin sekä tehdä tarkennuksia ja esittää lisäkysymyksiä molemminpuolisen ymmärryksen parantamiseksi. Haastatteluissa kysymyksiä voidaan tarkentaa ja tavoitteita selventää havainnollistavin esimerkein. (Hirsjärvi ja Hurme 2008: 35–36.)

Puolistrukturoidussa haastattelussa haastattelija puuttuu haastatteluun siten, että sitä ohjataan haluttuun suuntaan tarkentavilla kysymyksillä. Rakenne on jokseenkin ennalta määritelty, muttei kuitenkaan täysin strukturoitu, kuten esimerkiksi lomakehaastattelussa. (Hirsjärvi ja Hurme 2008: 35–36.) Haastattelulle on ennakkoon määritelty suhteellisen löyhät aihealueet, joiden pohjalta keskustelua käydään (Ghauri ja Grønhaug 2002, 101).

Kattavan aineiston keräämistä tavoiteltiin siten, että haastatteluihin pyrittiin saamaan alan asiantuntijoita erilaisista tehtävistä. Haastatteluaineistoa pyrittiin keräämään henkilöiltä, joilla olisi erilaisia näkemyksiä ohjelmistorobotiikasta, sekä niiden kontrolloinnista. Haastateltavia henkilöitä pyrittiin kokoamaan erilaisista rooleista ja henkilöistä, joilla on mahdollisimman monipuolisesti erilaisia näkemyksiä ohjelmistoroboteista ja niiden kontrolloinnista. Näin ollen haastattelukysymykset ja haastattelun eteneminen saattoivat vaihdella suhteessa haastateltavan henkilön asiantuntija-alueeseen. Kunkin

haastattelun aikana ja jälkeen tehtyjen havainnointien seurauksena, tutkimuskysymyksiin tehtiin tarvittaessa muokkauksia ja tarkennuksia. Näin pyrittiin syventämään ymmärrystä ja tuomaan esille uusia näkökulmia haastatteluissa esille nousseista aiheista.

Haastateltavat valittiin lumipallo-otantaa (*snowball sampling*) hyödyntäen. Lumipallo-otannassa etsitään aluksi organisaation avainhenkilöitä, joilta tiedustellaan haastatteluun soveltuvia henkilöitä. Haastattelun yhteydessä haastateltavilta henkilöiltä kysytään edelleen sopivia haastateltavia henkilöitä. Lumipallo-otantaa jatketaan, kunnes soveltuvia haastateltavia ei enää löydy tai aineisto saturaatio saadaan riittävälle tasolle. (Hirsjärvi ja Hurme 2000.) Saturaatiolla tarkoitetaan sitä, että empiirinen aineisto saavuttaa kyllästymispisteen, jossa hankittu tieto alkaa toistaa itseään, eikä varsinaisesti tuo enää uusia näkökulmia käsiteltävään aiheeseen (Eskola ja Suoranta 1998, 62–216). Luotettavuuden varmistamiseksi suoritettiin useita haastatteluja, kunnes todettiin, että haastatteluissa ilmenneet näkökulmat alkoivat olemaan hyvin samankaltaisia. Lukumääräisesti haastattelujen määrä on suhteellisen pieni.

4.4 Aineistonkeruu ja aineiston analysointi

Haastateltavat henkilöt kerättiin ottamalla sähköpostitse yhteyttä organisaation avainhenkilöihin. Lumipallo-otantaa soveltamalla kerättiin haastateltavia organisaation eri osastoilta, jotta aihealueesta saatiin mahdollisimman laaja näkökanta. Näkökulman laajentamiseksi haastatteluihin osallistui henkilöitä, joilla on kokemusta sisäisen kehittämisen lisäksi ulkoisille asiakkaille konsultoinnista sekä prosessiautomaatiojärjestelmien tai itse robottien auditoinneista. Haastateltavien valinnassa pyrittiin kokoamaan tarkoituksenmukainen otos. Tarkoituksenmukainen otos on sellainen, että valituilla asiantuntijoilla on tutkittavan aiheen näkökulmasta tarvittava kokemus, ominaisuudet ja tieto (Silverman 2000, 104). Haastateltavat asiantuntijat on esitelty alla Taulukossa 2:

Haastateltava:	**Nykyinen ammatti-nimike:**	**Tausta ohjelmistorobotiikkaan ja sisäiseen valvontaan liittyen:**
Asiantuntija 1	Controller	Toiminut osana virtuaalista RPA-hankeryhmää 4 vuoden ajan. On osana useissa organisaation sisäisissä RPA-hankkeissa.
Asiantuntija 2	IT-Asiantuntija, konsultti	Toiminut ohjelmistorobotiikan konsulttina, jolloin ollut mukana automatisoitavien prosessien määrittelyssä, robottien kehittämisessä, testauksessa ja käyttöönotossa. Nyt toimii IT-asiantuntijana ja toisinaan tuottaa ohjelmistorobotiikan potentiaalianalyysejä ulkoisille asiakkaille. Lisäksi ohjelmistorobotiikka vahvasti läsnä asiakasorganisaatioiden IT-ympäristöjä, joihin liittyen nykyään konsultoi.
Asiantuntija 3	Ohjelmistorobottikehittäjä, konsultti	Osana organisaation Enterprise Design Services -tiimiä. Sertifioitu RPA-kehittäjä, joka on ollut mukana sisäisissä automaatioprojekteissa, mutta myös asiakasprojekteissa.
Asiantuntija 4	IT-tarkastaja	Tällä hetkellä toimii IT-tarkastajana ja data-analyytikkona. Omaa taustaa myös ohjelmistokehittäjänä. Ohjelmistorobotiikka näkyy työssä osana auditoitavia IT-järjestelmiä sekä varsinaisena robottien auditointina.
Asiantuntija 5	Tietoturvapäällikkö, konsultti	Organisaation tietoturvapäällikkönä toimiminen, sekä tietoturva-asiantuntijan tehtävät, erityisesti hallinnolliseen tietoturvaan liittyen. Ohjelmistorobotiikka näkyy työssä osana asiakas ja kohdeorganisaation tietoturvaympäristöä.
Asiantuntija 6	Johtaa organisaation prosessiautomaatiopalveluita	Johtaa organisaation älykkään automaation palveluita. Roolissaan vastaa ulkoisille asiakkaille tarjottavista palveluista sekä sisäisestä automaatiokehittämisestä.

Taulukko 2. Haastateltavien asiantuntijoiden esittely

Haastattelut suoritettiin 12.10-26.10.2020 välisenä aikana. Haastatteluista kaksi suoritettiin lähihaastatteluina ja loput neljä etänä Teams-sovelluksen kautta. Haastatteluiden keskimääräinen kesto oli 55,5 minuuttia. Kunkin haastattelun ajankohta ja kesto löytyy alla olevasta Taulukko 4:stä:

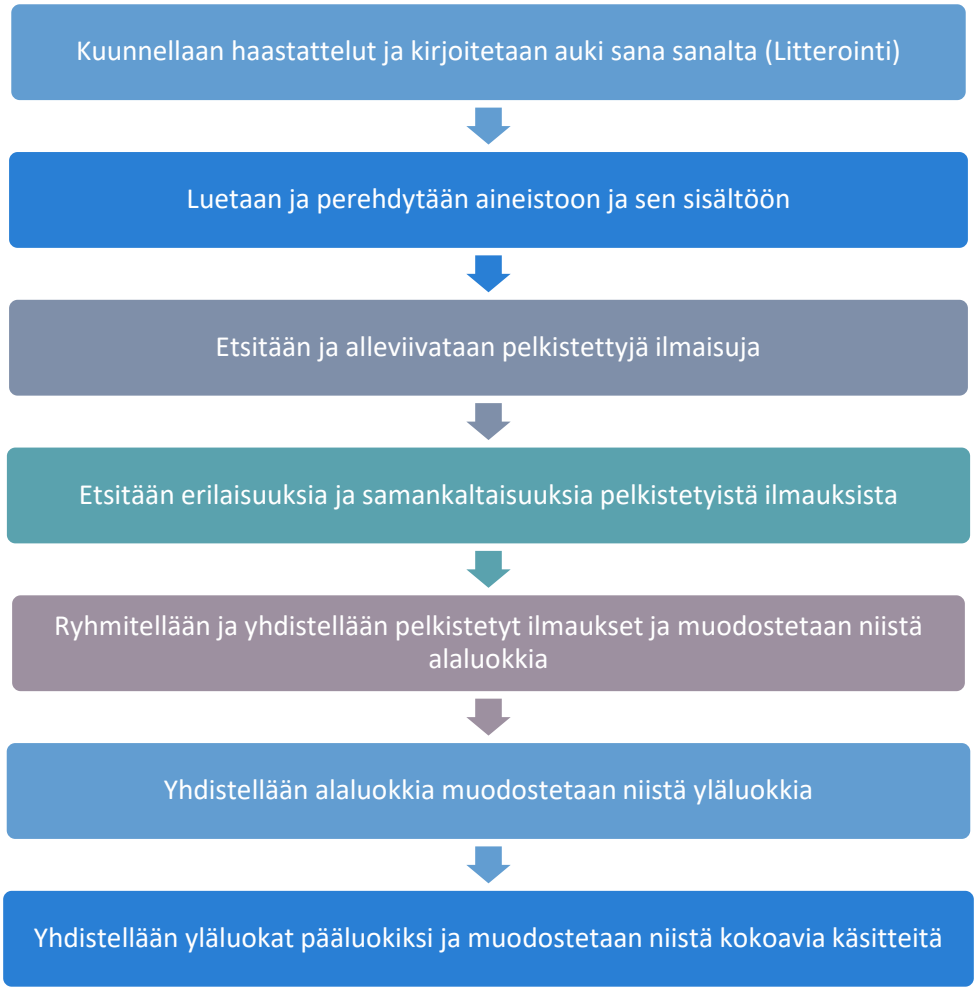
Haastateltava	**Päivämäärä**	**Haastattelun kesto**
Asiantuntija 1	12.10.2020	58 minuuttia
Asiantuntija 2	14.10.2020	53 minuuttia
Asiantuntija 3	14.10.2020	61 minuuttia
Asiantuntija 4	15.10.2020	52 minuuttia
Asiantuntija 5	16.10.2020	56 minuuttia
Asiantuntija 6	26.10.2020	54 minuuttia

Taulukko 3. Haastattelujen ajankohta ja kesto

Aineistoanalyysi alkaa jo haastattelutilanteessa haastattelijan tekemän havainnoinnin kautta (Hirsjärvi ja Hurme 2008: 136–137). Tutkija teki haastattelujen aikana muistiinpanoja tekemistään havainnoista ja haastatteluissa heränneistä kysymyksistä. Kun haastattelut oli suoritettu, ne purettiin haastattelujen aikana nauhoitettujen nauhoitteiden litteroinnilla. Kaikki haastattelut on litteroitu alusta loppuun 48tunnin sisällä haastattelujen suorittamisesta. Mahdollisimman nopeasti haastattelun jälkeen suoritettu litterointi parantaa aineiston laatua (Hirsjärvi ja Hurme 2008: 185). Lisäksi litteroinnin yhteydessä tehtiin havaintoja ja aineiston analysointia, reflektoimalla haastattelun aikana tehtyihin muistiinpanoihin ja havaintoihin. Litteroinnin jälkeen aineistosta poistettiin kaikki salassa pidettävä aineisto ja tunnistetiedot.

Tutkimusanalyysissä hyödynnettiin teoriaohjaavaa aineistoanalyysiä, jonka tavoitteena on antaa teorian ohjata tutkimuksen etenemistä. Lähtökohtaisesti analyysissä noudatetaan induktiivista päättelyä, mutta tutkimusta pyritään ohjaamaan valittua teoriaa tai viitekehystä soveltamalla. (Tuominen ja Sarajärvi 2018.) Tutkimuksessa tämä näkyy siten,

että tutkija on ensin tutustunut aiempaan aihealuetta käsittelevään tutkimukseen ja aineistoon, ja sen pohjalta on johdettu haastatteluiden pohjana käytetyt teemat. Haastatteluaineiston purkamisen ja aineistoanalyysin apuna käytettiin Tuomi ja Sarajärven (2018) kuvaamaa aineistolähtöisen sisällönanalyysin prosessia (Kuvio 9). Aineiston purkamisessa ja analysoinnissa ei seurattu alla olevan prosessin jokaista vaihetta, mutta sitä sovellettiin aineistoanalyysin apuna.



Kuvio 5 Aineistolähtöisen sisällönanalyysin eteneminen (Tuomi ja Sarajärvi, 2018)

Jokainen haastattelu noudatti ennalta määriteltyä neljää teemaa. Litteroinnin jälkeen jokaiselle litteroidulle haastattelulle annettiin oma väri ja haastattelut ryhmiteltiin teemojen mukaisesti siten, että haastattelut olivat värikoodein eroteltavissa. Tämän jälkeen aineiston purkamista jatkettiin edelleen teemoittain. Ryhmittelyä tehtiin kontrollityypeittäin sekä tutkimuksen tarkastelutasojen perusteella. Näin tutkimusaineistosta muodostettiin alaluokat, mihin perustuen tutkimustuloksia alettiin muodostamaan. Aineistoanalyysin perusteella tehty ryhmittely ja aineistoanalyysin tulokset on esitelty tarkemmin seuraavassa tutkimustuloksia käsittelevässä kappaleessa.

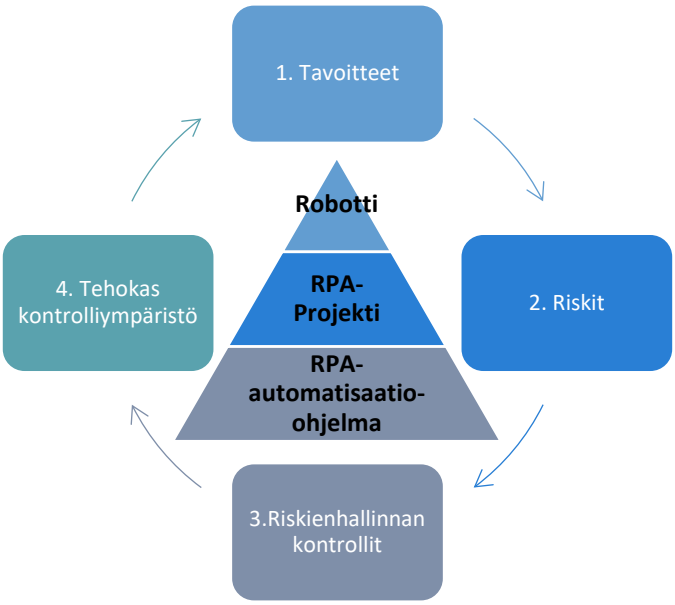
Teoreettinen viitekehys ja haastattelun teemat viestittiin haastateltaville etukäteen ennen haastatteluja (kts. Liite 1. Haastattelukutsu). Teoreettisessa viitekehyksessä on määritelty kolme tarkasteltavaa tasoa. Nämä ovat ohjelmistorobottitaso, prosessitaso sekä ohjelmistorobotiikkaohjelmataso. Asetettujen teemojen ja tarkasteltavien tasojen perusteella on tarkoitus syventää ymmärrystä siitä millaisin keinoin organisaatiot voivat hallita ohjelmistorobotteihin liittyviä riskejä ja huolehtia siitä, että ohjelmistorobotiikka todella edistää organisaation tavoitteiden saavuttamista. Teoreettinen viitekehys on kuvattu tarkemmin kappaleessa 5. Tutkimustulokset.

Teemat on johdettu tutkielman ensimmäisen osan teoriakatselmuksesta. Ohjelmistorobotiikkaa käsittelevässä teoriakappaleessa 3.2 Ohjelmistorobotiikka ja prosessiautomaatio tarkastelee ohjelmistorobotiikkaa käsittelevää teoriaa näiden neljän teeman valossa. Aiemmassa tutkimuksessa on selkeästi paneuduttu teemoihin 1. *Tavoitteet*, sekä 2. *Riskit*. Jonkin verran aiempaa tutkimusta löytyi myös teeman 3. mukaisista *Riskienhallinnan kontrolleista*. Neljännen teeman mukainen yhteenveto ohjelmistorobottien hallinnan kannalta tehokkaasta kontrolliympäristön vaatimuksista kuitenkin vaatii tarkempaa tutkimusta. Tätä tutkimusongelmaa haastatteluilla lähdettiin selvittämään. Tarkastelua tehtiin robotti-, automaatioprosessi- ja ohjelmistorobotiikkaohjelmatasolla mahdollisimman kattavan kuvan saamiseksi kontrolliympäristöön kohdistuvista vaatimuksista.

5 Tutkimustulokset

Tutkimustulokset on esitelty alla olevan kaavion mukaisesti. Kaavio kuvaa tutkimuksen pohjana käytettyä teoreettista viitekehystä. Haastatteluissa on ensinnäkin pyritty selvittämään millaisia tavoitteita ohjelmistoroboteilla ja prosessiautomaatiolla tavoitellaan. Toisekseen kartoitettiin näiden tavoitteiden toteutumisen esteenä olevat kriittisimmät riskit. Kolmanneksi arvioitiin riskien kannalta tehokkaimpia kontrolleja ja riskienhallintamenetelmiä, joiden perusteella lopuksi yhteenvetona arvioitiin millaisia vaatimuksia ohjelmistorobotiikka asettaa organisaation kontrolliympäristölle. Neljäs kontrolliympäristöä käsittelevä osio toimii siis eräänlaisena yhteenvetona, jonka tavoitteena on kuvata millä keinoin organisaatiossa voidaan edistää tavoitteiden mukaista ohjelmistorobotiikkatoimintaa. Tarkastelun taustalla on teoriaosassa esitelty sisäisen valvonnan tutkimuksessa esitelty prosessi kontrollien asettamiseen. Tämä prosessi etenee tavoitteiden asettamisesta riskien arviointiin ja näiden perusteella asianmukaisten kontrollien suunnitteluun ja käyttöönottoon. (Sihvonen 2019 s. 89.)

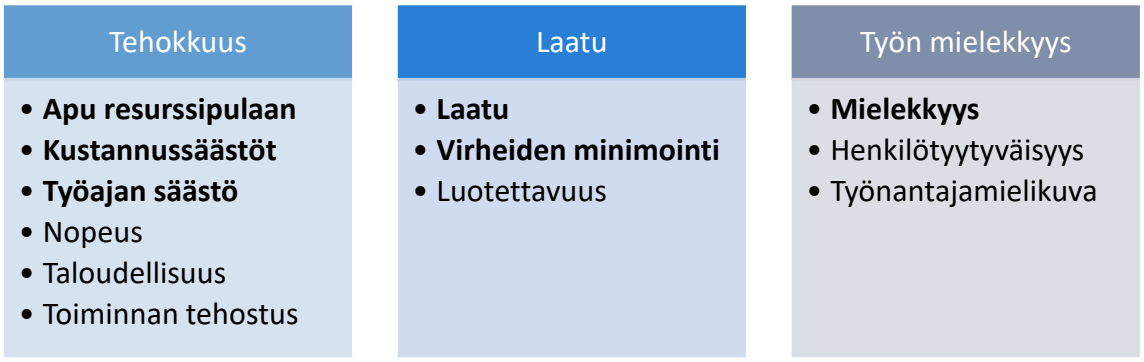
Haastatteluissa pyrittiin tarkastelemaan riskejä ja kontrolleja ohjelmistorobotti-, automaatioprosessi- ja ohjelmistorobotiikkaohjelmatasolla. Näin tarkastelussa pyrittiin saavuttamaan mahdollisimman laaja kuva ohjelmistorobotiikan hallinnasta ja sen haasteista. Tarkastelun tavoitteena on yhdistää osaksi teoreettista viitekehystä organisaatiotason tiedonhallintaan liittyvä tutkimus sekä yksittäisten valvontatoimenpiteiden ja IT-kontrollien tehokkuuteen liittyvä tutkimus. Tämän kappaleen alaluvut jakautuvat siis seuraavien neljän haastatteluteeman ympärille ja erityisesti riskien ja riskienhallinnan kappaleissa tarkastelu on vielä jaoteltu eri tarkastelutasojen mukaisesti. Tutkimuksen teemat on alla olevassa kuvassa esitetty numeroituna prosessina. Tarkastelutasot taas on kuviossa esitetty prosessin sisällä pyramidina.



