LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

# Laadun- ja riskienhallinta johtamisjärjestelmässä ISO 9001:2015 ja ISO 31000:2009 mukaisesti

Karhunen, Joonas & Reinvall, Niko

2015 Leppävaara

**Laurea-ammattikorkeakoulu**
Leppävaara

# Laadun- ja riskienhallinta johtamisjärjestelmässä ISO 9001:2015 ja ISO 31000:2009 mukaisesti

Karhunen, Joonas & Reinvall Niko
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Huhtikuu, 2015

**Laurea-ammattikorkeakoulu** **Tiivistelmä**
Leppävaara
Turvallisuusalan koulutusohjelma

Karhunen Joonas & Reinvall Niko

**Laadun- ja riskienhallinta johtamisjärjestelmässä ISO 9001:2015 ja ISO 31000:2009 mukaisesti**

Vuosi 2015 Sivumäärä 65

Tämän opinnäytetyön tarkoituksena on tarkastella riskienhallinnan ja laadunhallintajärjestelmien suhdetta ISO 9001:2015 ja ISO 31000:2009-standardien viitekehyksessä, tutkimuskysymyksen ollessa ”miten ja miksi integroida ISO 9001 mukaista laadunhallintaa ja ISO 31000 mukaista riskienhallintaa organisaation johtamisjärjestelmään”. Lisäksi työssä tarkastellaan standardien välisiä yhtymäkohtia ja riskienhallinnan merkitystä ISO 9001:2015 mukaisessa laadunhallintajärjestelmässä.

Työn tilaajana ja työelämäkumppanina toimii Suomen Turvallisuusosaaminen Oy, joka on akateemisesti suuntautunut turvallisuusalan asiantuntijaorganisaatio. Suomen Turvallisuusosaaminen Oy tarjoaa turvallisuuteen ja riskienhallintaan liittyvää koulutusta, avustaa turvallisuuden tutkimus- ja kehittämisprojektien toteuttamisessa sekä tuottaa turvallisuusalan oppikirjoja ja julkaisuja.

Tämä opinnäytetyö on laadullinen tutkimus, jonka pääasiallisena tutkimusmenetelmänä on narratiivinen kirjallisuuskatsaus ja tavoitteena tutkia aihealueen teoriaa ja tuottaa tekstiä syksyllä 2015 julkaistavaa oppikirjateosta varten. Keskeisinä aineistoina tutkimuksessa käytettiin ISO/DIS 9001:2014 standardiluonnosta ”Laadunhallintajärjestelmät – vaatimukset” sekä ISO 31000:2009 standardia ”Riskienhallinta – periaatteet ja ohjeet”. Näiden standardien näkökulmista kerättiin niiden soveltamista käsittelevää aineistoa tietoperustan muodostamiseen, jotta opiskelijat kykenivät muodostamaan riittävän laajan käsityksen aihealueesta johtopäätösten ja soveltamisohjeen laatimiseen. Metodinsa mukaisesti kirjoitusote on narratiivinen ja tutustuttaa lukijansa kummankin standardin keskeisiin seikkoihin.

Opinnäytetyön tuotoksena on ISO 31000–standardiin perustuvan kokonaisvaltaisen riskienhallinnan mallin mukainen kuvaus ISO 9001:2015 riskienhallinnan vaatimuksista ja siirtymävaiheen toimenpiteistä siirryttäessä ISO 9001:2008 mukaisesta laadunhallintajärjestelmästä ISO 9001:2015:een. Standardien vaatima toimintaympäristön määrittely toteutetaan PESTLE ja SWOT-menetelmiä yhdistävällä työkalulla, jonka käyttö ohjeistetaan osana opinnäytetyötä.

Johtopäätöksinä todettiin seikkaperäisen ja kattavan toimintaympäristön määrittelyn olevan erittäin tärkeä tekijä niin laadun- kuin riskienhallinnankin näkökulmasta, ja että riskienhallintaa intergroiva, prosessiajatteluun perustava laadunhallintajärjestelmä hyötyy ajanmukaisesta ja ajoittain rohkean ennakoivastakin toimintaympäristön tilannekuvasta. Saumattomasti toteutetut laadun- ja riskienhallinnan ratkaisut osana johtamisjärjestelmää tukevat toisiaan ja ilmentävät kokonaisvaltaisen riskienhallinnan ydinajatusta.

Asiasanat: ISO 9001, ISO 31000, kokonaisvaltainen riskienhallinta, laadunhallintajärjestelmä,

**Laurea University of Applied Sciences** **Abstract**
Leppävaara
Degree programme in Security Management

Karhunen Joonas & Reinvall Niko

**Quality and Risk Management in a Management System as per ISO 9001:2015 and 31000:2009**

Year 2015 Pages 65

The aim of this thesis is to examine the relation of risk management and quality management systems in the context of the standards ISO 9001:2015 and ISO 31000:2009. The research problem is how to integrate ISO 9001 compatible quality management and ISO 31000 compatible risk management into a management system.

The thesis was commissioned by Suomen Turvallisuusosaaminen Oy, which is an academically orientated security consultant organization. Suomen Turvallisuusosaaminen Oy provides security and risk management training, helps with security research and development projects and produces textbooks and publications for the security sector.

The thesis was conducted as a qualitative research which uses a narrative literature review as its primary research method and aims to study the theories of the given field and produce text for a textbook that will be published in the autumn 2015. The publication of the draft international standard ISO/DIS 9001:2014 "Quality management systems – requirements" and international standard ISO 31000 "Risk management – principles and guidelines" formed the fundamental material for the thesis. By reflecting these standards to the literature, the students formed a knowledge basis to draw conclusions and create a guide to apply these standards in practice. The thesis is written in a narrative style and it familiarizes the reader to fundamentals of the two standards.

The product of the thesis is a description of the risk management requirements of ISO 9001:2015 implementing a comprehensive model of risk management based on ISO 31000:2009. The actions in the transitional phase from ISO 9001:2008 based quality management system to ISO 9001:2015 are also described. Defining the operational environment for the organization is accomplished with a tool combining PESTLE and SWOT methods and the use of the tool is instructed as a part of the thesis.

As conclusions, it was found that a detailed and comprehensive definition of the organization's operational environment and context is a a very important factor from both quality and risk management perspectives, and that a process-based management system integrating risk management will benefit from timely and occasionally boldly proactive situational awareness of the operational environment. Seamlessly implemented quality and risk management solutions as components of the management system support each other and represent the core idea of comprehensive risk management.

Keywords: comprehensive Risk Management, ISO 9001, ISO 31000, Quality Management

Sisällys

# 1 Johdanto

Riskienhallinta, turvallisuusjohtaminen ja laadunhallinta koskettavat niin pienten kuin suurtenkin yritysten ja organisaatioiden toimintoja ja niiden kehittämistyötä. Palveluiden ja tuotteiden korkean tason saavuttamiseksi ja ylläpitämiseksi organisaation tulee kehittää prosesseja joissa suunnitellaan, laaditaan, tarkistetaan ja korjataan toimintamalleja aikaisempien järjestelmien pohjalta tai luomalla kokonaan uusia käytäntöjä. Näiden prosessien kehittämiseksi on käytössä useita työkaluja ja viitekehyksiä joiden avulla organisaatioiden käytäntöjä voidaan parantaa ja yhdenmukaistaa.

Kansainvälinen standardoimisliitto ISO (the International Organization for Standardization) tuottaa ja julkaisee kansainvälisiä standardeja laajasti eri alojen organisaatioiden ja yritysten tarpeisiin. Standardeja päivitetään ja laaditaan yhteistyössä eri maiden kansallisten standardoimiselinten kanssa hyödyntäen kyseisen alan asiantuntijoita. Uudistamistyö on luonteeltaan jatkuvaa ja pyrkii vastamaan jatkuvaan toimintaympäristön muutokseen. Näistä standardeista ISO 9000-sarja käsittelee laadunhallintajärjestelmiä ja ISO 31000-sarja riskienhallintaa. (Croft 2012, Moeller 2011, 331-332.)

ISO käynnisti vuonna 2012 viidennen sukupolven standardien laatimisen ja uudet laadunhallintajärjestelmästandardit ISO 9000 ja ISO 9001 valmistuvat vuonna 2015 osana standardien jatkuvaa kehittämistä ja uudistamista. Kyseessä on merkittävä uudistus, jonka kaltainen on viimeksi ISO 9000-perheen osalta julkaistu vuonna 2000 (Croft 2012). Standardin uudet vaatimukset etenkin riskienhallinnan osalta luovat tarpeen selkeälle ja helppokäyttöiselle opasteokselle uudistetun laadunhallintajärjestelmän käyttöönotosta.

Helmikuussa 2015 tarjoutui kirjoittajille mahdollisuus osallistua ISO 9001 ja ISO 31000 standardeiden soveltamista käsittelevän oppikirjateoksen laatimiseen. Oppikirjateos tullaan suuntaamaan organisaatioille, joilla on jo käytössä ISO 9001-standardin mukainen laadunhallintajärjestelmä ja joka haluaa päivittää sen uuden ISO 9001:2015 revision mukaiseksi. Uusi standardi asettaa vaatimuksia riskienhallinnalle, jota käsitellään synergiasyistä saman standardiperheen riskienhallintaa koskevalla ISO 31000 standardilla. Opinnäytetyön tärkeimpänä teemana on laadunhallintajärjestelmän päivittämiseen liittyvät siirtymävaiheen toimenpiteet ja riskienhallintatoimenpiteiden yhtenäistäminen ISO 9001 standardin mukaisen laadunhallinnan kanssa.

# 2 Opinnäytetyön tavoite ja menetelmät

Opinnäytetyön tavoitteena on tutkia laadun- ja riskienhallinnan vaatimuksia ISO 9001:2015 ja ISO 31000:2008-standardien viitekehyksissä sekä tarkastella niiden prosessien integraation mahdollisuuksia ja hyötyjä. Kirjallisuuskatsauksien tuotoksia ja johtopäätöksiä hyödynnetään suunnitellun oppikirjateoksen osina. Opinnäytetyön jatkosuunnitelmien kannalta tavoitteeksi katsottiin riittävän tietoperustan kartuttaminen käsiteltävien ilmiöiden viitekehyksestä, jotta kirjoittajat kykenevät asiantuntijatekstin tuottaminen sellaisella tasolla että jatkosuunnitelmat voidaan toteuttaa.

## 2.1 Tutkimuskysymys ja rajaukset

Työelämäyhteistyön asettaman rajauksen mukaisesti laadunhallintaa ja riskienhallintaa tarkastellaan ISO 9001 ja ISO 31000 standardien näkökulmista. Tutkimuskysymykseksi kirjoittajat määrittelivät ”miten ja miksi integroida ISO 31000 mukaista riskienhallintaa ja ISO 9001 mukaista laadunhallintaa organisaation johtamisjärjestelmään”.

Tutkimuskysymyksen asettelulla haluttiin selvittää millainen muutosprosessi organisaation tulee suunnitella ja toteuttaa päivittäessään laadunhallintajärjestelmäänsä ISO 9001:2015:teen. Kysymyksen ”miksi”-osalla haluttiin selvittää ISO 9001:2015:sta ja ISO 31000:n väliset mahdolliset positiiviset synergiat. Tutkimuskysymyksessä tulee ilmi työn keskeisiä käsitteitä ja tavoitteita, tutkimuksen toteuttamisen näkökulman ollessa erityisesti käytännönläheisyys ja sovellettavuus työelämän tarpeisiin. Tutkimuksen tyypin ollessa laadullinen tutkimus on tutkimuskysymyksen kehittyminen ja tarkentuminen tutkimuksen edetessä mahdollista (Hirsjärvi, Remes, Sajavaara 2011, 117).

Edelleen työelämäyhteistyön rajaamana opinnäytetyö käsittelee laadunhallintajärjestelmän muutosta organisaatiossa, joka on jo entuudestaan ISO 9001:2008-sertifioitu ja haluaa päivittää laadunhallintajärjestelmänsä ISO 9001:2015:n mukaiseksi. ISO 9000-standardiperheen mukaisen laadunhallintajärjestelmän piirteitä, prosessiajattelua ja yleisiä periaatteita kuvataan siinä määrin kun se lukijan johdattelemiseksi on katsottu hyödylliseksi. 31000-standardin mukaista riskienhallintaa käsitellään perusteellisemmin sen edustaessa laadunhallintajärjestelmän näkökulmasta uutta toimintatapaa.

Riskiksi koettiin opinnäytetyön julkisuuden vaikutukset sen jatkotuotoksien menekkiin. Valmista teosta ei saada alustavan suunnitelman vastaisesti opinnäytetyön aikataulun puitteissa katselmoitavaksi, joten opinnäytetyötä ei voida arvioida sen viitekehyksessä. Riskiksi todettiin

myös, että opinnäytetyön ulkopuolisista tekijöistä johtuen opinnäytetyö saattaisi myöhästyä tai olla riittämätön täyttämään opinnäytetyölle asetettuja kriteereitä.

Jatkotuotoksille hahmotellun rakenteen mukaisesti Karhunen tutkii ISO 9001:2015 – standardin erityispiirteitä ja vaikutusta ISO 9001:2008:aa jo käyttävän organisaation toimintaan, ja Reinvall keskittyy ISO 31000 mukaisen riskienhallinnan tutkimiseen. Jatkotuotoksen muista osista vastaa työelämäyhteistyön edustajana toimiva Jyri Paasonen.

## 2.2 Tutkimuksen tyyppi

Tämä opinäytetyö on tyypiltään tutkielmatyyppinen laadullinen tutkimus, jonka tietoperusta laadittiin kahden, eri teemoja koskettavan kirjallisuuskatsauksen keinoin.

Laadullisen tutkimuksen luonteeseen kuuluu keskittyminen erityisesti laadulliseen tietoon määrällisen rinnalla ja pyritään ymmärtämään aihealueita mahdollisimman kokonaisvaltaisesti. Laadullisessa tutkimuksessa on vaikeaa, ehkä jopa mahdotonta saavuttaa objektiivisia päätelmiä, sillä laadullisen tutkimuksen erityispiirteitä on arvoihin ja tutkijoiden kokemuksiin nojautuminen. Tietoa hankitaan kokonaisvaltaisesti erilaiset näkökulmat huomioiden ja aineiston kokoamisessa pyritään todenmukaisuuteen ja luonnollisuuteen. (Hirsjärvi ym. 2011, 151–156.)

Laadullisessa tutkimuksessa tutkimusasetelma elää tutkijan havaintojen pohjalta. Tutkimussuunnitelma voi siis muuttua tutkimuksen edetessä ja hyvän laadullisen tutkimuksen tekijällä pitääkin olla näkemystä ja kokemusta suunnitelman parantamisesta. Toisin kuin laadullisen tutkimuksen rinnakkaismenetelmässä määrällisessä tutkimuksessa, tutkimuksen perusasetelmana ei ole hypoteesien testaaminen vaan tutkittavan asian monitahoinen tarkastelu kokonaisvaltaisen kuvan saavuttamiseksi. Tiedonkeruussa kohdejoukko valitaan tutkimuksen kannalta tärkeiden ja olennaisten toimijoiden joukosta, eikä käytetä satunnaisotantaa. Laadullisen tutkimuksen metodit aineiston hankinnassa käyttävät hyödykseen inhimillistä havainnointia ja keskustelevaa otetta. Tutkittavien näkökulmia tarkastellaan osana kokonaisuutta ainutlaatuisina näkemyksinä ja uutta tietoa tuotetaan näiden pohjalta. Tiedonkeruumetodeja ovat esimerkiksi kirjallisuuskatsaukset, teemahaastattelut, havainnointi, ryhmähaastattelut ja erilaisten dokumenttilähteiden diskurssianalyysit. (Hirsjärvi ym. 2011, 155.)

