Ohjelmistokehitysprojektien ohjelmistoriskit

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Visamäki, Tietojenkäsittelyn koulutusohjelma

Kevät, 2018

Matti Murtomäki

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutusohjelma
Visamäki

Tekijä Matti Murtomäki **Vuosi** 2018

Työn nimi Ohjelmistokehitysprojektien ohjelmistoriskit

Työn ohjaaja Lasse Seppänen

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli löytää vastauksia ohjelmistokehitysprojektien riskienhallinnan kehittämiseksi, tutkimalla ohjelmistoprojekteissa käytettävien ohjelmistojen riskejä. Tämän lisäksi pyrittiin selvittämään riskienhallinnan keskeisimmät käsitteet sekä merkitys ohjelmistokehitysprojektienhallinnalle. Opinnäytetyön aihe kehittyi opintojen ja kiinnostuksen myötä - ilman varsinaista toimeksiantajaa.

Tutkimus koostettiin riskienhallintaa koskevaa lähde- ja ammattikirjallisuutta sekä tieteellisiä tutkimuksia monipuolisesti hyödyntäen. Tutkimuksen tueksi teoreettiseen viitekehykseen sisällytettiin viitteellinen ohjelmistokehitysprojekti Potta. Tutkimuksen rakenne koostui analyysimenetelmästä, johon sisältyi kirjallisuusselvitys. Toisena tutkimusmenetelmänä sovellettiin teemahaastattelua, jonka avulla tavoiteltiin mahdollisimman uutta tutkimustietoa.

Tutkimuksen avulla kyettiin selvittämään vastaukset kaikkiin kolmeen tutkimuskysymykseen. Ohjelmistojen riskit huomioidaan olennaisesti ohjelmistoprojektien suunnittelussa. Ohjelmistoprojektien riskienhallinta on organisaatiotasoinen kysymys, jossa riskienhallinnan tehokkuus mitataan yhteistyökumppanien, henkilöstön osaamisen ja organisaation panostuksen kautta. Tutkimuksen perusteella voi todeta, että etenkin teknologian ja toimintaympäristöjen kehitys luo uusia uhkatekijöitä, jotka tulisi huomioida ohjelmistokehitysprojektien suunnittelussa.

Avainsanat Ohjelmistokehitys, Projektinhallinta, Riskienhallinta, Ohjelmistoriski, Riskiarviointi

Sivut 45 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology
Visamäki

Author Matti Murtomäki **Year** 2018

Subject Software risks in software development projects

Supervisor Lasse Seppänen

ABSTRACT

The aim of this thesis was to complete a research to define software risks related to software development projects. Furthermore, the thesis was intended to define solutions for developing software risk management in software development projects. The research also strived to give a definition of software development risk management. The subject of the thesis developed by own interests and during the Bachelor's of Business Studies, without any special customer.

The content of the research was compiled versatilely from professional literature and dissertations. The thesis also includes a theoretical framework, which was compiled to support the research with a referential software development project Potta. The structure of the thesis consists of two separate research methods. An analytical process was built to guide the research throughout the whole structure of the thesis. The process included literature survey to examine software risks in software development projects. Another research method was a semi-structured interview, which defined the most recent information about software risks.

The research revealed essential issues considered as software risks. In today's risk management, attention focuses on the deployment of software in the project as well as the usability and complexity of software. In addition, employees' knowledge and skills were determined effectively. However, there are still many threat areas which must be focused on to achieve better results for project and risk management. Especially technology and environment changes in the future might cause various questions about threats.

Keywords Software development, Project management, Risk management, Software risk, Risk assessment

Pages 45 pages

Sisällys

1 JOHDANTO

Opinnäytetyö on tutkimus ohjelmistoprojektien toteutuksessa käytettävien ohjelmistojen riskeistä. Kiinnostus opinnäytetyön aiheeseen kehittyi tietojenkäsittelyn ja etenkin projektinhallinnan opintojen myötä. Tietojenkäsittelyn opintoihin sisältyivät olennaisena osana ohjelmointi ja ohjelmistot. Ohjelmistot ovat suuressa roolissa myös ohjelmistokehitysprojektien toteutuksessa. Riskienhallinnan osuus projektien menestyksessä on merkittävä, sen avulla kyetään hallitsemaan projektien kriittisimpiä osa-alueita. Tutkimuksen tarkoitus on laajentaa projektinhallinnan opintojen myötä hankittua osaamista sekä syventää tietämystä riskienhallinnasta ohjelmistokehitysprojekteissa.

Tutkimuksen avulla syvennytään ohjelmistokehitysprojektien riskienhallintaan, ja pyritään selvittämään ohjelmistoriskien merkitys projektinhallinnalle. Opinnäytetyön tutkimus perustuu tutkimusmenetelmään, jossa teoreettisen viitekehyksen avulla rakennetaan yleiskuva tutkimusongelmasta. Tutkimuksen ja teoreettisen viitekehyksen tukena on käytetty Helsingin yliopiston Potta-ohjelmistokehitysprojektia. Potta-projekti on viitteellinen projekti tutkimuksen ja loppuanalyysin tueksi, jonka avulla ohjelmistoprojektien riskienhallintaa voidaan mahdollisesti kehittää. Varsinainen teoriaosa käsittelee riskienhallintaa ja riskienhallinnan menetelmiä ohjelmistokehitysprojekteissa sekä yleisellä tasolla. Tutkimuksen avulla on tarkoitus saada vastauksia ohjelmistoriskin määritteelle, jonka jälkeen analyysissä sovelletaan kerättyä teoriatietoa ja tutkimustuloksia Potta-projektin riskienhallinnan kehittämiseksi. Tutkimuksen päämääränä on antaa kuva ohjelmistoprojektien riskienhallinnan nykytilasta sekä mahdollisesti uusia näkökulmia ja ehdotuksia riskienhallinnan kehittämiseksi.

Tutkimuskysymykset:

Miten ohjelmistojen käyttö on huomioitu projektisuunnitelmassa?
Miten ohjelmistojen hallinta ja käyttäminen on huomioitu riskienhallinnan näkökulmasta?
Miten ohjelmistoriskit on nykyisellään määritelty riskeiksi?

2 TUTKIMUSMENETELMÄT

Tutkimukseen sovelletaan kahta erilaista tutkimusmenetelmää: haastattelua ja analyysimenetelmää. Haastattelun ensisijainen tavoite on selvittää, miten ohjelmistokehitysprojektien ohjelmistoihin liittyvät riskit on määritelty projektienhallinnan näkökulmasta. Haastattelun avulla pyritään saamaan vastauksia tutkimuskysymyksiin työelämää hyödyntäen. Analyysimenetelmän osana suoritetaan kirjallisuusselvitys, jonka avulla tutkitaan ohjelmistoihin liittyvät riskitekijät projekteissa ja organisaatioissa. Analyysimenetelmä määrittelee tutkimukselle rakenteen ja toimintatavat, joiden mukaan tutkimus etenee. Molempien menetelmien avulla on tarkoitus tutkia ohjelmistoriskien määritteitä. Tutkimuksen loppuosa koostuu analyysista, joka laaditaan teoriaosan, tutkimushaastattelun ja kirjallisuusselvityksen pohjalta.

2.1 Tutkimushaastattelu

Opinnäytetyön tutkimuksessa käytetään puolistrukturoitua haastattelua, eli teemahaastattelua. Haastattelun kysymykset perustuvat teoreettisen viitekehyksen pohjalle, ja ne noudattavat pitkälti tutkimuskysymysten muotoilua. Kysymysten muotoilu on kaikille haastateltaville samanlainen. Teemahaastattelun valinta ja tutkimuskysymysten muotoilu perustuvat tutkimusaiheen käsitteellisyyteen. (Kajaanin ammattikorkeakoulu) Haastatteluun laaditaan neljä suuntaa antavaa kysymystä. Kysymysten muotoilulla tavoitellaan mahdollisimman kattavia vastauksia, joihin vastaaja voi itse laatia vastauksen lyhyesti, tai mahdollisesti hyvinkin laajasti.

2.2 Ankkuroidun teorian tutkimus

Opinnäytetyö rakentuu laadullisen, eli kvalitatiivisen - Grounded Theory-tutkimusmenetelmän pohjalle. Grounded Theory, eli suomennettuna ankkuroitu teoria -nimitystä käytetään paikoitellen kuvaamaan aineistolähtöistä tutkimusta. Ankkuroidun teorian tutkimuksessa on tarkoituksena käsitteellistää ja luoda suhteita kerätyn teorian käsitteiden välille. (Jyväskylän ylipisto 2015.)

Tutkimuksen aineisto voidaan kerätä monista eri lähteistä. Lähteinä voivat toimia muun muassa haastattelut, viralliset dokumentit, sanomalehdet tai kirjat. Mikä tahansa lähde, mistä on mahdollista kerätä tutkittavaan aineistoon liittyvää tietoa. Ankkuroidun teorian tutkimuksessa voidaan erottaa kolmesta viiteen erilaista vaihetta. Vaiheet muodostavat keskenään vuorottelevan prosessin, mikä toistuu tutkimuksen alusta loppuun saakka. Prosessin eri vaiheiden tulee sekoittua ja kietoutua toisiinsa läpi koko tutkimuksen rakenteen. Ankkuroidun tutkimuksen eri vaiheissa edetään tutkittavaan ongelmaan vaiheittain. (Virtuaali ammattikorkeakoulu)

Ensimmäisessä vaiheessa kuvataan tutkimuksen käsitteet, joiden avulla muodostetaan tutkimukselle karkeat suuntaviivat ja eräänlainen avain

teorian muodostamiseen. Karkeiden suuntaviivojen avulla pystytään rajaamaan tutkimusongelmaa, minkä lisäksi ne mahdollistavat tutkimuksen rakenteen kategorioimisen. (Virtuaali ammattikorkeakoulu)

Toisessa vaiheessa on olennaista yhdistää tutkimusaineisto etsimällä yhteyksiä kategorioiden välillä. Kategorioiden liittyminen toisiinsa muodostaen selkeän suhteen toisen vaiheen teorian rakenteelle. Aineiston keskeisen käsitteen, eli pääkategorian muodostamisen jälkeen on mahdollista laatia alakategorioita. Eri kategorioiden nivoutuminen pääkategoriaan muodostaa käsiteyhdistelmiä, joiden avulla syntyy toisen vaiheen teoria. (Virtuaali ammattikorkeakoulu)

Kolmannessa vaiheessa kerätään aineistoa, jota vertaillaan kriittisesti kerättyyn teoriaan. Aineistojen vertailu ja kerääminen ovat kolmannen vaiheen olennaisin tavoite. Negatiivisen tutkimusmateriaalin avulla on mahdollista testata aineiston kriittisyyttä, sekä tehdä tutkimushypoteeseja ja rajata olettamuksia. (Virtuaali ammattikorkeakoulu)

Neljäs vaihe koostuu perustellun teorian muodostamisesta, joka koostuu kategorioiden integroimisesta. Tässä vaiheessa tutkimuksessa esille kohonneita teorioita vertaillaan kerättyyn tutkimustietoon ja pyritään perustelemaan tutkimusvalintoja. Tutkimukselle on mahdollista luoda ilmiötä selittävät suhteet, yhdistelemällä kategorioita avainkategorian ympärille, sekä vertailemalla uusia teorioita aineiston perustelemiseksi. (Virtuaali ammattikorkeakoulu)

Viidennessä vaiheessa tutkimukselle kirjoitetaan raportti, tai mahdollisesti tutkitaan lisää teorioiden välisiä suhteita. Tutkimusaineistosta laaditaan johtopäätökset, sekä kuvataan, kuinka tutkimusaineiston teorian perusteella on saavutettu vastaukset tutkimuskysymyksiin. (Virtuaali ammattikorkeakoulu)

3 PROJEKTIN JA OHJELMISTOKEHITYKSEN ELINKAARIMALLIT

Onnistunut IT-projekti vaatii suunnittelun ja toteutuksen, jossa hyödynnetään yleisiä projektinhallinnan työkaluja ja tekniikoita. Sisällön suunnittelu, aikataulutus ja riskianalyysi ovat olennaisia projektinhallinnassa. Projektit voivat sisältää laitteiston, ohjelmiston tai palvelun toteutuksen, mutta projektinhallinnan työkalut ja tekniikat ovat samanlaisia. (Taylor 2004, 38.)

Larry Richmanin (2011) mukaan A Guide to the Project Management Body of Knowledge (PMBOK Guide) määrittelee IT-projektien vaiheet projektin elinkaareksi, joka noudattaa yleistä projektinhallinnan rakennetta. Rakenteeseen kuuluu viisi vaihetta. Projektin aloituksen aikana projekti määritellään ja vahvistetaan. Suunnitteluvaiheeseen kuuluvat projektin sisällön ja rakenteen määritteleminen. Varsinaisen toteutusvaiheen aikana projektihenkilöstö ja muut resurssit toteuttavat projektisuunnitelman mukaisesti määriteltyjä projektinvaiheita. Seuranta- ja tarkkailuvaiheessa projektisuunnitelman mukaista toteutumista tarkkaillaan sekä reagoidaan projektisuunnitelmaan mahdollisesti tulleihin muutoksiin. Viimeisessä vaiheessa, jota kutsutaan viimeistelyksi, kaikki projektin aktiviteetit ja prosessit viimeistellään, ja lopuksi projekti suljetaan. (Richman 2011, 21.)

Yleinen ohjelmistokehityksen elinkaarimalli SDLC kattaa kaikkien niin sanottujen ennustavien ohjelmistokehitysmallien vaiheet. Ennustaviin ohjelmistokehitysmalleihin kuuluvat muun muassa Waterfall ja V-model, jotka ovat yleisimpiä ohjelmistoprojektien toteutusmalleja. SDLC-ohjelmistokehityksen elinkaarimalli määrittelee ohjelmistokehitysvaiheet seuraavien vaiheiden kautta: määrittely, suunnittelu, toteutus, vahvistus, käyttöönotto ja ylläpito. (Stephens 2015, 276.) SDLC-malliin on myös monia muita lähestymistapoja, jotka noudattavat samaa perinteistä kaavaa. Yksi yleisimmistä on ketterä ohjelmistokehitysmalli Scrum. SDLC-malli toteutetaan Scrum-mallin periaatteiden mukaisesti tietyin aikavälein iteratiivisesti. (Mahalakshmi, Sundarar 2013, 195.)

Projektin elinkaaren PLC pitää sisällään suunnittelun, ohjauksen ja johtamisen, keskittyy ohjelmistoelinkaarimallin tekniseen puoleen ja itse tuotteen toteuttamiseen. Elinkaarien välillä vallitsee kuitenkin selkeä suhde, joka on paremmin nähtävissä kuvasta 1. (Taylor 2004, 43.)

Project Life Cycle (PLC) Phases	**Initiation Phase**		**Planning Phase**		**Monitor and Control Phase**	**Closeout Phase**	**Customer Service and System Maintenance**
Software or Systems Development Life Cycle (SDLC) Phases	**Concept**	**Requirements**	**Design**	**Implementation**	**Integration and Test**	**System Installation**	**Maintenance or Support**
	Project Activities •Gather data •Identify project requirements •Establish project scope •Develop high-level WBS •Estimate resources •Develop charter **Systems Development Activities** •Define product requirements •Develop feasibility analysis •Define product scope •Develop systems architecture		**Project Activities** •Assemble project team •Develop detailed WBS •Develop network analysis •Develop budget and schedule estimates •Write project plan •Kickoff project **Systems Development Activities** •Conduct trade-off analyses •Finalize product requirements •Complete preliminary design		**Project Activities** •Set up project organization •Set up and execute work packages •Direct, monitor, and control project **Systems Development Activities** •Complete preliminary design •Obtain design approval and sign-off •Develop detail designs •Construct system •Conduct unit, system, and integration tests •Deliver system	**Project Activities** •Conduct technical and financial audits •Obtain customer acceptance •Prepare transfer responsibility plan •Evaluate and document results •Close project office **Systems Development Activities** •Install and test system	**Project Activities** •Transfer project responsibility •Develop customer survey plan •Follow-up with customer •Provide customer service and maintain system **Systems Development Activities** •Operate and maintain system

Kuva 1. Projektin ja ohjelmistokehityksen elinkaaret ja aktiviteetit (Taylor 2004, 42).

3.1 Ohjelmistot ohjelmistonkehityksen elinkaarimallin eri vaiheissa

Projektin alkuvaihe vaatii huomattavan määrän dokumentoinnin ohjelmistoja, kuten myös projektinhallintaan ja suunnitteluun tarkoitettuja ohjelmistoja. (Chemuturi 2013, 159.) Vaatimusmäärittelyn perinteisiin työkaluihin voidaan luetella vuokaaviot, päätöspuut ja päätöstaulukot. Vaatimusmäärittelyjen tekniikat voidaan toteuttaa erilaisten vaatimusmäärittelyyn tarkoitettujen dokumentoinnin työkalujen avulla. (Mohapatra 2010, 93.) Vaatimusmäärittelyyn on myös monia muita mallinnustyökaluja, jotka soveltuvat vaatimusmäärittelyn vaativampiin osa-alueisiin. (Mohapatra 2010, 131.)

Ohjelmistojen suunnittelun lähtökohtana on ympäristö, johon ohjelmistoprojekti toteutetaan. Projektin toteutuksen laitteistot ja ohjelmistot valitaan tarpeen mukaan, ja siten että ne toimivat kokonaisuutena. (Stephens 2015, 87.) Ohjelmistojen kehittämiseen on lukuisia erilaisia ohjelmistoja, joita voidaan käyttää ohjelmistoprojektien toteutuksessa. Kehitysvaiheen työkaluihin voidaan luetella muun muassa ohjelmistokehitin, jonka avulla voi suorittaa erilaisia ohjelmiston kehittämisen vaiheita. (Stephens 2015, 146.)