Kuvio 6. Tutkimuksen teoreettinen viitekehys ja teemat

5.1 Ohjelmistorobotiikan hyödyt

Ohjelmistorobotiikalla tavoiteltavista hyödyistä haastateltavat olivat hyvin yksimielisiä. Haastatteluissa esille nousseet hyödyt voidaan jakaa kolmeen kategoriaan. Haastattelujen perusteella prosessiautomatisaatiolla tavoitellaan useimmiten tehokkuuden, laadun tai työn mielekkyyden parantamiseen liittyviä hyötyjä. Alla olevassa kuviossa on vedetty yhteen haastatteluissa esille nousseet hyödyt, joita ohjelmistorobotiikalla useimmiten tavoitellaan. Kuviossa on korostettuna sellaiset hyödyt, jotka nimettiin haastatteluissa useamman kerran. Haastatteluissa esitetyt hyödyt ovat hyvin linjassa aiempien tutkimusten kanssa. Esimerkiksi Türkyılmaz ja Birol (2019) sekä Seasongood (2016) korostivat tutkimuksessaan ohjelmistorobotiikkaan liittyviä tehokkuushyötyjä. Lacity, Willcocks ja Craig (2015) mainitsivat tutkimuksessaan myös prosessien laatuun liittyvät hyödyt. Aiempaa tutkimusta ohjelmistorobotiikan hyödyistä on käsitelty tarkemmin tutkielman teoriaosan kappaleessa 3.2.1 Ohjelmistorobotiikan hyödyt.



Kuvio 7. Ohjelmistorobotiikan hyödyt

Tutkimuksen tavoitteiden kannalta ohjelmistorobotiikan hyötyihin ei paneuduta tässä yhteydessä sen tarkemmin. Haastatteluissa hyötyjä käsiteltiin vain pintapuolisesti, koska ohjelmistorobottien hyödyistä on suhteellisen paljon aiempaa tutkimusta. Hyötyjen määrittelyllä pyrittiin pohjustamaan tavoitteiden toteutumisen esteenä olevien riskien määrittelyä. Kontrolliympäristön tavoitteenahan on edesauttaa tavoitteiden toteutumista hallitsemalla tavoitteiden esteenä olevia riskejä. Seuraavassa kappaleessa esitellään haastatteluissa esiin nostettuja riskejä, jotka toteutuessaan voivat estää tässä kappaleessa mainittujen tavoitteiden saavuttamisen.

5.2 Ohjelmistorobotiikan riskit

Haastattelujen toisena teemana olivat ohjelmistorobotteihin liittyvät riskit. Kappaleessa tarkastellaan millaisia riskejä robotteihin sekä niiden käytön yleistymiseen liittyy. Riskejä tarkastellaan Ohjelmistorobotiikkaohjelma-, prosessi- ja robottitasolla. Tavoitteena on tarkastella mitkä ovat kriittisimmät tavoitteiden toteutumisen esteenä olevat riskit. Kappaleessa käydään läpi haastatteluissa esiin nousseita riskejä. Riskit on jaoteltu tarkasteltavien tasojen mukaan ja jokainen taso eritellään seuraavaksi omissa alakappaleissaan.

5.2.1 Ohjelmatason riskit

Ohjelmatason riskit vaikuttavat negatiivisesti kaikkiin organisaation automatisoituihin prosesseihin sekä robotteihin. Tasoluokittelussa nämä riskit vaikuttavan koko robotiikkaohjelman menestykseen. Tässä tutkielmassa ohjelmatason riskien on ajateltu kasvavan, kun ohjelmistorobotiikan käyttö organisaatiossa yleistyy. Ohjelmistorobotiikkaohjelmatason riskit korreloivat prosessiautomaation volyymin ja monimutkaisuuden kanssa. Näin ollen ohjelmatason riskit tulevat kriittisemmiksi vasta ohjelmistorobotiikan käyttöönoton myöhemmässä vaiheessa toiminnan laajentuessa. Mitä laajamittaisempaa ohjelmistorobotiikan käyttö on, sitä isommat niihin liittyvät riskitkin ovat.

Jotta ohjelmistorobotiikan laajamittaisesta käyttöönotosta saadaan irti maksimaalinen hyöty, on niitä johdettava organisaationlaajuisesti. Esimerkiksi DeBrusk (2017) ja Fung (2014) korostivat tutkimuksissaan erilaisten käyttöönottostrategioiden käyttökelpoisuutta laajamittaisen käyttöönoton edesauttajana. Kahdessa haastattelussa tuotiin esiin ohjelmistorobotiikkaan liittyvät strategiset riskit. Asiantuntija 6 nosti suurimmaksi ohjelmistorobotiikkaan liittyväksi riskiksi sen, ettei ohjelmistorobotiikkaa saada skaalattua organisaatioon. Lisäksi hän mainitsee riskin siitä, että ohjelmistorobotiikkaohjelman tavoitteet eivät olisikaan linjassa organisaation strategian kanssa:

> *Isoin riski on se, että miten tuo ohjelmistorobotiikka tai älykäs automaatio saadaan skaalattua organisaatioon, kun yleensä se jää sinne yhdelle yksikölle. Mikäli organisaatiolla ei ole hallintamalli kunnossa niin ei sitä saada skaalattua. Tallaisia asioita on mietittävä, että miten sitä kysyntää saadaan stimuloitua esimerkiksi siellä organisaatioyksiköissä ja miten sitä tietoisuutta saadaan nostettua koko organisaatiossa. Sitten on riskinä se, ettei ohjelmatavoitteita ole sidottu organisaation strategiaan.*

Ohjelmistorobotiikan käyttöönoton kannalta merkittävä riski on se, että varsinaisen ohjelmistorobotiikkaohjelman käyttöönotto epäonnistuu. Eli robotiikkaa ei saada skaalattua organisaatioon ja toiminta jää yksittäisten prosessien automatisoinniksi. Tarvitaan

siis visio sitä, mihin suuntaan ohjelmistorobotiikkaa halutaan kehittää ja selkeä strategia, jonka avulla tavoitteet saavutetaan. Kun toiminta saadaan sidottua osaksi organisaation tavoitteita ja strategiaa, edellytykset ohjelmistorobotiikkaohjelman menestykselle paranevat. Riski piilee siinä, ettei ohjelmistorobotiikan kehityksessä päästä alkua pidemmälle, koska ensikokeilut ovat epäonnistuneet. Tätä riskiä ovat tutkimuksessaan korostaneet myös Lacity ja Willcocks (2016b), jotka korostivat erityisesti keskijohdon sitouttamista vision toteuttamisessa. Haastattelussaan Asiantuntija 3 taas kuvasi riskiä epäonnistuneesta käyttöönottostrategiasta seuraavasti:

> *Riippuen siitä porukasta (robotiikan kehittäjät) ja niiden kokemuksesta, että aloitetaanko ohjelmistorobotiikkaohjelma liian isosti. Ei se välttämättä niin kokeneelle väelle ole niin iso kompastuskivi, jos on hoidettu isoja juttuja. Mutta jos ajatellaan vaikka jotakin virastoa, joka alkaa omin voimin puuhastelemaan robotiikkaa ja ottaa liian ison palan purtavaksi niin sitten kun alkaa tulemaan niitä vaikeuksia niin alkaako se into tekemiseen laantua. Ja sitten jos siinä kehityksessä kestää ja näyttää ettei tuloksia synny niin alkaako siellä sitten päättävässä asemassa olevat henkilöt vetämään tukensa pois koko projektilta, ja sitä myöten katoaa rahoituskin siltä hankkeelta ja koko robotiikkahankkeelle tulee huono maine.*

Ohjelmistorobottien kehittäminen on suhteellisen helppoa ja niiden leviäminen usein alkaa kokeilun kautta, yksittäisten prosessien automatisoinnista. Kehittäjinä ei siis välttämättä ole kokenut joukko sovelluskehittäjiä. Tällöin kaikkia riskejä ja parhaita käytäntöjä ei välttämättä osata ottaa huomioon. Asiantuntijoille itsestään selvät riskit ja toiminnan kipukohdat eivät välttämättä tule mieleen henkilölle, joka kokeilee ohjelmistorobotiikkaa ensimmäistä kertaa. Asiantuntija 6 kuvasi tätä ongelmaa seuraavasti:

> *Meillä on sisäisesti riskienhallinta huomioituna, ja esimerkiksi riskianalyysit pitää tehdä alustoille ja yksittäisille ratkaisuille. Ja toimintaa ohjaa esimerkiksi meidän politiikkamme. Toki tämä on harvinaislaatuinen tapaus. Useimmiten riskienhallintaa ei ole toteutettu kovin hyvin. Tämä on yleinen ongelma, kun kyseessä on kevyt*

IT, että näitä on helppo kenen tahansa tehdä, niin yleensä se kehitys jää vähän tutkan alle. -Asiantuntija 6

Hallitsematon ohjelmistorobotiikan kehittäminen nousikin haastatteluissa yhdeksi kriittisimmistä riskeistä. Neljässä haastattelussa tuotiin esiin puutteellinen ohjelmistorobotiikan hallinta. Aiemmassa tutkimuksessa on korostettu hallintamallin merkitystä ohjelmistorobotiikkaan liittyvien riskien hallinnan apuna (Willcocks ja muut 2015). Samalla esimerkiksi Asatiani Kämäräinen ja Penttinen (2019) ovat nostaneet esiin tutkimuksessaan ristiriidan prosessikohtaisen ohjelmistorobotiikan ja organisaatiotasoisen hallintamallin välillä. Robottien yleistyessä ja niiden määrän kasvaessa korostuu asianmukaisen johtamisen tarve. Robottien johtamisen apuna toimii ennakkoon määritelty hallintamalli. Koska ohjelmistorobotiikka on ilmiönä suhteellisen uusi ja sen kehittäminen on helppoa, sen käyttöönotto on organisaatioissa levinnyt kokeilun kautta pirstaloidusti eri organisaatioyksiköissä. Näin varsinaista hallintamallia ei ole ennakkoon määritelty. Hallitsematon kehittäminen tuo mukanaan useita eri riskejä. Asiantuntija 2 kuvaa tätä ilmiötä ja siihen liittyviä riskejä seuraavasti:

Ohjelmistorobotteja tehdään hyvin pirstaloidusti eri liiketoimintayksiköiden sisällä ja sellainen kokonaisvaltainen hallintamalli puuttuu aika monelta organisaatiolta. Eli organisaatiolla ei ole täysin tiedossa mitä robotteja on käytössä ja miten ne vaikuttavat liiketoimintaprosesseihin ja muiden yksiköiden toimintaan. Eli voi olla joku yksikkö, joka tekee jotakin prosessia, josta ne on automatisoinut oman yksikkönsä tehtäviä robotilla ja sitten nämä tämän yksikön tekemiset voivat vaikuttaa seuraavan yksikön toimintaan. Siispä, jos siellä ensimmäisessä yksikössä on mennyt botti vinoon, niin se vaikuttaa seuraavan yksikön toimintaan. Esimerkiksi eräässä yrityksessä oli toiminta seisonut toisessa yksikössä turhaan, kun siellä ei tiedetty, että ensimmäisessä yksikössä on robotti kaatunut. -Asiantuntija 2

Organisaation liiketoimintayksiköiden toiminta on sidoksissa toisiinsa, joten yksittäisen yksikön toiminnalla on merkittävä vaikutus sen rinnalla toimiviin liiketoimintayksiköihin. Riskien vaikutus voi siis ulottua useisiin liiketoimintayksiköihin, joten riskejä tulisi hallita

organisaatioyksikköä laajemmassa mittakaavassa. Asiantuntija 5 kuvaa hallitsemattoman ohjelmistorobotiikkakehityksen ongelmaa seuraavasti:

> *Riski on mielestäni juuri se, että ei olisi keskitettyä (ohjelmistorobotiikka) instanssia. Kun kompetenssiosaaminen ja kyky tehdä näitä (robotteja) kasvaa, niin ei ehkä ole ymmärretty, että sillä robotilla saattaa olla vaikutusta myös muihin järjestelmiin. Eli jos ajatellaan, että meillä on IT-infra, jossa pyörii satoja automatisoituja prosesseja, niin kun mentäisiin hallitsemattomasti muokkaamaan jotain, niin yhtäkkiä meillä lakkaa toimimasta kaikki. Eli itse näkisin, ettei pitäisi isommassa kaavassa harrastaa ohjelmistorobottien tekoa, ellei sillä ole joku selkeä hallintamalli rakennettuna. Eli näkisin suurimman riskin olevan se, että me automatisoisimme liikaa hallitsemattomasti ja sitten me olisimme ongelmissa sen takia.* -Asiantuntija 5

Kriittiseksi tekijäksi ohjelmistorobotiikkaohjelman menestyksen kannalta mainittiin myös resursseihin ja niiden jakautumiseen liittyvät taloudelliset riskit. Strategisesti on tärkeää, että ohjelmistorobotiikkaan liittyviä hyötyjä voidaan luotettavasti seurata ja resursseja tehokkaasti kohdistaa. Huonon ohjelmistorobotiikan johtamisen vuoksi menetetty kilpailuetu ja hukatut resurssit ovat validi liiketoimintariski. Asiantuntija 3 kuvaa taloudellisia riskejä seuraavasti:

> *Pahimmillaan on mennyt siihen robotin tekemiseen investoitu aika ja raha ihan hukkaan eikä olla saatu siitä mitään vastineeksi. Ennemminkin aikaansaatu hämmennystä ja muuta tämän kaltaista. Ja kenties sitten ihmiset joutuvat paikkailemaan robotin jälkiä, niin eihän siitä ainakaan kiitosta saa. Ja taloudellisiin riskeihin liittyen niin, jos kotitehtävät on tehty alkuun huonosti ja jälkiä joudutaan jatkuvasti paikkailemaan monen yrityksen ja erehdyksen kautta, niin se väistämättä johtaa sitten ajan ja rahan menettämiseen.* -Asiantuntija 3

Asiantuntija 2 mainitsi resursseihin liittyviin riskeihin myös sen, että poikkeustilanteissa organisaatiolla ei välttämättä ole käytössään tarvittavia henkilöstöresursseja toiminnan normaalin jatkuvuuden varmistamiseksi.

> *Yhdessä organisaatiossa oli huomattu, että jos robotti lakkaa toimimasta heillä ei ole resursseja toteuttaa sitä prosessia, koska robotti edustaa niin suurta osuutta työvoimasta. Eli jos se robotti lopettaa toimimisen, niin he eivät pysty suoriutumaan omista työtehtävistään sen jälkeen. Heillä ei siis ole henkilöresursseja korvaamaan sitä robottia.* -Asiantuntija 2

5.2.2 Prosessitason riskit

Ohjelmistorobotiikkaan liittyviä riskejä pohdittaessa on huomioitava, että prosessiautomaatio on nimensä mukaisesti prosessikohtaista. Kuten haastatteluissakin nousi esille, ohjelmistorobotiikkaan ei suoranaisesti voida nimetä yleispäteviä ”kaikki prosessit kattavia” -kontrolleja, koska niihin liittyvät kriittiset riskit vaihtelevat automatisoitavan prosessin mukaan. Tässä tutkielmassa tätä on korostettu erittelemällä haastatteluissa ilmenneitä prosessikohtaisia riskejä omassa kappaleessaan. Prosessitasolla riskit vaikuttavat automatisoitavan prosessin toimintaan, mutta eivät välttämättä ulotu koko ohjelmistorobotiikkaohjelman laajuiseksi. Näiden riskien voidaan siis ajatella ulottuvan tiettyyn prosessiin ja siinä toimiviin robotteihin. Niiden vaikutus ei kuitenkaan välttämättä ulotu koko ohjelmistorobotiikkaohjelman laajuiseksi. Prosessitasolla riskien kriittisyys vaihtelee prosessikohtaisesti. Automatisoitavan prosessin riskisyyteen vaikuttaa esimerkiksi prosessin monimutkaisuus ja prosessikohtaiset tekijät. Riskisyyttä voidaan tarkastella eri näkökulmista. Riskien kriittisyys voi liittyä esimerkiksi vahingonkorvausvelvollisuuteen tai liiketoimintakriittisyyteen. Prosessikohtaisesti olisikin tärkeää pohtia mitkä ovat tietyn prosessin näkökulmasta kriittisimmät riskit. Asiantuntija 4 kuvasi prosessien kriittisyyttä seuraavasti:

> *Yksi riski liittyy toiminnan monimutkaisuuteen. Suurimmalla osalla yrityksistä ne robotit ei tee mitään kriittistä. Esimerkiksi minun asiakkaillani, jos prosessissa menisi tiedonsiirrossa jotakin pieleen niin riski on se, ettei heidän asiakkaansa saisikaan tarjousta. Eli ei kyseessä maailman fataalein riski ole. Ei ole riskiä siitä, että jouduttaisiin vahingonkorvausvelvollisuuteen.* -Asiantuntija 4

Vaikka organisaatiossa onkin usein ryhdytty automatisoimaan suhteellisen vähäriskisiä prosesseja, on toiminnan laajetessa prosessikohtaisia riskejä tarkasteltava yhä kriittisemmin. Siirryttäessä yhä kriittisempien prosessien automatisointiin, prosessikohtaiset riskitkin yleensä muuttuvat kriittisemmiksi. Esimerkiksi Asiantuntija 6 mainitsee haastattelussaan riskin siitä, ettei automatisoitavan prosessin osalta olisi tehty riittävää selvitystä prosessia koskevasta regulaatiosta. Robottien kehityksessä ei välttämättä ole mukana esimerkiksi lakiasioihin perehtynyttä asiantuntijaa.