Työn varhaisessa vaiheessa todettiin että opinnäytetyön kannalta on tärkeää pystyä tarkasti määrittelemään riskienhallinta ja laadunhallinta ISO-standardien mukaan, jotta niiden soveltaminen käytäntöön on mahdollista. Laadun- ja riskienhallinnan käsitteet pitävät sisällään niin moninaista sisältöä, että käytettyjen lähteiden rajaaminen ja kriittinen tarkastelu korostui opinnäytetyön tekemisessä ja kirjallisuuskatsauksessa. Samaa aihealuetta lähestytään

useiden kirjoittajien toimesta monelta eri kannalta, joten opinnäytetyön kannalta tärkeäksi teemaksi nousi kahden hallintajärjestelmän osan, riskien- ja laadunhallinnan yhtenäistäminen.

## 2.3 Kirjallisuuskatsaus

Opinnäytetyötä varten tehdyt kirjallisuuskatsaukset ovat tyypiltään narratiivista kuvailevaa yleiskatsausta. Kuvailevalla kirjallisuuskatsauksella pyritään saamaan mahdollisimman laaja kuva käsiteltävästä aiheesta ja perehtyä aihetta koskevaan ammattikirjallisuuteen. Kuvaileva kirjallisuuskatsaus valikoitui opinnäytetyön pääasialliseksi tutkimusmenetelmäksi juuri laaja-alaisuutensa vuoksi.

Tutkittava kenttä on laaja ja opinnäytetyön tavoitteena on luoda käyttökelpoista tietoa eri organisaatioille laadun- ja riskienhallintaan liittyen. Tietoa on tarjolla paljon, mutta se on hajanaista, eikä sovellettavuus käytäntöön ole aina teosten ydinteemana. Kirjallisuuskatsauksessa korostuu kriittisyys lähteitä kohtaan, sekä teosten keskinäinen vertailu. Kirjallisuuskatsaus ei ole tiivistelmä tai referaatti yhdestä tai useammasta teoksesta, vaan kirjallisuuskatsaus vaatii tutkijalta aineiston kriittistä analysointia ja tutkimuksellista otetta. Opinnäytetyön tekemisessä korostuikin aineiston ja lähteiden valinta siten, että ne parhaiten tukevat tutkittavaa aihealuetta. Tämä vaati useiden eri tietokantojen ja teosten kriittistä ja tarkkaa läpikäyntiä. (Salminen 2001, 3-6.)

Kirjallisuuskatsaukset voidaan jakaa kuvaileviin, systemaattisiin ja meta-analyyttisiin kirjallisuuskatsauksiin. Kuvaileva kirjallisuuskatsaus on itsenäinen tutkimusmetodi, jolla pystytään tuottamaan uutta tietoa, mutta myös etsimään lisäkysymyksiä esimerkiksi systemaattista kirjallisuuskatsausta tai muuta jatkotutkimusta varten. Kuvaileva kirjallisuuskatsaus tarjoaa myös hyvin laaja-alaisen kuvan käsiteltävästä aiheesta, kun taas esimerkiksi systemaattinen kirjallisuuskatsaus on rajatumpi ja keskittyy vain tiettyyn alueeseen olemassa olevasta tutkimustiedosta.

Suuri otos tuo mahdollisuuden saada hyvä yleiskuva aiheesta, mutta se asettaa vaatimuksia myös aineiston kriittiselle tarkastelulle. Näistä syistä kuvaileva kirjallisuuskatsaus sopii opinnäytetyön laajuudessa tehtävään tutkimustyöhön. Opinnäytetyössä tutkimme laadunhallintaa ja riskienhallintaa ilmiönä ISO-standardien näkökulmasta, joka pidettiin kirjallisuuskatsausta tehdessä johtoajatuksena. (Salminen 2001, 6-8.)

Kuvailevan kirjallisuuskatsauksen suuntauksiksi määritellään narratiiviset ja integroivat kirjallisuuskatsaukset. Narratiiviset kirjallisuuskatsaukset voidaan edelleen jakaa toimituksellisiin ja kommentoiviin kirjallisuuskatsauksiin, sekä yleiskatsauksiin. Yleiskatsaus on narratiivisista

kirjallisuuskatsauksista laajin. Narratiivisella kirjallisuuskatsauksella pyritään teorioiden yhtenäistämiseen ja tuottamaan helppolukuista tekstiä. Narratiivisen kirjallisuuskatsauksen luonne ei ensisijaisesti ole kriittinen, mutta siinä voi olla piirteitä integroivasta kirjallisuuskatsauksesta, joka nojautuu vahvemmin kriittisyyteen. Narratiivisella katsauksella ei pyritä tiukan analyyttiseen tulokseen vaan tuottamaan ajankohtaista, helposti sovellettavissa olevaa tietoa. Tästä syystä sitä on hyödynnetty paljon muun muassa opetuksen alalla ja se soveltuu hyvin oppimateriaalin tuottamiseen. Opinnäytetyön jatkotavoitteena onkin tuottaa oppikirjateos eri organisaatioiden käyttöön, joten narratiivinen kirjallisuuskatsaus soveltuu opinnäytetyön toteuttamiseen parhaiten. (Salminen 2001, 3-8.)

Opinnäytetyön teoriapohjan rakentaminen aloitettiin alustavalla kirjallisuuskatsauksella. Opiskelijat tutustuivat aihealueen ammattikirjallisuuteen, tutkimuksiin ja artikkeleihin kartoittamalla nykyistä tietoperustaa ja sen hyödynnettävyyttä opinnäytetyön toteuttamiseen. Työnjako opiskelijoiden välillä suoritettiin siten, että Karhunen tutustui laadunhallintaan sekä ISO 9001 standardiin ja Reinvall riskienhallintaan sekä ISO 31000 standardiin. Aiheesta on olemassa runsaasti kirjallisuutta, joten kirjallisuuskatsauksen yhtenä pääteemana oli löytää lähteet, jotka tukevat opinnäytetyön työelämälähtöistä näkökulmaa ja tavoitteita. Opinnäytetyön kannalta tärkeänä menetelmänä nähdäänkin juuri nykyiseen kirjallisuuteen, uusiin tutkimuksiin sekä standardeihin tarkasti perehtyminen, jotta tuotoksena syntyvää teosta voidaan käyttää asialähteenä organisaatioiden johtamisen kehittämisessä.

Teoriapohjan rakentamiseen kuuluu tärkeänä osana työn keskeisten käsitteiden määrittely. Tällä varmistetaan tutkimuksen yksiselitteinen ymmärtäminen ja mahdollistetaan usean kirjoittajan yhteistyön sujuvuus. Kirjallisuuskatsauksien tuotokset kuvataan kappaleessa 5.

## 2.4 Lähdeaineisto

Kun opinnäytetyöllä pyritään hyödyttämään eri organisaatioita mahdollisimman laaja-alaisesti, on resurssitehokasta tarkastella aiheeseen liittyvää ammattikirjallisuutta ja yhteistyökumppaneilta saatavia dokumentteja. Pelkillä haastatteluilla ei olisi ollut mahdollista tuottaa riittävää aineistoa opinnäytetyöhön varattavan rajallisen ajan puitteissa. Haastattelujen osalta koettiin ongelmallisuudeksi tuleva kilpailuasetelma tiettyjen asiantuntijaorganisaatioiden kanssa, sillä opinnäytetyön jatkosuunnitelmana oli alusta saakka kaupallisen julkaisun ja siihen liittyvien koulututusten laatiminen.

Kirjallisuuskatsauksissa käytettyjä tietokantoja olivat ABI/inform, EBSCO, FINLEX, Google Books, Google Scholar, Laurus ja Helmet. Tiedonhaun työkaluina käytettiin kunkin tietokannan omia hakukoneita. Verkkolähteitä etsittiin pääasiassa Google-hakukoneella. Tiedonhaun ensimmäisessä vaiheessa, alustavassa lukemisessa tuotettiin kirjoittajille kokonaiskuva laa-

dunhallinnan ja riskienhallinnan piirteistä sekä niiden seikkaperäisestä soveltamisesta. Tässä vaiheessa ei sivuutettu yleistajuistakaan aihepiirin kirjallisuutta, vaan käytettiin mahdollisimman laajaa otantaa tutkimuskysymysten ja rajauksen tarkentamiseksi.

Hakusanoina laadunhallinnan osalta käytettiin seuraavia: laadunhallinta, laadunhallintajärjestelmä, laadunhallinta AND prosessi, laatujärjestelmä, laatujohtaminen, ISO 9000, ISO 9001 AND risk, quality management AND history, quality management AND systems, quality management AND risk.

Riskienhallinnan osalta käytettiin hakutermejä riski, riskienhallinta, riskienhallintajärjestelmä, risk, risk AND management, risk AND management AND system. Lisäksi käytettiin näiden yhdistelmiä kuten risk AND quality AND management.

Löytyneestä aineistosta tarkastettiin sen ajanmukaisuus ja sidonnaisuus ISO 9001-standardiin, ja rajattiin kirjallisuuskatsauksen ulkopuolelle sellaista aineistoa jonka kytkös tutkimusongelmaan vaikutti heikolta tai olemattomalta. Vapaasti käytettävien ja lainattavien aineistojen lisäksi hankittiin Draft International Standard ISO/DIS 9001: Quality management systems — Requirements, jonka avulla voitiin varmistua oletettujen rakennemuutosten todellisuudesta ja vaikutuksista laadunhallintajärjestelmän prosesseihin.

## 2.5 Keskeiset käsitteet

Laatu:
Tuotteen jatkuva yhdenmukaisuus (engl: consistent confromance) asiakasvaatimuksiin (Slack, Chambers & Johnson 2010, 498).

Laadunhallinta:
Prosessit ja toimenpiteet, joilla varmistetaan tuotteen laadun jatkuvuus ja kyky täyttää organisaation, sidosryhmien ja asiakkaan sille asettamat vaatimukset (Slack, Chambers & Johnson 2010, 495).

Laadunhallintajärjestelmä:
Laadunhallintajärjestelmä (engl. Quality Management System) on ohjausjärjestelmä, jonka tehtävänä on varmistaa asiakaan tyytyväisyys toimitettuun tuotteeseen. Järjestelmälle ominaista on seuraamisen ja ohjaamisen kattavat toimintaprosessit sekä jatkuva parantaminen (Pesonen 2007, 50-51.)

Toimintaprosessi:

Organisaation suunnittelun ja ohjaamisen perusyksikkö. Toimintaprosessi alkaa suunnittelu- tai tuotekehitystyön syötteestä ja päättyy tuotoksen, valmiin tuotteen luovuttamiseen asiakkaalle. Asikas voi olla sisäinen tai ulkoinen. Prosessi on looginen, toistuva sarja määriteltyjä tehtäviä joita voidaan mitata ja joilla on selvä alku- ja päätepiste (Lecklin 2006, 123; Kvist, Arhomaa, Järvelin & Räikkönen 1995, 9.)

Riski:
Epävarmuuden vaikutus tavoitteisiin. Tapahtumien seurausten ja niiden todennäköisyyksien yhdistelmä. (ISO DIS 9001:2014; SFS-ISO 3100 2009, 12–16.)

Riskienhallinta:
Riskien ohjattua järjestelmällistä huomioimista organisaation johtamisessa (SFS-ISO 3100 2009, 12–16).

Riskin arviointi:
Riskin tunnistamisesta, riskianalyysistä ja riskin merkityksen arvioinnista koostuva prosessi (SFS-ISO 3100 2009, 12-16).

Riskiperustainen lähestymistapa:
Riskit tunnistetaan, arvioidaan ja huomioidaan kaikissa laadunhallintajärjestelmän soveltamisalan mukaisissa prosesseissa aina strategisesta suunnittelusta toimintaprosesseihin ja katselmuksiin (IAF 2014).

Kokonaisvaltainen riskienhallinta:
Riskejä hallitaan kokonaisuutena ja riskienhallinnan prosessit ovat kytkettyjä organisaation muihin toimintoihin. Riskienhallinta on jatkuvaa sekä osa strategiaa ja johtamista. (Pöyry 2008.)

Tuote:
Pesosen (2007, 11) mukaan tuotteella tarkoitetaan prosessin aikaansaannosta; palvelutuotetta, käsinkosketeltavaa tavaraa tai kokonaisuutta jonka tuottamiseen organisaatio tähtää.

# 3 Laadunhallinta organisaatiossa ISO 9001-standardin mukaisesti

ISO 9000-standardisarja on tarkoitettu kaikentyyppisille ja kaikenkokoisille organisaatioille laadunhallintajärjestelmän toteuttamiseen. Standardisarja koostuu neljästä standardista, jotka muodostavat johdonmukaisen laadunhallintajärjestelmästandardien kokonaisuuden. (SFS 2001,8.) ISO 9000-sarja on koko lähes kolmikymmenvuotisen historiansa ajan ollut ISO-standardiperheen suosituin standardi, ja vuonna 2013 ISO 9001:2008 sertifikaatin sai globaalisti 1 129 446 organisaatiota. Luvussa on kolmen prosenttiyksikön kasvu vuoden 2012 tasoon. (Croft 2012; ISO 2015.) Tämän kappaleen keskiössä on ISO 9001-standardi, joka määrittää vaatimukset laadunhallintajärjestelmälle.

Aiheesta tekee ajankohtaisen oletettavasti syyskuussa 2015 julkaistava ISO 9001:2015-revisio, joka tulee sisältämään velvoittavia vaatimuksia riskienhallinnan ulottamisesta laatujärjestelmään (ISO/DIS 9001:2014, 9, 45). ISO 9001:2008-sertifikaatit vanhentuvat kolmen vuoden kuluttua uuden revision lanseerauksesta, eikä sen voimassaoloaikana enää myönnetä ISO 9001:2008:n mukaisia sertifikaatteja (IAF 2015). Croft (2012) odottaa uudistettujen laadunhallintajärjestelmien vaatimusten luovan vakaan pohjan vähintään kymmeneksi vuodeksi ja vastaavan laadunhallintajärjestelmien muutospaineisiin ja tekniseen kehitykseen kuluneen 15 vuoden ajalta.

Standardin edelliset versiot ovat julkaistu 1987, 1994, 2000 ja 2008, joista vuoden 2000-versiota voidaan pitää merkittävänä uudistuksena (Croft 2012). Julkaisuista on vastannut ja vastaa tekninen komitea ISO/TC 176/SC2. Tätä työtä kirjoittaessa päivittyvä standardi on Draft International Standard-vaiheessa, ja siihen viitataan muodossa ISO/DIS 9001:2014. On otettava huomioon, että lopullinen julkaisu voi vielä sisältää muutoksia tämän työn lähteenä käytettyyn versioon.