Chemuturi (2009, 125) määrittelee testaustyökalut dokumentoinnin ja testauksen välineiksi, joita projektin tiimi käyttää samanaikaisesti ja rinnakkain. Testauksen työkalujen käyttö tulisi huomioida jo projektisuunnitelmassa. Uusien testaustyökalujen konfigurointi yrityksen tarpeisiin tulisi huomioida heti käyttöönottovaiheessa. Myös mahdollisen konfiguroinnin tuottaman ohjelmakoodin tallennus, sekä työvaiheiden dokumentointi on oleellista. Työkalun uudelleen käyttöönottovaiheessa tallennettujen muutosten hyödyntäminen on taloudellista ja nopeaa.

Hyväksymistestauksessa tuotteen tulisi vastata määrityksiä, minkä jälkeen asiakkaan on mahdollista hyväksyä virallisesti tuotteen vastaanotto. Päätösvaihe pitää sisällään runsaasti dokumentointiin liittyviä työvaiheita. Dokumentoinnin vaiheisiin kuuluvat olennaisina viimeistellyn tuotteen raportointi, lopullisten sopimuksien laatiminen, palkkioiden hyväksyminen, sekä monia projektinhallintaan liittyviä toimenpiteitä, kuten opittujen asioiden raportointi. Opittujen asioiden dokumentointi edesauttaa riskienhallintaa ennakoimaan ja poistamaan mahdollisia riskejä, joita projektinkulun aikana on tullut vastaan. (Kendrick 2009, 251.)

Lopullisen tuotteen ylläpito ja tukiprosessit noudattavat perinteistä ohjelmistoprojektien rakennetta. Tuotteeseen lisätään uusia ominaisuuksia tai korjataan jo olemassa olevia. Muutosten lisäys tapahtuu iteratiivisesti noudattaen projektinelinkaaren vaiheita. (Tripathy, Naik & Tripathy 2014, 8.)

Tiedon jakaminen ja ylläpito ovat olennaisia projektin kannalta. Versionhallinta on tärkeä jakelukanava, jonka avulla voidaan hallita projektien dokumentaatiota, lähdekoodeja, testitapauksia ja käyttöohjeita. Olennaisinta versionhallinnassa on versioiden palauttaminen sekä mahdollisuus hallita dokumentteja tai työversioita samanaikaisesti projektitiimin kesken. Versionhallinnan avulla voidaan jakaa työversioita maailmanlaajuisesti, ja ne ovat aina ajantasaisia. (Holcombe 2008, 264.)

Organisaation viestinnän muotoihin kuuluvat sisäinen ja ulkoinen viestiminen. Sisäisen viestinnän muodot pitävät sisällään päivittäiset kontaktit työntekijöiden kesken, tapaamiset ja tiedotustilaisuudet. Ulkoisen viestinnän muotoihin voidaan luetella muun muassa markkinointi, julkiset esitykset ja haastattelut sekä nettissivut. Organisaation viestinnän toteutukseen vaaditaan monia ohjelmistoja ja kanavia, jotta organisaation kilpailukyky ja tehokkuus saadaan taattua. Tämän päivän digitalisaation ja kanavien myötä teknologian käyttö organisaation viestinnässä on kasvanut huimasti. (Satyendra 2013.)

3.2 **Riskit**

Projektissa riski voi olla mikä tahansa ennalta arvaamaton tapahtuma, joka liittyy projektin toteutukseen. Riski on kahden muuttujan toteuma: tapahtuman oletettu seuraus ja todennäköisyys riskin toteutumiselle. (Kendrick 2009, 11.) Michael ja Deborah Dobsonin mukaan The PMBOK Guide rajaa riskit epäsuotuisiin tapahtumiin, joilla on merkittävä vaikutus projektin

päämäärään. Riskit voivat olla positiivisia tai negatiivisia, mutta niissä yhdistyvät epävarmuus ja vaikutus. Joissain tapauksissa tietämys riskin olemassa olosta on melko tarkka, kun taas joissakin tapauksissa riskin todennäköisyys on hyvin vaikeasti analysoitavissa. (Dobson & Dobson 2011, 3.)

Tomi Männistö lainaa opinnäytetyössään Haikalan & Mikkosen (2013) riskimääritelmää, jonka mukaan riski mielletään ongelmaksi, joka saattaa muodostua projektissa. Riskeihin liittyy kaksi olennaista tekijää: todennäköisyys ja vakavuus. Todennäköisyyden ollessa 100% kysymyksessä on tosiasia eikä riski. Riskille on ominaista, että toteutuessaan se aiheuttaa projektille menetyksiä tai projektin epäonnistumisen.

ISO 31000:2018-standardi määrittelee riskin elementtinä, joka voi yksinään tai yhdessä muiden elementtien kanssa aiheuttaa riskin. Riski voi olla tapahtuma tai muutos, jonka seurauksena päämäärään tai kohteeseen aiheutuu riskitapahtumia. Riskitapahtuman seuraus voi olla negatiivinen tai positiivinen, ja se voidaan arvioida määrällisenä tai laadullisena. Todennäköisyys riskin ilmenemiseen on mitattavissa ja määritettävissä objektiivisesti tai subjektiivisesti, sekä määrällisesti että laadullisesti matematiikan keinoin. (ISO Online Browsing Platform 2018.)

4 RISKIENHALLINTA

Projektien voidaan määritellä olevan jo ennen käynnistymistään suuri riski, mutta vielä suuremmaksi riski kasvaa, jos projektit toteutetaan riittämättömin projektin johtamisprosessein. Projektit, jotka toteutetaan ilman riittävää riskienmäärittelyä, epäonnistuvat hyvin todennäköisesti. Projektianalyysit sekä riskienhallinta yhdessä muiden projektihallintaprosessien kanssa varmistavat, että projektin toteutus vastaa suunniteltua. (Kendrick 2009, 25.)

Projektisuunnitelman laatiminen kuuluu olennaisena osana ohjelmistoprojektien toteutukseen. Ilman projektisuunnitelman tekoa ja ylläpitoa ei ole mahdollista suorittaa töiden, aikataulun, budjetin ja resurssien organisointia. Projektisuunnitelmaan tulee myös määrittää oma osionsa riskienhallinnalle. Projektisuunnitelman riskienhallinnan osioon tulee kirjata projektin toteutusvaiheeseen arvioidut riskit. (Taylor 2004, 134.)

Projektinhallinnan olennaisuuksiin kuuluu myös riskienhallintasuunnitelma. Riskienhallintasuunnitelmassa tulee kuvata riskit ja riskienhallintamenettelyt tarkemmalla tasolla kuin projektisuunnitelmassa. Suunnitelma sisältää muun muassa vastuujaon, kommunikaation ja dokumentoinnin suunnittelun. Riskienhallintasuunnitelman liitteisiin voidaan luetella riskienhallinta taulukot tai matriisit, joita käytetään riskien arvioinnissa. (Taylor 2004, 159.) Mika Paananen korostaa pro gradu -tutkielmassaan riskienhallintasuunnitelman laatimista ennen riskientunnistamista. Lisäksi hän kuvaa riskientunnistamisen välineisiin riskienhallintakehyksen ja riskienhallinnan mallin, jotka ovat kaksi yleisintä riskien tunnistamisen työkalua (Kuva 2 ja 4). (Sommerville 2004.)

Yleisesti ottaen projektien riskienhallinta pitää sisällään aikataulu-, budjetti ja resurssisuunnittelun sekä ammattitaidon ja sopivuuden arvioinnin yrityksen strategian osalle. Riskienhallinnan suunnittelu tulisi aloittaa hyvin aikaisessa vaiheessa, jolloin projektin toteutuksesta ei edes ole täyttä varmuutta. (Taylor 2004, 156.) Aikataulutuksen, budjetoinnin ja resurssoinnin lisäksi riskienhallinta pitää sisällään riskien tunnistamisen ja määrittämisen sekä suunnittelun riskien hallitsemiseksi ja ehkäisemiseksi. Riskien hallitseminen ja ehkäiseminen pitävät sisällään haittojen todennäköisyyksien ja seurauksien arvioinnin. (Leach 2014, 53.)

Erilaiset laatustandardit liittyvät voimakkaasti organisaation riskienhallinnan arviointiin. Ohjelmistokehityksen laatustandardien joukkoon kuuluu useampia standardeja, joista yleisimmistä on CMMI, joka jakautuu neljään eri kategoriaan pitäen sisällään myös projektinhallinnan osa-alueen. (Paananen 2008, 19.) Riskienhallintaosat sisältyvät projektinhallinnan prosessialueisiin, joita CMMI-mallissa on seitsemän. Riskienhallinnan osa-alueille on määritetty riskienhallintastrategian luomisen lisäksi, riskien tunnistaminen ja analysointi sekä lievennys. (Arkko 2013, 20.)

Smithin ja Pichlerin (2005) mukaan ketterien ohjelmistomenetelmien käytössä on käytettävä riskienhallinnan parhaita käytäntöjä. Tähän on syynä perinteisten riskienhallintamenetelmien heikko skaalautuvuus ketteriin projektinhallintamenetelmiin.

4.1 **Riskienhallintasuunnitelma**

Riskienhallintasuunnitelma tulisi laatia ISO Guide 73:2009-standardin mukaan aina organisaation laajuisena, vaikka suunnitelmia olisikin laadittu projektikohtaisesti useampia, tai suunnitelmia eri tasoille ja prosesseille. (ISO 31000:2009.) Riskienhallintasuunnitelman tulee määritellä riskienhallintaprosessit, jotka ovat kuvattuna riskienhallintamallissa (Kuva 4). Riskienhallintasuunnitelmaan tulee kuvata tarkasti vaiheet ja toimenpiteet, jotka projektinhenkilöstö on sitoutunut noudattamaan projektin kulun aikana. Vastuualueiden tarkka määritteleminen, joiden avulla saavutetaan riskien havainnointi mahdollisimman tarkasti. Havainnoinnin tehokkuus toteutuu projektinryhmälle tarkkaan määritettyjen riskienhallinnan vastuiden ja tehokkaan riskien dokumentoinnin myötä. Riskienhallintamenetelmien lisäksi, riskienhallintasuunnitelmaan on olennaista määritellä uhkatekijät, jotka on havaittu aiemmissa projekteissa. (Taylor 2003, 159.) Myös Raydugin (2013, 30-32) korostaa riskienhallintasuunnitelman laatimisessa vastuiden jakamista, sekä projektihenkilöiden vastuualueiden ja prosessien tarkkaa kirjaamista projektisuunnitelmaan. Suunnitelmaan tulisi myös dokumentoida prosessit, joista mahdolliset ongelma-alueet voi identifioida ja arvioida. Raydugin mukaan suunnitelmassa tulisi myös identifioida tilanteet, joissa riskit pitää jättää huomioimatta.

Suunnitelmaan tulee laatia oma osionsa budjetille, jonka tulee perustua riskiarviointeihin ja mahdollisiin riskien aiheuttamiin kustannuksiin, jotka ovat korvattavissa laaditusta budjetista. Riskien mittaamiseen ja tulkintaan yrityksillä on suuntaviivat, joiden perusteella riskien painoarvoa mitataan. Vastuu riskienhallinnasta kuuluu projektipäällikölle. Projekteissa saattaa kuitenkin tulla vastaan tilanteita, jolloin riskin kustannusarvion ylittäessä tietyn rajan, projektipäällikön vastuu päätöksestä siirtyy asiakkaalle. (Taylor 2003, 159-160.)

Riskirekisterin laatiminen sekä ylläpitäminen kaikkien projektinriskien osalle on tärkeää riskienhallintasuunnitelmaa laatiessa. Suunnitelmaan tulee myös määritellä tarvittavat riskienarviointi -ohjelmistot ja muut projektinhallintatyökalut. Raydugin painottaa Riskienhallintasuunnitelman

ylläpitämisen ja päivittämisen merkitystä projektin eri kehitysvaiheissa. Riskienhallinnan tehokkuus voidaan todeta hallitsemattomien ja havaitsemattomien uhkatekijöiden avulla, toisin kuin mittaamalla onnistunutta riskienhallintaa ja hallittuja riskejä. (Raydugin 2013, 32.)

Riskienhallintasuunnitelmaan tulee määrittää vastuualueet ja toimenpiteet viestinnälle. Näihin tulee luetella henkilöt, jotka vastaanottavat riskiraportit ja henkilöstö, joka on vastuussa riskien minimoimisesta. Lopuksi, ennen Riskienhallintasuunnitelman liitteitä tulee suunnitelmaan laatia prosessit riskien jäljitys ja reaktiotehokkuus-strategialle. Dokumentoinnin laatuvaatimukset, sekä opittujen asioiden taltioiminen kuuluvat hyvän Riskienhallintasuunnitelman sisältöön. Riskienhallintasuunnitelman liitteisiin useimmiten kuuluvat riskienhallinta taulukot ja matriisit, sekä riskienhallintasuunnitelma, jossa on yksityiskohtaiset strategiat riskienhallinta taulukoissa esitetyille riskeille. (Taylor 2003, 159-160.)

4.2 ISO 31000 –riskienhallintastandardi

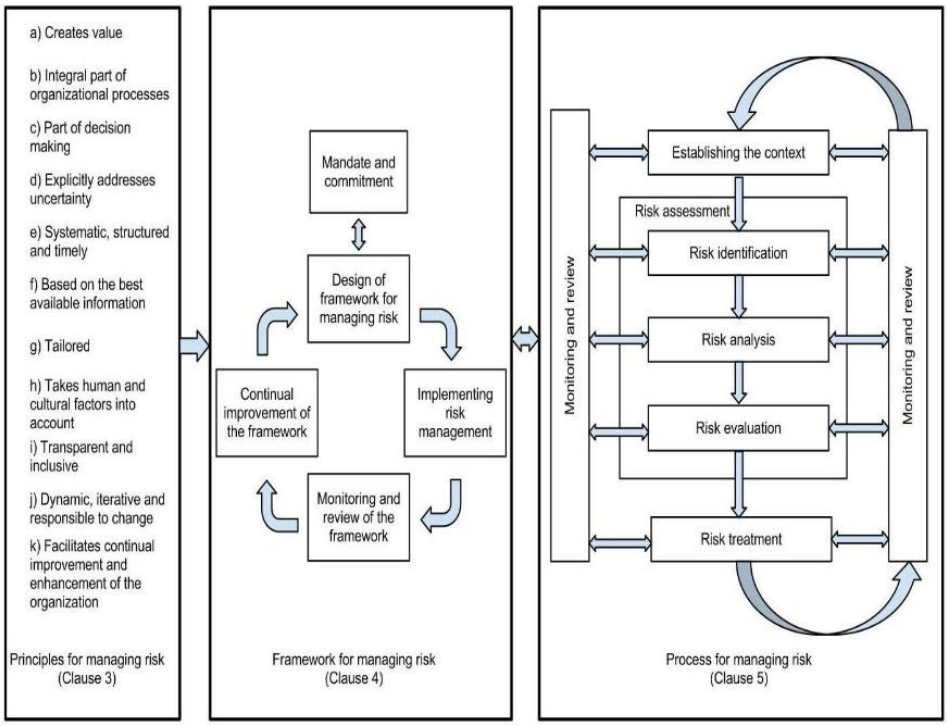
ISO 31000:2009 on kansainvälisen standardointijärjestön vuonna 2009 julkaisema riskienhallinnan viitekehys. Standardi on riskienhallinnan yleinen standardi, jota voidaan käyttää kaikenlaisissa organisaatioissa, sekä hallitsemaan riskejä liiketoiminnan eri osa-alueilla. ISO 31000-standardin riskienhallinta perustuu periaatteisiin, kehykseen ja prosesseihin, joiden avulla saavutetaan suorituskykyinen, voimassa oleva ja johdonmukainen riskienhallinta. Riskienhallinnan standardista on julkaistu vuonna 2018 uusi painos ISO 31000:2018. Uuden julkaisun mainittavimmat muutokset kiinnittävät huomiota organisaation ylemmän johdon sitoutumisesta riskienhallintaan, sekä uuden osaamisen ja jo ennestään hankitun osaamisen hyödyntämiseen. Uudessa viitekehyksessä painotetaan avoimen mallin ylläpitämistä monimutkaisissa konteksteissa sekä iteratiivisuuden ja analyysien kehittämistä organisaation riskienhallinnassa. (ISO Online Browsing Platform 2018)

Tehokkaan riskienhallinnan suorituskyky määritellään ISO 31000-standardin toimintaperiaatteille seuraavasti (ISO 31000:2009):

1. luo ja suojaa arvoa
2. Integroitu yrityksen prosesseihin
3. Osa päätöksentekoa
4. Käsittelee selkeästi epävarmuutta
5. Systemaattinen, ohjattu ja ajastettu
6. Perustuu parhaaseen ja uusimpaan tietoon
7. Räätälöity yrityksen tarpeisiin
8. Huomioi inhimilliset ja kulttuuriset tekijät
9. Näkyvä ja osallistava
10. Dynaaminen, iteratiivinen ja muutokseen sopeutuva
11. Organisaation jatkuvan parantamisen kehittäjä

Lisäksi ISO-standardi luokittelee seuraavanlaiset erinomaisuuden ominaisuudet: jatkuva kehitysmallin parannus, täysi vastuu riskeistä, ohjelmisto päätöksen tekoon ja dokumentointiin, jatkuva kommunikaation riskienhallinnalle ja täysi integraatio organisaation rakenteeseen. (ISO 31000:2009.)

ISO 31000:2009-standardin järjestelmän arkkitehtuurimallissa kuvataan riskienhallinnan periaatteet, jatkuvan kehityksen malli ja riskienhallinnan prosessi. (Kuva 2).



Kuva 2. Riskienhallinta arkkitehtuuri (ISO 31000:2009).