> *Pahimmassa tapauksessa on tapauksia, joissa ne botit tekevät jotain väärin. Joko ne on kehitetty tekemään jotain väärin tai sitten ei ole tunnettu regulaatiota riittävän tarkasti ja on tehty botti sellaiseen paikkaan, minne sitä ei olisi saanut tehdä. Botti esimerkiksi tekee jotain lainvastaista, mistä sitten tulee tietenkin mainittavia maineriskejä.* -Asiantuntija 6

Myöskin Asatiani, Kämäräinen ja Penttinen (2019) tutkimus tukee näitä havaintoja. He korostivat substanssiasiantuntijoiden merkitystä esimerkiksi prosessikohtaisten riskien tunnistamisessa. Lisäksi prosessitasolla kriittinen riskitekijä on varmistaa, ettei robotit vaaranna organisaatiossa käytettävän tiedon laatua. Tiedon eheyteen liittyvien riskien kriittisyys vaihtelee riippuen prosessikohtaisista erityispiirteistä. Esimerkiksi tiedon määrä, laatu ja monimutkaisuus vaikuttavat kaikki riskien kriittisyyteen. Automatisoitavat prosessit ovat erilaisia. Tietoa saadaan eri lähteistä eri prosessin vaiheissa ja sitä muokata eri menetelmin. Aina kun tietoa siirretään tai muokataan, on mahdollisuus tiedon vahingoittumiselle. Kun robotit käsittelevät tietoa, on organisaatiossa tiedostettava riski tiedon eheyden rikkoutumiselle. Automatisoidun prosessin osalta ei voida

tuudittautua ajatukseen siitä, että robotti ei tee inhimillisiä virheitä, joten sen tuottama tieto on aina oikein. Asiantuntija 5 kuvaa riskiä, joka liittyy robotin tuottaman tiedon eheyteen seuraavasti:

> *Jos ajatellaan että se botti tekee kaikki työtehtävät ajasta tappiin, niin se on vähän väärä mielikuva. Siellä saattaa mennä botti poikittain tai tulla jotain muuta virhettä, joka sitten aiheuttaa sen, että se sekoittaa kaikki muutkin tiedot. Esimerkiksi asiakkailla on ollut tämän tyyppisiä tapauksia, missä jokin piste tai pilkkuvirhe on aiheuttanut ongelmia. Tämä on ehkä yksi asia mihin haluaisin puuttua, että tavallaan sillä (robotilla) voidaan rikkoa sitä tiedon eheyttä*. - Asiantuntija 5

Robotin tuottaman tiedon lisäksi on kiinnitettävä huomiota robottiin tulevan tiedon laatuun. Robotti ei osaa kyseenalaistaa saamansa tiedon oikeellisuutta, vaan käsittelee tiedon sellaisenaan. Pahimmillaan robotti rikkoo tiedon eheyttä vielä lisää. Asiantuntija 4 korostaa robottiin tulevan tiedon eheyttä seuraavasti:

> *Riskit mitä mekin olemme IT-tarkastuksissa varmentaneet, on se, että tieto mitä se robotti lukee tai mistä se sitä tietoa lukee, ettei kukaan ole sitä päässyt koskaan vahingossa tai tahallaan muokkaamaan. Että se tieto pysyy näin oikeana.* -Asiantuntija 4

Tiedon eheyteen liittyvien riskien suuruus vaihtelee sen mukaan, kuinka kriittisestä tiedosta on kyse. Mikäli robotin käsittelemä tieto on suhteellisen vähäarvoista, tiedon eheyteen liittyvät riskit eivät välttämättä ole liiketoimintakriittisiä. Mikäli robotin käsittelemän tiedon arvioidaan olevan vähäarvoista, voidaan tiedon eheyteen liittyvien riskien arvioida olevan siedettävällä tasolla. Jos robotti käsittelee esimerkiksi lain nojalla sensitiivistä tietoa, riskit voidaan arvioida erittäin liiketoimintakriittisiksi. Asiantuntija 5 kuvaa tätä riskienarviointiprosessia seuraavasti:

> *Onko se tieto nyt oikeasti sellaista mitä voidaan ryhtyä robotisoimaan ja voiko sillä saada myöhemmin aikaan jotain ongelmia. Eli käytännössä onko ne oikeudet*

järkeviä. Onko se taho, joka tekee sitä robottia oikeutettu pääsemään käsiksi tähän robotin käsittelemään dataan vai pitäisikö sitä tietoa pystyä suojaamaan jotenkin. -Asiantuntija 5

Tiedon eheyteen saattaa myös vaikuttaa se millaista dataa prosessissa käsitellään ja millaisesta lähteestä tietoa luetaan. Erityyppiseen tietoon saattaa liittyä erityispiirteitä, jotka saattavat altistaa prosessin tietynlaisille riskeille. Haastattelussaan Asiantuntija 3 kertoi tiedon eheyteen liittyvistä riskeistä seuraavasti:

Vaikka se aineisto olisikin muodollisesti oikeaa, on otettava myös huomioon se, millaista aineistoa käsitellään. Riskinä voi esimerkiksi olla, että liitedokumentteja luetaan suoranaisista valokuvista, jolloin se kuvan laatu saattaa vaihdella ja botilla voi olla vaikeuksia saada siitä selvää. Tällöin botti voi luulla toimivansa oikein, mutta lukeekin sitten vääriä tietoja. Esimerkkinä botti saattaisi lukea tiedostosta väärän veroprosentin, joka sitten johtaa virheeseen. -Asiantuntija 3

Tiedon eheyttä on hyvä tarkastella koko prosessin näkökulmasta. Pääasiallisesti robotti parantaa tiedon eheyttä, mutta logiikka saattaa tietyissä tapauksissa pettää. Esimerkiksi virheen tai poikkeuksen takia robotti saattaa ryhtyä toimimaan epätoivotusti. Pahimmassa tapauksessa robotti saattaa systemaattisesti vahingoittaa organisaatiodataa. Asiantuntija 1 kertoo vastaavasta tilanteesta seuraavasti:

Yhdessä esimerkkitapauksessa meillä oli robotti, jonka tarkoituksena oli tallentaa muutokset eräässä toisessa tietojärjestelmässä meidän toiminnanohjausjärjestelmäämme. Kun aloimme viemään tätä projektia eteenpäin, huomasimme riskin tiedon eheyden rikkoutumiselle. Jos robotin lukemalla raportilla, yksikin rivi oli väärin, robotti alkaa yhdistää sopimattomasti sitä tietoa sinne toiminnanohjausjärjestelmään. Yksi pieni virhe lähdedatassa ja robotti voisi sekoittaa kaikki loputkin niistä tiedoista. -Asiantuntija 1

Vaikka ohjelmistorobotiikassa hyödynnetäänkin virtuaalisia työntekijöitä, jotka eivät sorru inhimillisiin virheisiin, robotit toimivat ihmisten ohjaamana ja heidän kanssaan yhteistyössä. Inhimillisten virheiden riski on siis läsnä robottien käyttöönoton jälkeenkin. Haastatteluissa korostettiin robottien vähentävän inhimillisten virheiden riskiä, mutta riskin mahdollisuus on kuitenkin tärkeää tiedostaa, jotta kriittisten prosessien osalta niitä voidaan tarvittaessa hallita. Prosessikohtaisesti on hyvä tiedostaa, että aina kun jossakin prosessin vaiheessa on mukana ihmisiä, on mahdollisuus inhimillisille virheille. Esimerkiksi robottien suunnittelussa ja käyttöönotossa ihmisten rooli on merkittävä. Robotin elinkaaren näkökulmasta nämä vaiheet ovat inhimillisten riskien näkökulmasta kriittisimpiä. Inhimillisiä riskejä Asiantuntija 3 kuvaa seuraavan esimerkin kautta:

> *On otettava huomioon se ihmisen toiminta. Että jos katselmointipalaveri järjestetään perjantaina klo 14 ja se kestää kaksi tuntia, niin mitenkä paljon siinä jaksaa enää ennen neljää kiinnittää näihin asioihin huomiota.* -Asiantuntija 3

Ihmisten rooli on suuri erityisesti ohjelmistorobotin käyttöönottoa edeltävissä vaiheissa. Tämän vuoksi esimerkiksi suunnitteluvaiheessa on monia ihmisiin liittyviä riskejä. Haastatteluissa ilmenneet riskit liittyvät esimerkiksi ihmisten ymmärrykseen, sitouttamiseen ja muutosvastarintaan. Ihmisten ja robottien väliseen suhteeseen on paneuduttu myös aiemmassa tutkimuksessa. Tutkimuksessaan Vedder ym (2016) totesivat työntekijöiden usein kokevan, että ohjelmistorobotit vaarantavat heidän työpaikkansa, mikä usein johtaa muutosvastarintaan. Ihmisiin liittyvien riskien kriittisyyteen vaikuttaa myös tietyn ihmisen rooli prosessissa. Kriittisissä rooleissa toimivia henkilöitä kutsutaan avainhenkilöiksi. Haastattelussaan Asiantuntija 1 antoi seuraavan esimerkin avainhenkilöihin liittyvästä riskistä:

> *Yksi riski on se, ettei suunnittelussa ole mukana ne henkilöt, jotka oikeasti tekevät sitä prosessia. Nämä henkilöt ovat ne, jotka osaavat tuoda ilmi kaikkia niitä erilaisia tapauksia, joita prosessissa pitää huomioida ja joita pitää sitten palastella.*
> -Asiantuntija 1

Vaikka prosessia suorittavat avainhenkilöt, eli ns. substanssiosaajat saadaan sitoutettua osaksi ohjelmistorobotin kehitysprosessia, mainitsee Asiantuntija 2 yhtenä riskinä myös sen, ettei itse robotin kehittäjä ymmärrä tätä substanssiosaajaa. Teknisen osaajan ja substanssiosaajan välillä saattaa olla jonkinlainen kuilu eivätkä he täysin ymmärrä toisiaan, mikä saattaa lisätä riskiä virheille robotin toimintalogiikassa.

> *Kun robottia lähdetään kehittämään ja vaatimusmäärittelyä tekemään, niin RPA-kehittäjältä vaaditaan substanssisanaston ymmärtämistä. Kehittäjän on ymmärrettävä se prosessi, kun substanssiasiantuntija selittää, että miten tämä prosessi menee. Jos vaatimusmäärittely menee pieleen, koska siinä ei ole osattu huomioida kaikkia asioita tai kehittäjä ei ole täysin ymmärtänyt prosessin luonnetta, niin prosessi saattaa olla hyvin kankea, eikä vastaa tarkoitustaan. Tällöin kehittämiseen hukataan resursseja ja takaisinmaksuaika lykkääntyy.* -Asiantuntija 2

Inhimillisistä riskeistä kriittisimpiä ovat usein väärinkäytöksiin liittyvät riskit. Haastatteluissa väärinkäytösriskit eivät nousseet yhdeksi kriittisimmistä ohjelmistorobotteihin liittyvistä riskeistä, mutta riskin todettiin kuitenkin olevan läsnä. Riskinä on, ettei väärinkäytöksen mahdollisuutta tiedosteta eikä asianmukaisia kontrolleja niiden hallitsemiseksi ole asetettu. Myös Denver (2020) on tutkimuksessaan tuonut esiin väärinkäytösriskien mahdollisuuden etenkin ohjelmistorobotiikan hyvin tuntevien henkilöiden toimesta. Väärinkäytösriskeistä Asiantuntija 2 kertoi haastattelussaan seuraavasti:

> *Väärinkäytöksistä tulee mieleen, että kehitysvaiheessa on otettava huomioon, miten se prosessi etenee. Kehitysprosessi ei voi olla sellainen, että minä suunnittelisin, toteuttaisin ja käyttöönottaisin sen robotin, vaan siellä on oltava myös ulkopuolisia tahoja. Ja se väärinkäytös voi myös tapahtua sieltä toisesta suunnasta, että riippuen siitä millaisia prosesseja on automatisoitu. Hyödyntääkö prosessi vain järjestelmässä olevaa tietoa vai onko sillä joku data-aineisto, joka toimii*

lähtötietona sille prosessille, jolloin nousee tärkeäksi se, kuka pääsee tätä tietoa muokkaamaan. -Asiantuntija 2

Väärinkäytöksille siis tunnistettiin tietyt riskipisteet, joihin tulisi kiinnittää huomiota. Myöskin Asiantuntija 6 tunnisti väärinkäytösriskien kannalta muutaman kriittisen vaiheen. Kriittisiksi pisteiksi tunnistettiin erityisesti ohjelmistorobottien tuotantoympäristö sekä ohjelmistorobottien elinkaaren kehitysvaihe. Haastattelussaan Asiantuntija 6 kommentoi väärinkäytösriskejä seuraavasti:

Väärinkäytösriskien osalta olennaista on se, että kuka pääsee sinne tuotannossa olevaa bottia muokkaamaan. Jos sen botin muokkaaminen on mahdollista niin se tietenkin avaa uusia väyliä väärinkäytöksille. Ja sama kehitysvaiheessa. Organisaatiolla pitää olla kontrollit siinä kehitysprosessissa, että pystytään varmentumaan siitä, ettei väärinkäytösmahdollisuutta ole sisäänrakennettu sinne bottiin. -Asiantuntija 6

Haastatteluissa korostettiin, että ohjelmistorobotiikka pienentää riskiä väärinkäytöksille, muttei kokonaan poista niitä. Riskin mahdollisuus on hyvä tiedostaa, jotta voidaan tarvittaessa etukäteen varmistaa tarvittavat riskienhallintatoimenpiteet väärinkäytösriskien hallitsemiseksi. Asiantuntija 4 kommentoi väärinkäytösriskiä ja ohjelmistorobottien vaikutusta riskin suuruuteen verrattuna ihmisen suorittamaan prosessiin seuraavasti:

Periaatteessa väärinkäytösriskejä voi olla sellaisia, että robotti on tarkoituksella koodattu väärin. Riskinä on se, että koodaaja on jostain syystä halunnut tehdä sen toiminnallisuuden virheen. Tai sitten joku manipuloi sitä dataa mitä se robotti käyttää. Todennäköisesti siinä on kuitenkin niitä väärinkäytöksen paikkoja vähemmän, kun se robotti tekee sen. Eli joko se koodi on väärin, mitä ei lähtökohtaisesti pitäisi tulla, jos robotti on hyvin testattu ja sitä testaa useampi ihminen. Tai vaihtoehtoisesti siinä robotin lukemassa ja kirjoittamassa tiedossa. Eli jää nämä kaksi pistettä missä se voi tulla. -Asiantuntija 4

Lopuksi on huomioitava virheiden riski. Potentiaalisten virheiden vaikutusta on pohdittava prosessikohtaisesti. Kriittisiä virheitä pyritään välttämään asianmukaisilla riskienhallintatoimenpiteillä. Täten potentiaalisia virheitä on tunnistettava jo ennakkoon. Prosessikohtaisesti on useita kohtia, joissa voidaan epähuomiossa tehdä kriittisiä virheitä. Haastatteluissa tuotiin ilmi useampia virheen paikkoja, jotka toteutuessaan aiheuttaisivat suuriakin menetyksiä. Esimerkiksi Asiantuntija 1 huomauttaa, että jo robotiikkainvestoinnin alkutaipaleella voidaan mennä vikaan, jos investointilaskelmissa tehdään virheitä:

> *Kustannussäästönäkökulmasta me lähdemme aina laskemaan robotin kustannuksia. Ensin lasketaan, kuinka toistuvasta tehtävästä on kyse ja kuinka kauan yhdellä henkilöllä menee sen tehtävän suorittamiseen, ja mikä on robotin takaisinmaksuaika. Sitten lasketaan, kuinka paljon robotin koodaamiseen menee aikaa. Virhelaskelmiin voi liittyä esimerkiksi strategisesti se riski, että me kohdistamme resurssit väärin.* -Asiantuntija 1

5.2.3 Robottitason riskit

Robottitason riskit ulottuvat yhteen robottiin. Robottitasolla tarkastelua tehdään teknisestä näkökulmasta, pohtien ohjelmistoroboteille tyypillisiä erityispiirteitä, jotka voidaan ajatella riskitekijöiksi. Kuten tämän tutkielman teoriaosassa jo kerrottiinkin, ohjelmistorobotit eivät reagoi tehokkaasti muutoksiin (DeBrusk 2017). Täten robottitason riskit ovat pitkälti sidoksissa järjestelmäriippuvuuteen ja poikkeuksien hallintaan. Nämä riskit ovat siinä mielessä robottikohtaisia, että niitä aiheuttaa yksittäisen robotin toimintoympäristössä tapahtuvat muutokset. Näin riskit eivät realisoituessaan vaikuta kaikkiin organisaatiossa operoiviin robotteihin. Robotit vaativat siis jatkuvaa seurantaa, jotta voidaan varmistua siitä, ettei pienet muutokset robottien toimintaympäristössä tai niiden vastaanottamassa datassa saa aikaan koko robotin kaatumista. Asiantuntija 3 kommentoi ohjelmistorobottien toimintaa ja muutoksensietokykyä seuraavasti:

> *Loppupeleissä se (robotti) ei ole muuta kuin nopea idiootti. Se tekee juuri niiden sääntöjen puitteissa mitä sille on annettu. Eihän se sen kummemmin jää katselemaan, että mitä sille on annettu tai katselemaan perään, että mitä tuli tehtyä. Sehän siinä on sellainen selkä riski.* -Asiantuntija 3

Haastatteluissa korostettiin ohjelmistorobottien järjestelmäriippuvuutta ja sen aiheuttamia riskejä. Ohjelmistorobotit operoivat samoissa käyttöliittymissä kuin ihmiset, mutta toisin kuin ihmiset, ne eivät ole järjestelmien käytön suhteen joustavia. Muutokset käyttöliittymissä johtavat usein ongelmiin robotin toiminnassa. Tätä ilmiötä Asiantuntija 3 kuvaa seuraavasti:

> *Silloin jos se tieto tulee jostain käyttäjäorganisaation ulkopuolelta, niin siellähän voi tapahtua muutoksia, jotka johtavat siihen, että siinä robottiin tulevassa tiedossa on tapahtunut jotain pienen pieniä muutoksia joihin ihminen ei välttämättä kiinnitä sen kummempaa huomiota, mutta robotti saattaa seota siitä ihan täysin. Eli se robotti ei sitten pysty suoriutumaan, kun ei löydäkään tietoa samasta paikasta missä se on aina ollut. Käytännön esimerkkinä eräässä robotissa piti lukea tietoa vastaanotetusta dokumentista ennalta määritellyn avainsanan perusteella. Jos tässä avainsanassa tapahtuisi jotain muutosta, esimerkiksi sijamuoto muuttuisi, niin robotti ei osaisi lukea tätä tiedostoa. Ilman asianmukaista seurantaa, on riski sille, että jäätäisiin vain ihmettelemään, kun näitä tiedostoja ei olekaan enää vastaanotettu.* Asiantuntija 3

Järjestelmämuutoksien seurauksena robotteja on ohjelmoitava uudestaan. Muutokset ohjelmistorobottiin vaativat aikaa ja resursseja, ja pahimmillaan seisauttavat muita liiketoimintaprosesseja. Lisäksi robottien kehitys saattaa viivästyä, kun järjestelmiin tehdään muutoksia. Vastaavasta riskistä Asiantuntija 1 kertoo seuraavasti:

> *Esimerkiksi meillä eräs prosessi on viivästynyt, kun robotti ei pääse tekemään muutoksia suoraan tietokantaan vaan nämä muutokset on tehtävä desktopin*

> *kautta. Nyt tähän järjestelmään on tulossa järjestelmäpäivitys, jonka seurauksena tämä desktop-näkymä sitten muuttuu. Eli käytännössä joudumme nyt odottamaan, että saamme tuotantoon sen uuden näkymän.* -Asiantuntija 1

Myöskin Asiantuntija 2 korostaa, että taloudellisten tavoitteiden toteutumisen näkökulmasta riskit robottitasolla liittyvät usein järjestelmäriippuvuuteen. Vaikka robotin kehitys ja testaus on tehty oikein, pienetkin päivitykset sen toimintaympäristössä aiheuttavat sen, että robotti lakkaa toimimasta. Haastattelussaan Asiantuntija 2 korostaa myös puutteellista viestintää osana ongelmaa:

> *Jos ajatellaan, että robotti itsessään toimii ihan hyvin ja tuottaa ne sille asetetut taloudelliset tavoitteet, niin mikä estää sen taloudellisen tavoitteen toteutumisen on se, että se robotti lakkaa toimimasta. Tämä taas johtuu siitä, että on esimerkiksi tehty järjestelmäpäivitys, mutta siitä ei ole informoitu robottia kehittävälle taholle. -Asiantuntija 2*

Järjestelmämuutoksien lisäksi muutkin poikkeustilanteet saattavat olla robottien toiminnan kannalta ongelmallisia. Poikkeuksien vaikutus toiminnan jatkuvuuteen saattaa olla suuri. Kuten tutkielman teoriaosassa jo kerrottiin, ohjelmistorobotiikka toimii parhaiten mahdollisimman stabiilissa ympäristössä, jossa on mahdollisimman vähän poikkeuksia. Fung (2014) ja Slaby (2012) esittelivät tutkimuksissaan vaatimuksia ohjelmistorobotiikalla automatisoitaville prosesseille. Heidän tutkimustuloksiaan on esitelty tarkemmin tämän tutkielman teoriaosassa Taulukossa 1. Robottikohtaisia riskejä voidaan pienentää valitsemalla automatisoitaviksi prosesseiksi sellaisia, joissa täyttyy mahdollisimman moni näistä vaatimuksista. Kuitenkin robottien yleistymisen myötä, teknologiaa todennäköisesti lähdetään implementoimaan osaksi yhä dynaamisempia ympäristöjä, jolloin poikkeuksiin liittyvien riskien todennäköisyyskin kasvaa.