## 3.1 Laadunhallinnan taustaa

1920-luvulta aina 1940-luvun loppuun tuotteen laadusta varmistuttiin laadunvalvonnalla. Toisin sanoen valmiita tuotteita tarkastettiin tuotantolinjan lopussa, ja kelpaamattomat poistettiin joukosta (BSI Education 2008). Laadunhallinnan kehitys eteni Euroopassa pääosin atlantillisen puolustusyhteistyön kautta (Martincic 1997; Vanguard 2012). Yhdysvaltojen ja Englannin sotateollisuuden asiakasnäkökulma oli hyvin kvantitatatiivinen; loppukäyttäjän näkökulmasta laatuvaatimukset täyttävien tuotteiden määrällinen saatavuus oli täysin ensisijaista. Laadunvalvontatyökaluina käytettiin tilastollisia meneltelmiä, joista tunnetuimpana mainitaan Shewartin 1924 esittelemät ohjauskaaviot (engl. control chart) joita myös kehittäjänsä mukaan Shewartin kaavioiksi kutsutaan (Chandra 2001, 1). Iso-Britanniassa hallituksen sotataloustuotannosta vastaavat osastot alkoivat auditoimaan toimittajiaan varmistuakseen tuotannon oi-

keista toimintavoista. Sotateollisuuden tarpeena oli yhtenäistää tuotantolaitosten laaduntuontantokykyä ja varmistaa eri tuotantoketjuista saatavien tuotteiden yhteensopivuus. Sodan jälkeen monet siviilisektorin toimijat olivat omaksuneet auditointien toimintamalleja ja varsinkin autoteollisuuden piirissä siitä tuli tavanomaista. Tilanne alkoi saada kaoottisia piirteitä, kun useat asiakkaat auditoivat tuotantolaitoksien laatujärjestelmiä kukin omien spesifikaatioidensa mukaisesti (Knowles 2011, 39.)

Toisen maailmansodan jälkeen 1940-luvun lopussa teollisuuttaan jälleenrakentavan Japanin tiede- ja teollisuusyhteisö oli vaikuttunut maassa väestönlaskentaan liittyvissä tehtävissä toimineen ja myöhemmin maailmanmaineeseen kohonneen William Edwards Demingin työstä. Deming kutsuttiin vuonna 1950 luennoimaan Japanin teollisuusväelle tilastollisesta prosessinohjauksesta. (Sallis 2002, 7.) Deming kehotti tukalassa tilanteessa olevia kuulijoitaan kehittämään tuotantomenetelmät ja tuotteet korkeimmalle mahdolliselle tasolle asiakasvaatimuksiin vastaamiseksi. Myöhemmin edelleen Sallisin mukaan (2002,7-8) Japanissa Demingin, Juranin ja muiden yhdysvaltalaisiasiantuntijoiden neuvot otettiin vakavasti ja niistä kehittyi myöhemmin Total Quality Control, jonka avulla Japani nousi 1970–80-luvuilla johtavaksi maaksi autoteollisuuden, elektroniikan ja kestotuotteiden saralla. Sallis (2002, 8) kuvaa tätä kaiken paljolti ”kaiken ohittavan laadusta huolehtimisen” ansioksi, kun Silén (1998, 70) puolestaan tarkastelee japanilaisten menestystä pitkäjänteisen laatukulttuurin hedelmänä, jonka avulla ylimääräiset laatukustannukset on pystytty pudottamaan vain muutamaan prosenttiin liikevaihdosta. Total Quality Control tunnetaan länsimaissa nykyään nimellä TQM, Total Quality Managemen (Silén 1998, 38).

ISO 9000-standardiperhe juontaa juurensa brittiläisiin BS 9000 (julk. 1971), BS 4891 (1972) BS 5179 (1974) ja BS 5750 (1979–1981)-standardeihin (Knowles 2011, 38–39). Näistä viimeksimainittu oli paitsi ensimmäinen ohjaava, myös velvoittava ja sen ensimmäinen osa hyväksyttiin 1987 kansainväliseksi standardiksi ISO 9001:1987, jota Owen & Maidmentin (1996) mukaan historiallisesti kehnosta laadustaan tunnetut britit saattoivat pitää suurena saavutuksena. 1970-luvulla puhuttin yleisesti laadunvarmistuksesta (engl. quality assurance), ja standardit olivat lähtökohtaisesti tarkoitettu teollisen tuotannon laadun ohjaukseen (BSI Education 2008). Menettelyssä ei asiakkaalle näkyviltä osin ole mitään vikaa: toimitettavat tuotteet ovat sitä mitä on luvattu. Tämän tyyppinen laadunvalvonta voi nykyäänkin olla täysin perusteltu ja tehokas osa laadunhallintaa, ja sitä toteutetaankin automatisoidusti esimerkiksi mikropiiriteollisuudessa.

Palveluliiketoimintaan kuvatun kaltainen laadunhallinnan järjestely ei kuitenkaan sellaisenaan sovi, eikä se kuvaa nykyaikaista laatuajattelua, jossa laatunäkökulman tulisi olla läsnä kaikessa päätöksenteossa. Asiakasrajapinnassa tapahtuvaa toimitusta, palveluprosessia, ei voi vetää takaisin tai keskeyttää ilman negatiivistia vaikutusta asiakastyytyväisyyteen (Pesonen 2007,

34). Silén (1998, 38) toteaakin, ettei laatua voi luoda vain noukkimalla viallisia tuotteita pois, vaan laatu on rakennettava sisään tuotantoprosesseihin ja ennaltaehkäistä virheet. Palveluliiketoiminnassa laatuvirheet asiakasrajapinnassa ovat armottomia, kun taas tuotannollisessa toiminnassa pystytään suuremmalla todennäköisyydellä korjaamaan virheitä ennen asiakaskontaktia, vaikka laatua johdettaisiinkin huonosti tai ei ollenkaan.

## 3.2 Laadunhallintajärjestelmän hyödyt ja kritiikki

Laadunhallintajärjestelmän perimmäinen tarkoitus on varmistaa halutunlaisen lopputuotteen saatavuus. Tuotteen tai palvelun laatu kuvaa asiakkaalle konkreettisesti organisaation toimintaa ja suhteessa sille asetettuihin odotuksiin se on tärkein yksittäinen tekijä asiakastyytyväisyydelle tai tyytymättömyydelle. Laatu tai sen heikkous kuvaa asiakkaalle koko organisaation toimintaa. (Slack ym. 2010, 40.) Knowles (2011, 39) viittaa Sharman (2005), Herasin ym. (2002), Marcusin (2007) tutkimuksiin joiden mukaan ISO 9001-sertifiointi on korreloinut kohdeorganisaatioiden liiketoiminnan kehittymisen kanssa ja joissain tapauksissa ollut yhteydessä sen parantuneeseen kannattavuuteen.

Knowles (2011, 39) sekä Slack ym. (2010, 497) esittelevät Gummersoniin (1993) viitaten väittämiä, joilla laadunhallinnan tärkeyttä voidaan edelleen perustella. Laadunhallinta parantaa kannattavuutta, sillä ”kerralla oikein” tuottava prosessi vähentää kustannuksia ja lisää tuottavuutta. Laadunhallinta lisää luotettavuutta sillä tuotetut tuotteet ja palvelut ovat tasalaatuisia ja kun prosessin suorituskykyä eli sen laadun tuotantokykyä mitataan, sen kapasiteettiä voidaan ennustaa luotettavasti. Laatu myy ja kohentaa organisaation imagoa sekä vähentää painetta hintakilpailulle tai mahdollistaa sen paremmalla marginaalilla. Lisäksi laadunhallintajärjestelmä voi olla edellytys sidosryhmien, uusien asiakkuuksien tai kilpailutusten näkökulmasta.

Laadunhallintajärjestelmiä käsitellessä on syytä huomioida, että ISO 9001 ei ole ainoa tai aina väistämättä paras ja organisaatiolle sopivin laadunhallinnan toimintamalli. Laadunhallintajärjestelmän toteutustavan ja valinta on johdettava organisaation laadunhallinnalle asettamista tavoitteista. Jos tavoitteena on ISO 9001-sertifikaatti, ovat vaihtoehdot luonnollisesti vähissä.

ISO 9000-standardiperhe on laajasta hyväksynnästään ja käyttäjäpohjastaan huolimatta edelleen altis kritiikille. Jatkuvan standardien ja menettelyohjeiden käytön katsotaan kannustavan ”säännöillä johtamiseen” (engl. management by manual) ja toiminnan kuvaamisen, toimitaohjeiden, koulutusten, sisäisten tarkastusten sekä sertifioinnin suorittaminen olevan aikaa vievää ja kallista. Myös standardin kaavamaisuutta moititaan ja sen väitetään kannustavan ohjaamaan toimintaa pois luovempien johtamistapojen suunnasta (Slack ym. 2010, 514). Ei kuitenkaan ole selvää voidaanko näitä heikkouksia sälyttää yksinomaan ISO 9001:n syyksi.

Jos laadunhallintajärjestelmä ja laatujohtaminen ovat kulkeneet organisaatiossa eri polkuja, kuten Silén (1998) kuvaa vielä 1990-luvulla tavalliseksi, on sillä voinut olla negatiivisia vaikutuksia organisaation laaduntuottokyvyn ja toimintaprosessien kehitykseen. On pidettävä mielessä että organisaatio itse vastaa laatutavoitteidensa määrittelystä ja toimintatavoistaan. Tälläiset lopputulokset sotivat jo itsessään koko ISO 9000-standardiperheen ydinajatusta, jatkuvan parantamisen mallia vastaan. Jos laadunhallintajärjestelmä on toteutettu niin, että se ei tuota tietoa analysoitavaksi tai analysoitu tieto ei johda toimenpiteisiin, se ei myöskään voi auttaa organisaatiota minkäänlaisiin perusteltuihin johtopäätöksiin laadun tilasta. Laadunhallintajärjestelmä ei voi olla itsetarkoitus, vaan työkalu laadun hallitsemiseen (Pesonen 2007, 38, 53).

Hyvin johdetussa organisaatiossa laadunhallintaa ei käytetä irrallisena toimintona, vaan se on oleellinen osa organisaation toimintaa ja se huomioidaan systemaattisesti kaikessa päätöksenteossa. Tätä periaatetta ISO 9000-standardiperheen ennakoitiin seuraavissa sukupolvissaan painottavan ja näin myös kävi. (Silén 1998.) Syventymättä enempää kolmanteen ja neljänteen standardisukupolveen, ISO 9001:2015 sisältää edeltäjäänsä vähemmän ennalta määrättyjä vaatimuksia, vähentää dokumentaation painotusta ja korostaa toimintaympäristön, kokonaisvaltaisen riskienhallinnan ja asiakastyytyväisyyden näkökulmia (IAF 2015, 5).

ISO 9001 on Croftin (2012) mukaan usein organisaation ensimmäinen formaali hallintajärjestelmä. Sen katsotaan tuovan lisäarvoa sekä organisaatiolle ohjaamalla yksityiskohtaisesti hallintajärjestelmän suunnittelua sekä asiakkaille jotka saavat nauttia laatutyön hedelmistä (Slack ym. 2010, 514). Jos organisaatio ei koe tarpeelliseksi tai sidosryhmiltä ei siihen kohdistu painetta, ISO 9001 mukainen laadunhallintajärjestelmä voidaan varsin hyvin toteuttaa myös ilman kolmannen osapuolen sertifiointia. Se voidaan nähdä myös etappina matkalla Total Quality Managementiin (Knowles 2011, 39), jonka perusfilosofiaa Silén (1998, 24) katsoo ISO 9000-standardiperheen funktionaalisesti tulkitsevan.

ISO 9001 ei ota kantaa tuotteille asetettuihin laatuvaatimuksiin, vaan luo perustan organisaation laaduntuotantokyvylle ja mahdollistaa laadun johtamisen. Se ei ole autuaaksi tekevä tekevä järjestelmä jonka muodollisella toteutuksella organisaation laatuongelmat on hallittu ja ratkaistu, vaan johtamisjärjestelmä jonka avulla organisaatio voi ohjata toimintaprosessinsa sellaiseen järjestykseen, että laatuvaatimuksia ja tavoitteita on paitsi mahdollista asettaa, myös mahdollista saavuttaa ja nostaa.

## 3.3 Laadunhallintajärjestelmän toteuttaminen

Laadunhallintajärjestelmä on johtamisjärjestelmä, eli järjestelmä jonka avulla organisaatio ohjaa toimintaansa siten että asiakkaan tarpeet tuotteen tai palvelun osalta täytetään. Sen ensisijainen tehtävä on tuottaa tietoa asianomaisille henkilöille päätöksenteon tueksi, ja ohjata organisaatio jatkuvaan parantamiseen (Pesonen 2007, 50.) Laadunhallintajärjestelmän toteuttamisen tulee aina olla organisaation strateginen päätös, ja sen suunnitteluun ja jalkauttamiseen vaikuttavat organisaation toimintaympäristö ja sen muutokset. Järjestelmän suunnittelussa tulee huomioida: ennalta määritellyt tavoitteet, toimintaympäristöön ja tavoitteisiin kohdistuvat riskit, sidosryhmien tarpeet ja odotukset, tuotettavat palvelut ja tuotteet, organisaation prosessien monimutkaisuus ja niiden vuorovaikutus, työntekijöiden pätevyydet sekä organisaation rakenne ja koko (ISO/DIS 9001:2014, 6.)

Laadunhallintajärjestelmän tavoitteiden tulee johtua organisaation strategiasta (Slack ym. 2010, 495). Pesonen (2007, 62) saattaa strategian käsitettä enemmän laatuajattelun suuntaan toteamalla sen pelkistyvän kahteen pääkysymykseen: ”mitä tuotteita” ja ”kenelle”.

Laatupolitiikka on laadunhallintajärjestelmälle suuntaa osoittava dokumentti joka ilmaisee organisaation strategiset tavoitteet ja sen miten laadunhallintajärjestelmä ponnistelee tavoitteiden täyttämiseksi. Laatupolitiikassa konkreettiset laatutavoitteet ilmaistaan laadituiksi. Laatupolitiikka kertoo organisaatiolle ja sidosryhmille ”mihin pyritään”, laatutavoitteet kertovat organisaatiolle ”miten toimitaan” ja millaiset laatuvaatimukset tuotteelle asetetaan. Usein prosessien vuorovaikutussuhteiden selvittämiseksi on hyödyllistä laatia prosessikartta jo varsin aikaisessa vaiheessa. Tästä voi olla apua myös laadunhallintajärjestelmän rajauksesta päätettäessä.

Laadunhallintajärjestelmän rakenteen Pesonen (2007) jaottelee kolmeen osaan: toiminnan kuvauksiin, varsinaiseen toimintaan, ja toiminnan näyttöihin. Toiminnan kuvaus tarkoittaa organisaation prosessien tarkastelua ja suunnittelua siten, että niistä kyetään tunnistamaan lopputuloksen ja toimivuuden kannalta oleelliset seikat. Toiminnan kuvauksen tarkkuuteen vaikuttavat ISO/DIS 9001:2014 mukaan jo mainitut muuttujat eli ennalta määritellyt tavoitteet, toimintaympäristöön ja tavoitteisiin kohdistuvat riskit, sidosryhmien tarpeet ja odotukset, tuotettavat palvelut ja tuoteet, organisaation prosessien monimutkaisuus ja niiden vuorovaikutus, työntekijöiden pätevyydet sekä organisaation rakenne ja koko.