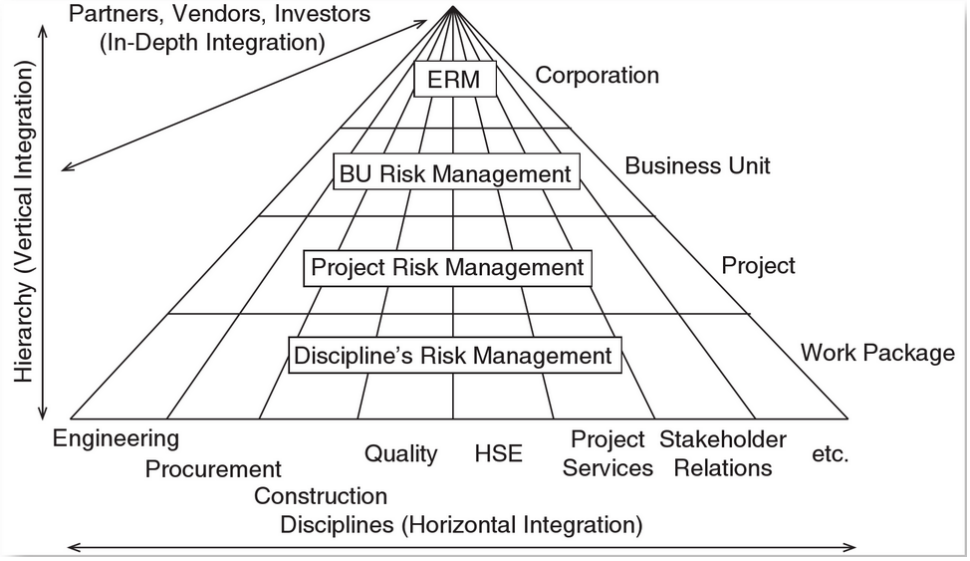
Kehyksen ominaispiirteisiin kuuluu riskienhallinnan vaatimusten dokumentointi kattavasti läpi koko ISO 31000-kehyksen, sisältäen muun muassa riskienottohalukkuuden, riskikriteerit ja riskiraportoinnin. Riskienottohalukkuus kuvataan kahdella eri tavalla. Ensimmäiseksi organisaation on arvioitava, miten riskeihin reagoidaan ja toiseksi organisaation on arvioita riskin arvo, eli paljonko menetetään riskin mahdollisen toteutumisen myötä. Riskikriteerien määrittäminen sisältää lakisääteiset asiat, jotka liittyvät organisaation riskienhallintaan, kuten esimerkiksi liiketoimintaetiikan ja ympäristökysymykset. Riskien raportoinnissa laaditaan suunnitelma riskien raportoinnin koostamisesta, eli miten riskit halutaan esittää organisaation johdolle. Yksittäisen riskin esittämisen sijaan riskeistä on mahdollista laatia kokonaisuuksia, jotka kuvaavat paremmin riskejä ja niihin liittyviä kysymyksiä. (ISO Guide 73:2009.)

4.3 **Riskienhallinta organisaatiossa**

Organisaation riskienhallintakaavio (Kuva 3) on tärkein elementti kuvaamaan riskienhallintaa osana yrityksen liiketoimintaa. Kaaviosta on nähtävissä yrityksen riskienhallinnan eri osa-alueiden sijoittuminen yrityksen liiketoimintaan. Kaavion pystysuorista linjoista on tulkittavissa, miten työ-,

projekti-, liiketoiminta- ja organisaation johtotaso integroituvat organisaation riskienhallintaan. (Raydugin 2013, 32–33.) Brisk & Juvonen (2011, 12) mainitsevat kandidaatintyössään riskienhallinnan olennaisimman piirteen olevan riskien keskinäisten riippuvuussuhteiden paljastaminen organisaatiossa.

Vaakasuuntaiset linjat kuvaavat erilaisten tieteenalojen projektien integroitumisen. Mallissa korostuu myös projektinomistajien, liikekumppanien ja muiden sidosryhmien integroituminen organisaation riskienhallintaan. (Raydugin 2013, 32–33.)



Kuva 3. Organizational framework (Raydugin 2013, 33).

4.4 Riskienhallinnan viitekehys

Software engineer Instituten Christopher Alberts ja Audrey Dorofee määrittelevät kolmivaiheisen riskienhallintakehyksen, jonka avulla voidaan hallita riskejä tehokkaasti. Kehystä voidaan käyttää jokaisessa ohjelmistokehityksen elinkaarimallin vaiheessa, mukaan lukien ohjelmiston hankinnan, kehityksen, toiminnan ja tietoturvallisuuden riskienhallinnassa. (Alberts & Dorofee, 2010, 12.)

Kolmivaiheisen riskienhallintakehyksen ensimmäisen vaiheen keskiö on riskienhallinnan valmistelussa. Valmisteluvaiheessa on oleellista, että projektissa mukana olevat tahot ovat sitoutuneet riskienhallintaan. On olennaista, että yrityksen johdon tuki riskienhallinnalle on konkreettista ja aktiivista. Riskienhallinnansuunnitelman laatiminen mahdollisimman kattavasti edellyttää projektin avainhenkilöiden sitoutumisen lisäksi riskien ja resurssien määrittämisen ennen varsinaisia riskienhallinnan toimenpiteitä. (Alberts & Dorofee 2010, 39–40.)

Riskienhallintakehyksen toisessa osassa vaiheet on jaoteltu kolmitasoisesti, mutta ne noudattavat kaikki riskienhallinnan toteutumisen vaiheita. Riskien arvioiminen ja suunnitelma riskien vähentämiseksi, sekä itsessään riskien minimoiminen toteuttavat ennalta suunniteltujen toimenpiteiden jatkuvuutta riskienhallintakehyksessä. Kommunikaatio ja dokumentointi sekä riskien uudelleen määrittäminen varmistavat riskienhallinnan varsinaisen toteutumisen. Työkalujen ja dokumentaation käyttö varmistavat prosessien ja sidosryhmien välisen toiminnan. Riskien todennäköisyysarviointi yhdessä resurssien tehokkaan toiminnan kanssa, varmistavat kehyksen toisen vaiheen tehokkaan toteutumisen. Riskienhallintakehyksen toisen vaiheen olennaisimpiin osiin kuuluvat tehokkaan kommunikaation ja dokumentoinnin toteutuminen. (Alberts & Dorofee 2010, 40–43.)

Kehyksen kolmannen vaiheen toimenpiteissä painottuvat riskienhallinnan ylläpito ja kehittäminen. Riskinarviointi ja vähentäminen ovat jatkuvan kehittämisen alla. Riskienhallinnan kehittäminen kerätyn aineiston ja opittujen asioiden perusteella, edesauttaa riskien minimoimisessa. Uusien standardien havainnointi, yhdistettynä riskienhallinnan työkalujen ja metodien kehittämiseen, maksimoivat riskienhallinnan tason. (Alberts & Dorofee 2010, 43–44.)

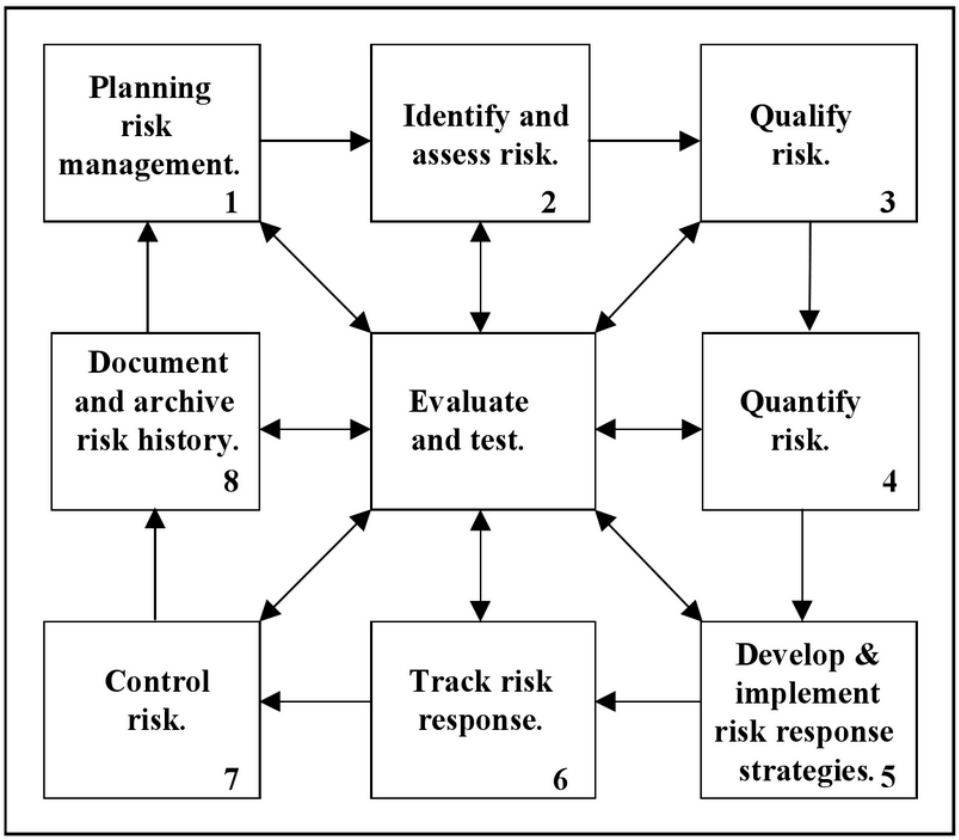
Alberts & Dorofeen riskienhallinnan kehyksen eri vaiheissa korostuvat kommunikoinnin ja dokumentoinnin tärkeys. Niiden avulla pystytään hyödyntämään mahdollisimman paljon jo opittuja asioita, sekä mahdollisesti kehittämään uusia näkökulmia. Riskien jatkuva dokumentointi ja tarkkailu, sekä työkalujen tehokas hyödyntäminen kehyksen eri vaiheissa mahdollistavat riskienhallinnan ylläpitämisen ja kehittämisen. (Alberts & Dorofee 2010, 39–44.)

ISO 31000:2009-standardin riskienhallintakehyksessä (Kuva 2) korostuvat riskienhallintakehyksen iteratiivisuus, suunnittelu, toteutus ja valvonta,

sekä riskienhallintamallin jatkuva kehittäminen. Mallissa korostuu ulkoisten ja sisäisten sidosryhmien sitouttaminen riskienhallintaan, sekä organisaation johdon tuki. Riskienhallintakehys määrittelee riskienhallinnan ominaisuuksiin organisaation liiketoiminnan, sekä riskienhallinnan integroinnin yrityksen liiketoimintaan ja kontekstiin. Kehyksen ominaisuuksiin kuuluvat myös edellisten lisäksi vastuun jaon, dokumentoinnin ja kommunikoinnin merkitys. (ISO 31000:2009.)

4.5 Riskienhallintaprosessi

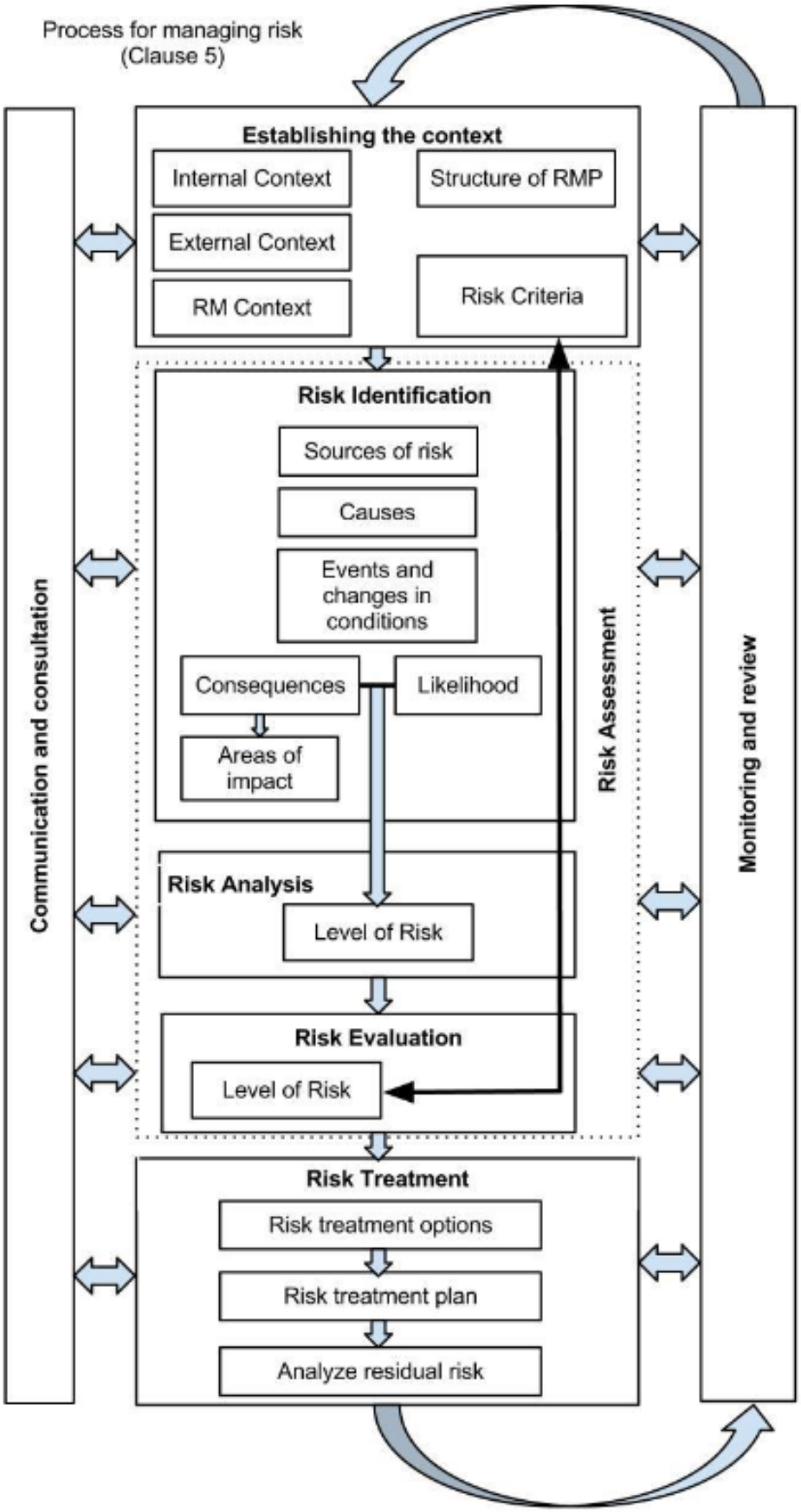
James Taylorin mukaan Project Management Institute (PMI) on määritellyt rakenteen riskienhallintaprosessille (Kuva 4) teoksessaan ”Guide to the Project Management Body of Knowledge (PMBOK Guide)”. Taylorin mukaan riskienhallinta on parhaiten toteutettu silloin, kun prosessit on tarkkaan määritelty ja dokumentoitu. Kaikkien projektissa toimivien tahojen tulee sitoutua noudattamaan tarkasti riskienhallinnan määrittelyä ja ohjeita. PMI:n riskienhallintamalli on implisiittinen, mutta ei kiinteä. Toisin sanoen eri ominaisuudet vaikuttavat toisiinsa, vaikka niillä on oletusarvo. Riskienhallintamalli on jatkuvan arvioinnin alla, sen ominaisuudet muuttuvat koko projektin elinkaaren aikana. (Taylor 2003, 155.)



Kuva 4. Riskienhallintamalli (Taylor 2003, 155).

Yuri Raudugin riskienhallintaprosessin toimintamallissa uhkatekijöiden tunnistus tapahtuu systemaattisesti. Tunnistuksen jälkeen uhkatekijöiden todennäköisyys arvioidaan, sekä lopuksi tehdään tarvittavat toimenpiteet uhkatekijöiden vähentämiseksi. Raydugin korostaa teoksessaan riskienhallintaprosessin olevan tärkein riskienhallinnantyökalu organisaation riskienhallintakehyksen (Kuva 3) jälkeen. Riskienhallintaprosessin tärkeimpänä ominaisuutena voidaan pitää toteutuksen herkkyyttä, eli aiotut ja osoitetut toimet tulevat dokumentoiduksi ja toteutetuksi. Prosessimallin systemaattisen etenemisen, sekä riskienhallinnan työkalujen tehokkaan käytön myötä saavutetaan tehokas riskienhallinta. (Raydugin 2013, 39–52.)

ISO 31000 standardin riskienhallinta prosessi (Kuva 5) on yksityiskohtainen riskienhallinnan prosessimalli, josta korostuu systemaattisuus ja menettelytavat ja käytännöt. Mallissa on kuvattu tarkalla tasolla riskienhallintaprosessin eteneminen, aina riskientunnistamisesta, analyysiin ja arviointiin. ISO 31000 mallissa korostuu myös viestintä ja konsultointi, sekä johtaminen ja tarkkailu. Prosessin pääpiirteisiin voidaan mainita riskien arvioiminen vertaamalla niitä riskikriteereihin, jonka jälkeen voidaan aloittaa toimenpiteet riskienkäsittelyyn. (ISO 31000:2009.)



Kuva 5. Risk management process. (ISO Guide 73:2009).

4.6 Riskien tunnistaminen

Richman (2011, 107) mukaan riskien tunnistamisen voisi kuvailla sanoin ”Mitä voi mennä pieleen”. Riskienhallinnan kannalta on olennaista tunnistaa mahdolliset riskit ja arvioida niiden vaikutus projektin toteutukseen. On arvioitava syyt sekä kuvata tilanteet ja ennusmerkit, jotka antavat viitteitä uhkatilanteista. Näin kyetään estämään tehokkaasti riskien ilmeneminen projekteissa. Riskitekijöiden identifiointia tulee hallita koko projektin elinkaaren ajan. Projektissa tapahtuvat muutokset saattavat vaikuttaa olemassa oleviin riskeihin, ja näin ollen riskien tunnistaminen ja arvioiminen on olennaista projektin joka vaiheessa. On myös huomioitavaa, että Paanasen (2008) lainaama Wallace (2004) luonnehtii useampien riskientunnistusmenetelmien käyttöä suositeltavaksi, etenkin jos projektin koko luokitellaan suureksi. Pienessä projektissa, jo itsessään projektin kompleksisuus saattaa muodostua riskitekijäksi.