5.3 Riskienhallinta ja kontrollit

Edellä mainittujen riskien hallinta vaatii organisaatiolta riskienhallintatoimenpiteitä ja riskejä vastaavia kontrolleja. Ohjelmistorobotiikka on ilmiönä suhteellisen uusi, ja sen käyttö organisaatioissa on vasta viime aikoina yleistynyt. Ohjelmistorobotiikan implementoinnin alkuvaiheessa toiminta on niin pientä, ettei riskien koeta olevan merkittäviä. Ohjelmistorobotiikan käytön yleistyessä ja toiminnan levitessä yhä laajemmalle organisaation toimintoihin, riskienhallinnan merkitys korostuu. Riskienhallinta vaatii, että riskienhallintatoimenpiteet ja kontrollit on otettu käyttöön jo ennen riskien realisoitumista. Ohjelmistorobotteja käyttävien organisaatioiden tulee uudelleenanalysoida ohjelmistorobotteihin liittyviä riskejä aika-ajoin. Analyysien pohjalta voidaan arvioida ovatko riskit hyväksyttävällä tasolla vai tulisiko niitä ryhtyä ennaltaehkäisemään. Tässä kappaleessa esitellään haastatteluissa esiin nousseita riskienhallinnan menetelmiä ja kontrolleja ohjelmistorobottien hallintaan. Ensimmäisen alaotsikon alla esitellään haastateltavien näkemyksiä ohjelmistorobotteihin liittyvästä riskienhallinnasta. Kuten tämän tutkielman teoriaosassa jo kerrottiin, riskienhallintaa suoritetaan kontrollien avulla (Lahti ja Salminen 2014). Kolmessa viimeisessä alakappaleessa käsitellään näitä kontrolleja ohjelmistorobotiikkaohjelma-, prosessi ja robottitasolla. Kappaleen tavoitteena on esitellä haastatteluissa nousseita riskienhallintakeinoja, edellisessä kappaleessa esiin nousseille riskeille.

5.3.1 Riskienhallinta

Haastateltavilta kysyttiin, miten heidän mielestään riskienhallinta on näkynyt ohjelmistorobotiikkaa hyödyntävissä organisaatioissa. Viidessä haastattelussa todettiin, että etukäteistä riskiarviota ei ohjelmistorobotiikkaan liittyen useinkaan ole tehtynä. Poikkeuksia löytyy, mutta yleisesti riskienhallinnan koettiin vielä puutteelliseksi. Sisäistä riskienhallintamallia tai riskienhallintaohjelmaa ei juuri löydy eikä riskiarviota useinkaan tehdä etukäteen.

> *Kyllä se (riskienhallinta) on paljon organisaatiokyvykkyydestä kiinni. Useinhan tätä RPA:ta tehdään IT-osaston ulkopuolella, jolloin ne hyvät käytännöt, missä olisi tämä riskienhallinta esimerkiksi huomioituna, ei ole ihan suoraan jalkautunut. En siltikään näe, että koska tämä on ns. kevyt-IT:tä, niin sen takia riskienhallintaa ei olisi tehtynä. Enemmän se on johtunut siitä, että tietoisuus ja tietämys ei ole vielä riittävää. Ne, jotka sitä ohjelmistorobotiikkaa ovat tehneet vuosia, niin heillä se on hyvässä kunnossa. Ja heillä se kustannustehokkuuskin on sitten paljon korkeampi, kun se maturiteetti on korkeammalla, niin yksittäisten robottien kehittäminen kestää vähemmän aikaa ja niin poispäin.* -Asiantuntija 6

Riskienhallinnassa on siis organisaatiokohtaisia eroja. Ohjelmistorobotiikkaan pätee useat IT-osastojen käyttämät parhaat käytännöt. Ohjelmistorobotiikkaa on kuitenkin helppo kehittää IT-osaston ulkopuolella, jolloin nämä riskienhallintatoimenpiteet helposti jäävät käyttöönottamatta. Riskien tunnistaminen tapahtuu usein robottien käyttöönoton jälkeen riskien realisoituessa. Riskienhallinta keskittyy siis ehkäisyn sijaan niiden vaikutuksien minimoimiseen. Tätä trendiä asiantuntija 2 kuvaa seuraavasti:

> *Riskejä ei ole minun mielestäni kartoitettu koskaan, kun minä olen ohjelmistorobotiikan kanssa ollut tekemisissä. Se oli yksi asia mitä itsekin olen havainnut, että ei hirveästi ole mietitty riskejä, että mikä tässä voisi mennä pieleen. Tai vaihtoehtoisesti, jos joku riski toteutuu, miten se sitten hoidetaan. Eli minulla ei ole tiedossa, että olisi tehty mitään suurempaa riskikartoitusta.* -Asiantuntija 2

Asiantuntija 3 ja Asiantuntija 4 kuitenkin korostivat, että heidän havaintojensa mukaan robotit, joiden kanssaan he ovat olleet tekemisissä eivät ole olleet niin kriittisiä, että etukäteen tapahtuvalle riskiarviolle olisi ollut tarvetta. Etenkin Asiantuntija 4 on ollut IT-tarkastusten puitteissa tekemisissä ohjelmistorobottien kanssa erityisesti vakuutus- ja pankkisektorin yrityksissä, joissa riskienhallinta on yleisesti hyvin hanskassa. Myöskin Asiantuntija 3 korosti, että prosessikohtaisia riskejä on kyllä kerätty ylös Process Design Document -tiedoston avulla. On kuitenkin muistettava, että toiminnan levitessä ja

monimutkaistuessa riskienhallinnan merkitys korostuu. Tulevaisuudessa organisaatioiden on yhä enemmän kiinnitettävä huomiota siihen, että riskienhallintamalli pysyy ohjelmistorobotiikan kehityksen mukana.

5.3.2 Ohjelmatason kontrollit

Ohjelmatason kontrolleilla pyritään hallitsemaan ohjelmatason riskejä. Niillä hallitaan suuria kokonaisuuksia ja ne ovat usein ohjeistuksia, sääntöjä ja politiikkoja, joita koko organisaation tulisi noudattaa. Organisaatiotason kontrollit viittaavat tässä yhteydessä COSO-viitekehyksen mukaiseen kontrolliympäristön määritelmään, jota esiteltiin tarkemmin tämän tutkielman kappaleessa 2.2.1 COSO määritelmä kontrolliympäristölle. Kuten COSO-viitekehyksen määritelmässä kuvattiin, organisaatiotason kontrolleja ovat esimerkiksi organisaation toimintaohjeet, kuvatut prosessit, controlling- ja sisäisen tarkastuksen toiminnot sekä määritellyt laskentaperiaatteet (Lahti ja Salminen s.53-54 2014).

Menestyksellinen ohjelmistorobotiikkaohjelma vaatii johtamista ja strategista ohjausta, jonka toteutumista voidaan seurata ja hallita ohjelmatason kontrollien avulla. Ohjelmatason kontrollien tavoitteena on, että ohjelmistorobotiikkaohjelman toiminta saavuttaa sille asetetut tavoitteet. Menestyksekkään ohjelmistorobotiikkaohjelman kannalta tavoitteiden tulisi noudattaa organisaation strategiaa. Lacity ja Willcocks (2016b) korostivat tutkimuksessaan ohjelmistorobotiikkaohjelman strategian ja vision merkitystä menestyksen ajurina. Ohjelmistorobotiikkaa tulisi ajaa strategisella tasolla eteenpäin. Näin mahdollisestaan ohjelmistorobotiikan menestyksekäs leviäminen organisaatiossa.

> *Tärkeää olisi lisätä tietoa siitä, mitä kaikkea prosessiautomaatiolla voidaan saavuttaa ja miksi nämä ovat kannattavia. Tallaisella automaatiojutulla pitäisi olla sponsori ihan johtoryhmässä asti. Johtavilla toimijoilla on selkeät tavoitteet sille toiminnalle ja ne on sidottu strategiaan. Ja sitten sponsori siellä johtoryhmässä vetää sitä toimintaa eteenpäin strategisella tasolla*. -Asiantuntija 6

Kun ohjelmistorobotiikan kehitys on sidottu strategiaan ja toiminta leviää menestyksekkäästi ympäri organisaation, on tätä kokonaisuutta pystyttävä johtamaan. Haastatteluiden perusteella hallintamalli nousi kriittisimmäksi ohjelmistorobotiikkaa sääntéleväksi kontrolliksi. Koska ohjelmistorobotiikka on hyvin prosessikohtaista, tarvitaan toiminnan laajetessa organisaatioon hallintamalli, jonka avulla hallitaan riskejä, maksimoidaan hyödyt ja varmistetaan että automaatio on linjassa organisaation tavoitteiden ja strategian kanssa. Myös Asatiani, Kämäräinen ja Penttinen (2019) korostivat tutkimuksessaan ohjelmistorobotiikan hallinnan merkitystä ja vertailivat erityyppisten hallintamallien hyötyjä ja haittoja. Myös haastatteluissa tuotiin esiin samoja teemoja:

> *Eli tarvitaan Governance-malli. Aivan kuten tietohallinnossa tai IT:ssä puhutaan niin sanotusta muutoshallintaryhmästä tai onko se IT-arkkitehtuuri, niin tiedetään mikä taho näistä vastaa. Joku omistaa sen koko robotiikkapalvelut kokonaisuuden. Esimerkiksi jos robotiikkaa työstetään UiPathin avulla ja käytetään tallaista Orgestratoria (UiPathin hallintatyökalu), niin organisaation tietoturva- ja IT-yksiköiden pitäisi katsoa se prosessi läpi, että organisaatiossa ymmärretään mitä kaikkea ollaan automatisoimassa.* -Asiantuntija 5

Kuten edellisessä ohjelmistorobotiikkaan liittyviä riskejä käsittelevässä kappaleessa on mainittu, valtaosa riskeistä on prosessikohtaisia. Riskien kriittisyys vaihtelee suuresti riippuen prosessista. Näin ollen yleisiä kaikkiin ohjelmistorobotteihin päteviä kontrolleja on hankalaa määritellä. Tämän vuoksi hallintamallin merkitys korostuu. Näin koko ohjelmistorobotiikka kokonaisuutta pyritään hallitsemaan siten, että jokainen prosessi täyttää riskienhallinnan näkökulmasta sille asetetut vaatimukset. Asiantuntija 5 kuvaa hallintamallin merkitystä prosessikohtaisten kontrolloinnin edesauttajana seuraavasti:

> *Niitä kontrolleja on aika vaikea määritellä etukäteen, vaan organisaatiossa pitää olla tarvittava Governance-malli, joka tarvittaessa tuottaa sinne kontrolliympäristöön ne tarvittavat kontrollit per automatisoitava prosessi.* -Asiantuntija 5

Hallintamalli ja kontrolliympäristö ovat siis vahvasti linkitettyinä toisiinsa. Hyvä hallintamalli parantaa kontrolliympäristön tehokkuutta. Myös Asiantuntija 2 korostaa hallintamallin merkitystä erityisesti järjestelmäriippuvuuteen liittyvien riskien kontrolloinnissa.

> *Esimerkiksi tuohon järjestelmäriippuvuuteen liittyen, niin aika paljon noita eri järjestelmiä tuolla organisaatiossa on, niin tietääkö kaikkien järjestelmien tekninen omistaja, että tässä kohtaa käytetään ohjelmistorobottia. Tässäkin korostuu se hallintamalli ja viestintä. Että tarvitaan sellainen ylätason ymmärrys näistä riippuvuuksista eri järjestelmien, henkilöiden, prosessien, osastojen ja yksikköjen välillä. Sellainen kokonaisuuden hallinta on äärimmäisen tärkeä.* -Asiantuntija 2

Hallintamallin tarkoituksena on siis koota kokonaisvaltainen näkemys organisaation ohjelmistorobotiikkaan liittyvistä tavoitteista ja seurata, että toteutus vastaa näitä tavoitteita. Tavoitteiden toteutumisen kannalta on tärkeää, että kaikki ohjelmistorobottien parissa työskentelevät tahot toimivat yhteistyössä keskenään ja viestintä näiden tahojen välillä toimii. Ohjelmatason kontrollina hallintamallin tulee kattaa kaikki organisaatiossa toimivat automaatioprosessit ja yksittäiset robotit. Hallintamallin tulisi ohjata jokaista uutta automaatioprojektia sekä jo toiminnassa olevaa robottia. Asiantuntija 2 kuvaa hallintamallin toimintaa seuraavasti:

> *Tarvitaan esimiehiä tai ohjausryhmiä, jotka hyväksyvät tämän prosessien automatisoinnin, sen testaustulokset ja itse robotin. Jokaisen robotin kehityspolku on systemaattinen, jotta ei pääse tapahtumaan näitä tilanteita, että tietyllä taholla on kaikki oikeudet ja hän pääsee tekemään mitä sattuu.* -Asiantuntija 2

Hallintamalli asettaa toimenpiteet, jotka tulee jokaisen prosessin osalta suorittaa. Näin varmistetaan, että jokainen tuotantoon tuleva robotti toimii toivotusti.

Esimerkiksi hallitsemattomat käyttöoikeudet oli haastatteluissa usein esille noussut riski. Tätä riskiä on esitelty edellä ohjelmatason riskejä käsittelevässä kappaleessa. Näiden

riskien hallintaan nousi haastatteluissa keskitetty käyttöoikeushallinta ja muut siihen liittyvät kontrollit. Keskitetty käyttöoikeushallinta tulisi olla osana ohjelmistorobotiikan hallintamallia. Koska hallitsemattomat käyttöoikeudet ohjelmistoroboteilla oli yksi riskejä käsittelevän kappaleen kriittisistä riskeistä, käydään myös käyttöoikeuksien hallinnan kontrolleja vielä erikseen läpi haastatteluissa nousseiden aiheiden pohjalta. Asiantuntija 5 korostaa keskitetyn käyttövaltuushallinnan merkitystä seuraavasti:

> *Näkisin, että tavoitteena on keskitetty käyttövaltuushallinta, mistä voidaan oikeasti katsoa, että mitä oikeuksia kenelläkin on mihinkin järjestelmään. Yhtä lailla, jos meillä on jokin tunnus, joka pyörittelee automatisoituja järjestelmiä, niin kyllä niistäkin pitää pystyä varmistamaan, että mihin kaikkialle tämä kyseinen automatisoitu prosessi oikeasti tekee jotain. Eli sellainen selkeä yksi paikka, mikä tietysti on osa sitä hallintamallia.* -Asiantuntija 5

Vaikka käyttöoikeuden haltijana on ihmisen sijaan robotti, tulee käyttövaltuushallintaan panostaa riskien minimoimiseksi. Riskipisteet ovat osittain samoja kuin ihmisten käyttövaltuuksien hallinnassa, mutta näissä on myös eroja. Esimerkiksi vaarallisia työyhdistelmiä tulisi välttää myös robottien osalta, ja tiettyihin järjestelmiin ei pitäisi olla pääsyä, vaikka käyttäjänä olisikin robotti. Toisaalta taas ihmiset vaihtavat salasanansa itsenäisesti, kun taas roboteille tämä tapahtuu esimerkiksi palveluntarjoajien salasanaholvien kautta. Asiantuntija 5 kuvaa käyttövaltuushallintaa edelleen seuraavasti:

> *Lisäksi, jos on jotakin suoria käyttövaltuuksia, niin ainakin ne on pystyttävä dokumentoimaan yhtä kattavasti kuin ihmisillekin. Eli tarvitaan selkeät nimeämiskäytännöt. On pystyttävä selkeästi erittelemään, että kyseessä on robotti. Ja ainahan se perustuu siihen, että annetaan vain sen verran oikeuksia, kun työtehtävän suorittamisen kannalta on tarpeellista. Lisäksi niitä oikeuksia tulisi säännöllisesti käydä läpi, että käytetäänkö niitä oikeasti. Jos joku taho sen tunnuksen saa käsiinsä, niin minimoidaan se, ettei ainakaan päästä sellaisiin järjestelmiin, mihin ei todellakaan tulisi päästä. Pidetään ne oikeudet oikeasti ajan tasalla ja*

> *varmistetaan, että sitä tunnusta ja salasanaa päivitetään myöskin näille roboteille. Tätä kautta sitten litigoidaan sitä riskiä, että joku sen tunnuksen saisi käyttöönsä.* -Asiantuntija 5

Lisäksi asiantuntija 4 kuvaa ohjelmistorobottien salasanojen päivittämistä seuraavasti:

> *Mitä itse olen havainnut, niin se robotti menee hakemaan sieltä palvelimelta jonkun tiedoston, ja tarvitsee sinne palvelimelle käyttöoikeuden. Niin mielestäni se on suoraan sanottuna paremmin hallinnassa ne käyttöoikeudet näiden robottien kanssa. Salasanat ovat paremmin salassa siellä BluePrism:in palvelimella niitä ei kukaan ihminen pääse selkokielisenä lukemaan ja robotti ei niitä taatusti kenellekään kerro. Ja nämä salasanat vaihdetaan myös tietyin väliajoin. Ellei nämä tunnukset vuoda jonnekin tai niitä ei käytä kukaan, jonka niitä ei kuuluisi käyttää, niin sanoisin, että se on parempi kuin että nämä tunnukset olisivat ihmisellä. Ihminen voi aina kertoa jollekin toiselle sen salasanansa.* -Asiantuntija 4

Käyttövaltuuksien hallinnassa on siis joitakin samoja piirteitä kuin ihmisten käyttämien käyttöoikeuksien hallinnassa, mutta erojakin löytyy. Tämän vuoksi organisaatiossa on hyvä keskitetysti pohtia, miten robottikäyttäjät huomioidaan käyttövaltuushallinnassa. Riskienhallinnan näkökulmasta on myös tiedostettava, että robottien käyttämien oikeuksien lisäksi on valvottava muita prosessin kannalta olennaisia käyttöoikeuksia. Kuten riskejä käsittelevässä kappaleessa mainittiin ohjelmistorobotit eivät reagoi hyvin muutokseen, joten pääsyä robotin käyttämään lähdedataan saattaa olla aiheellista rajoittaa. Lisäksi robottien muokkaamisen tulisi olla mahdollista vain rajatulle joukolle ihmisiä. Näistä henkilöistä on pidettävä tarkasti kirjaa. Asiantuntija 2 kuvaa näitä kontrolleja seuraavasti:

> *Käyttöoikeudet ovat aika olennaisessa osassa. Kenelle annetaan kehittäjänoikeudet, kuka pääsee esimerkiksi sinne Orgestratoriin (UiPathin hallintajärjestelmä), kuka pääsee hallitsemaan niitä robotteja ja kuka niitä pääsee muokkaamaan.*

> *Siihenkin pitää olla oma prosessinsa. Pitää olla tarkasti selvennettynä, että kuka vastaa ja mistä, ja kenellä on esimerkiksi kehittäjän rooli. On selvästi eriteltynä, keillä on kehittäjän oikeudet, ja muille osallisille annetaan sitten pelkät katseluoikeudet. Lisäksi kaiken pitää olla dokumentoituna, että kenellä on ja millaiset oikeudet. Lisäksi nousee esiin, että kenellä on käyttöoikeudet niihin aineistoihin, joita se botti käyttää. Esimerkiksi jos robotti lukee tietoa jostain excelistä, niin kuka pääsee niihin käsiksi.* -Asiantuntija 2

Kuten jo edellä käyttöoikeuksien yhteydessä mainittiin, omistajuustahojen määrittely on tärkeä kontrolli myöskin ohjelmistorobotiikkaan liittyen. Omistajuudetkin ovat osa hallintamallia. Hallintamallin tulisi rakentua niin, että kaikelle toiminnalle on nimetty omistajataho, joille on määritelty asianmukaiset vastuut. Asiantuntija 5 vertaili haastattelussaan ohjelmistorobottien ja ihmisten omistajuuksia seuraavasti:

> *Jokaiselle robotille pitäisi löytyä se omistajataho. Käytännössä se, että minä vastaan omalla tunnuksellani tehtävistä toimenpiteistä ja jos minun vastuullani on tehdä tallaisia automatisoituja prosesseja, niin kyllä se olen minä, joka vastaan siitä. Käytännössä se on omalla vastuullani, että se prosessi toimii oikein. Jos siellä tapahtuu jotain virhetilanteita, niin kaikki syyttävät sormet sitten ohjaavat minuun. Tämä on nyt se ensimmäinen asia mikä puuttuu. Tyypillisesti nämä riskit johtuvat yleensä siitä, että ei tiedetä mitä tapahtuu ja missä, niin se on yksi primäärinen kontrolli, että omistajuustahot on selkeästi määritelty.* -Asiantuntija 5

Automatisoitujen prosessien ei pitäisi antaa toimia vastuuttomasti. Jos kenellekään ei ole nimetty selkeää vastuuta prosessista, on vaarana liian suuri riskinotto. Lisäksi virhetilanteissa saatetaan olla tilanteessa, jossa ei tiedetä keneen tulisi ottaa yhteyttä. Jotta kontrollointi on mahdollisimman tehokasta, on määriteltävä omistava taho, sekä vastuun suuruus. Tätä kommentoi haastattelussaan Asiantuntija 6:

Yksi kontrolli ja hyvä käytäntö on se, että näillä prosessiautomaatioilla on hyvin määritellyt omistajuudet. Tämä kuuluu tietenkin siihen hallintamalliin, että sillä automaatiolla mitä käytetään, on omistaja. Ja korostaisin, että sen vastuun pitäisi olla aika suuri. Omistajan on pystyttävä kertomaan liiketoiminnallisesta näkökulmasta, että mitä kontrolleja siellä täytyy olla, koska ei se kehittäjä tätä tiedä, mutta sen liiketoimintavastuullisen pitää tietää. Ne IT-kontrollit on aika selkeitä, mutta nämä liiketoiminta-asiat ovat sellaisia, mitkä tulee sen hallintamallin kautta. -Asiantuntija 6

Asiantuntija 6 korostaa myös sitä, että prosessiautomaatiolle on nimettävä sekä tekninen omistaja, että liiketoimintaomistaja. Liiketoimintariskien hallinnan kannalta on tärkeää, että liiketoimintaomistaja ottaa vastuun robotin toiminnasta.