Dokumenttia joka sisältää hallintajärjestelmän toiminnan kuvaukset kutsutaan useimmiten laatukäsikirjaksi. Laatukäsikirjan ei ole syytä olla sertifioinnin dokumentaatiovaatimusten mukainen asiakirjanippu, vaan organisaation omista lähdökohdista, omilla termeillä ja omiin tavoitteisiin sidottu käsikirja, joka ilmentää asioden hoitamisesta suhteessa ISO 9001:2015 vaatimuksiin. Laatukäsikirja ei esiinny enää ISO 9001:2015 käsitteissä tai tekstissä, mutta laadunhallintajärjestelmä on siitä huolimatta kuvattava. On pidettävä mielessä, että ISO 9001

vaatii dokumentoidun laadunhallintajärjestelmän, ei dokumenttijärjestelmää (ISO 2008). Dokumentaation tuottamisen ei tulle olla toiminnan päämäärä, vaan tuottaa lisäarvoa (ISO 2001, 16).

Pesonen (2007, 55) esittää toiminnan kuvauksille esimerkinomaisen sadan asian mallin. Näistä asioista 10 on välttämättömiä prosessille ja 10 sellaista, joita ei saa tai voi tapahtua. Loput 80 uskotaan tekijöiden harkinnan, luovuuden ja osaamisen varaan. Jaottelu on toki aina tapauskohtaista mutta ydinajatus on, että turhaa kuvantamista ja kaavaan pakottamista vältetään. ISO 9001:2015-viitekehyksessä asia entisestään korostuu, sillä juuri tämä on työvaihe jossa riskienhallintaprosessi integroituu laadunhallintajärjestelmään yksittäisten prosessien tasolle (ISO/DIS 9001:2014). Prosesseja kuvatessa on syytä pitää mielessä kenelle niitä laaditaan, ja miksi. Varsinainen toiminta on prosessien toteutusta organisaatiossa annettujen toimintamallien ja työtapojen mukaisesti (Pesonen 2007, 53).

Toiminnan vaiheessa prosessi suorittaa sille määrättyä tehtävää tuottaen konkreettisen esineen, palvelutuotteen tai minkä tahansa mitattavissa olevan konkreettisen tuotoksen. Toiminta alkaa syötteen sisääntulosta, ja sen tuloksena on tuotos (ISO/DIS 9001:2014, 20). Toiminta suoritetaan sille laaditun kuvauksen mukaisesti. Toimintaprosesseihin on sisällytettävä niiden seuranta ja ohjaus (ISO/DIS 9001:2014, 33).

Toiminnan näytöt muodostuvat paitsi laadunhallintajärjestelmän ja prosessien kuvauksista, myös toimintaprosesseista jäävistä tallenteista (Pesonen 2007, 54). Näiden perusteella organisaatio voi näyttää toteen, että toiminta on kuvausten mukaista ja sitä seurataan. Nämä dokumentoidut tiedot muodostavat myös pohjan toiminnan analysoinnille ja arvioinnille (ISO/DIS 9001:2014). ISO 9001:2015 -revisiossa ei enää puhuta tallenteista tai dokumentoiduista menettelytavoista; kaikkea jäsenneltyä tietoa kutsutaan dokumentoiduksi tiedoksi (engl. documented information) (ISO/DIS 9001:2014, 46).

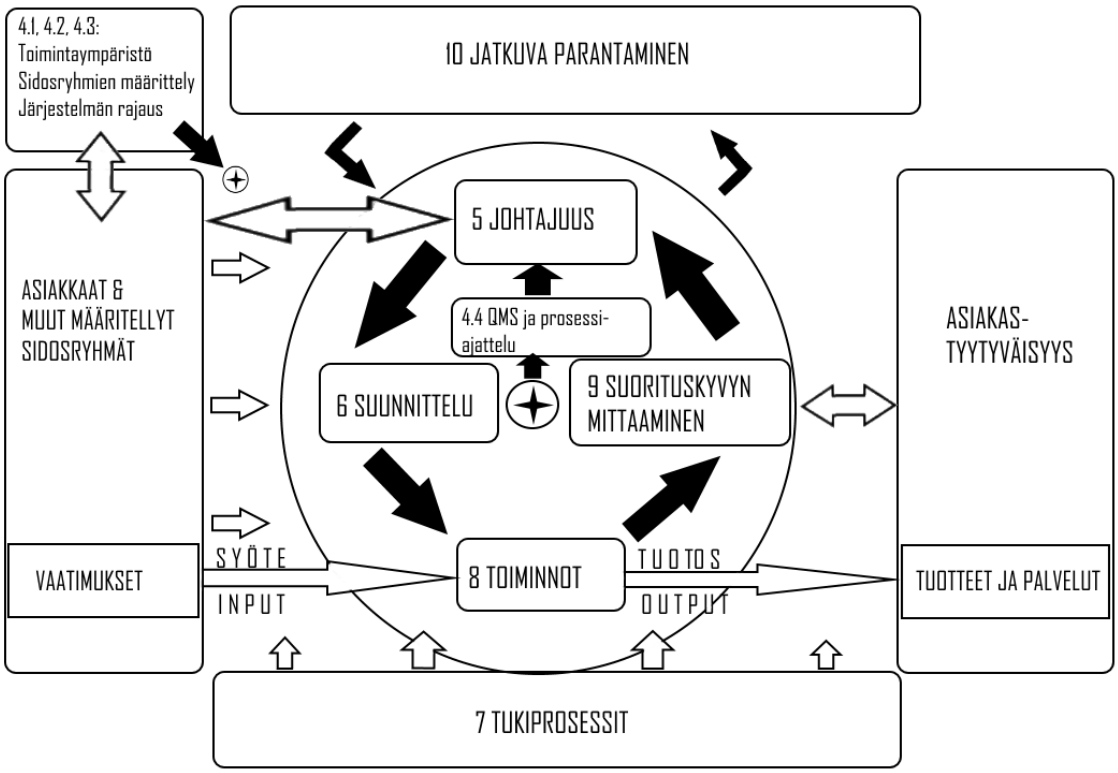
Yksi keskeisistä ISO 9001:n vaatimuksista on jatkuva parantaminen. Organisaation on määritettävä ja valittava kehittymismahdollisuutensa ja ryhdyttävä tarvittaviin toimenpiteisiin niiden edistämiseksi asiakasvaatimuksiin vastaamiseksi ja asiakastyytyväisyyden parantamiseksi. Parantamisprosessin tulee tähdätä laatupoikkeamien ennaltaehkäisyyn ja kykyyn vastata tunnettuihin ja ennakoituihin laatuvaatimuksiin (ISO/DIS 9001:2014, 42.) Parantamisen tulee olla organisaatiolle pysyvä tavoite, johon päästään jatkuvilla pienillä parannuksilla ja ajoittaisilla isoilla harppauksilla (Pesonen 2007, 80).

Yksinkertaistettununa jatkuvan parantamisen mallia voi kuvata seuraavalla tavalla. Jos tuotetussa laadussa ei ole parantamisen varaa tai tarvetta parempaan ole, voi organisaatio pohtia onko tuotannon tehostaminen ja kannattavuuden parantaminen mahdollista. Organisaatio ei

kuvittele koskaan olevansa valmis, vaan säilyttää kyvyn tunnistaa ja reagoida asiakasvaatimuksiin, parhaimmillaan jo ennen kuin asiakkaat itsekään tietävät tarpeensa.

## 3.4 Laadunhallinnan prosessi

ISO 9001:2015 mukainen laadunhallinta perustuu prosessiajatteluun, kuten edeltäjänsä versiosta ISO 9001:2000 lähtien. Prosessimallin tärkeimpinä hyötyinä pidetään alentuneita kustannuksia tehostuneen resurssien käytön sekä lyhentyvien läpimenoaikojen seurauksena, sekä edelleen parantuneita, konsistenttejä ja ennustettavia tuloksia (ISO 2012.) Tässä kappaleessa käsitellään ISO/DIS 9001:2015 mukaista laadunhallintaprosessia kokonaisuutena ja jäljempänä yksittäisenä toimintaprosessina. ISO 9001:2015 laadunhallintajärjestelmää kuvataan kokonaisuudessaan Kuvion 1 prosessikartalla.

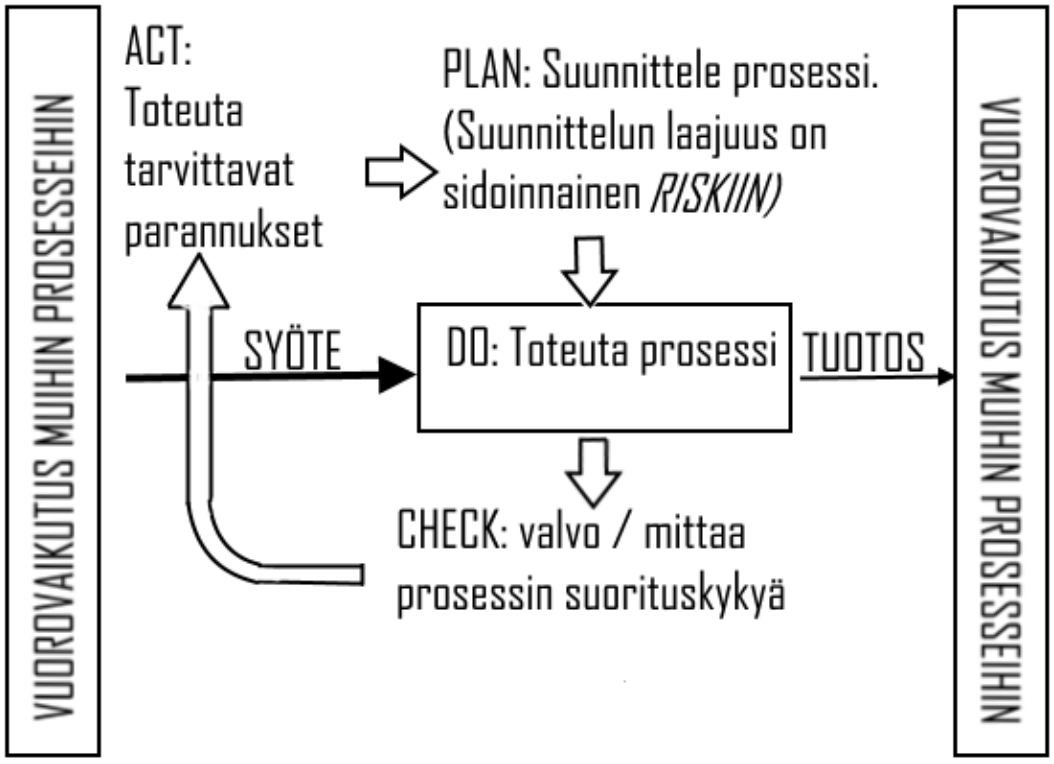



Kuvio 1. Laadunhallintajärjestelmän prosessikartta ISO/DIS 9001:2014:ää mukaillen.

Laadunhallintaprosessi pitää sisällään sekä horisontaalisia että vertikaalisia prosesseja. Horisontaalisille prosesseille ominaista on pyrkimys muuttaa organisaation osaaminen lisäarvoksi asiakkaalle, kun taas vertikaalisilla prosesseilla kuvataan organisaation johtamista (Kvist, Arhomaa, Järvelin & Räikkönen 1995, 11–12). Kuvion vasen pystypalkki kuvaa asiakkaita, sidosryhmiä ja heidän vaatimuksiaan. Näihin vuorovaikuttaa toimintaympäristö, sidosryhmien tunnistaminen ja laadunhallintajärjestelmän rajaus.

Syötteet (INPUT) asiakas- ja sidosryhmävaatimusten rajapinnasta ohjataan organisaation toimintaan prosesseina, joiden tuotteina (OUTPUT) ovat valmiit tuotteet ja palvelut sekä edelleen asiakastyytyväisyys. Toiminnan keskiössä on Demingin mallin mukainen Plan-Do-Check-Act-(jäljempänä PDCA) -silmukka, johon vuorovaikuttavat jo mainittujen lisäksi jatkuvan parantamisen, tukitoimintojen ja asiakastyytyväisyyden prosessit (ISO/DIS 9001:2014; Pesonen 2007). Numerointi komponenttien otsikoissa viittaa ISO/DIS 9001:2014 otsikoihin.

Kuviossa 2 on avattuna yksittäinen toimintaprosessi. Sen syötteenä ja tuotteena on vuorovaikutus muihin organisaation prosesseihin, olivatpa ne mitä hyvänsä. PDCA-mallin mukainen prosessi alkaa suunnittelusta, ja tässä ISO 9001:2015 ottaa ensimmäistä kertaa kantaa riskiin, ja toteaa suunnittelun laajuuden riippuvan prosessiin liittyvistä riskeistä. Käytännössä tämän prosessimallin mukainen toiminta edellyttää organisaatoilta riskien tunnistamista ja arviointia jokaisessa laadunhallintajärjestelmän soveltamisalan mukaisessa prosessissa.




Kuvio 2. Toimintaprosessi ISO/DIS 9001:2014:ää mukaillen.

DO-vaiheessa organisaatio toteuttaa suunnitelman mukaista toimintaa, CHECK-vaiheen valvoessa ja mitatessa prosessin tehokkuutta. Mittaamisesta on jäätävä tallenne, dokumentti (ISO/DIS 9001:2014, 40), jonka sisältämä tieto mahdollistaa prosessin suorituskyvyn arvionnin ja sen ohjaamisen. Mitä ei tunnisteta, ei voida mitata ja mitä ei mitata, ei voida faktaan perustuen johtaa. ACT-vaiheessa analysoidun tiedon (jota saadaan myös muiden vuorovaikutta-

vien prosessien kautta) perusteella tehdään johtopäätökset ja mahdolliset muutokset prosessin suunnitteluun, PLAN-vaiheeseen.