Tyypillisimpiin projektiriskien tunnistamisen osa-alueisiin voidaan luetella projektin scope, laatu, hinta ja aikataulu. Projekti pitää sisällään myös paljon muita osa-alueita, jotka tulisi huomioida riskienhallinnassa. Riskientunnistamisessa tulisi huomioida kaikki uudet asiat, jotka liittyvät projektin toteutukseen. Informaation kulun ja henkilöstön osaamisen tunnistaminen, sekä riskienhallinnan osaamisen puutteiden tehokas havaitseminen kuuluvat toimivaan riskienhallinnan rakenteeseen. (Raydugin 2013, 103–105.)

Riskien tunnistamisessa on järkevää hyödyntää moninäköisyyttä. Ohjelmistoprojektien riskintunnistamisessa on suositeltavaa hyödyntää eri näkökulmia. Riskinarvioinnin jaottelu sidosryhmien, projektin toteuttajien ja liiketoiminnan osaajien kesken yhdistettynä eri abstraktiotasoihin, kuten esimerkiksi jaottelu ohjelmistotuotannon ja ulkoistuksen riskianalyysisessioihin. Puutteellinen riskinarviointi saattaa aiheuttaa ohjelmistoprojektien riskianalyysiin puutteita. Asiakkaan ja käyttäjän näkökulman tuominen riskien arviointiin on tärkeä ottaa huomioon. (Vuori 2010, 34–35.) Matti Vuori jaottelee riskien tunnistamisen kolmeen eri luokkaan. Kriittisimmällä, eli 3-tasolla ohjelmistoprojektien riskientunnistamisessa voidaan hyödyntää tarkistuslistoja, SWOT-analyysia, aivoriihi-menetelmää ja potentiaalisten ongelmien analyysia. Kriittisen tason riskien määrittelyyn on tärkeää kutsua projektin ulkopuolisia ammattilaisia, jotka ovat kykeneviä vastaamaan riskientunnistamisesta. Normaalitason riskientunnistamisesta huolehtii määritelty ryhmä, joka käyttää työvälineenä riskilistaa. Ideoivien menetelmien käyttö on suositeltavaa 2-tason riskientunnistamisessa. Alhainen eli 1-taso edellyttää riskien tunnistamista ja esittelyä, mutta riskianalyysi voidaan tehdä harkinnan mukaisesti, eikä menetelmien käyttöä edellytetä. (Vuori 2010, 37–38.)

Paananen (2008) huomioi pro gradu -tutkielmassaan, että Boehmin (1989) mukaan projektien parhaiten tunnetut osa-alueet ja tekniset haasteet huomioidaan riskienhallinnassa useimmiten tehokkaasti. Boehm kuitenkin suosittelee riskientunnistamiseksi hajotus-katselmointitekniikkaa. Hajotustekniikalla tarkoitetaan projektisuunnitelman tai vaatimusmäärittelyn

epämääräisten kokonaisuuksien purkamista osiin. Tällä tavalla projektidokumenttien yllättäviä riskejä sisältävät osa-alueet tulevat huomioiduiksi.

Projektipäällikön lisäksi projektitiimin tulisi aktiivisesti osallistua riskien määrittämiseen. Projektitiimin osallistuminen riskienmäärittelyyn toimii etenkin ketterien projektimallien toteutuksessa. Tiimin toteuttamassa riskientunnistus sessiossa voisi hyödyntää tunnetuimpia riskianalyysimenetelmiä, joihin voidaan luetella: FMEA, poikkeamatarkastelu ja erilaiset herkkyysanalyysit. (Vuori 2010, 39–41.) Michael ja Deborah Dobson mainitsevat aivoriihi työskentelyn ja riskienhallintatyökalujen lisäksi myös dokumentaation merkityksen riskientunnistuksessa. Kerätyn dokumentaation läpikäynnin ja projektin osien systemaattinen läpikäynti varmistavat tehokkaan riskien määrittelyn. (Dobson & Dobson 2011, 29–35.)

Mika Paananen (2008) määrittelee riskientunnistamisen rungoksi PMBOK (2001) laatiman riskien tunnistamisen järjestyksen, josta on huomioitavissa selkeä johdonmukaisuus. Ensimmäiseksi riskientunnistamisessa tulee huomioida dokumenttien tarkastus, jonka jälkeen on järkevää laatia sopivat tiedonkeräystekniikat ja tarkastuslistat. Näiden jälkeen oletusanalyysien laatiminen, jolla tarkoitetaan projektin ylioptimistisesti huomioitujen osien purkamista. Näihin osiin voidaan esimerkiksi luetella olettamukset, jotka koskevat ylisuuria tai muuten perusteettomia arvioita osaamisesta. Viimeisenä listalla mainitaan diagrammitekniikat, joiden avulla kyetään mallintamaan projektin prosesseja sekä tapahtumien jaksottumista. (PMBOK 2001.)

Paanasen (2008) mukaan riskien tunnistamisen rungosta on havaittavissa selkeä yhteys projektin kulkuun. Riskeihin voidaan porautua suuremmasta mittakaavasta yksityiskohtaisempaan riskien tunnistamiseen, ja lopulta riskianalyysin toteuttamiseen. Tiedon keräystekniikoista, joita voidaan hyödyntää (PMPOK) riskientunnistamisen rungossa, Paananen mainitsee aivoriihi- ja delphi-tekniikan sekä erilaiset haastattelut ja SWOT-analyysin. (PMBOK 2001.)

Ohjelmiston elinkaaren eri vaiheissa on järkevää huomioida vaatimusmäärittelylle tarkastuslistojen ja dokumenttien katselmoinnit yhdessä aivoriihi sessioiden kanssa. (Paananen 2008, 45-46.) Yuri Rayduginin mukaan tehokkaan riskienmäärittelyn voi suorittaa Delphi-äänestystekniikan avulla työpajoissa. Projektin alkuvaihetta lukuun ottamatta Delphi-tekniikan käyttöön ei tarvitse käyttää aikaa, kuin joitakin kertoja viikossa muutamien tuntien ajan. (Raydugin 2013, 95.)

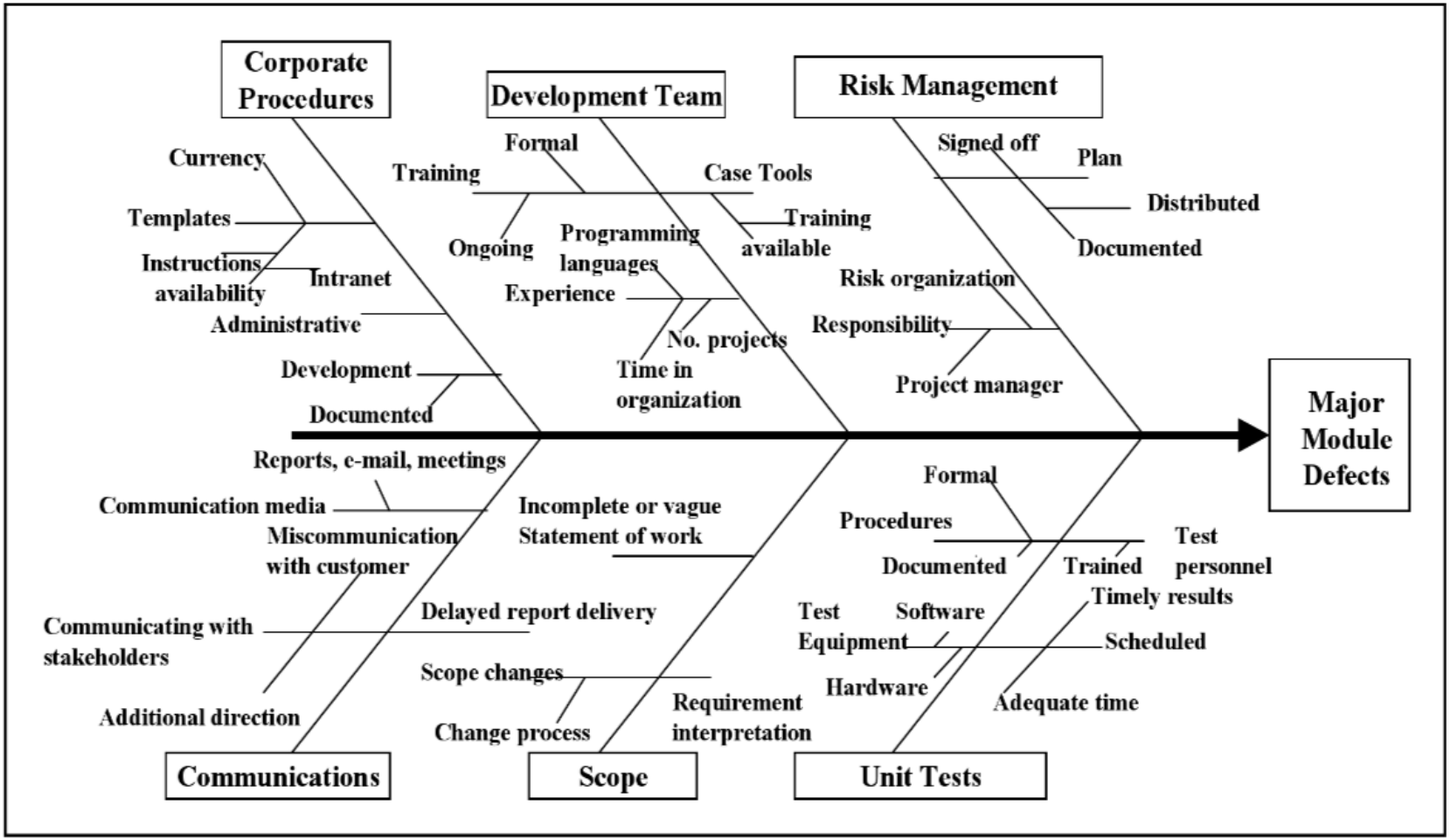
4.7 **Riskianalyysi**

Mikko Hallila (2016) muotoilee insinöörityössään kattavan riskianalyysin laatimisen olevan tärkein osa-alue riskienhallinnassa. Riskianalyysin tavoitteena ei ole poistaa tai minimoida riskejä, vaan riskianalyysin tärkein tehtävä on tunnistaa riskit ajoissa, sekä arvioida niiden esiintymistiheys ja vaikutusalue. Riskianalyysin perustana voidaan pitää mahdollisen

pahimman tappion määrittämistä. (Juvonen, M. Koskensyrjä, M. Kuhanen, L. Ojala, V. Pentti, A. Porvari, P. Talala, T. 2014.)

Riskien identifioinnin perusteella laaditaan riskirekisteri, johon kirjataan määritellyt riskit. Jotta riskianalyysi on riittävä, pitää riskirekisteriin arvioida riskien vakavuusaste ja toimenpiteet uhkatekijöiden varalle. (Dobson & Dobson 2011, 35.) Kotkansalo, Parkkila, & Tarvainen (2017, 9) arvioivat yksittäisen riskianalyysitekniikan olevan riittämätön kattavan riskienhallinnan toteuttamiseksi. Paras tehokkuus saavutetaan näin ollen erilaisten riskianalyysitekniikoiden yhdistelmillä. Riskianalyysien yhdistämistekniikoilla voidaan löytää parhaat ominaisuudet riskiarviointiin.

Kotkansalon, Parkkilan, & Tarvaisen (2017) kirjallisuusselvityksessä Rantanen (2014) määrittelee riskien tunnistamisen ehkäisevän organisaation keskeisten tehtävien suorittamista. Mahdollisen riskin kirjaaminen erilaisiin riskien koontitaulukoihin on oleellista, jotta riski on analysoitavissa. Esimerkkinä, Rantanen mainitsee riskin olevan arvioitavissa vakavuusasteen ja kertoimen avulla. Tällöin voidaan tulkita jonkin uhkatekijän toteutumista todennäköisyyden mukaan.



Kuva 6. Riskianalyysin syy- ja seuraussuhde taulukko. (Taylor 2003, 162).

4.7.1 Laadullinen analyysi

Michael ja Deborah Dobsonin mukaan The PMBOK Guide jaottelee riskianalyysien jakautuvan kahteen eri ryhmään, laadulliseen ja määrälliseen riskianalyysiin. Laadullisen analyysin riskirekisteri tulee määritellä todennäköisyyden ja vaikutusasteen mukaiseen järjestykseen. Riskirekisterin päivityksen yhteydessä tulee huomioida rekisterin priorisoinnin tärkeys tulevia analyysejä varten. Priorisoinnilla kyetään pitämään yllä riskirekisterin järjestys, ja ennen kaikkea kaikkien riskien systemaattinen vaikutusten esiintyminen ja arviointi. (Dobson & Dobson 2011, 38–39.) Tom Kendrickin mukaan laadullisen riskianalyysin tulokset määritellään paremmuusjärjestykseen, jolloin riskit ovat kategorioitu järjestykseen, jossa ne tulisi käsitellä. Laadullista analyysia voidaan pitää todennäköisyysarvion vuoksi verrattain epätarkkana. (Kendrick 2009, 132–133.) Riskien tunnistamisen olennaisimmat kysymykset ovat: miten määritellä todennäköisyys ja vaikutus. Useimmiten vaikutuksen arviointi on helpompaa kuin todennäköisyyden arviointi. (Dobson & Dobson 2011, 38–39.) Riskin vaikutus voidaan arvioida hajautettuna mahdollisuutena, jonka vaikutusalue on monialainen. Vaikutusalue voi myös kohdistua yhteen helposti ennustettavaan kohteeseen, jolloin määrittely on suhteellisen yksikertaista. (Kendrick 2009, 135.)

Laadullinen analyysi jaottelee jokaisen riskin yhteen tai useampaan vakavuustasoon, jossa määritellään kaikki mahdolliset seuraukset riskitapahtumalle. Analyysin vakavuustasot voidaan määritellä esimerkiksi: pieni vaikutus, keskisuuri vaikutus ja niin edelleen. Hyvin useasti laadullisen analyysin riskitasoja määritellään korkeintaan kolmesta viiteen kappaletta. (Kendrick 2009, 133.)

Laadullisen riskianalyysin työkaluihin voidaan luokitella arviointitaulukot ja matriisit, joiden avulla määritellään riskille todennäköisyys ja vaikutussuhteet. Riskienmäärittteleminen tapahtuu riskipäällikön arvioinnin perusteella, tai mahdollisesti hyödyntäen menneiden projektien riskienhallinnan havaintoja. (Kendrick 2009, 140–144.)

4.7.2 Määrällinen analyysi

Riskien numeerista arviointia voidaan pitää määrällisen analyysin ominaispiirteenä (Dobson & Dobson 2011, 39.), kuten myös jo ennestään määritellyn tiedon hyödyntämistä analyysin laatimisessa. (Kendrick 2009, 133.) Määrällinen analyysi perustuu todennäköisyyslaskentaan, ja sen toteuttamisessa voidaan käyttää riskianalyysityökaluja, kuten Monte Carlo-simulaatiota tai PERT-analyysiä. (Dobson & Dobson 2011, 39.) Kendrick (2009, 134.) mainitsee myös Delphi-tekniikan, tietokone mallinnuksen ja asiantuntijoiden merkityksen määrällisen analyysin toteuttamisessa. (Kendrick

Määrällinen analyysi vaatii verrattain enemmän toimenpiteitä kuin laadullinen analyysi, mutta määrällisen analyysin voidaan todeta, antavan tarkemman tulosten arvioinnin kuin laadullinen analyysi. Aikataulun ja

budjetin riskienmäärittelemisessä käytetään määrällistä analyysiä. Määrällinen analyysi antaa kokonaisvaltaisen kuvan projektinriskeistä, ja näin ollen se soveltuukin vaativampien riskien tarkempaan analyysiin. (Kendrick 2009, 132.) Herkkyysanalyysi, tarkat matemaattiset metodit, päätöspuut ja erilaiset mallinnustekniikat kykenevät arvioimaan pidemmälle projektien riskejä, niitä voidaan myös hyödyntää hyvin laajalti projektin eri riskien arvioinnissa. Määrällisessä arvioinnissa voidaan hyödyntää laadullisen analyysin työkaluja, kuten riskienhallinta taulukkoa tai matriisia. Matriisin voi muuntaa määrällisen analyysin työkaluksi korvaamalla rivit ja sarakkeet kohtisuorilla akseleilla. (Kendrick 2009, 144–145.)