Siellä on oltava aina se tekninen omistaja ja liiketoimintaomistaja. Ja yleensä siellä on vain tekninen omistaja. Tässä olisi tarvetta sille, että liiketoiminta ottaa siitä vastuuta riittävästi. -Asiantuntija 6

5.3.3 Prosessitason kontrollit

Ohjelmistorobotiikkaohjelmatason kontrollien tavoitteena on ohjata organisaation ohjelmistorobotiikkaan liittyvää toimintaa kohti organisaation sille asettamia tavoitteita. Nämä kontrollit ovat usein ohjelmistorobotiikkaa ohjaavia käytäntöjä ja toimintasääntöjä. Ohjelmistorobotiikalle on tyypillistä prosessikohtaisuus, sillä yksittäinen robotti usein rakennetaan automatisoitavan prosessin ympärille. Jo englanninkielinen nimi *Robotic Process Automation* korostaa prosessikohtaisuutta. Täten ohjelmatasolla määritellyt toimintatavat ja säännöt tulisi saada osaksi jokaista automatisoitavaa ja automatisoitua prosessia. Tämän merkitystä korosti esimerkiksi Asiantuntija 2 seuraavasti:

Tarvitaan sellainen yksiselitteisesti määritelty kehitysprosessi. End-to-end -prosessi ohjelmistorobotiikkaan, eli mitä vaiheita ja mitä hyväksyntöjä, millaisissa

ohjausryhmissä ja millaisilla foorumeilla tätä asiaa käsitellään. Kun joku tunnistaa jonkin potentiaalisen kohteen automaatiolle, niin mihin se asia menee siitä, ja kuka sitä käsittelee. Minne idea laitetaan eteenpäin, kuka hyväksyy sen arvion ja siitä eteenpäin kuka vastaa ja kuka hyväksyy sen vaatimusmäärittelyn. Että prosessi on selkeästi määritelty koko robotin elinkaarelle, ihan siitä robotin käyttöönotosta siihen poistoon. -Asiantuntija 2

Prosessitasolla ohjelmistorobotiikkaa ohjaavien käytäntöjen osalta korostuu siis asianmukainen määrittely. Määrittely mahdollistaa, että jokaisessa automaatioprojektissa voidaan johdonmukaisesti noudattaa laadittuja käytäntöjä, ja ne voidaan selkeästi viestiä organisaatioon. Jokaisen automaatioprojektin tulisi seurata näitä määrittelyjä. Esimerkiksi edellisessä kappaleessa mainitut omistajuuksien ja vastuiden määrittelyt. Asiantuntija 2 kuvasi vaatimusmäärittelyn merkitystä haastattelussaan. Ohjelmatasolla annettu vaatimusmäärittely ohjaa jokaisen automaatioprojektin etenemistä ja asettaa raja-arvoja sille, mitä projekteja lähdetään kehittämään edelleen.

Ennakkoon tehty vaatimusmäärittely on tärkeää. Kehitykseen saadaan kulumaan tuhottomasti aikaa, kun aina löytyy poikkeuksen poikkeuksia. Kuinka paljon sitten kannattaa lähteä virittämään sitä robottia, ja kuinka moneen poikkeustilanteeseen se kannattaa ohjelmoida vastaamaan. Olennaisinta olisi saada sieltä se suurin massa. Eli ehkä tähän kehitykseenkin pätee se 80/20 jako, eli pieni osuus tapauksista edustaa suurta volyymiä. Eli kannattaako mallintaa esimerkiksi kolme yleisintä tapausta, joka kattaa 80 prosenttia tapauksista ja jättää ne todella erikoiset tapaukset mallintamatta. -Asiantuntija 2

Ennakkoon annetut määrittelyt ja raja-arvot auttavat toiminnan ohjaamisessa ja hallinnassa. Ohjelmatason määrittelyjen haasteena on määrittelyjen standardisoitavuus. Koska ohjelmistorobotiikka on hyvin prosessikohtaista, yleispätevien määrittelyjen antaminen on haastavaa. Ilman hallintamallia tai asianmukaisia seurannan ja raportoinnin työkaluja, on hankala antaa ennalta määriteltyjä raja-arvoja. Hyvin järjestetyt

raportoinnin työkalut, esimerkiksi tuntien seuranta, edesauttavat projektien ja prosessien keskinäisessä vertailussa. Tästä esimerkkinä Asiantuntija 1 kertoo seuraavasti:

> *Kustannusnäkökulmasta me lähdemme aina laskemaan robotin kustannuksia. Aluksi laskemme, kuinka toistuvasta tehtävästä on kyse, kuinka monta henkilöä sitä suorittaa ja kuinka paljon yhdellä henkilöllä menee aikaa siihen tehtävään. Sitten lasketaan, miten paljon sen botin koodaamiseen menee aikaa. Ja sitten vertaillaan näitä.* -Asiantuntija 1

Myös itse prosessit on aina määriteltävä ja kuvattava hyvin. Hyvä määrittely toimii pohjana muille kontrolleille. Tästä kertoi esimerkiksi Asiantuntija 3:

> *Ikään kuin olisi kyse mistä tahansa muusta tietojärjestelmäkehityksestä niin tehtäisiin katselmointeja ja läpikäyntejä. Jos se prosessi on kuvattu, niin siinähän on erilaisia tapoja pöytätestata sitä, että onko se prosessin kuvaus substanssiosaajan mielestä oikein. Kattaako prosessi kaikki palikat ja ovatko päättelysäännöt oikein.* -Asiantuntija 3

Kuten riskejä käsittelevässä kappaleessa jo mainittiin, robotit eivät siedä muutoksia. Stabiilissakin toimintaympäristössä saattaa tapahtua muutoksia eikä poikkeuksilta voida aina välttyä. Esimerkiksi robotin saamassa tiedossa tai robotin toiminnassa saattaa esiintyä poikkeuksia. Kuten tämän tutkielman teoriaosan kontrolleja käsittelevässä kappaleessa kerrottiin, organisaatiossa tulisi olla kontrolleja, joiden avulla pyritään hallitsemaan riskejä niiden toteutumisen jälkeen. Roboteissa tulisi esimerkiksi olla ohjelmoituna ennalta toimintaohjeet poikkeustilanteiden varalle, jottei toiminnan jatkuvuus kärsisi (Ratsula 2016 s. 244-245). Poikkeuksien hallinnan merkitystä korostivat tutkimuksessaan myös Merdan, Lepuschitz ja Axinia (2011). Tutkimuksessa kehotettiin organisaatioita luomaan sisäänrakennettuja toipumismekanismeja, joiden avulla poikkeamista aiheutuvia riskejä voidaan hallita (Merdan ja muut 2011). Samoja teemoja tuotiin esiin myös haastatteluissa:

> *Onhan tietenkin kaikki jatkuvuusasiat ja sen tyyppiset sellaisia mitä ei organisaatioissa välttämättä ole ajateltu. Jos kyseessä on esimerkiksi liiketoimintakriittinen prosessi niin sehän ei tietenkään riitä, että on arvioitu, että sellainen riski siihen liittyy. On oltava myös jonkinlainen jatkuvuussuunnitelma olemassa, että miten se prosessi suoritetaan, jos se automaatio ei ole käytettävissä.* -Asiantuntija 6

Myös haastatteluissa tuotiin esiin muutamia käytännön kontrolleja toiminnan jatkuvuuden varmistamiseksi. Kontrollien tarvetta tulisi aina arvioida prosessikohtaisesti. Toiminnan jatkuvuuden kontrollit ja toipumismekanismit vaihtelevat esimerkiksi prosessin liiketoimintakriittisyyden ja organisaation resurssien mukaan. Asiantuntija 2 mainitsi haastattelussaan erään organisaation toipumismekanismeista seuraavasti:

> *Poikkeuksia varten on sitten kehitetty sellaisia work aroundeja. Eli jos se robotti lakkaa toimimasta, niin voidaan vaihtoehtoisesti ajaa massana näitä aineistoja läpi. Ei sitten tarvitse yksitellen käsitellä läpi, ja saadaan toiminta jatkumaan.* -Asiantuntija 2

Myös Asiantuntija 4:n näkemyksen mukaan organisaatiot ovat panostaneet toiminnan jatkuvuuden kontrolleihin. Organisaation on pystyttävä vastaamaan poikkeustilanteeseen, jossa robotti lakkaa toimimasta. Väin varmistetaan toiminnan jatkuvuus poikkeustilanteesta huolimatta. Käytännössä tätä kontrolloidaan Asiantuntija 4:n mukaan seuraavasti:

> *Kummassakin tapauksessa sitä on ainakin varmennettu niin, että heillä on ensinnäkin useampi robotti-instanssi tekemässä sitä samaa tehtävää. Vaikka ne tekevät sitä samaa hommaa, niin niitä on kuitenkin useampi. Vaikka yksi instanssi taklaa, niin se on vähän sama kuin tietoliikenneverkko, että vaikka yksi linja katkeaa, niin toiminta silti jatkuu. Toisekseen, näissä kaikissa oli mietitty se, että kyllä sitä pystytään manuaalisestikin tekemään sitä tehtävää. Jos kävisi niin, että kaikki menisi*

> *totaalisen seis, että sillä robotilla ei pystytä tekemään enää mitään, niin sitten on vielä varotoimena, että prosessia aletaan tekemään manuaalisesti loppuun.* -Asiantuntija 4

Koska automatisoitavat prosessit ovat erilaisia, on prosessikohtaisesti arvioitava erilaisia poikkeustilanteita, joissa robotti voi ryhtyä toimimaan hallitsemattomasti. Tällöin riskinä on esimerkiksi tiedon eheyden rikkominen. Riskit ovat hyvin prosessikohtaisia, joten niin tulisi olla riskien hallintaan suunnitellut kontrollitkin. Asiantuntija 1 kuvaa prosessia, jossa havaittiin, että prosessi on erityisen altis tiedon eheyden rikkoutumiselle poikkeustilanteiden sattuessa, ja tätä riskiä varten ohjelmoitiin robottiin seuraavanlainen kontrolli:

> *Tätä (tiedon eheyttä) sitten kontrolloidaan niin, että jos se botti havaitsee 30 muutosta peräkkäin, niin se pysähtyy heti jo siinä ensimmäisessä ja vaatii manuaalisen tarkistuksen ennen kuin jatkaa toimintaansa. Eli ihmisen on vahvistettava, haluaako hän todella tehdä tämän muutoksen.* -Asiantuntija 1

Kuten kaikessa tietojärjestelmäkehityksessä, myös ohjelmistorobotiikassa tulee kiinnittää huomiota järjestelmäkehitykseen ja muutoshallintaan. Näillä kontrolloidaan ohjelmistorobottien suunnittelua, kehitystä ja muita niissä tapahtuvia muutoksia (Ratsula 2016 s. 242-244). Asiantuntija 4 kuvaa muutoshallinnan prosesseja hänen tarkastamissaan asiakasorganisaatioissa seuraavasti:

> *Ne ovat aina olleet sellaisia prosesseja, joissa se robotti lukee yrityksen sisäistä järjestelmää, esimerkiksi käyttöliittymän kautta käy lukemassa sitä tietoa. Niin se on ollut hyvin hanskassa, että jos jostain syystä järjestelmän käyttöliittymä, mistä se robotti lukee tai mihin se kirjoittaa, jostain syystä muuttuu, niin siitä on selkeät prosessit, että miten se robotin kehitystiimi saa tiedon tästä muutoksesta.* -Asiantuntija 4

Yksi tärkeimmistä muutoshallinnan kontrolleista on asianmukainen testaus. Mitään muutoksia tai uusia ohjelmistorobotteja ei pitäisi viedä tuotantoon ilman asianmukaista testausta. Asiantuntija 3 kuvaa testauksen merkitystä kehitysprosessin eri vaiheissa:

> *Se testaus on tärkeää ennen tuotantoa, tuotannon aikana ja tuotannon jälkeenkin siihen asti, että on saatu varmuus siitä, että se robotti toimii oikein ja hyvin. Sillä robotilla pitäisi olla sellainen vierihoito.* -Asiantuntija 3

5.3.4 Robottitason kontrollit

Robottitason kontrolleissa olennaista on pohtia kunkin prosessin näkökulmasta, missä suhteessa vaaditaan manuaalisia kontrolleja verrattuna automaattisiin. Ohjelmistorobotteihin on suhteellisen helppo ohjelmoida erilaisia automaattisia kontrolleja. Manuaalisia kontrolleja tulisi käyttää, kun automaattiset kontrollit eivät ole järkeviä. Edellisessä kappaleessa Asiantuntija 2 esimerkiksi mainitsi, että resurssien tehokkaan käytön kannalta voi olla järkevää siirtää harvinaislaatuisimmat poikkeustapaukset manuaaliseen käsittelyyn sen sijaan, että ne automatisoitaisiin robotin suoritettavaksi. Automaattisten ja manuaalisten kontrollien tulisi kokonaisuutena pelata hyvin yhteen. Asiantuntija 4 antoi haastattelussaan esimerkkejä sille, kuinka robottiin on ohjelmoitu erilaisia automaattisia kontrolleja, joiden perusteella poikkeustapaukset siirretään manuaaliseen käsittelyyn:

> *Tässä on kriittistä se, että miten se robotti toipuu ongelmatilanteissa. Lähettääkö se automaattisesti jonkun sähköpostin, tai esimerkiksi listan. Ja miten kontrolloidaan sitä, että jos on useampia prosesseja, niin valvotaanko näitä sen robotin tuottamia raportteja.* -Asiantuntija 4

Edellisessä kappaleessa mainittuja poikkeustilanteita varten on robottiin ohjelmoitava automaattisia kontrolleja. Roboteissa tulisi aina olla automaattisena kontrollina pysäyttää toiminta, jos mitään epätavallista tulee vastaan. Näin vältetään tilanteet, joissa

tiedon eheyttä lähdettäisiin systemaattisesti rikkomaan. Tätä Asiantuntija 5 ja Asiantuntija 3 kuvasivat haastatteluissaan seuraavasti:

> *Jos se robotti kohtaa jotain hämmentävyyksiä, eikä tiedä miten toimia, niin se nostaa sitten käden pystyyn ja keskeyttää toimintansa, eikä tavallaan tuhoa sitä koko datan eheyttä sillä, että se alkaa puskea jotain väärää dataa*. -Asiantuntija 5

> *Ohjelmistokehityksen hyvien tapojen mukaan ne (kontrollit) pitäisi olla jo rakennettuna siihen robottiin, että sen pitää tarkistaa se tieto mitä se saa käsiteltäväkseen. Että kun robotti saa tietynlaisen sanoman, se tarkistaa noudattaako se sitä annettua määrittelyä ja jos ei noudata niin sitten käsi pystyyn ja ilmoitetaan että täällä on nyt jotain häikkää.* -Asiantuntija 3

Automaattisten kontrollien lisäksi tarvitaan manuaalisia kontrolleja. Esimerkiksi poikkeustapaukset olisi hyvä siirtää manuaaliseen käsittelyyn. Ohjelmistorobottiin ei välttämättä kannata tai edes pystytä ohjelmoimaan kaikkia päättelysääntöjä, jolloin manuaaliset tarkistukset ja käsittely on tärkeässä roolissa. Manuaalisten ja automaattisten päättelysääntöjen ja kontrollien määrä ja suhde tulisi suunnitella siten, että prosessi on mahdollisimman luotettava ja robottitason riskit ovat mahdollisimman hyvin hallinnassa. Manuaalisten ja automaattisten kontrollien tehokkaasta yhdistelystä kertoo esimerkiksi Asiantuntija 4:

> *Jos sen robotin toiminnassa on virheitä, niin heillä on todella hyvät prosessit ollut siitä, että robotti kirjoittaa lokia, ja siitä lähtee sitten sähköpostiviestit eteenpäin ja sitä asiaa lähdetään sitten manuaalisesti tutkimaan*. -Asiantuntija 4

5.4 Vaatimukset kontrolliympäristölle

Kontrolliympäristön näkökulmasta on olennaista tunnistaa missä vaiheessa oman organisaation ohjelmistorobotiikkatoiminta on. Kontrolliympäristön merkitys ja sille asetetut vaatimukset kasvavat ohjelmistorobotiikkatoiminnan maturiteetin kasvaessa. Useimmat organisaatiot ovat vielä kehityksen alkuvaiheessa. Muutaman onnistuneen implementoinnin jälkeen usko ohjelmistorobotiikkaan kasvaa ja osaaminen karttuu. Tämän seurauksena ohjelmistorobotiikan hyötyjä lähdetään tavoittelemaan uusien prosessien automatisoinnilla. Lisäksi on pidettävä mielessä toimintaan liittyvät riskit. On arvioitava, onko organisaation kontrolliympäristö riittävän tehokas vastaamaan ohjelmistorobotiikan mukanaan tuomiin haasteisiin. Ohjelmistorobotiikalle on tyypillistä riskien prosessikohtaisuus. Automatisoitujen prosessien määrän kasvaessa, myös riskipinta kasvaa. Lisäksi automatisoitavat prosessit usein monimutkaistuvat toiminnan laajentuessa. Tätä asiantuntija 6 kuvasi haastattelussaan seuraavasti:

> *Onhan se vääjäämätöntä, että aluksi otetaan ne low hanging fruits, mitkä ovat niitä yksinkertaisia prosesseja, millä on iso vaikutus. Sitten kun ne ovat kuihtuneet pois, niin on mietittävä, miten sitä kysyntää saadaan ylläpidettyä ja automatisoitua enemmän. Tässä tulee usein kyseeseen myös yhä sophistikoituneemmat ratkaisut, jotka sitten mahdollisesti yhdistelevät koneoppimista ja muuta. Tyypillisesti se etenee näin*. -Asiantuntija 6

Ohjelmistorobotiikan leviäminen tapahtuu organisaatiossa usein kokeilun kautta. Alkuun hankitaan ensimmäisiä kokemuksia, minkä jälkeen toimintaa laajennetaan uusien prosessien automatisointiin. Tämä tukee Fungin (2014) ja Slabyn (2012) tutkimuksissa esiin nousseita havaintoja prosessiautomaatiolle soveltuvista prosesseista. Tarkempaa tietoa heidän tutkimustuloksistaan löytyy tämän tutkielman teoriaosan kappaleesta 3.1 *Ohjelmistorobotiikan käyttö* Taulukosta 2: *Vaatimukset automatisoitavalle prosessille*. Mitä laajemmalle ja monimutkaisemmaksi toiminta etenee, sitä isompi tarve on ohjelmistorobotiikan hallinnalle ja valvonnalle. Luotettavan kontrolliympäristön näkökulmasta on tärkeää luoda hallintamalli jo mahdollisimman varhain. Hyvä hallintamalli parantaa

välittömästi kontrolliympäristön laatua, mutta sen hyödyt realisoituvat erityisesti tulevaisuudessa. Ohjelmistorobotiikan leviämisen ja hallintamallin yhteyttä kuvaa Asiantuntija 2 seuraavasti:

> *Muutama vuosi sitten, monissa organisaatioissa ohjelmistorobotiikka oli vielä niin uusi asia, niin oltiin pitkälti sellaisessa kokeiluvaiheessa. Mielessä oli vain kustannussäästöt ja haluttiin vain niitä ensimmäisiä kokemuksia ohjelmistorobotiikasta. Tällä hetkellä se on lähtenyt leviämään, eli sitä on organisaatioissa käytössä useita kymmeniä robotteja. Ja se selkein mitä on pitänyt tehdä nyt kun se ohjelmistorobotiikka on yleistynyt, on se kokonaisuuden ohjelmatason hallinta.* -Asiantuntija 2

Ohjelmistorobotiikan kehitys tapahtuu organisaation näkökulmasta alhaalta ylös, kun taas hallintamallin ideana on johtaa ohjelmistorobotiikkaa ylhäältä alas. Ohjelmistorobotiikan kehitys alkaa usein yksittäisestä projektista yksittäisessä organisaatioyksikössä. Tällöin organisaatiotason hallintamallia ei koeta vielä kovin tarpeelliseksi. Kuten teoriaosassa jo kappaleessa 3.1 Ohjelmistorobotiikan käyttö organisaatiossa mainittiin, hallintamallin käyttöönotto voi tuntua turhalta, kun organisaatiossa toimii vain muutama robotti. Valmis hallintamalli saa kuitenkin kiitosta viimeistään siinä vaiheessa, kun toiminnassa on kymmeniä tai satoja robotteja (Mancher ja muut 2018). Tätä ongelmaa kuvaa Asiantuntija 6 seuraavasti:

> *Ohjelmistorobotiikan käyttö aloitetaan usein pilotoimalla, eli ryhdytään tekemään niin sanotusti bottom-up. Tällöin ei missään vaiheessa tehdä sitä hallintamallia, vaan toiminta on kokeilutyyppistä. Tämä on iso ongelma monissa organisaatioissa*.
> -Asiantuntija 6

Näin voidaan todeta, että tehokas ohjelmistorobotiikan kontrolliympäristö vaatii tuekseen hallintamallin. Hallintamallin tulisi olla riittävän joustava, jotta se tukee ohjelmistorobotiikan prosessikohtaista luonnetta. Hallintamalli auttaa ohjaamaan ohjelmistorobottien kehitystä ja ohjelmistorobotiikan leviämistä organisaatiossa. Sen tulisi myös

varmentaa toiminnan luotettavuus ja tuotettavien robottien laatu. Sitä mukaan, kun automatisoidaan uusia prosesseja ja käyttöönotetaan uusia robotteja, tulisi hallintamallin varmistaa, että kontrolliympäristöön tuotetaan kaikki tarvittavat uudet kontrollit. Tästä Asiantuntija 5 kertoi haastattelussaan seuraavasti:

> *Kaikki muutokset, joita tullaan ottamaan käyttöön, niin jonkun ne pitää ymmärtää. Ei voida vain mennä sokeana. Miten itse näen asian tietoturvan näkökulmasta, niin meillä on määrätyt kontrollit millä me suojaamme meidän tietojamme ja varmistetaan, että meidän järjestelmämme on käytettäviä ja tiedot eheitä. Jos meillä on orkesteri erilaisia robotteja pyörimässä, niin kyllä ne kaikki kontrollit, joita meillä on tunnistettavissa sieltä riskiarvioinnista pitää olla tiedossa. Liittyi se sitten yhteen tai useampaan automatisoituun prosessiin niin ne pitää olla siellä kontrolliympäristön kuvauksessa. -Asiantuntija 5*

Perinteisin tapa seurata kontrolleja ja varmistua kontrolliympäristön laadusta on kontrollien testaus. Kontrollien testauksessa arvioidaan kontrollin toimivuus tarkastelemalla riittävän kattavaa otosta tietyn prosessin tuotoksesta ja päättelemällä otoksen perusteella toimiiko tietty kontrolli suunnitellusti. Kontrollien testaaminen on työlästä ja vaatii organisaation ulkopuolisen objektiivisen henkilön. (Sihvonen 2019 s. 122-123). Tästä esimerkkinä Asiantuntija 5 jatkaa seuraavasti:

> *Esimerkiksi tietoturvassa meidän työmme perustuu siihen, että meillä on karkeasti 200 erilaista kontrollia ja niiden toimivuus verifioidaan säännöllisesti vähintään vuosittain. Nyt kun sinne toimintaympäristöön tulee uusia toiminnallisuuksia niin siihen meidän 200:n listaamme pitää sitten lisätä niitä RPA tyyppisiä kontrolleja, mitä on tunnistettu. Oli niitä sitten 50 tai 500 niin ne pitää listata ylös ja niihin pitää suunnitella, että miten verifioidaan, että se kyseinen kontrolli on toiminut. Se on tietenkin isompi hallinnollinen kuorma, mutta välttämätöntä, jotta näitä robotteja voidaan järkevästi hallinnoida ja riskejä hallita. Mitä enemmän ja mitä syvemmälle me menemme tuohon automaatioon, niin sitä enemmän meillä pitää*

> *olla niitä kontrolleja, jotka varmistavat, että se tekeminen on turvallista.* -Asiantuntija 5

Jonkinlainen viitekehys toiminnan organisoimiseksi olisi suositeltavaa. Ulkoisilta asiantuntijoilta voi hakea apua toiminnan asianmukaiseen järjestämiseen. Kohdeorganisaatiolla on esimerkiksi käytössä kontrolliviitekehys asiakkaiden automaatioympäristöjen tarkastamiseen, kertoo Asiantuntija 6

> *Meillä on asiakkaiden automaatioympäristöjen tarkastamiseen oma viitekehys. Suosittelen tämän tyyppisen kontrolliviitekehyksen hyödyntämistä, kun organisaatiossa ohjelmistorobotiikkaa viedään eteenpäin. Tietenkin ymmärrän, että sellaisia ei ole hirveästi saatavilla.* -Asiantuntija 6

Ohjelmistorobotiikkaan liittyviä ohjeistuksia löytyy ainakin tilintarkastajille ohjelmistorobottien tarkistuksen tueksi, mutta varsinaista sisäisen valvonnan viitekehystä ei ohjelmistorobotiikkaan vielä ole. Kontrolliympäristön ja hallintamallin luomiseksi voidaankin hyödyntää erilaisia IT ja sisäisen valvonnan viitekehyksiä. Tämän tutkielman teoriaosassa on kuvailtu kahta riippumattomien organisaatioiden lanseeraamia viitekehyksiä. COSO-viitekehys sisäisen valvonnan ja COBIT-viitekehys hyvään tiedonhallintatapaan. Organisaatiossa voidaan peilata omaa kontrolliympäristöä näihin viitekehyksiin, ja räätälöidä tarpeidensa pohjalta omaa toimintaa kuvaavan viitekehys. Myöskin asiantuntija 2 kuvaa hyötyjä yhden yhtenäisen viitekehyksen käytöstä seuraavasti:

> *Eli periaatteessa koko elinkaari sille robotille pitäisi tapahtua selkeästi. Kaikkia robotteja esimerkiksi arvioidaan saman viitekehyksen avulla, että onko manuaalisia toimenpiteitä vaativia kohtia, onko sähköisiä toimenpiteitä, kuinka monta järjestelmää prosessiin liittyy ja millaisia ne ovat. Näiden tietojen perusteella sitten lähdettäisiin tarkasti käsittelemään sitä robottien kehitystä. Periaatteessa se, että kaikkien robottien business case -arviot ovat vertailukelpoisia, kun ne aina käsitellään samaa kaavaa noudattaen. Samalla tämä auttaa resurssien kohdistamisessa*

ja vähentää riskiä siitä, että lähdettäisiin viemään eteenpäin sellaista prosessia, jota ei oikeasti kuuluisi automatisoida. -Asiantuntija 2

Ennalta määritelty viitekehys auttaa varmistamaan, että tiettyihin ennalta määriteltyihin riskeihin voidaan ottaa kantaa jo heti robotin kehitysvaiheessa. Ohjelmistorobotin kehittäjä on usein tekninen asiantuntija, eikä välttämättä osaa kehityksessä ottaa huomioon kaikkia liiketoiminnan kannalta kriittisiä riskejä tai niiden hallinnan kannalta tehokkaita kontrolleja. Tiettyä viitekehystä seuraamalla voidaan ohjata robottien kehitystä. Lisäksi voidaan määritellä ehtoja sille, millä kriteerein ohjelmistorobotiikkaa lähdetään kehittämään. Kun kehitykselle on asetettu tietynlaiset raamit, on kokonaisuus helpompi hahmottaa ja hallinta selkeytyy. Yleismitalliset määritelmät koko organisaation ohjelmistorobotiikkatoiminnalle auttavat eri toimijoita pelaamaan paremmin yhteen. Viitekehyksen lisäksi erilaiset matriisit auttavat varmistamaan, että tietyt kontrollit esimerkiksi asianmukaisten vastuullisten nimeäminen, on järjestetty jokaisen automatisoidun prosessin osalta. Asiantuntija 2 ehdottaa esimerkiksi vastuunjakotaulukkojen hyödyntämistä toiminnan organisoinnin tukena:

Pitää olla tietyn tasoinen ohjausryhmä, jonka vastuulla se toiminnan järjestäminen on. Tarvitaan joku organisoitu tapa ohjata sitä toimintaa. Esimerkiksi sellainen RACI-matriisi, eli vastuunjakotaulukko pitäisi täyttää jokaisesta asiasta. Eli kuka on vastuussa tunnistamisesta, ketä informoidaan, ketä konsultoidaan ja kuka on loppupeleissä vastuussa. -Asiantuntija 2

Tehokkaan ja luotettavan kontrolliympäristön tulisi vastata ennalta määriteltyjä riskejä. Osana kontrolliympäristöä olisi siis hyvä olla toiminnan laajuutta vastaava riskienhallintajärjestelmä. Kun toiminta on vielä pientä, riskejä voidaan arvioida prosessikohtaisesti, esimerkiksi jonkinlaisen täytettävän prosessikohtaisen dokumentin kautta. Toiminnan laajetessa robotti- ja prosessikohtaisten riskien lisäksi on otettava tarkasteluun mukaan myös ohjelmistorobotiikkaohjelmatason riskit. Riskienhallinnassakin nousee esiin ristiriita ylhäältä-alas tapahtuvan hallinnan ja alhaalta-ylös tapahtuvan ohjelmistorobotiikan

leviämisen välillä. Ohjelmistorobotiikan levitessä, tarve riskienhallinnalle kasvaa prosessitasolta ohjelmatasolle. Asiantuntija 2 kuvaa riskienhallintaa seuraavasti:

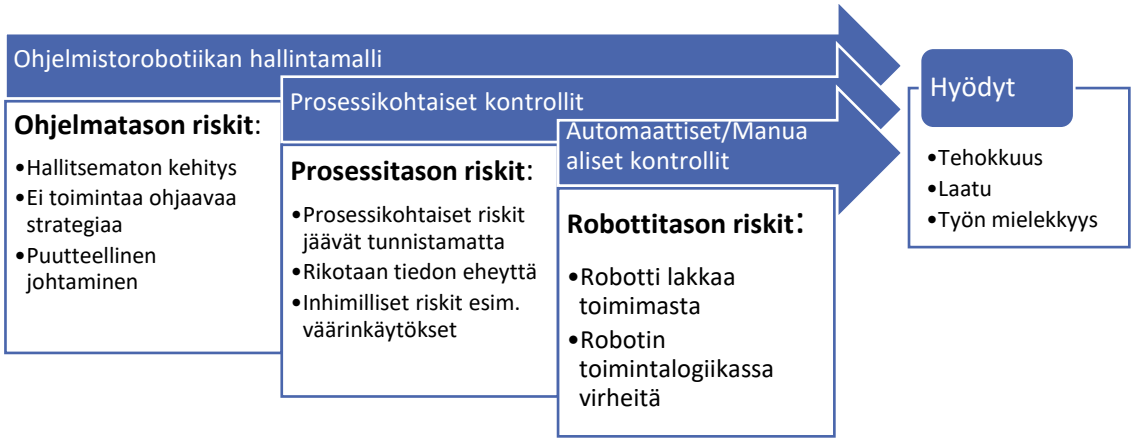
> *Kyllä riskejä pitäisi tunnistaa jokaisella näistä tasoista. Tunnistaa mitkä ovat yhden robotin riskit ja mitkä robotiikkaohjelman riskit, että niitäkin on sitten käsiteltävä eri tasoilla. Etenkin ylätasolla, kun tarkastellaan robotiikkaohjelmaa, niin pitäisi tunnistaa näitä riippuvuuksia eri yksiköiden ja robottien välillä. Eli ensin kokonaisuuden hallinta ja sitten kun niitä riskejä on tunnistettu, mennään niihin riskienhallintakeinoihin. Ohjelmatasolla määritellään, lähdetäänkö ehkäisemään riskejä, poistamaan riskiä, vai minimoimaan riskiä. Riskit kuuluvat liiketoimintaan, mutta on arvioitava millaisia riskejä, ollaan valmiita ottamaan. Millaisia ovat riskien todennäköisyys ja vaikuttavuus. Riskejä otetaan, mutta ne olisi ensin tunnistettava, jotta voidaan harkiten päättää, mitä toimenpiteitä tulee tehdä.* -Asiantuntija 2

Tämän tyyppinen riskienhallinta vaatii ohjelmatason organisointia ja hallintamallia. Organisaatiossa on siis tiedostettava, että toiminnan laajetessa keskitetystä hallintamallista ja riskienhallinnasta on saatavissa merkittäviä hyötyjä.

6 Johtopäätökset

6.1 Tutkimustulokset

Ohjelmistorobottien käyttöönotto osaksi liiketoimintaa asettaa uudentyyppisiä vaatimuksia organisaation kontrolliympäristölle. Kontrolliympäristön tavoitteena on valvoa organisaatiotavoitteiden mukaista toimintaa. Mikäli ohjelmistoroboteilla voidaan vaarantaa näiden tavoitteiden toteutuminen, tulee kontrolliympäristön vastata ohjelmistorobotiikan mukanaan tuomiin riskeihin. Kriittisiä ohjelmistorobotiikkaan liittyviä riskejä ovat sellaiset, jotka toteutuessaan estävät tavoitteiden täyttymisen. Riskien kriittisyyden kannalta on tärkeää arvioida organisaation ohjelmistorobotiikkatoiminnan laajuutta ja monimutkaisuutta. Mitä laajempaa ja monimutkaisempaa toiminta on, sitä suuremmaksi vaatimukset kontrolliympäristölle kasvavat. Kuvio 6 kuvaa yhteenvetona aiemmissa kappaleissa havaittuja riskejä ja niiden mukaisia kontrolleja kolmella tutkimuksessa käytetyllä tarkastelutasolla. Kuvio perustuu tutkielman teoriaosan kappaleessa 2.3 *Kontrollit* esitettyyn Kuvioon 2 *Kontrollien asettaminen*. Riskejä vastaavien kontrollien tavoitteena on edesauttaa ohjelmistoroboteilla haettavia tavoitteita, joiden tulisi olla linjassa organisaation tavoitteiden kanssa.



Kuvio 8. Tutkimustulosten tiivistäminen

Tutkimustulosten perusteella voidaan päätellä, että ohjelmistorobotiikan hallinnan kannalta on tärkeää tiedostaa mitkä organisaation tavoitteet laajamittaisen ohjelmistorobotiikan käyttöönoton osalta ovat ja missä vaiheessa käyttöönottoa edetään. Kriittisimmäksi ohjelmistorobotiikkaan liittyväksi riskiksi tutkimuksen perusteella osoittautui hallitsematon kehittäminen. Tämä riski on otettava huomioon jo ohjelmistorobotiikan käyttöönoton ensivaiheessa.

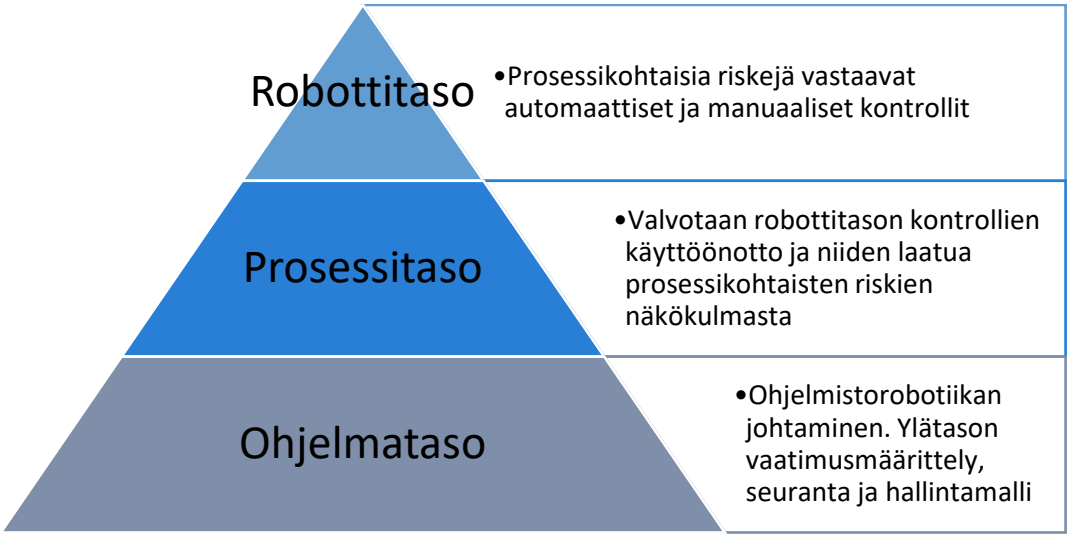
Haastatteluissa todettiin, että toistaiseksi käyttöönotetut robotit ovat olleet vähäriskisiä, eikä niillä ole automatisoitu kriittisiä prosesseja. Näin toimintatavaksi on sopinut, ettei varsinaista riskienhallintaa tai sisäistä ohjelmistorobottien valvontaa ole tarvinnut suorittaa. Riskeihin on vastattu sitä mukaan, kun ne ovat toteutuneet. Kontrollit ovat olleet lähinnä prosessitason kontrolleja, esimerkiksi toiminnallisuuksien testaamista ennen robotin tuotantoon viemistä. Vaarana on se, että toiminnan laajentuessa ja monimutkaistuessa, riskienhallintaan ei enää riitä ad hoc-lähtöinen lähestymistapa. Ohjelmistorobotiikan laajamittaisen käyttöönoton tulisi seurata ohjelmistorobotiikkatoimintaa ohjaavaa strategiaa. Tähän strategiaan tulisi ottaa myös mukaan riskienhallintastrategia, joka on linjassa käyttöönottostrategian kanssa. Näin varmistetaan, että toiminnan laajentuessa, riskienhallintatoimenpiteet skaalautuvat toiminnan laajuuteen sopiviksi. Riskienhallintastrategian tavoitteena on ehkäistä hallitsemattoman ohjelmistorobotiikkakehityksen riskiä.

Riskienhallinnan kannalta tehokkaimmaksi kontrolliksi nousi keskitetty ohjelmistorobotiikan hallintamalli. Hallintamallin avulla varmistetaan, että organisaatiossa tuotetaan jokaiseen automatisoitavaan prosessiin tarvittavat kontrollit. Näin varmistetaan strategian mukaisen riskienhallinnan toteutuminen. Tehokkaan hallintamallin osat vaihtelevat organisaatiokohtaisesti, mutta haastatteluissa korostui muutama ohjelmistorobotiikan näkökulmasta kriittinen tekijä, jotka hallintamallissa tulisi vähintään olla huomioituna.