# 4 Riskienhallinta organisaatiossa ISO 31000-standardin mukaisesti

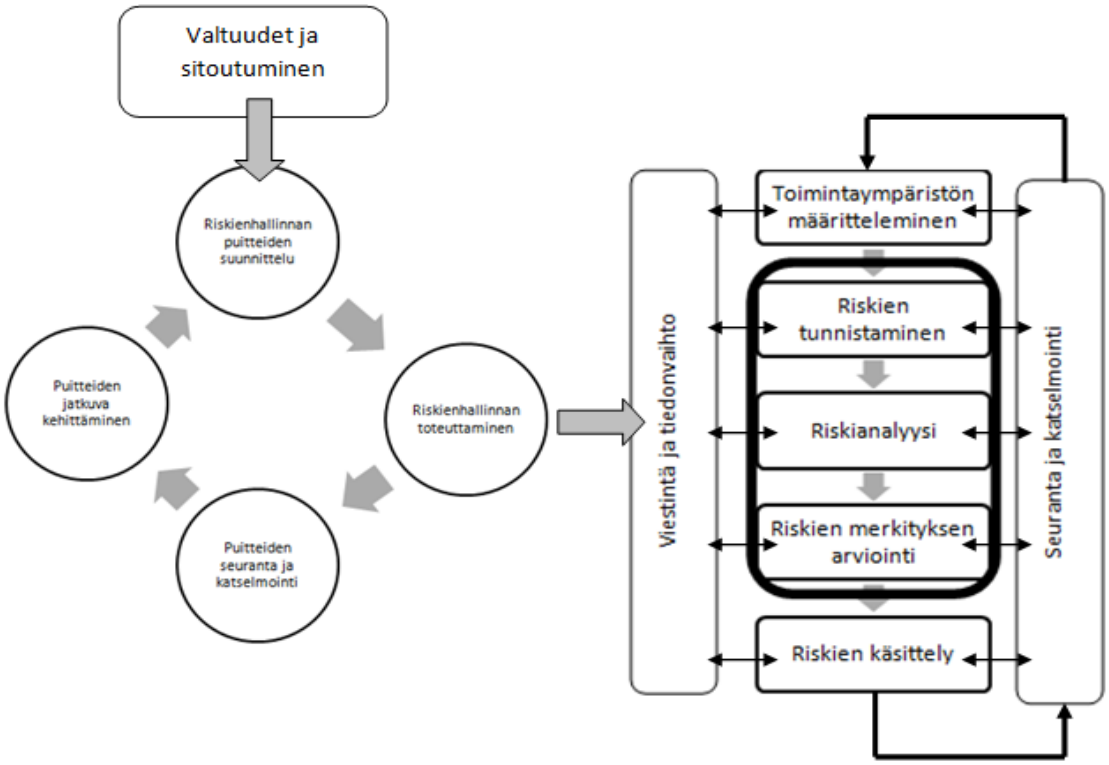
SFS-ISO 31000-standardi käsittelee julkisten ja yksityisten yritysten, järjestöjen, ryhmien ja yksittäisten henkilöiden riskienhallinnan periaatteita ja soveltamisohjeita. Organisaatioiden tarpeet ja tavoitteet riskienhallinnan suhteen vaihtelevat toiminnan erityispiirteiden mukaisesti joten standardilla ei pyritä yhtenäistämään eri organisaatioiden riskienhallintajärjestelmiä, vaan yhtenäistämään käytäntöjä organisaation sisällä ja eri standardien välillä. Moeller mukailee teoksessaan standardissa esitettyä väitettä, että ISO 31000 standardi ei rajoitu tiettyyn teollisuudenalaan tai sektoriin, vaan sitä voidaan soveltaa kaikkien organisaatioiden riskienhallinnan tarpeisiin eri toiminnoissa organisaation koko elinkaaren aikana. Riskienhallintaa hyödyntäviä toimintoja ja osa-alueita voivat olla esimerkiksi strategia ja päätöksenteko, toimenpiteet, prosessit, projektit, tuotteet, palvelut sekä yrityksen voimavarojen hallinta. (Moeller 2011, 331–334; SFS-ISO 31000:2009, 4-12.)

Riski määritellään SFS-ISO 31000:n mukaan epävarmuuden vaikutuksina tavoitteisiin. Vaikutukset eivät rajaudu koskemaan ainoastaan yrityksen kannalta negatiivisia tai haitallisia seurauksia, vaan myös positiivisia tuloksia. Tästä seuraa, että riskien hallintaan voidaan liittää niin uhkien kuin mahdollisuuksienkin tarkastelua. (SFS-ISO 31000:2009, 12.) The Institute of Risk Management, IRM, määrittelee riskin tapahtumien todennäköisyyksien ja niiden seurausten yhdistelmänä. Myös IRM:n määritelmässä seuraukset voivat olla tarkasteltavan kohteen kannalta positiivisia tai negatiivisia. Tämä määritelmä on tunnistettu myös SFS-ISO 31000-standardissa. (Hopkin, P. 2012,13–15.)

Riskienhallinta määritellään SFS-ISO 31000 standardissa koordinoituna toimintana, jolla organisaatiota johdetaan ja ohjataan riskien osalta (SFS-ISO 31000:2009, 12). Roper taas määrittelee riskienhallinnan prosessiksi, jossa valitaan ja otetaan käyttöön vastatoimia, joilla riski saadaan hyväksyttävälle tasolle hyväksyttävillä kustannuksilla (1999, 13). Riskejä voidaan hallita erilaisin keinoin. Muun muassa Kuusela ja Ollikainen esittävät riskienhallinnan teoreettisiksi keinoiksi riskialttiin toiminnan välttämisen, riskin ottamisen, riskin hyväksymisen, suojautumisen riskiltä ja vahinkojen rajoittamisen sekä riskin siirtämisen muualle (2005, 15–16).

Standardi noudattaa Demingin mallia, jossa suunnittelun, toteuttamisen, seurannan ja katselmoinnin, sekä toimenpiteiden kehittämisen vaiheet vuorottelevat ja täydentävät toisiaan luoden jatkuvan kehittämisen prosessin (Kuvio 3) (Sousa, De Almeida & Dias 2012, 263). Laajasti hyödynnetty Demingin malli ilmenee muun muassa riskienhallinnan puitteiden ja riskienhallinnan toteuttamisen prosesseissa. Riskienhallinnan puitteiden osalta puitteiden suunnitte-

lu, riskienhallinnan toteuttaminen, puitteiden seuranta ja katselmointi, sekä puitteiden jatkuva kehittäminen muodostavat erillisen prosessin, joka kehittää organisaation riskienhallintaa ja auttaa kohdentamaan siihen määrättäviä resursseja. Johdon sitoutuminen riskienhallintaan edesauttaa riskienhallinnan tehokasta toteuttamista ja on edellytys sen vaikuttavuudelle. Riskienhallinnan tulee aina tuoda yritykselle lisäarvoa ja tukea koko organisaation jatkuvaa kehittämistä. Riskienhallinta organisaatiossa ei suinkaan ole erillinen saareke vaan se tulee integroida organisaation prosesseihin ja johtamisjärjestelmään järjestelmällisenä ja tarkasti koordinoituna osana. (SFS-ISO 31000:2009, 10.)




Kuvio 3. Riskienhallinnan puitteet ja riskienhallintaprosessi (SFS-ISO 31000:2009, 10.)

ISO 31000:2009 mukaisen riskienhallintajärjestelmän prosessi alkaa riskienhallintatoimenpiteiden valtuuttamisella ja sitoutumisella riskienhallinnan periaatteisiin, jonka jälkeen aloitetaan riskienhallinnan puitteiden suunnittelu. Riskienhallinnan toteuttaminen on prosessi riskienhallinnan puitteiden prosessin sisällä ja seuraa järjestyksessä riskienhallinnan puitteiden suunnittelua. Riskienhallinnan toteuttamisen prosessiin kuuluu toimintaympäristön määritteleminen, riskien tunnistaminen, riskianalyysi, riskien merkityksen arviointi, sekä riskien käsittely. Seurantaa ja katselmointia, sekä viestintää ja tiedonantoa sovelletaan jokaisessa riskienhallinnan toteuttamisen prosessin vaiheessa. Myös riskien arvioinnin tuloksia kokonaisuudessaan katselmoidaan, toimintaympäristöä määritellään tulosten mukaan tarvittaessa uudelleen ja prosessia jatketaan kuvion 3 esittämällä tavalla. Riskienhallinnan toteuttamisen pro-

sessin jälkeen puitteita seurataan ja katselmoidaan sekä kehitetään. (SFS-ISO 31000:2009, 10.)

## 4.1 Riskienhallinnan puitteet

SFS-ISO 31000-standardin mukaisen riskienhallintaprosessin ensimmäinen vaihe on riskienhallinnan puitteiden määrittely. Riskienhallinnan puitteiden kannalta on ensisijaisen tärkeää selvittää riskienhallinnan tavoitteet. Lisäksi tulee arvioida, minkälaisia riskienhallinnan toimenpiteitä organisaation prosesseissa tulisi soveltaa ja minkä vuoksi. Hopkin (2009, 81) viittaa teoksessaan australialaiseen AS 4360-standardiin, jossa puitteiden määrittelyyn käytetään kolmea komponenttia, riskienhallinnan puitteita sekä sisäisiä ja ulkoisia puitteita. ISO 31000:2009–standardin mukaiseen riskienhallinnan puitteiden määrittelyyn kuuluu riskienhallinnan vastuutahojen ja valtuuksien määrittäminen ja johdon sitoutumisen varmistaminen. Tehokas riskienhallinta on koordinoitua, hyvin johdettua ja se ulottuu organisaation jokaiselle tasolle. (SFS-ISO 31000:2009, 26; Hopkin 2012, 81–83.).

Hopkinin (2012, 83) mukaan organisaation sisällä ja ulkopuolella on moninaisia toimintaympäristöjä ja -malleja joiden tunnistaminen ja yhtenäistäminen edesauttavat riskienhallinnan toteuttamista. Riskienhallinnan puitteita ei kuitenkaan ole tarkoituksenmukaista käyttää johtamisjärjestelmän rakenteen määrittelemiseen, vaan riskienhallinta tulisi rakentaa olemassa olevien rakenteiden tueksi vastaamaan organisaation tarpeita. ISO 31000:2009 -standardia voidaan käyttää myös organisaation käytössä olevien riskienhallintatoimenpiteiden ja prosessien erillisten osien arviointiin ja yhdenmukaistamiseen. (SFS-ISO 31000:2009, 26; Hopkin 2012, 81–83.).

### 4.1.1 Riskienhallintapolitiikka ja -suunnitelma

Puitteiden määrittely osana riskienhallintaa on myös itsessään prosessi, jossa suunniteltuja puitteita toteutetaan, seurataan ja kehitetään jatkuvasti. Koko prosessin aikana on organisaation johdon vahva sitoutuminen ja suunnitelmallinen toiminta riskienhallinnan jalkauttamisen kannalta avainasemassa. Johto määrittelee organisaation riskienhallintapolitiikan. Leinon, Steinerin & Wahlroosin (2005, 128) mukaan riskienhallintapolitiikka on lyhyt ja pelkistetty dokumentti, josta käy ilmi riskienhallinnan periaatteet ja tavoitteet, sekä laajuus, jolla riskienhallintaa toteutetaan.

Riskienhallinnan tavoitteiden tulee olla linjassa organisaation tavoitteiden ja strategian kanssa. Riskienhallintapolitiikka sisältää myös riskienhallintaan liittyvät tehtävät ja vastuutahot, joiden avulla kaikkien osapuolten tehtävät ovat selvillä ja organisointi on määritelty. Riskienhallinnan toteuttaminen vaatii resursseja ja niiden varaaminen vastuutahoille kirjataan ris-

kienhallintapolitiikkaan. Politiikassa voidaan kuvata myös organisaation rakennetta ja miten riskienhallintaa on sovellettu tai tullaan soveltamaan sen eri tasoilla. Lopuksi johto hyväksyy riskienhallintapolitiikan, vahvistaa sitoutumisensa siihen ja viestii sen asianmukaisille tahoille. (Leino ym. 2005, 128; SFS-ISO 31000:2009, 27–28.)

Riskienhallinnan puitteiden osana laaditaan myös riskienhallintasuunnitelma, joka kattaa puitteissa määriteltyjä osa alueita kuvailemalla riskienhallintaan sovellettavia toimintamalleja ja osatekijöitä sekä esittämällä riskienhallintaan varattavat resurssit. Riskienhallintasuunnitelma tulee laatia koko organisaatiolle, mutta sellainen voidaan laatia myös yksittäisille projekteille, toiminnoille tai organisaation osalle. (SFS-ISO 31000:2009: 14, 30.)

Riskienhallintasuunnitelmassa kuvataan keinot joilla riskienhallintapolitiikassa määritetyt tavoitteet saavutetaan. Suunnitelmassa kuvataan riskienhallinnan vastuutahot ja menettelytavat. Riskienhallintasuunnitelma on riskienhallintapolitiikkaa täydentävä dokumentti, joka tarkentaa politiikassa kuvailtuja suurpiirteisempiä linjoja kuvailemalla muun muassa toimenpiteiden suoritusjärjestystä, sekä aikataulua. Riskienhallintasuunnitelmaan voidaan nimetä vastuuhenkilöitä riskienhallinnan toiminnoille. Suunnitelmaa tulee väliajoin kehittää ja päivittää muun muassa suoritettujen toimenpiteiden ja riskitason tai organisaatiorakenteen muutosten mukaan. (SFS-ISO 31000:2009, 14.)

### 4.1.2 Riskienhallinnan suorituskyvyn mittaaminen

Organisaation suorituskykyä voidaan mitata erilaisilla mittareilla. Samoin riskienhallinnalle tulisi määritellä mittareita, joiden avulla sen vaikuttavuutta arvioidaan. Riskienhallinnan vaikuttavuuden mittarit riippuvat riskienhallinnan tavoitteista ja niiden tulisi olla yhteneviä organisaation suorituskykyindikaattorien kanssa. Riskienhallinnalle voidaan valita konkreettisia tavoitteita, joihin pääsemistä voidaan arvioida objektiivisesti. Riskienhallinnan suorituskykymittarit ovat toimintaa ohjailevia ja niistä voidaan saada hyödyllistä tietoa organisaation riskitasosta. Riskienhallinnan suorituskyvyn mittaaminen vaatii usein riskien ja riskitasojen arviointia, jolloin muutokset pystytään havaitsemaan. (SFS-ISO 31000:2009, 28.)

Kuusela & Ollikainen (2005, 20-28) mainitsevat riskien numeeristen arvojen määrittämiseen tilastollisia ja todennäköisyyslaskennan menetelmiä, jotka ovat olleet pohjana perinteisessä riskien arvioinnissa. Tilastotiedon ja todennäköisyyslaskennan hyödyntäminen on toki läsnä myös nykyaikaisessa riskienarvioinnissa. Yksi keino arvioida riskienhallinnan vaikuttavuutta on asettaa tavoite tietyn riskin suuruuden pienentämiselle tiettyyn ajankohtaan mennessä. Jos riskin numeerinen arvo pienenee riskienhallintatoimenpiteiden seurauksena, saadaan tietoa riskienhallinnan suorituskyvystä (SFS-ISO 31000:2009, 28).

### 4.1.3 Vastuut ja velvollisuudet

Organisaation jäsenten tulee olla tietoisia roolistaan riskienhallinnassa. Lisäksi tulee huomioida urakoitsijoiden ja tavarantoimittajien kaltaisten sidosryhmien rooli organisaation riskienhallinnassa. Riskienhallinnassa voidaan puhua riskin omistajuudesta. Riskin omistajalla on vastuu tietyn riskin huomioimisesta organisaation toiminnassa. Omistajuus voi liittyä myös organisaation ydinprosesseihin ja riippuvuussuhteisiin. Riskienhallinnan ollessa osa yrityksen toimintaa jokaisella tasolla on luonnollista, että riskin omistaja on sama kuin henkilö tai taho, joka vastaa prosesseista, johon riski pääasiallisesti liittyy. Vastuut tulisi määritellä niin yksiselitteisesti ja selvästi, ettei väärinymmärrysten ja vastuun siirtämisen vaaraa ole. Riskien omistajuuden pääpaino on merkittävissä riskeissä, mutta myös pienempien riskien vastuuttaminen nimetyille tahoille tehostaa riskienhallintaa ja auttaa havaitsemaan muutoksia riskitasoissa. (Hopkin 2012,96–97.)