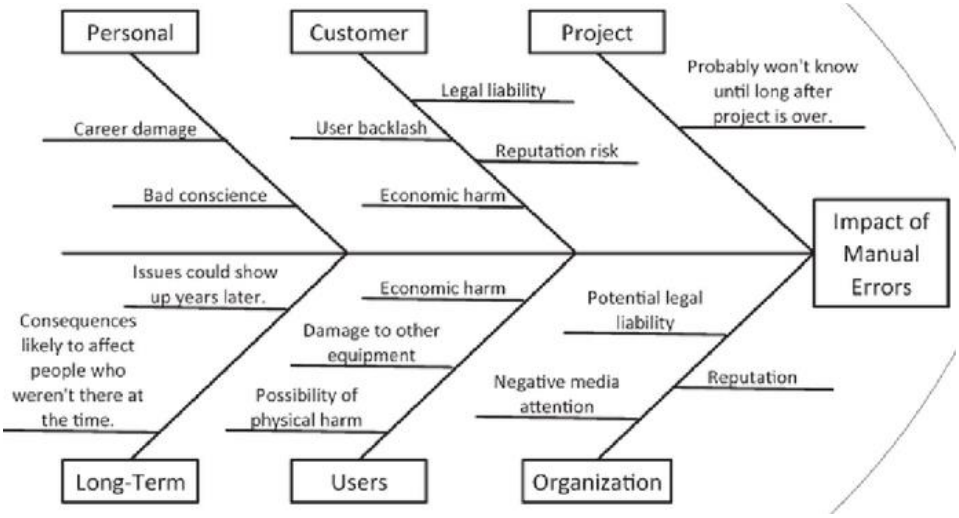
Ensimmäisissä riskienhallintatutkimuksissa havaittu taksonomia on Paanasen (2008) mukaan riskiluokittelun ja tarkastuslistan yhdistelmä. Taksonomian attribuutit määritellään useimmiten kyselylomakkeiden avulla. Taksonomiassa riskit luokitellaan hierarkkisiin kokonaisuuksiin, joista niiden väliset suhteet ovat helposti tulkittavissa. (Carr 1993.) Yuri Raydugin esittelee kehittyneemmän kolmijakoisen organisaation riskienhallintaan soveltuvan riskiluokittelun risk breakdown structure (RBS), jossa organisaation liiketoiminta yhdistyy riskienluokitteluun. Raydugin toteaa RBS-mallin datan käsittelyn ja analysoinnin olevan mahdollista kehittyneempien tietokantojen avulla. Tietokannan rakenteen tulisi noudattaa kuvan 3 rakennetta, jolloin data olisi jaoteltu yrityksen eri liiketoimialueiden tarpeisiin. (Raydugin 2013, 95.)

4.8 Riskin mittaaminen

Riskien mittaamiseen on erilaisia matemaattisia lähestymistapoja. IT-projektien riskienhallinnassa yksi yleisimmistä on määritellä riskille arvo, Riski = todennäköisyys * vaikutus (R = T * V). (Dobson & Dobson 2011, 57.) Hallilan (2016) mukaan riskienhallintataulukossa määritellään riskin esiintymistiheys, todennäköisyyskerroin ja todennäköisyys uhkatekijän toteutumiselle. Esiintymistiheyden perusteella kyetään määrittämään uhkatekijän esiintymistiheys esimerkiksi vuositasolla. (Juvonen, M. Koskensyrjä, M. Kuhanen, L. Ojala, V. Pentti, A. Porvari, P. Talala, T. 2014.)

Riskienmäärittelyssä on olennaista huomioida: historiadata ja menneiden projektien dokumentaatio, testaus ja testitulokset, riskitekijöihin liittyvien asiantuntijoiden haastattelut, käyttäjäkyselyt ja asiakastyytyväisyystiedot, teollisuusdata ja skenaarionanalyysi ja simulointi. (Dobson & Dobson 2011, 52.)

Riskien vaikutusalueet voidaan luokitella kuuteen eri luokkaan (Kuva 7). Mahdollisten uhkatekijöiden vaikutusalueiden määrittelyssä ei tulisi unohtaa myös mahdollisuuksien saavuttamista. Projektiriskien vaikutusalueisiin voidaan luetella: projektiriskit, organisaatioriskit, asiakasriskit, käyttäjäriskit, henkilöriskit ja pitkän aikavälin riskit. Dobson & Dobson 2011, 41–43.)



Kuva 7. Vaikutus alueiden syys- ja seuraussuhde. (Dobson & Dobson 2011, 43).

Kotkansalo, Parkkila, & Tarvainen (2017) mukaan SFS 5438,1988-standardi luokittelee erilaisia riskienarviointiprosesseja yli 30 kappaletta (Kuva 8). Vika-, vaikutus- ja kriittisyysanalyysien avulla pystytään tunnistamaan ongelmia, jotka vaikuttavat järjestelmän suorituskykyyn. Erilaisia prosessin mittaamiseen tarkoitettuja analyysimenetelmiä voidaan käyttää prosessien ja laitteistojen riskiarviointeihin. VVA-analyysimenetelmä perustuu komponentti- ja osajärjestelmätason analyysiin, mistä voidaan määrittää vioittumiskriteerit. Järjestelmän vikojen mittauksessa (VVA) huomioi järjestelmävikoja, toimintahäiriöitä, käyttörajoituksia ja suorituskykyongelmia. (VVA:n) tehokkuus ilmenee erityisesti osissa, jotka vaikuttavat koko järjestelmän toimintaan. (VVKA:n) eroavaisuus VVA-menetelmään perustuu kriittisyysarviointiin. VVA-menetelmän kriittisyysaste perustuu yksinkertaiseen riskiarviointiin asteikolla yhdestä viiteen, kun taas VVKA-analyysissä käytetään kriittisyysmatriisia, josta kriittisyysarvot voidaan tulkittavissa tarkemmin. (FS 5438, 1988.)

SFMEA-analyysi on ohjelmistojen virhetoiminta- ja vaikutusanalyysi, jonka avulla pystytään analysoimaan ohjelmiston virheellistä toimintaa. SFTA on ohjelmiston vikapuuanalyysi. Molempia analyysejä voidaan käyttää ohjelmiston toteutuksen eri vaiheissa, kuten vaatimusmäärittelyssä, suunnittelussa ja toteutusvaiheessa. (Vyas 2015, 29.) Myös Kotkansalo, Parkkila & Tarvainen kuvaavat tutkimusraportissaan ohjelmisto FMEA -arviointimenetelmän, jonka voidaan luokitella kuuluvaksi FMEA riskianalyysimenetelmien joukkoon. FMECA- ja FMEA-analyyseillä pystytään arvioimaan tärkeysluokitus, joka perustuu vikaantumismuodon aiheuttamaan riskitasoon, vikaantumistodennäköisyyteen tai vaihtoehtoisesti riskitason ja vikaantumismuodon yhdistelmään. (SFS-EN60812:en.)

Työkalut ja tekniikat	Riskinarviointiprosessi					Katso Liite
	Riskin tunnistaminen	Riskianalyysi			Riskin merkityksen arviointi	
		Seuraus	Todennäköisyys	Riskitaso		
Aivoriihi	SA[1)]	NA[2)]	NA	NA	NA	B 01
Ohjatut tai osittain ohjatut haastattelut	SA	NA	NA	NA	NA	B 02
Delfoi	SA	NA	NA	NA	NA	B 03
Tarkistusluettelot	SA	NA	NA	NA	NA	B 04
Alustava vaara-analyysi	SA	NA	NA	NA	NA	B 05
Poikkeamatarkastelu (HAZOP)	SA	SA	A[3)]	A	A	B 06
Vaara-analyysi ja kriittiset seurantapisteet (HACCP)	SA	SA	NA	NA	SA	B 07
Ympäristöriskien arviointi	SA	SA	SA	SA	SA	B 08
Rakenne « Mitä jos? » (SWIFT)	SA	SA	SA	SA	SA	B 09
Skenaarioanalyysi	SA	SA	A	A	A	B 10
Liiketoiminta-analyysi	A	SA	A	A	A	B 11
Juurisyiden analyysi	NA	SA	SA	SA	SA	B 12
Vika- ja vaikutusanalyysi	SA	SA	SA	SA	SA	B 13
Vikapuuanalyysi	A	NA	SA	A	A	B 14
Tapahtumapuuanalyysi	A	SA	A	A	NA	B 15
Syy- ja seurausanalyysi	A	SA	SA	A	A	B 16
Syy-ja vaikutusanalyysi	SA	SA	NA	NA	NA	B 17
Kerrossuojausanalyysi (LOPA)	A	SA	A	A	NA	B 18
Päätöspuu	NA	SA	SA	A	A	B 19
Ihmisen luotettavuuden analyysi	SA	SA	SA	SA	A	B 20
Rusettianalyysi	NA	A	SA	SA	A	B 21
Toimintavarmuuskeskeinen kunnossapito	SA	SA	SA	SA	SA	B 22
Piilopiirien analyysi	A	NA	NA	NA	NA	B 23
Markov-analyysi	A	SA	NA	NA	NA	B 24
Monte Carlo simulointi	NA	NA	NA	NA	SA	B 25
Bayestilastot ja Bayesverkot	NA	SA	NA	NA	SA	B 26
FN käyrät (uhriluvut)	A	SA	SA	A	SA	B 27
Riski-indeksit	A	SA	SA	A	SA	B 28
Seuraus/todennäköisyys matriisi	SA	SA	SA	SA	A	B 29
Kustannus/hyöty analyysi	A	SA	A	A	A	B 30
Monikriteerianalyysi (MCDA)	A	SA	A	SA	A	B 31

1) Erittäin soveltuva (SA).
2) Ei soveltuva (NA).
3) Soveltuva (A).

Kuva 8. Riskiarvioinnin työkalut ja tekniikat. (SFS-EN31010).

5 KIRJALLISUUSTUTKIMUS - OHJELMISTORISKIT

Kirjallisuustutkimusosan avulla haetaan vastausta tutkimuskysymykseen: Miten ohjelmistoriskit on nykyisellään määritelty riskeiksi? Tutkimuksen pääpaino on ammattikirjallisuuden ohjelmistoriskien määritelmässä. On kuitenkin oleellista löytää laajalti ohjelmistoriskejä, jotka tulisi huomioida ohjelmistokehitysprojektien toteutuksessa.

Kirjallisuuden lisäksi lähteinä toimivat tieteelliset tutkimukset ja aihetta koskevat materiaalit. Ohjelmistoriskien tunnistamisessa on olennaisinta tunnistaa tekijät, joilla on jonkinlainen syys- ja seuraussuhde projektissa käytettäviin ohjelmistoihin.

5.1 Tutkimuksen tulokset

Jouni Meriläinen (2003) kuvaa seminaariesitelmässään vika- ja vaikutusanalyysien olevan alun perin tarkoitettu järjestelmien kuluvien osien mittaamiseen. Menetelmien soveltuvuus ohjelmistojen mittaamiseen on kaksijakoinen. Laitteistoissa joita ohjelmistot käyttävät, voi esiintyä vikoja, mutta itse ohjelmisto ei voi vikaantua. Ohjelmiston lähdekoodi on joko toimiva tai virheellinen, mutta itse ohjelmisto ei vioitu käytön aikana. (Red 2002.) Meriläinen kuvailee ohjelmistovirheen esiintyvän tietyissä tilanteissa, joiden syy on tuntematon. Muussa tapauksessa ohjelmistovirheen lähdekoodi korjattaisiin. (HaH 2002.) Meriläinen lainaa teoksessaan P.L Goddardia, jonka mukaan ei ole merkitystä onko vika laitteistossa vai ohjelmistossa. Vian esiintyessä satunnaisesti, sitä voidaan kuitenkin menestyksellisesti mitata. Ohjelman vikojen mittaamiseen voidaan käyttää ohjelmistojen eri toiminnallisuuksien arviointia, kuten esimerkiksi ”ohjelmisto kaatuu”, ”Ohjelma pysähtyy” ja niin edelleen. (God 2000.)

Hannu Tanhuamäki (2006) kuvaa ohjelmistovirheen aiheuttavan mahdollisesti järjestelmävian, jos vian korjausta ei tehdä riittävän ajoissa. Hän myös mainitsee ohjelmistovirheet suunnitteluvirheinä, jotka ovat järjestelmissä jo niiden kehittämisestä asti. (Knight 2003.) Myös Kendrickin mukaan ohjelmistojen kaatuminen, lukkiutuminen tai muut järjestelmään liittyvät ongelmat saattavat johtua laitteiden ja ohjelmistojen yhteistoiminnasta. Integraatio-ongelmat voidaan liittää järjestelmien toimintaan vaikuttaviin häiriöihin. Suurien projektien osittaminen pienempiin kokonaisuuksiin asettaa vaatimuksia järjestelmien integraatiolle. Vaatimuksena ei ainoastaan ole hajautettujen laitteiden ja komponenttien toiminta. Integroinnin jälkeen niiden täytyy toimia myös kokonaisuutena järjestelmässä. (Kendrick 2009, 44.)

Paananen (2008) esittelee pro gradu -tutkielmassaan riskiluokittelujen eroavaisuuksia, joiden mukaan ohjelmistojen tehokkuuden väärin arvioiminen voidaan mukaan luokitella useampiin riskiluokkiin. Esimerkiksi, strategisen ohjelmoijan menetys ja ohjelmiston tehokkuuden arviointi voidaan

luokitella seuraavin riskiluokkiin: ulkoiset riskit, kustannusriskit, aikataulu-riskit, tekniikkariskit ja toiminnan riskit. (Murch 2001.)

Tharwon Arnuphaptrairong (2011) listaa kirjallisuustutkimuksessaan ohjelmistoprojektien riskejä, joita on määritetty 12:sta eri tutkimuksesta. Tutkimuksen tulokset on kerätty ohjelmistokehitysprojektien riskeistä vuosilta 1988-2003. Tharwonin tutkimuksesta voidaan todeta ohjelmisto-projektien sisältävän ohjelmistoihin liittyviä riskejä ainakin uusien ja monimutkaisten teknologioiden käytön, korkean teknisen monimutkaisuuden sekä kehittymättömän teknologian osalle. (Han &Huag 2007.) Lisäksi Tharwonin tutkimuksesta voidaan havaita puutteita teknologian käytössä projektinhallinnan osalle. (Addision 2003.)

Taylor (2003, 178) uuden testaamattoman teknologian käyttöönottoon sisältyy suurempi riski, kuin ennestään tunnetun ja testatun teknologian. Kendrick (2009, 44) Peril-tietokantaan kerättyjen ohjelmistoprojektien riskien perusteella voidaan todeta ohjelmisto- ja laitteisto-ongelmat yleisimmiksi vikariskeiksi. Ongelmallisin osa-alue Kendrickin mukaan on uusi ja ennestään kokeilematon teknologia, jossa saattaa ilmetä puutteita toiminnallisuuden ja luotettavuuden osalta. Kendrick (2009, 46) Tämän lisäksi teknologian käyttöönotto projektin elinkaaren eri vaiheissa on huomioitu liian myöhään. Uhkatekijäksi voidaan myös mainita uuden teknologian vaatimien odottamattomien muutosten vaikutus. Ohjelmistojen käyttöönottoon liittyviin riskeihin Leach (2014, 254) mainitsee teoksessaan teknologia riskit. Etenkin harvemmin käytetyn teknologian käyttöönoton voisi mainita huomioitavaksi riskitekijäksi.

Peril-tietokannan tiedoista voi todeta, että kaksi kolmasosaa Learning curve-tekniikalla todennetuista riskeistä koostuu viidestä erilaisesta tekijästä. Näiden tietojen perusteella - uusien ohjelmistojen monimutkaisuus on huomattavan aliarvioitu uhkatekijä. (Kendrick 2009, 69.) Harris (2009, 39) mainitsee projektitoteutuksen riskeihin: tarvittavan kokemuksen ja taitojen saatavuuden. Huomion arvoista on myös projektin koko ja tekninen monimutkaisuus, joihin tulee kiinnittää huomiota projektihenkilöstön osaamisen ja kokemuksen kartoituksessa. Kendrick (2009, 69) Lisäksi projektiin vaikuttavia riskejä ovat muun muassa kokematon ja osaamaton projektin henkilöstö. Jyrki Kontion mukaan edellisten riskitekijöiden lisäksi epävarmat vaatimusmäärittelyt vaikuttavat projektin toteutukseen. Riskitapahtumina voidaan mainita ainakin järjestelmän kaatuminen, avainhenkilön lopettaminen, liiallinen ajankäyttö uusien menetelmien ja työtapojen opiskeluun sekä merkittävät vaatimusmäärittelymuutokset. Seurauksina voidaan mainita ainakin työn viivästyminen, työn uudelleen toteuttaminen, henkilöstön ja pätevyyden vajaus sekä järjestelmän toiminnan katkot ”The Riskit Method for Software Risk Management, version 1.00” opetusmateriaalissaan. (Kontio, 10.)

Hoodat & Rashidi (2009, 447) luokittelevat ohjelmistoprojektien riskejä muun muassa aikatauluun, laatuun ja hintaan vaikuttavien tekijöiden

mukaan. Ohjelmistojen vaikutuksen voi huomata kaikissa edellä mainituissa luokissa. Projektityökalujen hallinta ja osaaminen vaikuttavat projektiaikatauluun ja laatuun negatiivisesti. Laatuun ja hintaan vaikuttavat ympäristö- ja teknologia muutokset. Harris (2009) identifioi ohjelmistoprojektien riskejä (Tesch, Kloppenborg & Frolick 2007) tutkimuksesta, josta voidaan havaita vaatimusmäärittelyjen ongelmille kaksi eri syytä: muutokset vaatimusmäärittelyssä on toteutettu heikosti sekä projektin laajuus - vaatimukset on jätetty huomioimatta teknologian vuoksi.

Mahdolliset organisaatio muutokset, kuten uudelleen sijoittuminen tai järjestäminen aiheuttavat vaatimuksia liiketoiminnan eri osa-alueille. Muutokset projektin toteutuksessa vaikuttavat negatiivisesti muun muassa henkilöstön-, teknisen infrastruktuurin- ja yhtäjaksoisuuden osa-alueille. Vaikutuksen voi huomata kasvaneina kuluina ja aikatauluviiveinä. Infrastruktuurimuutokset vaativat useasti laitteistojen ja ohjelmistojen integroinnin uuteen ympäristöön. (Harris 2009, 52–53.) Lisäksi Kendrickin (2009, 44) mukaan ohjelmistot eivät välttämättä toimi kaikissa ympäristöissä.

Kendrick (2009, 69) Tietohallinnon johtaman palvelukokonaisuuden (Infrastruktuuri) ongelmien vaikutus projektin aikatauluun on ilmeinen. Tietokonejärjestelmien, tukipalvelujen ja tietoliikenteen katkeaminen vaikuttaa vääjäämättä projektin aikatauluun.