Ohjelmistorobottien kehittäminen on suhteellisen yksinkertaista ja helppoa. Kehitykseen ei välttämättä vaadita IT-osaston tukea, vaan kehitystä voidaan toteuttaa itsenäisesti

liiketoimintayksiköissä. Verrattuna perinteisiin tietojärjestelmiin ohjelmistorobotiikka on luonteeltaan prosessikohtaista ja niiden elinkaari on verrattain lyhyt. Nämä piirteet puoltavat hallintamallin tärkeyttä. Koska erilaiset automatisoitavat prosessit ja siten myös riskit saattavat vaihdella suuresti, tulisi hallintamallin varmistaa, että eri prosessien ainutlaatuisista piirteistä huolimatta riskit ovat hallinnassa. Hallintamallin tulisi varmistaa, että jokaisen prosessin osalta kriittiset pisteet on otettu huomioon, ja niiden valvontaan soveltuvat kontrollit tuotetaan organisaation kontrolliympäristöön.

Tehokas kontrolliympäristö vaatii sen, että riskejä hallitaan eri tasoilla. Tutkielmassa on tarkasteltu ohjelmistorobotiikkaan liittyviä riskejä ohjelma-, prosessi- ja ohjelmistorobottitasolla. Ohjelmatasolla luodaan pohja tehokkaalle kontrolliympäristölle. Ohjelmatasolla määritellään riskienhallintavaatimukset, seurataan tavoitteiden saavuttamista, testataan kontrollien tehokkuutta ja määritellään ylätason hallintamalli ohjelmistorobotiikkatoiminnan ohjaamiseksi. Prosessitasolla valvotaan, että ohjelmatasolla määritellyt vaatimukset toteutuvat jokaisen automaatioprosessin osalta. Prosessitasolla on myös valvottava robottitason kontrollien toteutumisesta. Robottitasolla varmennetaan, että yksittäisen robotin asianmukaiseen valvontaan on asetettu sopivassa suhteessa automaattisia ja manuaalisia kontrolleja. Robottitasolla arvioidaan kontrollien teknistä toteutusta ja sitä, missä suhteessa toteutetaan automaattisia ja manuaalisia kontrolleja.



Kuvio 9. Kontrolloinnin tarve eri tasoilla.

Näiden vuorovaikutussuhteiden ja huomioiden pohjalta organisaatioiden tulisi räätälöidä heidän tavoitteitaan ja toimintaansa tukeva malli ohjelmistorobotiikan hallintaan, joka edistää organisaation riskienhallintaa ja sisäistä valvontaa. Tulevaisuudessa näiden teemojen merkitys tulee entisestään korostumaan toiminnan monimutkaistuessa ja levitessä yhä laajemmalle.

6.2 Tutkimustulosten luotettavuus ja rajoitteet

Tutkimustulosten luotettavuuden arviointi on tärkeä osa tieteellistä tutkimusta. Näin varmistetaan tieteellisten standardien ylläpitäminen tieteellisessä tutkimuksessa. Erityisesti laadullisten tutkimustulosten luotettavuuden kyseenalaistaminen on tärkeää, koska sitä usein pidetään vähemmän tieteellisenä tutkimusmenetelmänä (Hirsijärvi et al. 2004, 217). Reliabiliteetti ja validiteetti ovat yleisimmin käytettyjä mittareita tutkimuksen luotettavuuden määrittämiseksi. (Saaranen-Kauppinen ja Puusniekka 2006, 24-25.) Reliabiliteetti eli luotettavuus viittaa tutkimustulosten toistettavuuteen, eli saatujen tulosten ei-sattumanvaraisuuteen (Vilkka 2005; Hirsjärvi, Remes ja Saajavaara 2005). Validiteetti

eli pätevyys taas viittaa käytetyn tutkimusmenetelmän, konseptin tai toimenpiteen kykyä mitata tai edustaa tutkittavaa ilmiötä. (Hirsijärvi ja muut 2004, 216.)

Reliaabeli tutkimus tuottaa toistettavissa olevia tutkimustuloksia (Eriksson ja Kovalainen 2008, 292). Mikäli tutkimustulokset ovat kovin satunnaisia ja uudelleen toistettaessa tutkimustulokset saattaisivat olla hyvin erilaiset, ei tutkimuksen luotettavuuden arvioida olevan kovin hyvällä tasolla. Esimerkiksi aika ja käytetyt tutkimusmenetelmät saattavat vaikuttaa saatuihin tutkimustuloksiin. Tutkimuksen reliabiliteetin voidaan arvioida olevan hyvä, mikäli samaan tutkimustulokseen päädyttäisiin eri aikoina ja erilaisia tutkimusmenetelmiä käyttäen (Saaranen-Kauppinen ja Puusniekka 2006, 26). Tämän tutkimuksen osalta tiedostetaan, että aika on rajoittava tekijä, sillä ohjelmistorobotiikka yleistyy jatkuvasti ja teknologinen kehitys etenee vauhdilla. Tutkimustavoitteena on kuitenkin tehdä kartoittavaa tutkimusta tuoreesta ilmiöstä, joten aikarajoitteella ei ajatella olevan merkittävää vaikutusta tutkimustavoitteen toteutumisen kannalta.

Toinen reliabiliteetin kriteeri on tutkimuksen toistettavuus. Täydellinen toistettavuus voi kuitenkin laadulliselle tutkimukselle olla haastavaa, koska tarkastelua tehdään ilmiön luonnollisessa ympäristössä tiettynä hetkenä (Koskinen et al. 2005, 258), joten tutkijan on yleensä itse pystyttävä osoittamaan tutkimuksen luotettavuus (Kananen 2017: 175). Luotettavuutta voitaisiin parantaa esimerkiksi suorittamalla useampi haastattelukierros (Kananen 2017, 95), mutta tämän tutkimuksen kartoittavan luonteen vuoksi, ensimmäisellä kierroksella päästiin jo riittävälle syvyystasolle. Mikäli jatkossa halutaan tehdä tarkempaa tutkimusta tietystä haastatteluissa esille nousseesta teemasta, on useamman haastattelukierroksen tarvetta harkittava uudelleen.

Lisäksi reliabiliteettia voidaan parantaa kuvaamalla tutkimusprosessi ja käytetyt tutkimusmenetelmät tarkasti. Lisäksi alkuperäisen tutkimusaineiston saatavuus, aineistonkeruun kriteerien tarkka dokumentointi ja mahdollisimman monien esimerkkitapausten kattaminen ovat menetelmiä laadullisen tutkimuksen luotettavuuden parantamiselle. (Silverman 2000, 188.) Tämän tutkimuksen laadun parantamiseksi tutkimusprosessi ja

valitut menetelmät on kuvattu ja perusteltu kappaleessa 4. Tutkimusteemojen johtaminen ja teoreettinen viitekehys. Rajoitteena on se, ettei tunnistettavuussyistä alkuperäinen tutkimusaineisto ja tutkimuksen äänitteet ole saatavilla. Tämän vuoksi tutkimuksessa on käytetty suoria lainauksia ensisijaisena tapana viitata haastatteluihin. Näin lukija voi itse tehdä tulkintoja asiantuntijoiden lausumista ja tutkijan tekemät tulkinnat asiantuntijoiden sanoista voidaan helpommin kyseenalaistaa.

Validi eli pätevä tutkimus voidaan ymmärtää tehtyjen tulkintojen logiikan ja johdonmukaisuuden tai tulosten yleistettävyyden kautta suhteessa muihin tutkittaviin tapauksiin (Koskinen ja muut 2005, 254). Validi tutkimus tuottaa siis sellaisia päätelmiä tutkittavasta tapauksesta, esimerkiksi kohdeorganisaatiosta, että samoihin päätelmiin päädyttäisiin vastaavalla tutkimuksella myös toisessa kohdeorganisaatiossa. Validiteettiin vaikuttaa siis tutkimuksen ja empiiristen tulosten uskottavuus ja aitous (Lukka ja Modell 2010, 464). Tutkimustulosten validiutta puoltaa se, että tutkimustulokset ovat hyvin linjassa aiemman tutkimuksen kanssa ja asiantuntijoiden näkemykset ovat hyvin linjassa keskenään.

Suurimpana rajoituksena validiteetin kannalta on haastateltavien suhteellisen vähäinen määrä. Haastattelujen lukumäärä vaikuttaa olennaisesti aineiston laatuun (Hirsjärvi ja muut 2008). Hirsjärvi ja Sarajärvi (2008, 58) antoivat optimaaliseksi haastattelujen määräksi 15. Tässä tutkimuksessa kuitenkin koettiin haastateltavien asiantuntijuuden ja soveltuvuuden perusteella aineiston luotettavuus riittäväksi. Luotettavuuden parantamiseksi haluttiin tutkimuksessa panostaa enemmän haastateltavien asiantuntijoiden valintaan, kuin haastatteluiden lukumäärään. Myös käsitteiden asianmukainen käyttö parantaa validiteettia (Vilkka 2005). Tämän tutkielman osalta asianmukainen käsitteiden käyttö havaittiin rajoittavaksi tekijäksi. Uutena ilmiönä ohjelmistorobotiikan kontrollointiin liittyvä käsitteistö ei ole vakiintunutta. Jo termit ohjelmistorobotiikka ja kontrolliympäristö saatetaan ymmärtää eri tavalla riippuen henkilön taustasta ja omakohtaisista kokemuksista. Tähän pyrittiin vastaamaan määrittelemällä käytetyt termit tutkielman teoriaosassa mahdollisimman kattavasti. Myös haastateltaville asiantuntijoille lähetettiin etukäteen ennen haastattelua haastattelukutsu, jossa oli esiteltynä tutkimuksen

teoreettinen viitekehys ja selitettynä auki tutkimuksen kannalta kriittisimmät termit (kts. Liite 1).

6.3 Jatkotutkimusehdotukset

Tutkimuksen tavoitteena oli tehdä kartoittavaa tutkimusta, joten haastateltaviksi valittiin asiantuntijoita aihepiirin eri osa-alueilta. Näin tavoiteltiin mahdollisimman kattavaa otantaa tutkittavaan aiheeseen. Yleistettävämpiä tutkimustuloksia jokaiselta osa-alueelta saataisiin, jos haastateltaisiin useampia saman asiantuntija-alueen edustajia. Yhtenä jatkotutkimusehdotuksena olisi kohdentaa otanta tietyn asiantuntija-alueen edustajiin. Tämän tutkielman perusteella, erityisesti liiketoimintaosaajien näkökulmaa tulisi tuoda yhä enemmän osaksi ohjelmistorobotiikan tutkimusta. Lisäksi vastaava tutkimus voitaisiin suorittaa uudelleen tietyn ajan kuluttua, jolloin voitaisiin tehdä ajallista vertailua ja tutkia mihin suuntaan ohjelmistorobotiikan hallinnassa on edetty ja millaisia valmiita hallintamalleja on esimerkiksi käytössä.

Tulevaisuudessa aihealuetta tulisi tutkia yhä enemmän. Jatkotutkimusmahdollisuuksia on useita. Ensinnäkin näiden laadullisten tulosten tueksi tarvittaisiin yhä määrällisempää kvalitatiivista tutkimusta. Näin tutkimustulokset olisivat yleistettävämpiä. Tämän haastattelun pohjalta voitaisiin esimerkiksi toteuttaa ensin kyselytutkimus, jossa tutkitaan erityyppisten organisaatioiden kokemuksia ohjelmistorobotiikan valvonnasta ja heillä käytetyistä kontrollimenetelmistä. Lisäksi voitaisiin tutkia tarkemmin organisaatioita, joissa laajamittainen ohjelmistorobotiikan käyttöönotto on jo edennyt ja toimiva hallintamalli on jo käyttöönotettu. Näin saavutettaisiin arvokasta informaatiota hallintamallin käyttöönoton ongelmakohdista, sen vaiheista ja siitä, miten ohjelmistorobotiikan prosessikohtaisuus on saatu huomioitua organisaatiotason hallintamallissa. Myöskin vertailua erityyppisten hallintamallien välillä olisi mielekästä suorittaa.

Lähteet

Aalst, W. Van der., Bichler, M. & Heinzl, A. (2018). Robotic process automation. *Business & Information Systems Engineering*, Vol. 60(4), 269-272.

Agoglia, C., Brown, K. & Hanno, D. (2003). Dickinson Technologies, Inc: Assessing control environment and fraud risk. *Issues in Accounting Education*, 18(1), pp. 71-78. DOI:10.2308/iace.2003.18.1.71

Altamuro, J. & Beatty, A. (2010). How does internal control regulation affect financial reporting? *Journal of accounting & economics*, 49(1-2), pp. 58-74. doi:10.1016/j.jacceco.2009.07.002

Anagnoste, S. (2018a) Setting up a robotic process automation center of excellence. *Management Dynamics in the Knowledge Economy*, Vol. 6(2), 307–322.

Asatiani, A., Kämäräinen, T. & Penttinen, E. (2019). *Unexpected Problems Associated with the Federated IT Governance Structure in Robotic Process Automation (RPA) Deployment*. Haettu osoitteesta: https://aaltodoc.aalto.fi/bitstream/handle/123456789/39966/isbn9789526086989.pdf?sequence=1&isAllowed=y

Asatiani, A. & Penttinen, E. (2016). Turning robotic process automation into commercial success – case OpusCapita. *Journal of Information Technology Teaching Cases*, 6(2), 67-74. Haettu osoitteesta: http://dx.doi.org.ezproxy.jyu.fi/10.1057/jittc.2016.5

Ayat, M., Masrom, M., Sahibuddin, S. & Sharifi, M. (2011). Issues in Implementing IT Governance in Small and Medium Enterprises. DOI 10.1109/ISMS.2011.40

Bendoly, E., Rosenzweig, E. D. & Stratman, J. K. (2009). The efficient use of enterprise information for strategic advantage: A data envelopment analysis. *Journal of op*

erations management, 27(4), pp. 310-323. DOI:10.1016/j.jom.2008.11.001

Brand, K. & Boonen, H. (2010). IT governance based on Cobit 4.1 – A Management Guide. 3. painos. Van Haren Publishing.

Can, T. K., Türkyılmaz, M., & Birol, B. (2019). Impact of RPA technologies on accounting systems. *Muhasebe Ve Finansman Dergisi*, (82) Retrieved from https://search-proquest-com.proxy.uwasa.fi/scholarly-journals/impact-rpa-technologies-on-accounting-systems/docview/2236841443/se-2?accountid=14797

Collier, P. M., Berry, A. J., & Burke, G. (2007). Risk and management accounting: Best practice guidelines for enterprise-wide internal control procedures. Oxford: Else vier/CIMA.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (1992), Internal Control–Integrated Framework, COSO, CA.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013), Internal Control–Integrated Framework, COSO, CA.

D'aquila, J. (2013). Coso's Internal Control Integrated Framework Updating The Original Concepts For Today's Environment. *The CPA Journal*, 83(10), Pp. 22-29.

D'aquila, J. (2014). Coso's Updated Internal Control and Enterprise Risk Management Frameworks. *The Cpa Journal*, 84(5), Pp. 54-59.

Davenport, T.H. (1993), Process Innovation: Reengineering Work Through Information Technology, Harvard Business Press, Boston, MA.

DeBrusk, C. (2017). Five robotic process automation risks to avoid. Cambridge: Massachusetts Institute of Technology, Cambridge, MA. Retrieved from https://search-proquest-com.proxy.uwasa.fi/docview/1954616050?accountid=14797

Dehning, B., Richardson, V. J. & Zmud, R. W. (2007). The financial performance effects of IT-based supply chain management systems in manufacturing firms. *Journal of operations management*, 25(4), pp. 806-824. doi:10.1016/j.jom.2006.09.001

Deloitte. (2018). Internal controls over financial reporting considerations for developing and implementing bots. Available at: https://www2.deloitte.com/us/en/pages/audit/articles/financial-reporting-rpa-risks-and-controls.html

Denver, C. (2020). AUDITING THE BOTS: To realize the benefits of robotic process auto mation, internal audit needs to help the business address the risks. (ITAudit). *In ternal Auditor*, 77(1), p. 16.

Dewett, T. & Jones, G.R. (2001), The role of information technology in the organization: a review, model, and assessment, *Journal of Management*, Vol. 27 No. 3, pp. 313-346.

Drew, J. (2015). Keep pace with tech changes. *Journal of Accountancy*, 220(4), p. 20.

Eriksson, P. & Kovalainen, A. (2008). Qualitative methods in business research. London: Sage.

Eskola, J. & Suoranta, J. (1998). Johdatus laadulliseen tutkimukseen. Tampere: Vasta paino.

Fraser, J. & Simkins B.J. (2010). Enterprise risk management today's leading research and best practices for tomorrow's executives. John Wiley & Sons, Hoboken, NJ.

Fung, H. (2013). Criteria, Use Cases and Effects of Information Technology Process Auto mation (ITPA). *Advances in Robotics & Automation*, 3(3). DOI:10.4172/2168-9695.1000124

Ghauri, P. & Grønhaug, K. (2002). Research methods in business studies: A practical guide (2nd ed.). Harlow: Financial Times Prentice Hall.

Grabski, S. V., and S. A. Leech. (2007). Complementary controls and ERP impletnentation success. International Journal of Accounting Information Systems 8 (1): 17-39. DOI: 10.1016/j.accinf.2006.12.002.

Grabski, S. V., Leech, S. A. & Schmidt, P. J. (2011). A review of ERP research: A future agenda for accounting information systems. (Literature Review Articles) (enter-prise resource planning) (Report). Journal of Information Systems, 25(1), p. 37. DOI:10.2308/jis.2011.25.1.37

Graham, L. (2015). Internal Control Audit and Compliance: Documentation and Testing Under the New COSO Framework, John Wiley & Sons, Hoboken, NJ.

Haislip, J. Z., Masli, A., Richardson, V. J. & Watson, M. W. (2015). External reputational penalties for CEOs and CFOs following information technology material weak nesses. *International journal of accounting information systems*, 17, pp. 1-15. DOI:10.1016/j.accinf.2015.01.002

Henderson, B. C., Kobelsky, K., Richardson, V. J. & Smith, R. E. (2010). The relevance of information technology expenditures. (Report). *Journal of Information Systems*,

24(2), p. 39. DOI:10.2308/jis.2010.24.2.39

Hirsjärvi, S. & Hurme, H. (2008). Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus Helsinki University Press

Hirsjärvi, S., Remes, P. & Sajavaara P. (2005). *Tutki ja kirjoita*. Jyväskylä: Gummerus Kirjapaino Oy.

Hunton, J. E. (2002). Blending information and communication technology with accounting research. (Commentary). *Accounting Horizons*, 16(1), p. 55. DOI:10.2308/acch.2002.16.1.55

Hunton, J. E., Mauldin, E. G. & Wheeler, P. R. (2008). Potential Functional and Dysfunctional Effects of Continuous Monitoring. *The Accounting Revie*w, 83(6), pp. 1551-1569. DOI:10.2308/accr.2008.83.6.1551

ISO/IEC. 2008. International standard ISO/IEC 38500. *Corporate governance of information technology*. First edition 2008-06-01. ISO copyright office. Switzerland.

Jajodia, S., List, W., Mcgregor, G. & Strous, L. (1997). *Integrity and Internal Control in Information Systems: Volume 1: Increasing the confidence in information systems*.

Jajodia, S. & Strous, L. (2004). *Integrity and internal control in information systems*.

Janvrin, D. J., Payne, E. A., Byrnes, P., Schneider, G. P. & Curtis, M. B. (2012). The updated COSO internal control-integrated framework: Recommendations and opportunities for future research. (Report). *Journal of Information Systems*, 26(2), p. 189.

DOI:10.2308/isys-50255

Jiles, L. (2020). GOVERN YOUR BOTS! Strategic Finance, 101(7), 24-31. Retrieved from https://search-proquest-com.proxy.uwasa.fi/docview/2336298882?accountid=14797

Järvinen, P. (2004) *On research methods*. Tampere: Opinpajan kirja.

Kaarlejärvi S. & Salminen T. (2018). *Älykäs taloushallinto: Automaation aika*. Helsinki: Alma Talent. 269 s. ISBN 978-952-14-3429-7.

Kananen, J. (2017*). Laadullinen tutkimus pro graduna ja opinnäytetyönä*. Jyväskylä: Jyväskylän ammattikorkeakoulu. 213 s. ISBN 978-951-830-456-5.