Hopkinin mukaan riskin omistajuuteen tulee liittää vastuun lisäksi myös valtuuksia (Hopkin 2012, 98). Riskin omistajalla tulee olla mahdollisuus käyttää riittäviä resursseja omistamansa riskin hallitsemiseen. Organisaation rakenteesta ja koosta riippuu miten vaikutusvaltaisessa asemassa riskin omistaja on ja mitkä tämän valtuudet toimia riskin hallinnan edellyttämällä tavalla. Henkilöiden ja tahojen suhtautuminen riskienhallintaan ja riskeihin tuleekin valita työnkuvan ja valtuuksien mukaan. Organisaation ylintä päätösvaltaa käyttävän elimen vastuulla voi olla riskienhallinnan strategioiden suurien linjojen vetäminen ja riskienhallinnan perustan luominen. Ylimmän johdon tulee ymmärtää merkittävimmät riskit ja pystyä johtamaan organisaatiota kriisissä. Linjajohdon tehtäviin kuuluu riskienhallinnan kehittäminen omalla toiminta-alueellaan ja toimia ylimmän johdon asettamien strategioiden mukaisesti toimeenpanemalla riskien hallitsemiseksi annettuja toimintaohjeita. Ylimmän johdon määrittelemät riskienhallintastrategiat ovat pitkälle riippuvaisia linjajohdon raportoinnista ja siten linjajohdon kyvystä tunnistaa muutoksia riskikentässä. Linjajohdon taas tulee vastaanottaa ja arvioida työntekijöiden tai muun organisaation tekevässä portaassa olevan henkilöstön ilmoituksia riskeihin liittyen. (Hopkin 2012, 98.)

Tekevän portaan tasolla riskienhallinta tarkoittaa linjajohdolta tulevien riskienhallinnan ohjeiden noudattamista ja riskienhallintaprosessin ymmärrystä omaan tehtävään liittyen. Tekevällä portaalla on usein paras näkemys nimenomaan omaan tehtäväänsä liittyvistä vahinkoriskeistä ja työntekijöiden raportointimahdollisuuksien tulisi olla hyvät. Työntekijät raportoivat hävikistä, vahingoista ja läheltä piti – tilanteista. Tekevän portaan henkilöstö on usein tekemisissä vierailijoiden, asiakkaiden ja muiden sidosryhmien kanssa, joten on luonnollista, että työntekijät tarkastelevat- ja ohjaavat sidosryhmiä käytäntöjen noudattamisessa. (Hopkin 2012, 98.)

Organisaation sisäisten vastuiden jakaminen ei ole yksiselitteistä, vaan riippuu toimenkuvista, tavoitteista ja organisaatiorakenteesta. Olennaista on, että vähintään merkittäville riskeille määritetään omistaja ja, että riskienhallinnan vastuut ja valtuudet ovat määritelty ja tiedotettu selkeästi. Lisäksi on huomioitava riittävät resurssit ja kannustimet riskienhallinnan toimenpiteiden suorittamiseen.

Organisaatiolla tulee olla mallit riskienhallinnan sisäiseen ja ulkoiseen viestintään ja raportointiin. Kuuselan ja Ollikaisen (2005, 16) mukaan riskiviestinnällä on vaikutusta myös riskin kokemiseen yksilötasolla ja on olennaista kuka riskeistä kertoo ja miten. Huonosti toteutettu viestintä ja tiedottaminen jättää sijaa huhuille ja väärän tiedon leviämiselle. Riskienhallinnasta tiedottamiselle on määrättävä vastuutaho sekä luotava järjestelmä, joka ylläpitää tärkeiden sidosryhmien tietoisuutta riskienhallinnan puitteista, riskienhallinnasta saadusta tiedosta ja riskeistä, sekä näiden muutoksista.

Vaikka riskienhallinnasta tiedottamisessa on hyvä noudattaa avoimuutta, on joidenkin seikkojen ja dokumenttien arkaluontoisuus otettava huomioon. Sisäiseen ja ulkoiseen tiedottamiseen ja raportointiin on siis hyvä luoda omat väylät ja mallit. Sisäisessä viestinnässä korostuu vastuun ja riskien omistajuuden vahvistaminen, kun taas ulkoisen raportoinnin tavoitteena on ulkoisten sidosryhmien osallistaminen ja sitä kautta organisaation luotettavuuden lisääminen. Kriisiviestintä on tärkeä osa organisaation viestintää, mutta riskienhallintaan liittyvän tiedottamisen ei tulisi rajoittua poikkeustilanteisiin. Hyvin toteutettu riskienhallinta voi olla kilpailuetu ja jopa vaatimus yhteistyölle muiden organisaatioiden kanssa. Riskienhallinnasta viestiminen on osa organisaation maineriskien hallintaa. (SFS-ISO 31000:2009, 30–31; Hopkin 2012, 50–53.)

## 4.2 Riskienhallinnan toteuttaminen

SFS-ISO 31000-standardissa riskienhallinnan toteuttaminen on prosessi riskienhallinnan puitteiden prosessin sisällä, joka seuraa riskienhallinnan puitteiden suunnittelua. Riskienhallinnan toteuttaminen sisältää riskienhallinnan puitteiden toteuttamisen ja riskienhallintaprosessin toteuttamisen osa-alueet. Riskienhallintaprosessi on kuvattu tarkemmin kappaleessa 5.3. Puitteiden toteuttamiseen kuuluu puitteiden suunnitteluvaiheessa määriteltyjen toimintojen ja suunnitelmien toimeenpano siten, että ne ovat linjassa organisaation muiden prosessien kanssa. Puitteiden toteuttamista ohjaa muun muassa riskienhallintapolitiikka ja – suunnitelma, sekä viranomaisvaatimukset ja lait. Toteuttamisvaiheessa viestintä ja tiedotus korostuu. Organisaation tulisi järjestää koulutuksia ja tiedotustilaisuuksia sisäisille sidosryhmille ja vaihdettava tietoa myös ulkoisten sidosryhmien kanssa varmistaakseen, että puitteet ovat sopivia. (ISO 31000:2009, 32.)

Riskienhallinnan puitteita tulee ISO 31000:2009:n mukaisesti seurata ja katselmoida, jotta niiden jatkuva kehittäminen on mahdollista ja riskienhallinnasta saadaan mahdollisimman tehokasta ja vaikuttavaa. Riskienhallinnan tasoa mitataan puitteiden suunnitteluvaiheessa määritellyillä suorituskykyindikaattoreilla ja mittareilla, jotta voidaan todeta riskienhallinnan kehityssuunta. Sisäisen ja ulkoisen toimintaympäristön muutosten huomioiminen osana riskienhallinnan puitteiden katselmointia toteutetaan yhteistoiminnassa toiminnan kannalta merkittävien sidosryhmien kanssa. Riskienhallinnan puitteiden toteuttamisen tulisi olla linjassa organisaation riskienhallintapolitiikan ja – suunnitelman kanssa ja niissä asetettujen tavoitteiden ja aikataulujen toteutumista tulee johdon toimesta tarkkailla. Organisaatio myös raportoi löydöksistään riskeihin, riskienhallintaan, politiikan noudattamiseen ja suunnitelmien edistymiseen liittyen. Kokonaisuudessaan organisaatio arvioi puitteiden vaikutusta organisaation riskienhallinnan jokaisella tasolla. Katselmoinnin perusteella puitteita, riskienhallintapolitiikkaa ja – suunnitelmaa kehitetään ja riskienhallinnan puitteiden prosessin käynnistyessä uudelleen tarkastellaan tehtyjen muutosten vaikutuksia lopputulokseen. (ISO 31000:2009, 33–34.)

SFS-ISO 31000-standardin mukainen riskienhallinta perustuu prosessiin, jossa määritellään riskienhallinnan periaatteet, puitteet ja riskienhallinnan toteuttamisen prosessi, jossa toimintaympäristön määritteleminen, riskien arviointi ja riskien käsittely muodostavat kokonaisuuden, jossa seuranta ja katselmointi, sekä viestintä ja tiedonvaihto ovat mukana jokaisessa vaiheessa. Riskien arviointiin kuuluu riskien tunnistamisen, riskianalyysin ja riskien merkityksen arvioinnin osa-alueet.

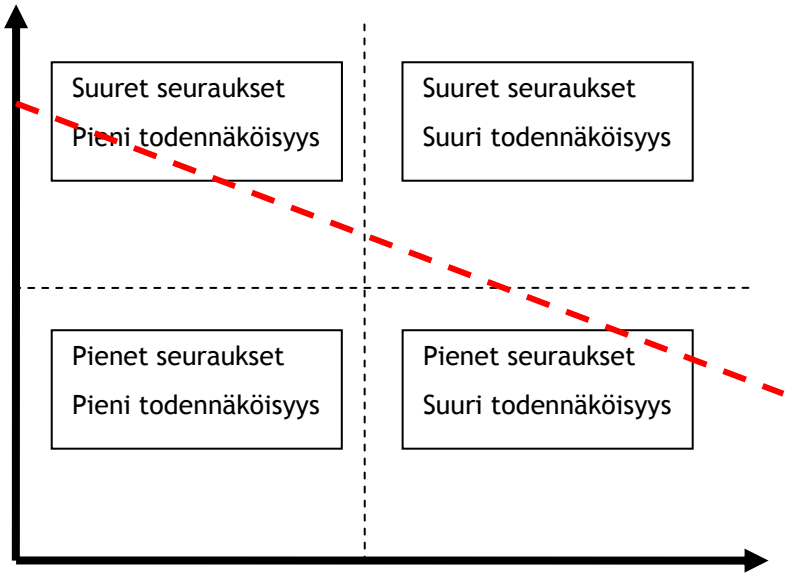
### 4.2.1 Riskikriteerien määritteleminen

Riskiä arvioidaan sen seurausten ja todennäköisyyden yhdistelmänä. Organisaation tulisi määritellä tunnusmerkit, jotka määrittelevät riskin käsitteen. Organisaatio määrittelee minkälaisia tapahtumia se voi kohdata, mitkä ovat niiden seuraukset ja syyt ja miten näitä tapahtumia voidaan objektiivisesti tarkastella ja mitata. Tapahtumilla on jokin todennäköisyys, joka täytyy määritellä ja luokitella. (SFS-ISO 31000:2009, 40.)

Riskitasolla tarkoitetaan seurausten ja todennäköisyyden yhdistelmänä ilmoitettua riskin suuruutta (SFS-ISO 31000:2009, 20). Yksi tapa määritellä riskitaso voi olla riskiluvun laskeminen käyttämällä erilaisia laskukaavoja. Riskiluku voidaan laskea määrittämällä seurauksille ja todennäköisyydelle numeerinen arvo ja kertomalla ne keskenään, jolloin saadaan numeerinen ja vertailukelpoinen arvo riskille. Organisaation riskienhallinnan kannalta on kuitenkin usein tärkeämpää arvioida riskit, joiden seuraukset ovat suuria tai vakavia, kuin niitä joiden seuraukset ovat pieniä, vaikkakin pienten seurausten riskien todennäköisyys olisi korkeampi. (Juvonen, Korhonen, Ojala, Salonen & Vuori 2005, 10; Hopkin 2012, 18–20.)

Laskukaava ”seuraus x todennäköisyys” antaa saman arvon riskille, jonka todennäköisyys on korkea ja seurausten vakavuus pieni, kuin riskille, jonka todennäköisyys on pieni, mutta vaikutukset organisaation kannalta vakavia. Tämä vääristymä saadaan korjattua painottamalla vaikutuksia laskukaavassa, esimerkiksi korottamalla seurauksille annettu lukuarvo toiseen potenssiin; ”seuraus$^2$ x todennäköisyys”. (Juvonen ym. 2005, 10; Hopkin 2012, 18–20.)

Riskitason kuvaamiseen voidaan käyttää niin kutsuttua riskimatriisia tai riskikuvaaja, joilla annetaan riskeille ja riskitasolle visuaalinen esitysmuoto. Riskimatriisiin voidaan kuvata myös hyväksyttävän riskin taso, joka esimerkkikuviossa on hahmoteltu punaisella katkoviivalla (Kuvio 4). Katkoviivan alle jäävät riskit ovat hyväksyttävällä riskitasolla ja yläpuolelle jäävät vaativat riskienhallintatoimenpiteitä. Riskejä voidaan sijoittaa riskimatriisiin niille laskettujen riskilukujen mukaisesti ja niille voidaan antaa erilaisia kuvaavia värikoodeja. (Hopkin 2012, 19–20.)




Kuvio 4. Riskikuvaaja (Hopkin 2012, 20)

Riskikriteerien määrittelemisessä tulisi huomioida, että ne ovat organisaation riskienhallintapolitiikan mukaisia. Kriteerien ajankohtaisuus ja sopivuus tulisi varmistaa katselmoimalla niitä jatkuvasti ja toteuttamalla riskikriteerien määrittely jokaisen riskienhallintaprosessin alussa. Riskit saattavat muodostaa myös erilaisia yhdistelmiä ja riskiryppäitä, joiden huomioiminen kriteerien määrittelemisessä on tärkeää. On huomioitava, että jotkin riskit saattavat altistaa myös muille riskeille. (SFS-ISO 31000:2009, 34, 40.)

### 4.2.2 Riskin arviointi

Riskin arviointi SFS-ISO 31000:n (2009, 40) mukaan koostuu riskien tunnistamisesta, riskianalyysistä ja riskin merkityksen arvioinnista. Riskin arviointi on prosessi, jolla pyritään löytämään organisaation kannalta merkittävät riskit. Riskien arviointi parantaa päätöksentekoon liittyvien lähtötekijöiden määrittelyä ja sitä kautta se auttaa organisaation strategian luomisessa ja kehittämisessä. Riskit voivat liittyä organisaation tavoitteisiin, sidosryhmien odotuksiin, ydinprosesseihin ja avainasemassa oleviin riippuvuussuhteisiin (Hopkin 2012, 139.)

Suomen riskienhallintayhdistys (SRHY) jaottelee riskit vahinkoriskeihin, operatiivisiin riskeihin ja talousriskeihin (Suomen riskienhallintayhdistys 2012a). Riskejä voidaan luokitella myös niiden arvojen mukaan, joihin riski vaikuttaa. Elinkeinoelämän keskusliitto (EK) määrittelee yrityksen suojattaviksi arvoiksi henkilöt, maineen, tiedon, omaisuuden ja ympäristön (Elinkeinoelämän keskusliitto 2015). Riskit voivat kohdistua yhteen tai useampaan yrityksen suojattavaan arvoon. Elinkeinoelämän keskusliiton lähestymistapa liittyy vahvemmin yritysturvallisuuteen ja turvallisuusjohtamiseen, kun taas Suomen riskienhallintayhdistyksen lähestymistapa edustaa kokonaisvaltaisempaa riskienhallintaa.