Lahnalahti (2013) koostaa tietoturvallisuuden ominaisuuksia ISO 27001-standardin pohjalta, joista voidaan todeta ohjelmistojen kuuluvan tietoturvallisuuden piirin. Ohjelmistojen lisäksi tietoturvan piirin voidaan luetella: viestintä ja tietoliikenne, henkilöstö, lait ja sitoumukset, häiriötilanteet ja pääsynhallinta. Edellisten lisäksi voidaan mainita avainsanat: luottamuksellisuus, eheys ja saatavuus, jotka tulee huomioida tietoturvallisuuden hallintajärjestelmän käyttöönotossa. (SFS-ISO/IEC 27001:2013.)

Tanhuamäen (2006) pro gradu -tutkielmassa tietoliikenne-, ohjelmisto- ja laitteistoturvallisuus on luokiteltu teknisen turvallisuuden alueeseen. Ohjelmistoturvallisuus kuuluu tietoturvallisuuden osa-alueeseen, johon luokitellaan kriittiset ohjelmistot, jotka on integroitu organisaation liiketoimintaan. Ohjelmistoturvallisuuteen kuuluvat eristämis-, tunnistamis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt sekä ohjelmistojen ylläpito ja päivitys. Toimintaympäristöt ja ohjelmistot tulee eristää siten, että vain sallittujen käyttäjien pääsy niihin on mahdollista. (Hallinnon kehittäminen tietoturvasanasto, 2005.) Addisonin (2003) tutkimuksen mukaan tietokantojen tietoturvassa on havaittu ongelmia, jotka ovat seurauksia puutteellisista toimintatavoista hallita tietoturvaa, eheyttä ja saatavuutta. (Arnuphaptrairong 2011, 2.)

Laukaan kunnan tilinpäätöksessä ohjelmistoriskit luokitellaan kuuluvaksi tietojärjestelmäriskeihin, sekä aina seuraavaan aliluokkaan tietoturvariskeihin. Tietoturvariskit määritellään negatiivisina tapahtumina, joiden seurauksena tieto saattaa joutua ulkopuolisten saataville. Myös tiedon saatavuus oikeaan aikaan, sekä tiedon virheettömyys luokitellaan kuuluvaksi

tietoturvariskeihin. Ohjelmistoriskien suurimmaksi ongelmaksi mainitaan tietoliikenneverkon haittaohjelmat. Haittaohjelmien torjuntaan on varauduttu roskapostisuodattamin. Muistitikkujen ja siirrettävien medioiden aiheuttamien uhkatekijöiden riskienhallintaan on käytetty automaattisesti päivittyviä viruksentorjuntaohjelmistoja. Muihin ohjelmistoriskeihin on varauduttu jo ennestään testattujen ja hyväksi todettujen järjestelmien hankinnalla, joihin löytyy osaamista organisaatiosta tai yleisesti markkinoilta. Ohjelmistojen ajantasaisuus ja lisenssien huomioiminen on myös otettu huomioon riskienhallinnassa. Tilinpäätöksessä mainitaan kasvavina ohjelmistoriskeinä älypuhelinten ja kannettavien laitteiden aiheuttamat ongelmat sekä sosiaalisen median käyttöön liittyvät riskitekijät. (Laukaa 2017.)

Brisk & Juvonen (2011) lainaavat Salmelaa (2008), jonka mukaan nopean informaatio- ja tietojärjestelmien kehittymisen myötä organisaatioiden prosessit ovat kasvaneet, mutta samalla myös organisaation riippuvuus monimutkaisista järjestelmistä on lisääntynyt. Brisk & Juvonen tuovat esiin myös Juvosen (2005) arvioinnin, jonka mukaan riskienhallinnan kannalta tietojärjestelmien riskit ovat vain jokseenkin hallittavissa. Juvosen mukaan tietojärjestelmien riskeihin voidaan luetella ainakin tieto- ja televerkkojen katkot, tietotekniikkarikokset, teknologioiden kehityssuunnat ja epäluotettavat ohjelmistot.

6 TEEMAHAASTATTELU PROJEKTIPÄÄLLIKÖILLE

Teemahaastattelu toteutettiin sähköpostikyselynä neljälle IT-alalla toimivalle projektipäällikölle. Projektipäälliköt työskentelevät vuonna 2011 perustetussa liiketoimintatiedon hallintaan (Business Intelligence) keskittyneessä yrityksessä. Haastattelukysymysten muotoilu perustui tutkimuskysymysten pohjalle, jotta vastausten analysoiminen kirjallisuusselvityksen tulosten kanssa olisi mahdollisimman yhteneväinen. Neljästä haastateltavasta kaksi henkilöä vastasi kysymyksiin.

Teemahaastattelun kysymykset:

1. Miten ohjelmistot tai ohjelmistojen käyttö on huomioitu projektisuunnitelmassa?
2. Miten ohjelmistot tai ohjelmistojen käyttö on huomioitu projektien riskiarvioinneissa?
3. Jos on, niin millaisia ohjelmistoriskejä on määritetty?
4. Miten ohjelmistojen hallinta ja käyttäminen on huomioitu riskienhallinnan näkökulmasta?

Kysymys 1: (A) luonnehti muutamiakin eri näkökulmia. Projektin ollessa ohjelmiston käyttöönottoprojekti, on suunnittelun huomioitava tuo nimenomainen ohjelmisto. Toisaalta suunnitelmassa on huomioitava ohjelmistot/välineet, joilla projekti toteutetaan koulutustarpeita ajatellen. (B) ohjelmistoprojektin projektisuunnitelmassa on myös huomioitava itse ohjelmiston toteutuksen lisäksi kaikki muut projektintoteutuksessa käytettävät ohjelmat. Esimerkiksi, käyttöliittymän toteutuksessa ohjelmistojen käytössä on huomioitava käytettävyys.

Kysymys 2: (A) mainitsi uusien tuntemattomien ohjelmistojen käyttöönoton, jolloin riskientunnistus on oleellista. On arvioitava, kuinka pystytään tunnistamaan a) kohonnut riski, b) kuinka riski pystytään minimoimaan tai poistamaan kokonaan. (B) luonnehti ohjelmistoriskien kuuluvan olennaisesti riskienhallintaan muiden projektiriskien ohella. Hän myös painottaa riskien vakavuuden merkityksen arviointia, ja riskien seuraamista tarkemmalla tasolla.

Kysymys 3: (A) käytettävyys ja soveltuvuus käyttötarkoitukseen. Myös ohjelmistonlaatu voidaan nähdä riskinä, mutta harvemmin kaupallisten tuotteiden käytössä. (B) mukaan huomioitavia riskien osa-alueita on useita, kuten: toiminnalliset haasteet, käytettävyyden ongelmat, luotettavuus, suorituskyky, ylläpidettävyys, turvallisuus.

Kysymys 4: (A) mukaan kyseiset asiat kuuluvat osaksi projektisuunnitelma, tai sen alla olevaan tuotantosuunnitelmaan. Muuten ohjelmistojen hallinta ja käyttäminen kuuluisivat osaltaan käytettävyyden ja soveltuvuuden riskien alle. (B) ylläpidettävyys(hallinta) ja käytettävyys on huomioitu riskienhallinnassa.

7 OHJELMISTOPROJEKTI POTTA

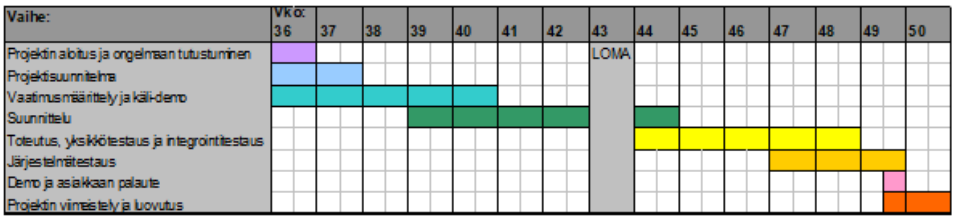
Opinnäytetyön teorian ja tutkimuksen tueksi valitsin Helsingin yliopiston opiskelijoiden toteuttaman Potta-projektin. Projektin dokumentaatio on osittain yleisesti käytettävissä, ja osaan materiaaleista vaaditaan projektiryhmäntunnukset. Opinnäytetyön toteutuksessa olen käyttänyt yleisessä jakelussa olevaa materiaalia, johon kuuluvat muun muassa opinnäytetyön liitteenä olevat projektisuunnitelma ja pöytäkirjat.

Potta-projekti on tietojenkäsittelytieteenlaitoksen ohjelmistotuotantoprojektina toteuttama tilanvarausjärjestelmä. Projektin sidosryhmiin kuuluvat projektihenkilöstö, projektin ohjaaja, projektin vastuuhenkilö ja asiakas. Projektitoteutuksen vastuut ja roolit on jaettu projektihenkilöstön kesken. Projekti kuitenkin toteutetaan tiimityönä, ja kaikki osallistuvat projektin sisällön suunnitteluun ja toteutukseen. (Salmelainen 2005, 1.)

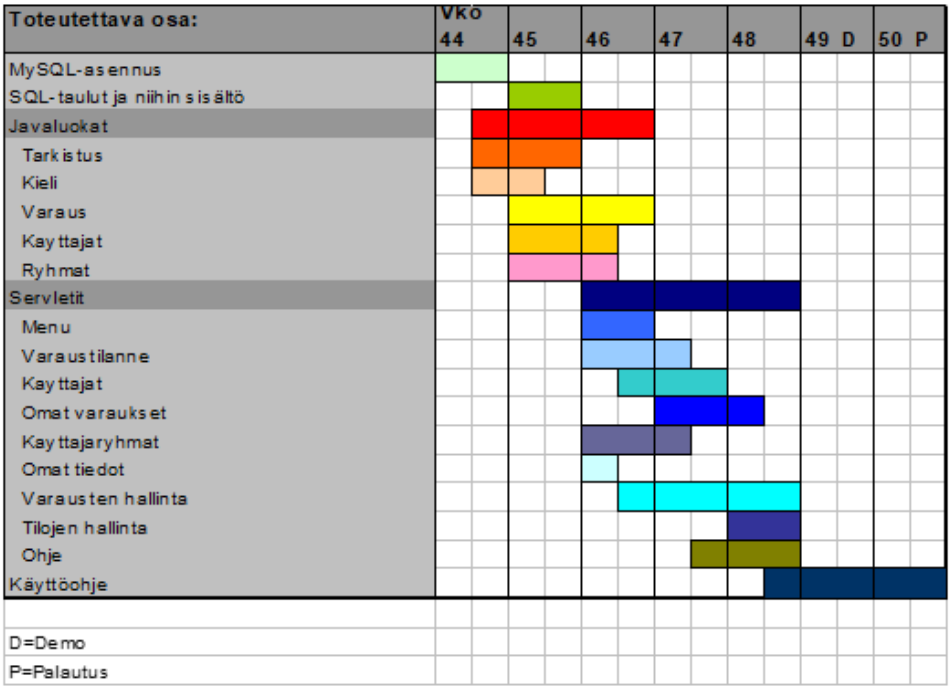
Jotta teoriaosan ja tutkimuksen avulla kerättyjen tietojen analyysistä Potta-projektin yhteydessä tulisi mahdollisimman selkeä. Lähestyn analyysin toteutusta ohjelmistojen riskienhallinnan näkökulmasta, ja jätän pois kaikki muut näkökulmat, jotka normaalisti projektinhallinnassa tulisi huomioida. Tutkimuksen ohjelmistoprojekti Potta-kappaleeseen koostetaan opinnäytetyön teoria- ja tutkimusosasta riskienhallinnan parhaimpia käytäntöjä, joiden avulla saavutetaan tehokas ja ajanmukainen ohjelmistoprojektien riskienhallinta.

Työkalu	**Kohde**
MS Word	Dokumentointi
MS Excel	Projektinhallinta, dokumentointi
Java, tekstieditorit	Ohjelmointi
PostgreSQL	Tietokanta
CVS	Versionhallinta
WWW	Kommunikointi
UML	Dokumentointi
Sähköposti	Kommunikointi
MSN Messenger	Kommunikointi

Kuva 9. Ohjelmistoprojekti Potta: Laitteisto- ja ohjelmistoympäristövaatimukset (Salmelainen 2005, 8).



Kuva 10. Ohjelmistoprojekti Potta: projektiaikataulu esitetty graafisesti (Salmelainen 2005, 8.)



Kuva 11. Ohjelmistoprojekti Potta: projektin toteutusaikataulu (Salmelainen 2005, 9).

7.1 Riskienhallintasuunnitelma

Potta-projektin tehostetun ohjelmistoriskienhallinnan toteuttamiseksi, projektisuunnitelman liitteeksi laaditaan jo ennen varsinaisen projektin aloitusta riskienhallintasuunnitelma. Teemahaastattelun tietojen perusteella (A) ja (B) luonnehtivat ohjelmistoriskien määrittelyn suoraan projektisuunnitelmaan. (A) mainitsee myös tuotantosuunnitelman osana projektisuunnitelmaa, johon mahdolliset riskienhallinnan määritteet voidaan dokumentoida.

Vastuun jaon lisäksi suunnitelmaan tulee laatia osio kommunikaation ja dokumentoinnin määrittelyille. (Taylor 2004, 156.) Alkuvaiheen riskienhallinnan toimenpiteisiin liitetään myös organisaation riskienhallintakehys (Kuva 3). Kehyksen avulla määritellään riskienhallinnalle mittakaavat, joiden avulla kyetään tunnistamaan riskien vaikutusalueet sekä arvioimaan mahdollinen organisaatiotasoinen riskienhallinnan kehittäminen. Kommunikaation merkitys suunnitelmassa korostuu mahdollisten vikatapahtumien ilmetessä. Suunnitelmaan on myös tarpeellista määritellä mahdolliset tukitoimenpiteet ja henkilöt, joiden vastuuvelvollisuus toimenpiteisiin jakautuu riskin vakavuusasteen mukaan. Korkeaksi määritellyn uhkatekijän tapahtuessa tukitoimenpiteisiin vastaamisen aikaraja lyhenee. Vuori (2010, 37–38) tarpeen tullen tulisi kutsua myös sidosryhmien edustajat ja mahdolliset asiaa tuntevat tahot kehittämään ratkaisua riskin minimoimiseksi.

Suunnitelmassa on oleellista huomioida, että ohjelmistoriskien tunnistaminen ja riskianalyysin toteuttaminen painottuu projektin aikaisiin vaiheisiin, jolloin pitää määritellä henkilöstön osaaminen ja koulutustarpeet. (Harris 2009, 39.) Olennaisin osa riskien tunnistamisessa on havaita riskien

seuraukset (Kuva 7). Tällöin on mahdollista määrittää riskien vaikutusalueet, jonka jälkeen on mahdollista valita oikeat toimenpiteet riskien vähentämiseksi. Seurausten vaikutus voidaan nähdä välittömänä, jolloin vaikutus useimmiten kohdistuu joko aikaan, laatuun tai budjettiin. Hyvänä esimerkkinä voi mainita Hoodatin & Rashidin (2009, 447) tutkimuksen, josta on havaittavissa projektityökalujen hallinnan ja osaamisen vaikuttavan projektiaikatauluun ja laatuun negatiivisesti, sekä ympäristö- ja teknologia muutosten vaikutuksen hintaan ja laatuun.

7.2 Riskientunnistaminen

Riskien tunnistamisen hyviin keinoihin voi laskea benchmarking-tekniikan, jonka avulla on mahdollista vertailla organisaation eri tasojen riskien tunnistamista projektiin sidoksissa olevien asiantuntijoiden kesken. Loppukädessä organisaation riskientunnistamisen taso on mitattavissa koko organisaation ja kaikkien sidosryhmien yhteistoiminnan tuloksesta. Tulokseen vaikuttaa olennaisesti organisaation aikaisempi panos riskienhallintaan ja sen osaamiseen. Riskien tunnistamisen ohella on oleellista taltioida tunnistetut riskit, jotta ne ovat jatkossa käytettävissä. Riskien taltioiminen tietokantaan tulee määritellä harkiten, jotta tiedot ovat mahdollisimman tehokkaasti analysoitavissa. Esimerkkinä voisi mainita Raydugin (2013, 95) RBS-mallin, jota on mahdollista hyödyntää kehittyneempien tietokantojen kanssa. Liiketoiminta-alueiden jaottelu mahdollistaa riskien kohdennuksen liiketoiminta-alueiden tarpeiden mukaisesti.

Riskien tunnistamisen alkuosassa keskiöön nousevat henkilöstön osaamisen ja uusien ohjelmistojen riskien tunnistus. Tehokkaimpina riskien tunnistamisen tekniikoina voidaan pitää perinteisiä riskien tunnistus menetelmiä, kuten dokumenttien katselmointeja, tiedonkeräystekniikoita ja tarkastuslistoja. (PMBOK 2001.) Myös Vuoren (2010, 37–38) mainitsemat SWOT-analyysi ja aivoriihi-menetelmä toimivat tehokkaasti, ja niitä voidaan myös käyttää projektin myöhäisemmissä vaiheissa. Carrin (1993) mainitseman riskitaksonomian laatimisen voi nähdä melko kankeana työkaluna. Riskitaksonomia laaditaan tavallisesti kyselylomakkeisiin perustuen, kun taas Vuoren mainitsemia SWOT-analyysia ja aivoriihi-menetelmää voidaan soveltaa palaverien yhteydessä, jolloin yhteiset näkökulmat ja neuvottelu nousevat esille.

Uusien tuntemattomien ohjelmistojen riskientunnistaminen on olennaista (A.) Lisäksi riskientunnistamisessa tulee huomioida uuden teknologian monimutkaisuus ja käyttöönotto, sekä arvioida tiedot mahdollisista ohjelmisto- ja laitteistovirheistä. Lähtökohtaisesti riskienhallinnan tulisi huolehtia mahdollisten ohjelmistoihin liittyvien virheiden ja riskitasojen selvittäminen valmistajien toteuttamista riskianalyyseistä. Vyas (2015, 29) virhetoiminta- ja vaikutusanalyysi SFMEA-analyysi. (A) mukaan ohjelmistonlaadun voi myös nähdä riskinä, mutta harvemmin kaupallisten tuotteiden käytössä.