Kerr, D. S. & Murthy, U. S. (2013). The importance of the CobiT framework IT processes for effective internal control over financial reporting in organizations: An international survey. *Information & management*, 50(7), pp. 590-597. DOI:10.1016/j.im.2013.07.012

King, B. A. – Hammond, T. – Harrington, J. (2017) Disruptive technology: Economic consequences of artificial intelligence and the robotics revolution. Journal of Strategic Innovation and Sustainability, Vol. 12(2), 53–67.

Kokina, J. & Blanchette, S. (2019). Early evidence of digital labor in accounting: Innovation with Robotic Process Automation. *International Journal of Accounting Information Systems*, 35. DOI:10.1016/j.accinf.2019.100431

Koskinen, I., Peltonen, T., & Alasuutari, P. (2005). *Laadulliset menetelmät kauppatieteissä*.

Tampere, Vastapaino.

Lacity M., Willcocks L. & Craig A. (2015a). Robotic Process Automation at Xchanging. The Outsourcing Unit Working Research Paper Series, Paper 15/03, http://eprints.lse.ac.uk/64518/1/OUWRPS_15_03_published.pdf.

Lacity, M., Willcocks, L. P. & Craig A. (2015b), Robotic Process Automation At Telefonica O2. The Outsourcing Unit Working Research Paper Series. pp: 3-4.

Lacity, M. & Willcocks, L. (2016) A New Approach to Automating Services. *MIT Sloan Management Review*, Vol. 58(1), 41-49.

Lahti, S. & Salminen, T. (2014). *Digitaalinen taloushallinto* (1. painos.). Helsinki: Talentum. 234 s.

Laudon, K.C. & Laudon, J.P. (2004), *Management Information Systems: Managing the Digital Firm*, Pearson, Prentice Hall, NJ.

Li, C., Peters, G., Richardson, V. & Watson, M. (2012). The consequences of information technology control weaknesses on management information systems: the case of Sarbanes– Oxley internal control reports. *MIS Quarterly*. 36(1), p. 179. doi:10.2307/41410413

Lukka, K. & Modell, S. (2010). Validation in interpretive management accounting research. Accounting, Organizations and Society. 35(4), p. 462–477.

Lähdemäki, J. (2013). COSO - moderni viitekehys sisäisen valvonnan toteutukseen. *Bal anssi: raportointi & hyvä hallinto*, 4, pp. 48-50.

Mack, N., Woodsong, C., MacQueen, K. M., Guest, G. & Namey, E. (2005). *Qualitative Research Methods: A Data Collector's Field Guide*. Family Health International, USA.

Madakam, S., Holmukhe, R. M., & Jaiswal, D. K. (2019). THE FUTURE DIGITAL WORK FORCE: ROBOTIC PROCESS AUTOMATION (RPA*). Journal of Information Systems and Technology Management: JISTEM*, 16, 1-17. DOI:http://dx.doi.org.proxy.uwasa.fi/10.4301/S1807-1775201916001

Mancher, M., Huff, C., Grabowski, R. & Thomas, J. (2018). DIGITAL FINANCE: THE ROBOTS ARE HERE. *The Journal of Government Financial Management*, 67(1), pp. 34-41.

Masli, A., Richardson, V. J., Sanchez, J. M. & Smith, R. E. (2011). The business value of IT: A synthesis and framework of archival research. (Report). *Journal of Information Systems*, 25(2), p. 81. DOI:10.2308/isys-10117

Merdan, M., Lepuschitz, W. & Axinia, E. (2011*). Advanced process automation using automation agents*.

Moeller, R.R. (2011), *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes*. John Wiley & Sons, Hoboken, NJ.

Moeller, R. R. (2013*). Executive's guide to coso internal controls: Understanding and implementing the new framework*. ProQuest Ebook Central https://ebookcentral-proquest-com.proxy.uwasa.fi

Moffitt, K. C., Rozario, A. M. & Vasarhelyi, M. A. (2018). Robotic Process Automation for Auditing. *Journal of Emerging Technologies in Accounting*, 15(1), pp. 1-10. DOI:10.2308/jeta-10589

Morris, J. J. (2011). The impact of enterprise resource planning (ERP) systems on the effectiveness of internal controls over financial reporting. (Academic Articles) (Report). *Journal of Information Systems*, 25(1), p. 129. DOI:10.2308/jis.2011.25.1.129

Nicolaou, A. I., Sedatole, K. L. & Lankton, N. K. (2011). Integrated Information Systems and Alliance Partner Trust. *Contemporary Accounting Research*, 28(3), pp. 1018-1045. DOI:10.1111/j.1911-3846.2011.01077.x

Ojiako, U. (2012). Using IS/IT to enhance service delivery. *Industrial Management & Data Systems*, 112(4), pp. 584-599. DOI:10.1108/02635571211225495

Osman, C. (2019). Robotic process automation: Lessons learned from case studies. *Informatica Economica*, 23(4), 66-75. DOI:http://dx.doi.org.proxy.uwasa.fi/10.12948/issn14531305/23.4.2019.06

Partanen, V. (2005). Taloushallinnon palvelujen tuottaminen palvelukeskusmallissa, *Tilisanomat* 4/2005, p.47-49

Piccoli, G. & Ives, B. (2005). IT-dependent strategic initiatives and sustained competitive advantage: A review and synthesis of the literature. *MIS Quarterly*, 29(4), pp. 747-776. DOI:10.2307/25148708

Power, M. (2013). The apparatus of fraud risk. Accounting, organizations and society, 38(6-7), pp. 525-543. DOI:10.1016/j.aos.2012.07.004

Premkumar, G., Richardson, V.J., & Zmud, R. (2004). Sustaining Competitive Advantage through a Value Net: The Case of Enterprise Rent-A-Car. *MIS Quarterly*. Executive, 3. pp. 189-199.

Ratsula, N. (2016*). Yrityksen sisäinen valvonta* (2., uudistettu painos.). Helsinki: Edita Publishing Oy. 314 s.

Rubino Michele, Vitolla, Filippo. (2014). Internal Control over financial reporting: Opportunities using the COBIT framework. *Managerial Auditing Journal*, Vol.29 No. 8, pp. 736-771.

Rubino, M. & Vitolla, F. (2014a). Internal control over financial reporting: Opportunities using the COBIT framework. *Managerial Auditing Journal*, 29(8). DOI:10.1108/MAJ-03-2014-1016.

Rubino, M., & Vitolla, F. (2014b). IT governance, risk management and internal control system: The role of the COBIT framework. Zagreb: Centar za istrazivanje i razvoj upravljanja d.o.o. Retrieved from https://search-proquest-com.proxy.uwasa.fi/conference-papers-proceedings/governance-risk-management-internal-control/docview/1635276139/se-2?accountid=14797

Rubino, M. & Vitolla, F. (2014c). Corporate governance and the information system: How a framework for IT governance supports ERM. *Corporate Governance*, 14(3), pp. 320-338. doi:10.1108/CG-06-2013-0067

Rubino, M., Vitolla, F. & Garzoni, A. (2017). How IT controls improve the control environ ment. *Management Research Review*, 40(2), pp. 218-234. DOI:10.1108/MRR-04-2016-0093

Rubino, M., Vitolla, F. & Garzoni, A. (2017). The impact of an IT governance framework on the internal control environment. *Records Management Journal*, 27(1), pp. 19-41. DOI:10.1108/RMJ-03-2016-0007

Saaranen-Kauppinen, A. & Puusniekka, A. (2009). *Menetelmäopetuksen tietovaranto*

KvaliMOTV: Kvalitatiivisten menetelmien verkko-oppikirja (Toinen vedos.). Tampere: Yhteiskuntatieteellinen tietoarkisto Tampereen yliopisto.

Sandrino-Arndt, B. (2008). People, Portfolios and Processes: The 3P Model of IT governance. Information Systems Control Journal, Volume 2/2008. ISACA. Luettavissa: http://www.isaca.org/Journal/Past-Issues/2008/Volume-2/Docments/jpdf0802-people-portfolios.pdf.

Schiano, W. & Weiss, J. W. (2006). Y2K all over again: How groupthink permeates IS and compromises security. *Business horizons*, 49(2), pp. 115-125. DOI:10.1016/j.bushor.2005.07.002

Seasongood, S. (2016). NOT JUST FOR THE ASSEMBLY LINE: A Case for Robotics in Accounting and Finance. *Financial Executive*, 32(1), pp. 31-32,35-36,39.

Shelleman, J. M. (1995). Levers of Control: How Managers Use Innovative Control Systems to Drive Strategic Renewal. The Academy of Management Executive, 9(2), p. 82.

Sihvonen, J. & Uusi-Hautamaa, L. (2019). *Väärinkäytökset yrityksissä: Estä, havaitse, kor jaa* (1. painos.). Helsinki: Alma Talent.

Silverman, D. (2000) *Doing qualitative research: A practical handbook*. Sage, London.

Simons, R. (1996). Levers of control: How managers use innovative control systems to drive strategic renewal. *The Internal Auditor*, 53(5), p. 12.

Steinhoff, J. C., Lewis, A. C. & Everson, K. E. (2018). The March of the Robots. (movement of intelligent automation). *The Journal of Government Financial Management*, 67(1), pp. 26-8.

Stoel, M. D. & Muhanna, W. A. (2011). IT internal control weaknesses and firm performance: An organizational liability lens. International journal of accounting information systems, 12(4), pp. 280-304. DOI:10.1016/j.accinf.2011.06.001

Tucker, I. (2018). GETTING A BETTER HANDLE ON COMPLIANCE AND CONTROLS. Strategic Finance, 100(6), 46. Retrieved from https://search-proquest-com.proxy.uwasa.fi/docview/2153607898?accountid=14797

Tucker, I. (2018). GETTING A BETTER HANDLE ON COMPLIANCE AND CONTROLS. Strategic Finance, 100(6), 46. Retrieved from https://search-proquest-com.proxy.uwasa.fi/docview/2153607898?accountid=14797

Tuomi, J. & Sarajärvi, A. (2018). Laadullinen tutkimus ja sisällönanalyysi (Uudistettu lai tos.). Helsinki: Kustannusosakeyhtiö Tammi.

Vedder, R. & Guynes, C. (2016). The Challenge Of Botsourcing. *The Review of Business Information Systems* (Online), 20(1), p. 1. DOI:10.19030/rbis.v20i1.9677

Vilkka, Hanna (2005). Tutki ja mittaa. 1. painos. Helsinki: Tammi

Weill, P. and Ross, J.W. (2004), *IT Governance. How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, Boston, MA.

Westland, J. C. (2000). Research Report: Modeling the Incidence of Postrelease Errors in Software. Information Systems Research, 11(3), pp. 320-324. DOI:10.1287/isre.11.3.320.12204

Zack, G. M. (2013). *Financial statement fraud : Strategies for detection and investigation*. ProQuest Ebook Central https://ebookcentral-proquest-com.proxy.uwasa.fi

Liitteet

Liite 1. Haastattelukutsu

HAASTATTELUKUTSU

OHJELMISTOROBOTIIKAN ASETTAMAT VAATIMUKSET ORGANISAATION KONTROLLIYMPÄRISTÖLLE

Tutkija: Sini Fröblom

Ohjaaja: Mikko Ranta, Vaasan yliopisto

TUTKIMUKSEN AIHE JA TAVOITTEET

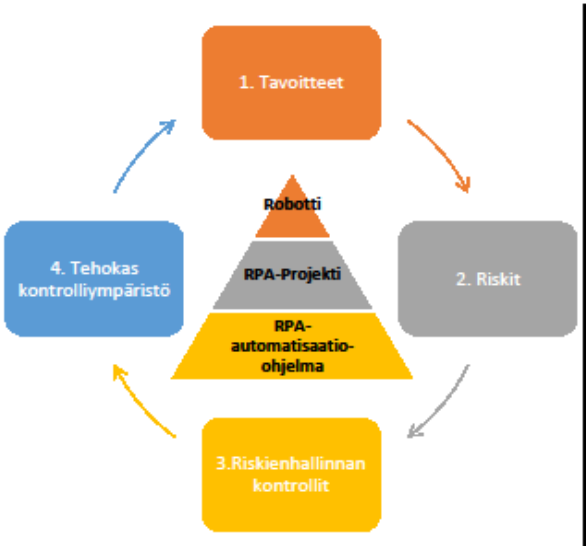
Tutkimuksen tavoitteena on tarkastella vaatimuksia, joita ohjelmistorobotiikan käytön ja käyttöönoton yleistyminen asettaa organisaation kontrolliympäristölle. Tarkoituksena on ensin kartoittaa ohjelmistorobotteihin liittyviä riskejä, ja sitten pohtia mitkä kontrollit olisivat tehokkaimmat näiden riskien hallitsemiseen. Tutkimuksen tavoitteena on saada syvempää ymmärrystä siitä, miten organisaation valvontatoimenpiteiden tulisi erota, kun työtehtäviä suorittaa ohjelmistorobotti, verrattuna tilanteeseen, jossa samaa työtehtävää suorittaa ihminen tai perinteinen tietojärjestelmä.

TUTKIMUSMENETELMÄ JA -AINEISTON KÄSITTELY

Toteutustapana on laadullinen tapaustutkimus, jonka aineisto kerätään teemahaastatteluilla lokakuun aikana. Haastateltavan luvalla haastattelut nauhoitetaan ja tutkimusaineisto litteroidaan analysointia varten. Litteroinnissa tunnistetiedot poistetaan anonymiteetin varmistamiseksi. Tutkija poistaa nauhoitukset heti tutkielman valmistumisen jälkeen. Halutessaan haastateltavat saavat tutustua aineistoon ennen tutkimuksen julkaisua.

TEOREETTINEN VIITEKEHYS:

Tutkimushaastattelu etenee alla olevan prosessikaavion mukaisesti. Prosessin vaiheet kuvaavat haastattelun eri teemoja ja tutkielman teoreettista viitekehystä. Tarkastelua tehdään robottitasolla, yksittäisen robotiikkaprojektin tasolla sekä koko organisaation ohjelmistorobotiikkaohjelmatasolla.



1. TAVOITTEET

Millaisia hyötyjä ohjelmistoroboteilla tavoitellaan?

2. RISKIT

Mitkä ovat kriittisimmät riskit ohjelmistoroboteilla haettujen tavoitteiden toteutumiselle?

3. RISKIENHALLINNAN KONTROLLIT

Ohjelmistorobottien ominaispiirteet huomioiden, millaiset käytännön kontrollit ovat tehokkaimmat em. riskien hallintaan ja robottien tavoitteiden mukaisen suoriutumisen valvontaan?

4. TEHOKAS KONTROLLIYMPÄRISTÖ

Miten varmistetaan kontrolliympäristön tehokkuus, kun prosesseja ja työtehtäviä suorittaa ihmisten tai perinteisten tietojärjestelmien sijaan ohjelmistorobotti?

Liite 2. Haastattelurunko

OHJELMISTOROBOTIIKAN ASETTAMAT VAATIMUKSET ORGANISAATION KONTROLLIYMPÄRISTÖLLE
HAASTATTELURUNKO:

HAASTATELTAVAN TAUSTA:

- Haastateltavan tehtävänkuva organisaatiossa ja suhde ohjelmistorobotiikkaan
    - *Miten ohjelmistorobotiikka näkyy työnkuvassasi?*
        - *Oletko ollut robottien käyttöönotossa mukana?*
        - *Konsultoinut robotteihin liittyen?*
        - *Tehnyt robotteihin liittyvää tarkastusta?*

1. TAVOITTEET:

- Millaisia hyötyjä RPA:lla tavoitellaan?
    - *Millaisia tavoitteita robottien käyttöönotolla kokemuksesi mukaan on?*
        - *Esim kustannussäästöt, toiminnan tehostaminen*

2. RISKIT tavoitteiden toteutumisen esteenä:

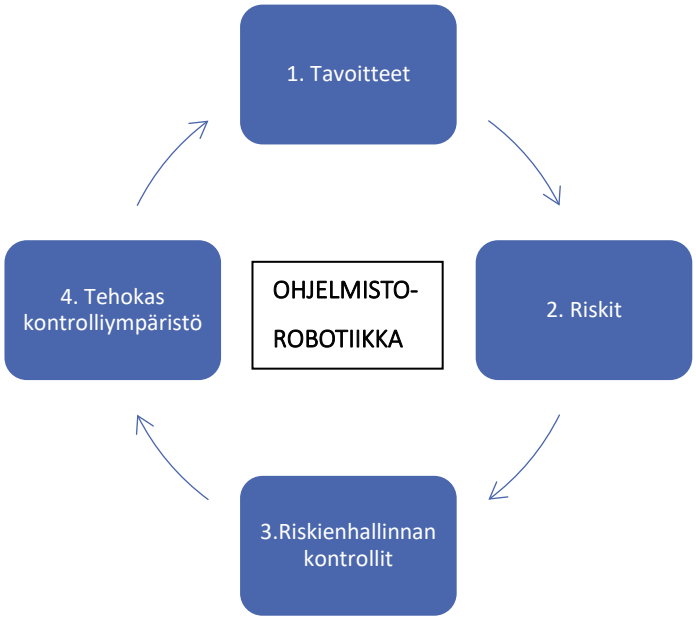
- Mitkä koet olevan kriittisimmät riskit ohjelmistorobotteihin liittyen?
    - Niiden RPA-projektien osalta, joissa olet ollut mukana:
        - Onko toteutettu minkälaista riskiarviointia tai riskienmääritystä?
        - Mitkä riskit on arvioitu kriittisimmiksi ja miksi?
            - Riskit suunnitteluvaiheessa
            - Riskit implementointi/käyttöönottovaiheessa
            - Riskit käyttöönoton jälkeen
            - Riskit Ohjelmistorobottiohjelmatasolla
            - Riskit käyttöönottoprojektitasolla
            - Riskit robottitasolla
            - Väärinkäytösriskit
            - Kontrolliriski

3. KONTROLLIT RISKIEN HALLINTAAN:

- Ohjelmistorobottien ominaispiirteet huomioiden, millaiset käytännön kontrollit ovat tehokkaimmat em. riskien hallintaan ja robottien tavoitteiden mukaisen suoriutumisen valvontaan?
    - *Millaisilla käytännön koontrolleilla robotteja on hallittu ja niiden toimintaa on seurattu niiden projektien osalta. joissa olet ollut mukana?*
        - Robotiikkaohjelmatasolla
        - RPA-projektitasolla
        - Yksittäisen robotin tasolla
    - *Mitkä kontrollit ovat olleet kaikkein tehokkaimpia ja miksi?*

4. TEHOKAS KONTROLLIYMPÄRISTÖ:

- Mitä vaatimuksia ohjelmistorobottien käyttöönotto asettaa organisaation kontrolliympäristölle?
    - *Mitä toimenpiteitä RPA:n käyttöönotolla on ollut organisaatioon ja sen kontrolleihin verrattuna aiempaan (manuaaliseen) prosessiin?*
        - Rakenteellisia muutoksia (esim. tietohallinto tai tiedon johtaminen)
        - Prosessimuutoksia (prosessien uudelleenorganisointia, virtaviivaistamista jne.)
        - Muutoksia riskienhallintaprosessissa
        - Muutoksia varsinaisissa kontrolleissa
    - *Miten uskoisit kontrolliympäristön muuttuvan tulevaisuudessa, ohjelmistorobottien yhä yleistyessä? Mitkä tekijät robottivaltaisemmassa ympäristössä mielestäsi korostuvat?*



1. TAVOITTEET

Millaisia hyötyjä ohjelmistoroboteilla tavoitellaan?

2. RISKIT

Mitkä ovat kriittisimmät riskit ohjelmistorobooteilla haettujen tavoitteiden toteutumiselle?

3. RISKIENHALLINNAN KONTROLLIT

Ohjelmistorobottien ominaispiirteet huomioiden, millaiset käytännön kontrollit ovat tehokkaimmat em. riskien hallintaan ja robottien tavoitteiden mukaisen suoriutumisen valvontaan?

4. TEHOKAS KONTROLLIYMPÄRISTÖ

Miten varmistetaan kontrolliympäristön tehokkuus, kun prosesseja ja työtehtäviä suorittaa ihmisten tai perinteisten tietojärjestelmien sijaan ohjelmistorobotti?