Riskien arvioinnissa on tärkeää päättää arvioidaanko riskiä sen nykyisellä tasolla, ottaen huomioon jo käytössä olevat hallintakeinot vai käsitelläänkö niin kutsuttua luontaista (inherent) riskiä, eli riskitasoa ilman riskinhallintakeinoja ja -menetelmiä. Riskiä, joka jää jäljelle hallintakeinojen jälkeen kutsutaan jäännösriskiksi. Etuna luontaisen riskin käytössä riskinarviointiprosessissa on, että saadaan kuva luontaisen ja hallitun riskin tasoeroista. Tällä voidaan saada tietoa yrityksen riskienhallinnan vaikuttavuudesta ja olemassa olevien riskinhallintakeinojen tehokkuudesta. Luontaisen riskin arviointi voi lähtökohtaisesti olla hyödyllistä, sillä se auttaa tunnistamaan kriittisiä riskinhallintakeinoja, mutta sen tason luotettava arviointi on vaikeaa. Kun arvioidaan riskiä nykyisten hallintakeinojen luomalla tasolla, on vaarana, että riskinhallintakeinojen oletetaan toimivan jatkuvasti ja yhtä tehokkaasti. Yksinkertaisempana prosessina se on kuitenkin helpompi toteuttaa ja tietyissä organisaatioissa ja toiminnoissa voi olla hyödyllisempää arvioida riskiä sen nykyisellä tasolla. (Hopkin 2012, 139–140, SFS-ISO 31000:2009, 40.)

### 4.2.3 Riskin tunnistaminen

Riskin tunnistamisella tarkoitetaan riskin lähteiden, vaikutusalueitten ja tapahtumien syiden ja seurausten löytämistä, tuntemista ja tallentamista. (SFS-ISO 31000:2009, 40; SFS-EN 31010:2010, 20). Riskien tunnistamisen lähtökohtana on organisaation strategia ja tavoitteet ja periaate, että tunnistamattomia riskejä ei voida hallita. Organisaation kaikki riskit tulee tunnistaa riippumatta riskilähteestä tai siitä onko lähde organisaation hallinnassa. Riskien

tunnistamisessa etsitään tapahtumia, potentiaalisia ongelmia ja mahdollisuuksia joiden realisoituminen tai hyödyntämättä jättäminen vaikuttaa organisaation toimintaan heikentävästi tai parantavasti. Näistä tapahtumista kerätään mahdollisimman kattava lista, jotta riskit saadaan huomioitua myös riskinhallintaprosessin seuraavissa vaiheissa. (SFS-ISO 31000:2009, 40; Suomen riskienhallintayhdistys 2012b.)

Riskien tunnistamiseen on käytössä erilaisia menetelmiä. ISO 31010–standardi kuvaa monia erilaisia työkaluja riskin tunnistamiseen, analysointiin ja merkitysten arviointiin. Käyttökelpoisia riskintunnistusmenetelmiä ovat muun muassa erilaiset kyselyt ja tarkastuslistat, työryhmät ja aivoriihet, tarkastukset ja auditoinnit, sekä erilaiset vuokaaviot ja riippuvuussuhteiden analyysit (Hopkin 2012,141). Suomen riskienhallintayhdistys suosittelee riskien tunnistamisen aloittamista karkealla haavoittuvuusanalyysillä (Suomen riskienhallintayhdistys 2012b). Suomen riskienhallintayhdistyksen mukaan riskien tunnistaminen kannattaa suorittaa järjestelmällisesti siirtymällä yleisestä yksityiskohtaiseen riskien tunnistamiseen. Organisaation kannattaa hyödyntää ulkopuolisia asiantuntijoita erityisesti niiden riskien tunnistamiseen, joista organisaatiolla itsellään ei ole vahvaa tietopohjaa. Riskien tunnistamista ei kuitenkaan voida tehdä täysin ulkopuolisen tahon toimesta, sillä organisaation toimintaan liittyvät erityispiirteet tulee huomioida tunnistamisessa. (Suomen riskienhallintayhdistys 2012b; Hopkin 2012, 139 -142)

SFS-EN 31010–standardissa riskien tunnistamiseksi ehdotetaan myös useamman menetelmän yhdistämistä. Organisaatio voi käyttää näyttöön perustuvia menetelmiä kuten tarkastuslistoja tai historiatietoja, asiantuntijoista koostuvien ryhmien työskentelyjä, sekä induktiivisen päättelyn tekniikoiden hyödyntämistä. Esimerkiksi poikkeamatarkastelu (HAZOP) on käyttökelpoinen työkalu riskien tunnistamisvaiheessa, erityisesti teollisiin prosesseihin liittyen. Riskien tunnistamisessa tulee huomioida niin laitteistojen ja ohjelmistojen tapahtumien poikkeamat, kuin inhimillisistä ja organisaatioon liittyvistä tapahtumista johtuvat riskit. Riskienhallinnassa ihminen muodostaa usein heikoimman lenkin. (SFS-EN 31010:2010, 20.)

### 4.2.4 Riskianalyysi

Riskianalyysi on riskien syiden ja seurausten, riskilähteiden ja todennäköisyyksien tarkastelua. Riskillä voi olla positiivisia tai negatiivisia seurauksia, tai jopa molempia. Riskianalyysissä pyritään havaitsemaan ne seikat, jotka vaikuttavat riskin todennäköisyyteen ja seurausten laajuuteen. Myös eri riskien väliset yhteydet ja riskilähteiden väliset riippuvuudet on huomioitava riskianalyysissä. Riippumatta siitä, onko riskianalyysissä arvioitu jäännösriskiä vai luontaista riskiä, on riskienhallintakeinot huomioitava riskianalyysivaiheessa. Tapoja ilmaista riskin seurausten laajuus ja todennäköisyys on monenlaisia, joten yhtenevät käytännöt organisaation sisällä ja tärkeimpien sidosryhmien kanssa edesauttavat vaikuttavan riskienhallinnan to-

teuttamista. Lisäksi riskianalyysin tulee olla linjassa organisaation riskienhallintapolitiikan ja –suunnitelman kanssa. (ISO 31000:2009,41–42.)

Riskin todennäköisyys vaihtelee nollan ja yhden välillä, jossa nolla tarkoittaa tilannetta, jossa riski ei tapahdu ja yksi kuvaa tilannetta, jossa riski tapahtuu varmasti. Riskiin liittyy kuitenkin olennaisesti epävarmuus, joten nollan ja yhden ääripäissä kyse ei ole riskistä. Riskin todennäköisyyttä ei usein pystytä arvioimaan kovinkaan tarkasti ja mitä monimutkaisemmasta prosessista tai tapahtumasta on kyse, sitä epätarkemmaksi riskin todennäköisyyden arviointi käy. (Kuusela & Ollikainen 2005, 27–29.)

Riskin todennäköisyyden arvioinnissa tulee huomioida myös mitä vakavuuden astetta arvioidaan. Otetaan esimerkiksi kaatumiset ja liukastumiset. Terveyden ja hyvinvoinnin laitoksen mukaan Suomessa sattuu vuosittain 390 000 kaatumista ja liukastumista, joista noin puolet vaatii sairaalahoitoa. Vakavia kaatumisia ja liukastumisia, eli yön yli sairaalahoitoa vaativia liukastumisia tapahtuu noin 5000 vuosittain (Terveyden ja hyvinvoinnin laitos 2014). Putoamiset ja kaatumiset aiheuttavat vuositasolla keskimäärin noin 1100 kuolemantapausta. (Terveyden ja hyvinvoinnin laitos 2015). Organisaation kannalta tämä tarkoittaa sitä, että sen tulee riskien todennäköisyyksissä huomioida myös seurausten vakavuuden todennäköisyys. Esimerkkiorganisaatio käyttää riskitasoa arvioidessaan työkaluna riskiluvun laskemista, jossa todennäköisyydelle ja seurauksille annetaan lukuarvo yhden ja kolmen väliltä ja riskiluku lasketaan todennäköisyyden ja seurausten vakavuuden neliön tulona. Jos riskin toteutumisen seurauksena voi olla kuolema tai vakava loukkaantuminen, saa seuraus lukuarvon kolme, sairaalahoitoa vaativaan loukkaantumiseen johtava riski saa arvon kaksi ja lievään loukkaantumiseen johtava arvon yksi. Todennäköisyyttä arvioidessa esimerkin puitteissa riittää määrittely, että lukuarvo kolme on todennäköinen ja yksi epätodennäköinen, lukuarvon kaksi sijoittuessa näiden väliin.

Liukastumisen riskiä voitaisiin kuvata taulukossa 1 esitetyillä riskikomponenttien riskiluvuilla:

| | | |
|---|---|---|
| **Liukastuminen – lievä loukkaantuminen:** | | |
| Todennäköisyys: 3 | Vakavuus: 1 | Riskiluku: $(3 \times 1^2) = 3$ |
| **Liukastuminen – sairaalahoitoa vaativa, ei vakava loukkaantuminen:** | | |
| Todennäköisyys: 3 (tai 2) | Vakavuus: 2 | Riskiluku $(3 \times 2^{2)} = 12$ |
| **Liukastuminen – vakava loukkaantuminen tai kuolema:** | | |
| Todennäköisyys: 1 | Vakavuus: 3 | Riskiluku $(1 \times 3^2) = 9$ |

Taulukko 1. Riskiluvun laskeminen riskin komponenteille.

Organisaation tulee määritellä miten todennäköisyys otetaan huomioon riskiä arvioitaessa. Valitaanko tarkasteltavaksi vain riskin todennäköisin seuraus, esimerkissä lievä loukkaantuminen tai sairaalahoitoa vaativa, ei vakava loukkaantuminen vai otetaanko liukastumisriskin kaikki mahdolliset lopputulokset huomioon erillisinä komponentteina. Riskeistä on mahdollista laskea myös erilaisia keskilukuja. Organisaation on vältettävä ajattelua jossa riskistä huomioidaan pahin mahdollinen seuraus ja yhdistetään se kaikkien tapahtumien todennäköisyyteen. Tällöin liukastumisen ja kaatumisen riski saisi esimerkissämme arvon 27, joka on valitun asteikon korkein riskiluku.

Riskienarvioinnin resurssien kannalta on kuitenkin vain harvoin mahdollista tai järkevää jakaa jokaista tunnistettua riskiä komponentteihin eri todennäköisyyksien ja seurausten yhdistelmien perusteella. Riskiluvun todennäköisyyttä ja vakavuutta kuvaavat asteikot voidaan valita tarpeen mukaan. Oheisessa taulukossa (Taulukko 2) esitetään riskimatriisi, jossa riskiluvut on laskettu edellä mainitun kaavan mukaisesti. Riskimatriisissa todennäköisyyden ja seurausten lukuarvot on määritelty välille 1-5. Matriisiin on erotettu liukastumisesimerkissä käytetty riskiluvun määritys arvoille 1-3.

**Riskimatriisi**

| Todennäköisyys \ Seuraukset | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | 1 | 4 | 9 | 16 | 25 |
| 2 | 2 | 8 | 18 | 32 | 50 |
| 3 | 3 | 12 | 27 | 48 | 75 |
| 4 | 4 | 16 | 36 | 64 | 100 |
| 5 | 5 | 20 | 45 | 80 | 125 |

Taulukko 2. Riskimatriisi.

Kun organisaatio päättää riskiluvun laskemisesta tai muusta riskitason määrittelystä, tulee sen sitoa eri tapahtumien vaikutukset konkreettisiin arvoihin. Arvojen valinta riippuu siitä, onko riskienhallinnan oltava vertailtavissa muiden organisaatioiden riskienhallinnan kanssa vai onko se ensisijassa organisaation sisäinen prosessi. Kuitenkin on huomioitava, että organisaation riskienhallinnan tulee kuitenkin olla sisäisesti yhtenevää ja muiden organisaation prosessien mukaista. Jos riskienhallinnan tuloksia on tarkoitus vertailla muiden organisaatioiden, esimer-

kiksi sidosryhmien vaatimusten ja luokittelujen mukaisesti on riskien tunnuslukujen valitsemisessa otettava nämä tahot huomioon.

Joskus riskin jakaminen komponentteihin on kuitenkin hyödyllistä, jos sama riski esimerkiksi koskee useampaa organisaation osaa, mutta jotkut osat ovat riskille alttiimpia kuin toiset. Käytetyssä liukastumisesimerkissä vanhukset ja muut rajoittuneen toimintakyvyn omaavat henkilöt ovat selvästi alttiimpia kaatumisille ja niistä aiheutuville loukkaantumisille. Riskiin voi vaikuttaa myös ajankohta. Talvella liukastumiset ovat todennäköisesti keliolosuhteiden takia yleisempiä, samoin hämärän aikaan. Riskin todennäköisyyttä ja seurauksia voidaan tarkastella erilaisten viitekehysten, kuten aikaa, paikkaa, ryhmää tai tilannetta koskevien erityispiirteiden avulla. (SFS-ISO 31000:2009, 42; Terveyden ja hyvinvoinnin laitos 2015.)

Riskin seuraukset voidaan määritellä käyttäen hyväksi organisaation suojattavia arvoja; omaisuutta, henkilöjä, mainetta, tietoa ja ympäristöä. Omaisuus on usein helpoiten mitattavissa, koska kiinteälle omaisuudelle on helppo antaa rahallinen arvo. Poikkeuksena tästä on erityistä tunne- tai kulttuuriarvoa omaava omaisuus ja organisaation on itse määriteltävä, minkälaiset omaisuuden menetykset ovat merkittäviä ja vakavia. Arvioinnin tukena voidaan käyttää esimerkiksi yrityksen liikevaihtoa tai yhdistyksen varallisuutta. Organisaation koon, arvojen ja varallisuuden pohjalta määritellyt tunnusluvut ovat käyttökelpoisimpia, sillä ne antavat todenmukaisen kuvan riskien toteutumisen vaikutuksista organisaatioon. Pienemmälle organisaatiolle 10 000€ rahallinen menetys voi olla merkittävä riski, kun taas suurelle yritykselle se kuuluu vähäisten seurausten piiriin. Taloudellisiin menetyksiin voidaan lukea myös riskit, jotka aiheuttavat yrityksen toiminnan keskeytymisen. Henkilöihin kohdistuvien riskien seurausten määrittelyssä voidaan käyttää esimerkiksi poissaolopäivien määrää tai työkyvyn menettämisen pituutta. Myös kuolemantapauksien mahdollisuus tulee huomioida riskin seurausten määrittelemisessä. Yrityksen maineeseen kohdistuvat riskit ovat hankalasti arvioitavissa. Sosiaalisen- ja elektronisen median aikakaudella organisaatioon kohdistuva negatiivinen julkisuus voi levitä nopeasti ja monia eri kanavia pitkin.

Organisaation tietoon kohdistuvien riskien seurausten määrittelyä auttaa jos organisaation tieto on turvaluokiteltua. Tietoa voidaan luokitella esimerkiksi julkiseksi, sisäiseksi, luottamukselliseksi ja salaiseksi. Tietoriskin seurausten määrittelyssä voidaan käyttää turvaluokitellun tiedon vuotamista ulkopuoliselle taholle tai tiedon eheyden tai saatavuuden heikkenemistä. Eheyden käsitteeseen liittyy tiedon yhtenevyys, tarkkuus ja luotettavuus sen koko elinkaaren aikana ja saatavuudella tarkoitetaan, että tieto on riittävän helposti saataville niille henkilöille, jotka sitä tarvitsevat. Ympäristöön kohdistuvat riskit vaikuttavat usein myös organisaation omaisuuteen ja maineeseen tai ympäristön henkiöihin ja ympäristöriskit voidaan arvioida näiden tekijöiden pohjalta. Ympäristöön kohdistuvia riskejä voidaan arvioida myös

itsenäisinä arvioimalla kunkin riskin toteutumisen vaikutuksia ympäröivään luontoon ja rakennettuun ympäristöön. (ISO-IEC 27000:2006, 10–15.)