Ohjelmistojen jakaminen vastuu henkilöiden kesken vaatii koulutustarpeiden ja mahdollisen valmennuksen arvioinnin. (Harris 2009, 88.) Osaamisen arviointi perustuu organisaation dokumentteihin, joista on havaittavissa henkilön osaaminen, koulutus ja kokemus. Ohjelmistojen käytön, käyttöönoton ja muiden ohjelmiston asennustoimenpiteiden varalle laaditaan vastuuhenkilöt. Näiden toimenpiteiden yhteydessä on suositeltavaa järjestää koulutuksen mahdollisuus. Teemahaastattelun perusteella myös (A) mainitsi uusien tuntemattomien ohjelmistojen käyttöönoton, jolloin riskientunnistus on oleellista. On arvioitava, kuinka pystytään tunnistamaan a) kohonnut riski, b) kuinka riski pystytään minimoimaan tai poistamaan kokonaan. (B) luonnehti ohjelmistoriskien kuuluvan olennaisesti riskienhallintaan muiden projektiriskien ohella. Hän myös painottaa riskien vakavuuden merkityksen arviointia, ja riskien seuraamista tarkemmalla tasolla.

Yleisemmin teollisuuden yrityksissä käytettyjä, mutta myös tietojärjestelmiin soveltuvia vika-, vaikutus- ja kriittisyysanalyysejä ei käsitellä tässä riskienhallintasuunnitelmassa tai siihen kuuluvissa liitteissä. (SFS 5438, 1988.) Järjestelmä- ja laitevikojen kirjaaminen projektin kulun aikana on kuitenkin määritetty projektiryhmän toimenkuvaan.

Yhteydenpito ulkoisten sidosryhmien kanssa nousee monesti suuremmaksi kynnykseksi kuin organisaation sisäinen yhteydenpito, siksi ulkoisten sidosryhmien vastuualueiden ja vastuuhenkilöiden määrittäminen suunnitelmaan on tärkeää. Yuri Raudygynin mukaan riskienhallinnan toteutuksessa on olennaisinta toteutuksen herkkyys. Vastuut ja toimenpiteet tulee olla selkeästi dokumentoitu, ja niiden toteutus on selkeästi määritetty. (Raydugin 2013, 39–52.)

7.3 **Riskianalyysi**

Ohjelmistoriskien laadulliseen analyysiin voi soveltaa paremmin määrälliseen analyysin ja historiadatan käytössä tunnettua PERT-analyysia, jossa laaditaan aikajana tehtäväkokonaisuuksien arviointia varten. Analyysin avulla arvioidaan useimmiten ajan ja budjetin hallintaa. (Dobson & Dobson 2011, 39.) Menetelmä soveltuisi myös ohjelmistojen osaamisen, koulutuksen ja käyttöönoton hallintaan, mutta tutkimuksessa määritettyjen riskien vuoksi opinnäytetyön riskianalyysinä käytetään laadullisen analyysin menetelmiä. Riskirekisterin laatiminen taulukon 1 tutkituista ohjelmistoriskeistä sekä riskienhallintamatriisin (taulukko 2) avulla.

Riskienhallintamatriisi on laadittu Dobson & Dobsonin (2011, 57) kaavalla, jonka avulla riskille voidaan määritellä arvo, Riski = todennäköisyys * vaikutus (R = T * V). Riskirekisterin laatimisessa on kiinnitetty huomiota olennaisimpiin riskeihin, joiden toteutuminen mahdollisesti estäisi projektin loppuun saattamisen. Toinen huomioitava näkökulma ovat riskit, joiden vaikutus kumuloituu muuhun projektiryhmään tai mahdollisesti muihin projektin kriittisiin osiin. Matalan riskin arviossa vaikutusalue on suppea, sekä vaikutus projektin toteutukseen vähäinen.

Ohjelmistojen (Kuva 9) riskianalyysiä laatiessa tulee kiinnittää huomiota ohjelmistojen aikaisempaan käyttökokemukseen ja osaaminen organisaation käytössä olevista osaamisrekistereistä. Ohjelmistojen käytön arviointi perustuu kokemukseen ja ohjelmistojen käytön haastavuuteen. Tarpeen mukaan ohjelmistojen käytölle järjestetään koulutus ja arvioidaan jatkotoimenpiteet mahdollisien haasteiden osalle projektin toteutuksessa. Ohjelmistojen käyttö itsessään, sekä projektin teknisen toteutuksen vaatimukset määrittävät ohjelmistoille kriittisyysasteen. Projektin suurimmat uhkatekijät, kuten aikataulun, laadun ja budjetin hallinta tulee huomioida riskienhallinnassa korkealle.

Laadullinen riskianalyysi laaditaan tutkimuksen tuottamien tulosten ja projektissa käytettävien ohjelmistojen perusteella. Riskirekisterin taulukkoon 1 laadittujen riskien vakavuusaste perustuu tutkimuksen tuloksiin ja projektiohjelmistojen keskinäiseen vertailuun. Projektin riskienhallinnassa ei huomioida kaikkia listattuja riskejä. Rayduginin (2013, 30–32) mukaan riskienhallintasuunnitelmaan tulisi myös identifioida tilanteet, joissa riskit pitää jättää huomioimatta.

Laadulliseen analyysiin on poimittu tutkimuksessa määritettyjä uhkatekijöitä, joiden katsotaan olennaisesti vaikuttavan projektin toteutukseen. Projektiaikataulun (Kuva 10) mukaiseen toteutukseen voidaan liittää järjestelmien ja laitteistojen toiminta. Ohjelmistojen integrointi eri ympäristöihin ja järjestelmäkokonaisuuksiin voidaan nähdä haasteena, joka tulee huomioida aikaisessa vaiheessa projektia (Kendrick 2009, 44.) Tämän lisäksi Kendrickin (2009, 46) mukaan teknologian käyttöönotto projektin elinkaaren eri vaiheissa tulisi huomioida riittävän ajoissa.

Teknisen toteutuksen, eli itse tuotteen vaatiman ohjelmistokehitys osaamisen, arkkitehtuurin, järjestelmän käyttöönoton vaatimat riskimäärittelyt (Kuva 1) tulee laatia hyvin aikaisessa vaiheessa projektia. Toteutuksessa tämä käytännössä tarkoittaa järjestelmä- ja ympäristövaatimuksien toteutusta, sekä ohjelmiston ja tietokannan toteutusta, jotka ovat nähtävissä kuvasta 11.

Ennen projektin aloitusta tulee huolehtia, että kaikilla projektiin osallistuvilla henkilöillä on tarvittavat tiedot tietoturvallisuuden osa-alueesta. Tietoturvaan liittyvistä toimenpiteistä, kuten henkilökohtaisten laitteiden käytöstä projektin aikana. Projektipäällikön tulee varmistaa, että tietoturvaasiat ovat projektihenkilöiden tiedossa. SFS-ISO/IEC 27001:2013-tietoturvastandardin mukaan tietoturvallisuuden piirin luetellaan: viestintä ja tietoliikenne, henkilöstö, lait ja sitoumukset sekä häiriötilanteet ja pääsynhallinta. (SFS-ISO/IEC 27001:2013.)

Kappaleessa 3.1 määritetyille ohjelmistokokonaisuuksille tulee laatia projektihenkilöiden kesken vastuunjaon mukaiset suunnitelmat käyttöönoton, ohjelmiston vaatimustason ja koulutustarpeiden mukaan. Kendrick (2009, 69) uusien ohjelmien käyttöönotossa tulee huomioida ohjelmistojen monimutkaisuus, joka on huomattavan aliarvioitu uhkatekijä. Laadullisen

analyysin arvio perustuu taulukon 2 riskienhallintamatriisin (taulukko 2) avulla arvioituihin tekijöihin. Riskienhallintamatriisin arvioinnin perusteella riskit on tunnistettu riskientarkistus listaan (taulukko 1).

Taulukko 1. Riskien tarkistuslista

Prio.	R/M arvio	Riski kategoria	Toimenpiteet riski vähennys/poisto
1	12	teknologian käyttöönotto	aikainen havaitseminen ja arviointi
2	12	kokemus ja taidot	arviointi ja koulutussuunnitelma
3	9	uusien ohjelmistojen monimutkaisuus	perehtyminen ja koulutus
4	8	lait ja sitoumukset	perehtyminen dokumentteihin
5	8	Haittaohjelmat	käyttöönoton todennus
6	8	pääsynhallinta (tunnukset)	tunnusten aikainen käyttöönotto
7	8	viestintä	viestinnän toimenpiteiden määrittä-minen
8	6	teknologiamuutokset (ohjelmiston vaihto)	uuden ohjelmiston käyttöönottoon ja ominaisuuksiin perehtyminen
9	6	infrastruktuurimuutokset	muutosten vaikutusten havainnointi
10	6	muistitikut ja siirrettävät mediat	tiedotus käytännöistä
11	3	sosiaalinen media	tiedotus käytännöistä
12	2	Ohjelmistovirheet	kirjaus ja mahdolliset toimenpiteet
13	2	laitteistovirheet	kirjaus ja mahdolliset toimenpiteet
14	1	Älypuhelimet ja kannettavat	tiedotus käytännöistä

Taulukko 2. Riskienhallintamatriisi

Riskien luokittelu-taulukko		Harvinainen	epätodennä-köinen	Yleinen	todennäköinen
Vakavuus		1	2	3	4
Matala	1	1	2	3	4
Normaali	2	2	4	6	8
Korkea	3	3	6	9	12
Erittäin korkea	4	4	8	12	16

8 LOPPUTULOKSET

Teemahaastattelun tuloksesta voi todeta, että ohjelmistokehitysprojekteissa ohjelmistojen käyttö huomioidaan projektinsuunnittelussa olennaisesti projektisuunnitelmaan. Riskit voidaan määritellä projektisuunnitelmaan tai vaihtoehtoisesti laatia tarkemmat riskienhallinnan toimenpiteet riskienhallintasuunnitelmaan tai projektisuunnitelman muihin liitteisiin. (A) ja (B) luonnehtivat teemahaastattelussa ohjelmistoriskien kuuluvan olennaisesti osaksi projektisuunnitelmaa ja projektin riskienhallintaa. Kokonaisuutena teemahaastattelun vastauksista voi huomata, että riskien tunnistaminen ja arviointi ovat tärkeässä osassa projektinkulkua. Riskienhallinnan merkitys itsessään jaottelee ohjelmistoriskit eri kategorioihin, joiden voidaan tulkita olevan organisaatiokohtaisen arvioinnin alla. (A) mainitsee ohjelmistojen hallinnan ja käyttämisen kuuluvan osaltaan käytettävyyden ja soveltuvuuden riskien alle.

Tulosten perusteella voikin arvioida, että riskienhallinnassa riskit luokitellaan moniin erilaisiin kategorioihin, eikä niille ole selkeää yksittäistä jakoa, vaan yksittäinen riski voidaan luokitella useampaan riskiluokkaan. Näin on myös riskien riippuvuussuhteita tulkittaessa. Esimerkkinä voidaan mainita Paanasen (2008) esittelemä Sommervillen (2004) riskiluokittelu, jonka perusteella Paananen listaa strategisen ohjelmoijan menetyksen ja ohjelmiston tehokkuus arvioinnin luokiteltavaksi Murchin (2001) mainitsemiin riskityyppeihin: ulkoiset riskit, kustannusriskit, aikatauluriskit, tekniikkariskit ja toiminnan riskit.

Teemahaastattelun ja teoriaosan tuloksena saatiin vastaus kysymykseen: miten ohjelmistojen hallinta ja käyttäminen on huomioitu riskienhallinnan näkökulmasta? Ohjelmistojen riskienhallinta ei juurikaan eroa muista projektissa hallittavien riskien hallinnasta. Ohjelmistoprojektien riskienhallitsemiseksi on määritetty erilaisia työkaluja ja tekniikoita, joiden avulla kyetään tunnistamaan, analysoimaan ja ehkäisemään projektin riskejä. Näiden työkalujen avulla on toteutettavissa myös ohjelmistojen riskienhallinta.

Olennaisin eroavaisuus projektin- ja riskienhallinnan välillä on organisaation panostus riskienhallintaan. Riskienhallintaa toteuttaessa tulisi aina huomioida koko organisaatio, ja riskienhallinnan kehittäminen organisaation laajuisena. Briskin & Juvosen (2011) lainaus Suomisen (2000) riskienhallinnan määritteestä, jonka mukaan riskienhallinnan olennaisin piirre on, riskien keskinäisten riippuvuussuhteiden paljastaminen organisaatiossa. Tällöin kysymykseen tulee riskien taltioiminen yhteiseen käyttöön, jonka myötä organisaation riskien tunnistaminen ja analysointi saadaan mahdollisimman hyvin yhtenäistettyä. Näin myös kyetään estämään resurssien ylikuormittumista - yhteisten palaverien ja sidosryhmien tarve vähenee.

Projektinhallinnan riskienmäärittteleminen itsessään on riippuvainen projektipäällikön osaamistasosta sekä organisaation panostuksesta

riskienhallintaan. Tähän on mahdollista vaikuttaa sisäisen tiimityöskentelyn ja yhteispelin kautta. Tosin varsinaiset toimenpiteet tapahtuvat vasta kun organisaation johto on määritellyt toimenpiteet ja prosessit riskienhallinnan kehittämiseksi.

Riskientunnistamisen merkitys korostuu tilanteessa, jossa riskienhallintaan ei ole panostettu tai se on otettu äskettäin käyttöön. Tässä tilanteessa riskien tunnistamiseen täytyy erityisesti panostaa. Riskien tunnistamisen tapoja voi olla hyvin monenlaisia. Voidaan esimerkiksi hyödyntää sidosryhmien apua, tai mahdollisesti hankkia ulkopuolista tietoa riskeistä, jolloin riskienhallinta saadaan tehokkaasti käynnistettyä. Tässä tilanteessa myös henkilöstön kokemus ja osaamisen arvo nousevat esiin. Vuonna 2018 uudistetun riskienhallinnan ISO 31000-standardin mainittavimmista muutoksista nimenomaan organisaation ylemmän johdon sitoutuminen, sekä uuden osaamisen ja jo ennestään hankitun osaamisen hyödyntäminen tulisi tässä kohtaa ottaa huomioon. (ISO Online Browsing Platform 2018.)

Organisaatiomuutosten ja palvelujen ulkoistamisen myötä tänä päivänä riskientunnistamisessa tulisi korostua entistä enemmän. Matti Vuoren mainitsemat riskinarvioinnin jaottelu sidosryhmien, projektin toteuttajien ja liiketoiminnan osaajien kesken yhdistettynä eri abstraktiotasoihin, kuten esimerkiksi jaottelu ohjelmistotuotannon ja ulkoistuksen riskianalyysisessioihin. (Vuori 2010, 34–35.) Riskinarvioinnin jaottelua tukee myös ISO 31000-standardi, jossa korostetaan avoimen mallin ylläpitämistä monimutkaisissa konteksteissa sekä iteratiivisuuden ja analyysien kehittämistä organisaation riskienhallinnassa. (ISO Online Browsing Platform 2018) Riskianalyysityökaluja ja tekniikoita on useita (Kuva 8), mutta monien soveltuvuus ohjelmistoriskien analysointiin on heikko. Uusien menetelmien soveltuvuutta ohjelmistokehitysprojektien riskienhallinnan kehittämiseen on kuitenkin hyvä seurata organisaation riskienhallinnassa.

Riskienhallinnan suunnittelussa on tärkeää huomioida riskienhallintamallien soveltuvuus eri tilanteisiin ja vaiheisiin projektissa. Esimerkkinä voisi lainata Paanasen (2008) lainaamaa Smithin ja Pichlerin (2005) luonnehdinnasta, jonka mukaan heikon skaalautuvuuden takia IT-projektien riskienhallinnassa on huomioitava, että ketterien ohjelmistokehitysmallien riskienhallinnassa on käytettävä riskienhallinnan parhaita käytäntöjä. Tätä ajatusmallia tukee myös Kotkansalon, Parkkilan, & Tarvaisen (2017, 7) arvio yksittäisen riskianalyysi tekniikan riittämättömyydestä kattavaan riskienhallintaan.

Paras tehokkuus saavutetaan näin ollen erilaisten riskianalyysitekniikoiden yhdistelmillä, joiden avulla saavutetaan parhaat ominaisuudet sekä soveltuvuus projektin eri osien riskientunnistamiseksi. IT-projektien riskientunnistamisen parhaimpiin keinoihin sisältyvät Vuoren (2010, 37–38.) tarkistuslistat, SWOT-analyysi ja aivoriihi-menetelmät. Niitä voidaan hyödyntää tehokkaasti perinteisten projektinhallintamallien ja ketterienmenetelmien yhteydessä, ja ne toimivat projektin elinkaaren eri vaiheissa.

Yleisesti IT-projektien riskienhallintaprosesseissa korostuu jatkuva valvonta, (Taylor 2003, 155.) systemaattisuus ja dokumentointi sekä toteutuksen herkkyys. Näiden avulla pyritään nopeaan ja tehokkaaseen riskienhallintaan. (Raydugin 2013, 39–52.) Taylorin ja Raydugin riskienhallintaprosessit soveltuvat etenkin perinteisiin projektinhallintamalleihin. Iteratiivisissa riskienhallintaprosesseissa korostuu jatkuvan tarkkailun ja valvonnan merkitys projektimuutosten suhteen. Iteratiivisen projektinhallintamallin riskienhallintaprosessiin ja sen kehittämiseen on suositeltavampana käyttää yleisen ISO 31000-riskienhallintastandardin periaatteita. (ISO 31000:2009) Niihin voi ainakin mainita muutokseen sopeutuvuuden, iteratiivisuuden, systemaattisuuden ja organisaation jatkuvan kehittämisen. Riskienhallintaprosesseja vertailtaessa Taylorin ja Raydugin malleissa riskienhallintaprosessille on laadittu selkeämpi kokonaisuus, joka on jatkuvan tarkkailun alla sekä valmis muutokseen. Sen sijaan ISO 31000-standardin riskienhallintaprosessi on jatkuvassa aloitustilassa ja valmiina muutokseen, siinä myös korostuu prosessin iteratiivisuus. (Kuva 5).

Projektin toteutuksen aikana on todennäköistä, että sen sisältöön, rakenteeseen tai ympäristöön tulee muutoksia, jotka aiheuttavat uhkatekijöitä. Mahdolliset työntekijöiden irtisanoutumiset, ohjelmistojen vaihdot ja useat muut syyt (kuva 6), josta voi todeta vaikutusalueiden olevan laajoja. Myös Harrisin (2009, 52–53) mainitsemat organisaatio muutokset - uudelleen sijoittuminen tai järjestäminen vaikuttavat negatiivisesti muun muassa henkilöstön-, teknisen infrastruktuurin- ja yhtäjaksoisuuden osa-alueille.

Projektien riskienhallinnassa muutoksenhallinnan merkitys on mainittava. Projektiin ja sen osiin kohdistuvien negatiivisten muutosten mahdollisimman nopea havainnointi, mahdollistaa uhkatekijöiden seurauksien minimoimisen mahdollisimman tehokkaasti. Muutoksenhallinnan kulmakiviin kuuluvat havainnointi ja muutokseen reagointi. Kommunikaatiosuunnitelman laatiminen tehostaa muutoksenhallinnan toimivuutta. (Leach 2014, 88.) Higuera, Gluch, Dorofee, Murphy, Walker & Williams (1994, 3–6) Projektin- ja riskienhallinnassa on tärkeää määritellä sidosryhmät ja vastuualueet, jotka vaikuttavat projektin toteutukseen. Tällöin on myös tärkeää huolehtia tiedonkulusta ja viestinnän toimivuudesta.

Teemahaastattelun ja kirjallisuusselvityksen avulla tunnistettiin eri lähteitä hyödyntäen lukuisa määrä riskejä. Kirjallisuus ja tieteelliset tutkimukset määrittelivät ohjelmistokehitysprojektien riskit ympäristöihin, joissa ohjelmistot toimivat. Muun muassa Harrisin (2009, 52–53) mainitsemat organisaatiomuutokset vaikuttavat projektin toteutukseen, kuten myös Kendrickin (2009, 69) määrittelemien palvelukokonaisuuksien häiriöt, joihin voidaan luetella tietokonejärjestelmät, tukipalvelut ja tietoliikenteen häiriöt. Aikaisempien tutkimusten perusteella ohjelmistokehitysprojektien riskit keskittyvät suurelta osin Taylorin (2003, 178) uuden teknologian käyttöönottoon sekä Kendrickin (2009, 69) ohjelmistojen monimutkaisuuden osa-alueisiin. Myös teemahaastattelun vastausten perusteella (A) ja (B) huomioivat teknologian käyttöönottoon ja ohjelmistojen monimutkaisuuden projektin riskienhallinnassa olennaisena. Useampien lähteiden perusteella ohjelmisto- ja laitteistovirheiden merkitys on projektiriskien arvioinneissa melko pieni, ja useimmiten (A) mukaan niihin ei juurikaan kiinnitetä huomiota, kun kysymys on tunnettujen ohjelmistotoimittajien tuotteesta.

Opinnäytetyön tutkimuksen perusteella voi huomata, ettei aikaisemmissa tutkimuksissa juurikaan kiinnitetty huomiota tietoturvan eri osa-alueisiin. Tietoturvan merkitys projektintoteutumisen kannalta ei ole kovinkaan suuri riski. Laukaan kunnan tilinpäätöksen perusteella yritysten ja organisaatioiden yleisiä tietoturvaongelmia on runsaasti. Projektipäällikön tehtäväalueeseen ei välttämättä kuulu virustorjuntaohjelmistojen hallinnasta tai ohjelmistojen ajantasaisuudesta huolehtiminen. Projektitiimiä tulisi kuitenkin ohjeistaa, miten toimia eristämis-, tunnistamis- ja pääsynvalvontamenettelyjen suhteen. (Hallinnon kehittäminen tietoturvasanasto, 2005.) Tulevaisuuden uhkatekijöihin voidaan laskea älypuhelinten ja kannettavienlaitteiden aiheuttamat tietoturvauhat sekä sosiaalisen mediakäytön. (Laukaa 2017.)

9 YHTEENVETO

Tutkimuksen avulla onnistuttiin löytämään vastaukset kaikkiin kolmeen tutkimuskysymykseen. Ohjelmistojen käyttö huomioidaan ohjelmistokehitysprojekteissa olennaisena osana projektin suunnittelua. Ohjelmistojen riskiarviointi voidaan toteuttaa nykyisin riskienhallinta menetelmin. Uusia riskienhallinnan menetelmiä ja toimintatapoja on kehitetty jonkin verran lisää. Kirjallisuustutkimuksen perusteella voi kuitenkin todeta, että ohjelmistoprojektien riskienhallintamenetelmät ovat ajanmukaiset. Tutkimuksen avulla todennettiin uusia ohjelmistoriskejä, joita ei ammattikirjallisuudessa tai aikaisemmissa tutkimuksissa määritelty.

Tutkimustuloksia voi pitää lähdetietojen ja tiedon kartoitus menetelmien pohjalta luotettavina. Tutkimuksessa käytettyjen kattavien tutkimusmateriaalien perusteella, määritellyt ohjelmistoriskit ja teoriaosa ovat ajantasaiset sekä vertaillen useista lähteistä rajattu. Tutkimustulosten avulla on mahdollista löytää parhaimpia käytäntöjä ja menetelmiä ohjelmistoprojektien riskientunnistamiseksi sekä analysointiin. Lisäksi tutkimustulosten pohjalta on mahdollista kehittää organisaatiotason riskienhallintaa parhaimpien riskienhallinnan käytäntöjen kautta. Ohjelmistoriskien kartoitus itsessään avaa riskien tunnistamisen näkökulmia ja antaa selkeän kuvan ohjelmistoriskeistä. Tekijälleen tutkimus avasi ohjelmistokehitysprojektien riskienhallinnan kokonaiskuvan, sekä kehitti yleisellä tasolla tunnistamaan ja havaitsemaan projektien riskejä.

Näkisin tulevaisuuden haasteina organisaatiorakenteiden ja yritysten välisten suhteiden muutokset. Niiden myötä riskienhallinnan käytäntöjen ja toimenpiteiden soveltuvuutta tulisi arvioida uudelleen. On myös mahdollista, että projektihallintamenetelmiin tulee uudistuksia, joiden toimesta riskienhallinnan menetelmien käyttöä ja soveltuvuutta projektien riskienhallintaan tulisi tarkkailla. Teknologian ja ohjelmistojen kehityssuuntiin tulee kiinnittää entistä enemmän huomiota, jotta riskienhallinnan tehokkuus saadaan maksimoitua. Varpe (2016) ottaa blogissaan kantaa digimurrokseen ja teknologian nopeaan kehittymiseen, joiden johdosta organisaation liiketoiminnan eri toimialueet, kuten informaatio- ja viestintäpalvelut, hallinto- ja tukipalvelut, yritys- ja asiantuntijapalvelut muuttuvat nopeasti. Myös Korpimies (2018) kirjoittaa blogipostauksessaan digimurroksesta sekä tietoturvan ja riskienhallinta hankkeiden osuudesta tämän päivän IT-investoinneissa. Näiden tekijöiden perusteella voi todeta, että riskienhallintaan ja sen kehittämiseen tulee kiinnittää entistä enemmän huomiota.

LÄHTEET

Arkko, L. (2013). *CCMI-MALLI – HYÖDYT JA HAASTEET PROJEKTINHALLINNAN NÄKÖKULMASTA.* Kandidaatintutkielma. Tietojärjestelmätiede. Jyväskylän yliopisto. Haettu 6.4.2018 osoitteesta. https://jyx.jyu.fi/dspace/bitstream/handle/123456789/41845/Lotta%20Arkko.pdf?sequence=1

Arnuphaptrairong, T. (2011). Proceedings of the International MultiConference of Engineerings and Computer Scientists 2011 Vol 1. *Top Ten Lists of Software Project Risks: Evidence from the Literature Survey.* Haettu 19.4.2018 osoitteesta. https://pdfs.semanticscholar.org/deae/e8d192415f3facc01f224485bd9aa4b2ae34.pdf

Brisk, S. Juvonen, H. (2011). Riskienhallinnan strategiat ja menetelmät pk-yrityksissä. Risk Management Strategies and Methods in Small and Medium-sized Enterprises. Kandidaatintyö. Teknistaloudellinen tiedekunta. Lappeenranta University of Technology. Haettu 11.4.2018 osoitteesta. https://www.doria.fi/bitstream/handle/10024/69903/nbnfi-fe201106231797.pdf?sequence=3

Chemuturi, M. (2013). *Mastering It Project Management, Best Practices Tools and Techniques*. Florida. J. Ross Publishing. https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/reader.action?docID=3319551&query=

Chemuturi, M. Cagley, T. (2009). *Mastering It Project Management, Best Practices Tools and Techniques*. Florida. J. Ross Publishing. https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/reader.action?docID=3319451&query=

Dobson, M. Dobson, D. (2011). *Project Risk and Cost Analysis. New York*. Amacom. https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/reader.action?docID=951442&query=

Flaus, J-M. (2013). *Risk Analysis: Socio-Technical and Industrial Systems*. London, Hoboken. ISTE Ltd and John Wiley & Sons, Inc. https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/reader.action?docID=1441765&query=

Haikala, I. Mikkonen, T. *Ohjelmistotuotannon käytännöt*. Hämeenlinna. Haettu 17.3.2018 osoitteesta: https://www.theseus.fi/bitstream/handle/10024/88789/Mannisto_Tomi.pdf?sequence=1&isAllowed=y

Hallila, M. (2016). *Vaativan toimitus projektin riskienhallinta*. Insinöörityö. Kemiantekniikka. Metropolia Ammattikorkeakoulu. Haettu 2.4.2018 osoitteesta. https://www.theseus.fi/bitstream/handle/10024/112328/Hallila_Mikko.pdf?sequence=1&isAllowed=y

Harris, E. (2009). *Strategic Project Risk Appraisal and Management.* Farnham. Taylor & Francis Group. https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/reader.action?docID=476364&query=

Higuera, R. Gluch, D. Dorofee, A. Murphy, R. Walker, J. Williams, R. (1994). *An Introduction to Team Risk Management (Version 1.0)*. Software institute. Carnegie Mellon University. Haettu 2.5.2018 osoitteesta. https://resources.sei.cmu.edu/asset_files/SpecialReport/1994_003_001_16253.pdf

Holcombe, M. (2008). *Running an Agile Software Development Project*. New Jersey. John Wiley & Sons, Incorporated https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/reader.action?docID=427745&query

Hoodat, H. Rashidi, H. (2009). World Academy of Science, Engineering and Technology 32 2009. *Classification and Analysis of Risks in Software Engineering.* Haettu 19.4.2018 osoitteesta. https://pdfs.semanticscholar.org/5b5a/6a175fedcce1fe52ee4900de252597a24d23.pdf

ISO (the International Organization for Standardization) (2018). *ISO 31000:2018 Risk management – Guidelines*. Haettu 27.3.2018 osoitteesta. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

Jyväskylän yliopisto. *Ankkuroitu teoria eli grounded theory.* Haettu 15.4.2018 osoitteesta. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineiston-analyysimenetelmat/ankkuroitu-teoria-eli-grounded-theory

Kajaanin ammattikorkeakoulu. Haastattelu. *Haastattelumuodot.* Haettu 16.4.2018 osoitteesta. https://www.kamk.fi/opari/Opinnaytetyopakki/Teoreettinen-materiaali/Tukimateriaali/Aineiston-keruumenetelmat/Haastattelu

Kendrick, T. (2009). *Identifying and Managing Project Risk: Essential Tools for Failure Proofing Your Project*. New York. Amacom. https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/reader.action?docID=420626

Kontio, J. *The Riskit Method for Software Risk Management*, Version 1.00. SoberIT. University of Maryland. Haettu 18.4.2018 osoitteesta. http://www.soberit.hut.fi/T-76.115/02-03/palautukset/groups/pmoc/de/riskit.pdf

Kotkansalo, A. Parkkila, L. Tarvainen, J. (2017). *Riskianalyysimenetelmien tarkastelu – Kirjallisuusselvitys.* Tutkimusraportit ja kokoomateokset. 23/2017 Haettu 29.3.2018 osoitteesta. https://www.theseus.fi/bitstream/handle/10024/137517/B%2023%202017%20kotkansalo%20parkkila%20tarvainen.pdf?sequence=1

Korpimies, A. (2018). *Kaikki puhuvat digitalisaatiosta – Suomen it-väellä riittää töitä ja paineet kasvavat.* https://www.tivi.fi/Kaikki_uutiset/kaikki-puhuvat-digitalisaatiosta-suomen-it-vaella-riittaa-toita-ja-paineet-kasvavat-6725820

Lahnalahti, J. (2013). Uusi SFS-ISO/IEC 27001:2013. *Tietoturvallisuus? Hallintajärjestelmä? Standardin SFS-ISO/IEC 27001:2013 näkökulmat.* Haettu 11.4.2018 osoitteesta. https://www.sfs.fi/files/4224/27001-julkaisu_2013-12-05_Lahnalahti.pdf

Laukaa Kunnanvaltuusto (2017). Tilinpäätös 2016. Haettu 13.4.2018 osoitteesta. http://laukaa02.hosting.documenta.fi/kokous/20171569-2-2.PDF

Leach, L. (2014). *Critical Chain Project Management*. Boston. Artech House. https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/reader.action?docID=1641591

Liuksiala, A (2012). *The use of the risk management standard ISO 31000 in Finnish organisations.* Master's Thesis. School of Management. University of Tampere. Haettu 27.3.2018 osoitteesta. http://tampub.uta.fi/bitstream/handle/10024/84249/gradu06462.pdf;sequence=1

Mahalakshmi, M. Sundarar, M. (2013). *Traditional SDLC Vs Scrum Methodology – A Comparative Study*. Volume 3. s.195. 3.3.2018 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.413.2992&rep=rep1&type=pdf

Meriläinen, J. (2003). *Riskianalyysimenetelmät*. Seminaariesitelmä. 21.4.2003. Haettu 11.4.2018 osoitteesta. https://www.cs.helsinki.fi/group/turvasem/papers/merilainen.pdf

Mohapatra, P. (2010). *Software engineering A Lifecycle Approach*. New Delhi. New age international (P) limited, publishers. https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/reader.action?docID=3017407&query=

Paananen, M. (2008). *Riskien tunnistaminen ohjelmistokehityksessä.* Pro gradu -tutkielma. Tietojenkäsittelytieteen laitos. Tampereen yliopisto. Haettu 6.4.2018 osoitteesta. http://tampub.uta.fi/bitstream/handle/10024/79073/gradu02553.pdf?sequence=1

Raydugin, Y. (2013). *Project Risk Management: Essential Methods for Project Teams and Decision Makers.* New Jersey. John Wiley & Sons, Inc. https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/reader.action?docID=1469456

Richman, L. (2011). *Successful project management*. New York. Amacom https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/reader.action?docID=1043635

Salmelainen, T. (2005). s.8. *Projektisuunnitelma Potta*. Helsinki; Helsingin yliopisto. s.8 https://www.cs.helsinki.fi/group/potta/projektisuunnitelma.doc

Satyendra. (2013*). Effective communication – A tool for organizational success.* 28.8.2013. Haettu 7.4.2018 osoitteesta. http://ispatguru.com/effective-communication-a-tool-for-organizational-success/

Software Engineering Institute (2010). Risk Management framework. Haettu 21.3.2018 osoitteesta. http://www.dtic.mil/dtic/tr/fulltext/u2/a528650.pdf

Stephens, R. (2015). *Beginning Software Engineering*. Indiana. Wiley & Sons https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/reader.action?docID=1895174&query=

Tanhuamäki, H. (2006). *Kriittisen tietojärjestelmän muutoksen hallinta.* Pro gradu -tutkielma. Tietojenkäsittelylaitos. Tampereen yliopisto. Haettu 17.4.2018 osoitteesta. http://tampub.uta.fi/bitstream/handle/10024/93207/gradu00904.pdf?sequence=1

Taylor, J. (2004). Managing information technology projects. New York. Amacom https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/reader.action?docID=243057&query=

Tripathy, P. Naik, S. Tripathy, P. (2014). *Software Evolution and Maintenance*. New Jersey. John Wiley & Sons, Incorporated. https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/reader.action?docID=1801248&query=

Varpe, R. (2016). *Digimurros haastaa työmarkkinat uudistumaan*. Haettu 24.5.2018 osoitteesta. https://www.palta.fi/tiedotteet/digimurros-haastaa-tyomarkkinat-uudistumaan/

Virtuaali ammattikorkeakoulu. Ylemmän AMK- tutkinnon metodifoorumi. *Grounded theory.* http://www2.amk.fi/digma.fi/www.amk.fi/opintojaksot/070901911934638907491193464144782/1194348654857/1194356926123.html

Vuori, M. (2010). *Riskienhallinta hajautetuissa ohjelmistoprojekteissa*. Haettu 1.4.2018 osoitteesta. https://www.mattivuori.net/julkaisuluettelo/liitteet/riskienhallinta_hajautetuissa_ohjelmistoprojekteissa.pdf

Vyas, P. (2015). *The applications of SFTA and SFMEA approaches during software development process: an analytical review.* Birla Institute of Technology and Science. Haettu 2.4.2018 osoitteesta. https://www.inderscienceonline.com/doi/pdf/10.1504/IJCCBS.2015.068851