Riskien seurausten ja todennäköisyyksien ilmaisutapa valitaan yhteneväiseksi riskikriteerien mukaan ja riskien arvioinnin tavoitteiden mukaan. Lisäksi riskitason ilmaisemiseen vaikuttaa riskin tyyppi, riskistä olemassa oleva tieto ja tapa jolla riskiä käsitellään jatkossa. Riskianalyysin toteutustapa voi olla määrällinen tai laadullinen ja se voidaan toteuttaa käyttämällä useita erilaisia riskianalyysityökaluja. Riskienhallintapolitiikka ja – suunnitelma määrittelevät miten yksityiskohtaisesti riskejä organisaatiossa tai sen osassa käsitellään. Riskianalyysin tarkkuuteen vaikuttaa myös saatavilla oleva tieto ja resurssit.

Riskienhallinnan menetelmiä kuvailevassa SFS-EN 31010:2009–standardissa riskianalyysin toteutustavat jaotellaan laadullisiin, semi-kvalitatiivisiin ja määrällisiin menetelmiin. Menetelmien välillä vaihtelua on erityisesti yksityiskohtaisuudessa ja analyysin tekoon vaaditussa tietomäärässä. Määrällisen riskianalyysin toteuttaminen vaatii tarkkoja numeerisia arvoja ja sen toteuttamisessa tulisi hyödyntää käytännön arvoja seurauksille ja todennäköisyyksille. Riskitason tulisi määrällisessä riskianalyysissä olla ennalta määritetty sekä riskienhallinnan puitteisiin ja toimintaympäristöön sidottu yksikkö. Yksikkö voi olla esimerkiksi rahallinen arvo, asiakasmäärä, tai aikamääre. Inhimillistä tekijää on määrällisellä riskianalyysillä vaikeaa arvioida. Määrällinen riskianalyysi sopii tilanteisiin, jossa riskin seurausten suuruus ja todennäköisyys pystytään määrittelemään tarkasti ja numeerisesti. Vedonlyönti nopan heitossa, voisi olla arkielämän yksinkertaistettu esimerkkitilanne, jossa määrällistä riskianalyysia voitaisiin hyvin käyttää, kun tiedetään tarkasti voittavan silmäluvun todennäköisyys, panoksena oleva rahasumma sekä voittokerroin. Jos lähtötilanteen tiedoista puuttuisi jokin, esimerkiksi voittokerroin, ei analyysiä voitaisi toteuttaa täysin määrällisenä. (SFS-EN 31010:2009, 22.)

Laadullisessa riskianalyysissä todennäköisyydelle, seurauksille, sekä riskitasolle annetaan selkokielinen termi. Esimerkiksi pieni, keskisuuri ja suuri. Jokaiselle termille määritellään selitys ja kehys organisaation riskinhallintasuunnitelman mukaisesti. Laadullinen riskianalyysi ei vaadi niin paljon lähtötietoja kuin määrällinen ja sitä voidaan käyttää tilanteissa, jossa esimerkiksi todennäköisyyttä tai seurausten suuruutta on vaikeaa tai mahdotontonta määritellä kovinkaan tarkasti. Semi-kvantitatiivinen riskianalyysi asettuu näiden kahden toteutustavan väliin yksityiskohtaisuuden osalta ja on yhdistelmä määrällistä ja laadullista riskianalyysiä. Semi kvantitatiivisessa toteutustavassa hyödyntävät numeerisia arvoja ja erilaisia laskukaavoja ja asteikkoja. (SFS-EN 31010:2009, 22.)

### 4.2.5 Riskin merkityksen arviointi

Riskin merkityksen arvioinnin tavoitteena on löytää riskit, joiden käsitteleminen on tarpeellista ja ensisijaista. Riskin merkittävyys voidaan arvioida vertaamalla riskianalyysissa havaittua riskitasoa riskikriteereihin. Organisaatio määrittelee tärkeysjärjestyksen riskeille sen omien arvojen ja asenteiden, sidosryhmien odotusten, sekä viranomaisten vaatimusten mukaisesti. Se miten organisaatio arvottaa omaisuuteen, henkilöihin, maineeseen, tietoon ja ympäristöön kohdistuvat riskit vaikuttaa osaltaan riskin merkittävyyteen. Riskin merkityksen arvioinnissa voidaan päätyä tilanteeseen, jossa riski päätetään jättää käsittelemättä tai riskit voivat vaatia lisäselvityksiä. Organisaation riskikriteerit ja riskinottohalukkuus vaikuttavat siihen, mitkä riskit käsitellään riskienhallintaprosessin viimeisessä vaiheessa. (SFS-ISO 31000:2009, 42.)

Jos riskien tunnistamisen ja riskianalyysin jälkeen organisaation ydinprosesseja uhkaavia riskejä on vielä niin suuri määrä, ettei niiden hallitseminen riskienhallinnan resurssien puitteissa, täytyy organisaation joko muuttaa riskikriteerejä tai lisätä riskienhallinnan resursseja.

## 4.3 Riskien käsittely

Riskien käsittely on prosessi, jossa tunnistettujen ja merkittäviksi havaittujen riskien hallitsemiseksi valitaan, toteutetaan, tarkastellaan ja katselmoidaan erilaisia hallintakeinoja, kunnes käsiteltävän riskin jäännösriskin taso on hyväksyttävällä tasolla. Riskiä voidaan käsitellä yhdellä tai useammalla eri hallintakeinolla, jotka eivät ole toisiaan poissulkevia. Riski voidaan torjua keskeyttämällä riskialtis toiminta tai päättämällä, ettei riskialtista toimintaa aloiteta lainkaan. Riskin lähde voidaan myös yrittää poistaa kokonaan. Tietyissä tapauksissa riskin tuomat mahdollisuudet voivat kannustaa organisaatiota ottamaan, tai jopa lisäämään riskiä. Riskin luonteeseen kuuluu todennäköisyyden ja seurausten suhde, joten muuttamalla toista tai molempia näistä komponenteista pystytään vaikuttamaan riskin suuruuteen. Riski voidaan siirtää tai jakaa eri osapuolten kanssa erilaisilla sopimuksilla, kuten vakuuttamalla. Riski voidaan myös säilyttää. Riskin käsittelemättä jättämisen tulisi kuitenkin olla tietoinen päätös, eikä olla seurausta heikosti ymmärretyistä seurauksista tai huonosti toteutetusta riskien arvioinnin prosessista. (SFS-ISO 31000:2009, 44.)

Riskialttiin toiminnan aloittamatta jättäminen tai keskeyttäminen on yksinkertainen ja tehokas tapa hallita riskiä, mutta käytännön toteutus on usein vaikeaa ja organisaation kannalta epäsuotuisaa. Nyrkkisääntönä voidaan pitää, että uutta toimintaa ei tule aloittaa, jos riskiä ei saada hyväksyttävälle tasolle. Tietyissä tapauksissa myös olemassa olevan toiminnan keskeyttäminen voi olla välttämätöntä liian suuren riskin vuoksi. Tämä saattaa kuitenkin riidellä organisaation ydintoimintojen toteuttamisen ja arvolupauksen kanssa. Kaikki riskit ja niiden seuraukset eivät kuitenkaan ole negatiivisia ja tämä tulee ottaa huomioon riskien käsittelytapojen valinnassa. Myös riskiin, jonka seuraukset nähdään organisaation kannalta negatiivisina

saattaa liittyä myös mahdollisuuksia ja positiivisia vaikutuksia. Lottoarvonnassa on todennäköisintä, ettei yhdellä arvotulla rivillä voita mitään. Samassa arvonnassa on kuitenkin pieni mahdollisuus voittaa suuria rahapalkintoja, eikä yksittäinen rivi ole kallis. Riski voidaan ottaa lottoamalla yksi rivi tai riskiä voidaan lisätä lottoamalla useampi rivi. Tällöin nostamalla negatiivisen seurauksen suuruutta saadaan hieman kasvatettua positiivisen seurauksen todennäköisyyttä. (Smith & Politowski 2013, 106.)

Uuden toiminnan tai toimintamallin aloittamisessa on kyse juuri riskin tuomien mahdollisuuksien ja uhkien tarkastelusta rinnakkain. Toisaalta uusi toiminta voi lisätä organisaation kassavirtaa tai muuten edistää sen toimintaa, mutta toisaalta uuden toiminnan aloittamiseen ohjatut resurssit saattavat mennä hukkaan, jos haluttuun tavoitteeseen ei päästä. Tällöin uuden toiminnan aloittamisen riskille voidaan laskea kaksi erillistä riskilukua, joista toinen kuvaa riskinottamisen luomia mahdollisuuksia ja toinen sen uhkia. Näiden komponenttien tarkastelu auttaa organisaatiota tekemään päätöksiä riskiperusteisesti.

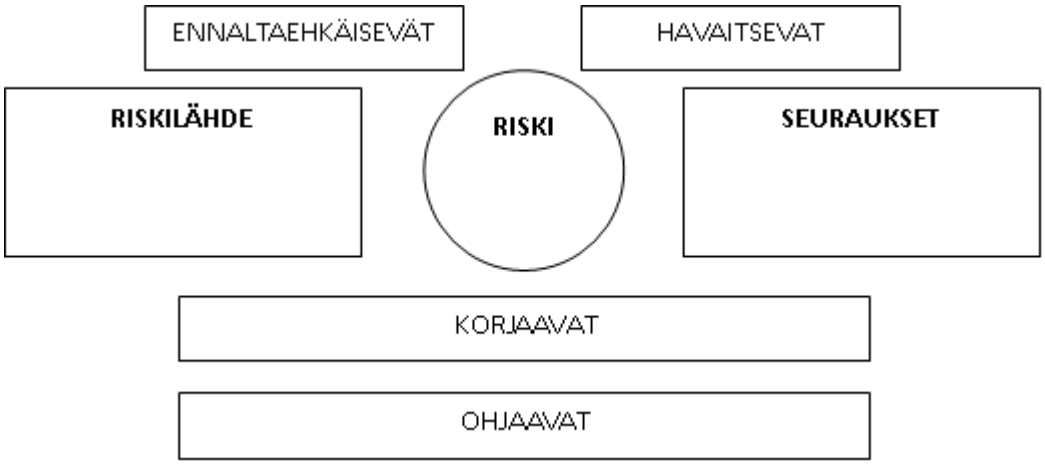
Kun tiedetään riskin lähde, voidaan riskin lähdettä muuttaa tai se voidaan poistaa kokonaan. Riskilähteen poistamisen kannalta erittäin tärkeää on kuitenkin tunnistaa riskilähde ja kaikki osatekijät, joihin riskilähteen poistaminen vaikuttaa. Organisaation tulee olla tietoinen riskilähteen muuttamisen seurauksista ja arvioida niiden pohjalta riskin käsittelytavan kannattavuutta. Käytännöllisemmäksi tuleekin usein vaikuttaa riskin todennäköisyyksiin ja seurauksiin. Riskin todennäköisyys ja seuraukset ovat usein verrattain helposti havaittavissa ja mitattavissa ja täten niihin vaikuttaminen eri keinoin muodostaa riskien käsittelyn selkärankaa. Organisaation on tunnistettava, kumpaan riskin komponenttiin riskienhallintatoimenpiteitä olisi tehokkaampaa kohdistaa. Esimerkiksi kauppaliikkeessä sähkökatkoksen todennäköisyyttä on vaikeaa pienentää mutta sen negatiivisia seurauksia voidaan pienentää varavoimageneraattoreilla. Samoin kauppaliikkeessä esimerkiksi onnistuneen kassakaappimurron todennäköisyyttä voidaan pienentää lisäämällä kiinteistön turvajärjestelyjä ja seurauksia pienentää vähentämällä kassakaapissa olevia rahavaroja. (Smith & Politowski 2013, 106–109 ; SFS-ISO 31000:2009, 44.)

Riskinkäsittelytavan valinta perustuu sen kustannusten ja vaadittavien resurssien määrään verrattuna saatuihin hyötyihin, viranomaisvaatimuksiin sekä yhteiskuntavastuuseen ja ympäristönsuojeluun. Riskin saamiseksi hyväksyttävälle tasolle saatetaan joutua käyttämään useampaa riskinkäsittelytapaa yhdessä ja joskus se on myös resurssitehokkainta. Sidosryhmien huomioiminen on tärkeää myös riskinkäsittelytapoja valittaessa ja jos eri tavat voivat vaikuttaa sidosryhmiin kohdistuviin riskeihin ja niiden toimintaan on kyseiset sidosryhmät otettava mukaan päätöksentekoon. Riskienkäsittelytapojen tehokkuus ja vaikutukset sidosryhmiin on huomioitava ja optimoitava. Riskin käsittely voi aiheuttaa seurausriskejä ja niiden tunnistaminen tulee ottaa osaksi riskinkäsittelymenetelmien valintaa ja seurannan tulee olla osa ris-

kinkäsittelysuunnitelmaa. Seurausriskejä ei tule käsitellä erillisinä, uusina riskeinä, vaan niiden yhteys alkuperäiseen riskiin tulee säilyttää riskienhallinnan kokonaisvaltaisuuden takaamiseksi. Riskin käsittelyn epäonnistuminen ja sitä kautta resurssien meneminen hukkaan on merkittävä riski joka tulee huomioida riskinkäsittelytapoja valittaessa. (SFS-ISO 31000:2009, 44; Smith & Politowski 2013, 106–109.)

Riskinkäsittelysuunnitelma sisältää valitut käsittelyvaihtoehdot ja niiden toteutuksen. Suunnitelman tulisi sisältää käsittelytapojen valintaperusteet, hyödyt, vaatimukset ja vastuutahot. Suunnitelma dokumentoi ehdotetut toimenpiteet, vaadittavat resurssit, sekä poikkeustilanteiden varalle tehdyt suunnitelmat. Riskien käsittelyn vaikuttavuuden seuranta vaatii erilaisten mittareiden ja valitsemista. Suunnitelmaan kirjataan myös riskienhallintatoimenpiteiden priorisointi, ajoitus ja aikataulu. Lisäksi kuvataan raportoinnin ja seurannan vaatimukset ja toteutustapa. (SFS-ISO 31000:2009, 44.)

Englanninkielisessä kirjallisuudessa viitataan usein riskien hallinnan neljään T-kirjaimeen, joilla tarkoitetaan riskin sietämistä (tolerate), käsittelyä (treat), siirtämistä (transfer) ja poistamista (terminate) (Hopkin 2012, 165–166). Riskien hallitsemisen keinoja voidaan jaotella myös niiden ajoituksen ja luonteen mukaan ennaltaehkäiseviin, korjaaviin, ohjaaviin ja havaitseviin kontrolleihin (Kuvio 5). Ennaltaehkäisevät kontrollit huomioivat riskin sen lähteellä ennen riskin realisoitumista ja havaitsevat kontrollit ovat seurauspainotteisia havaiten riskin seurauksia ja vaikutuksia organisaatiossa ja sen prosesseissa. Korjaavat ja ohjaavat kontrollit vaikuttavat riskin koko elinkaaren aikana. Ohjaaviin hallintakeinoihin kuuluu esimerkiksi työntekijöiden koulutus ja toimintaohjeiden laatiminen ja korjaaviin kontrolleihin luetaan muun muassa virheellisten työtapojen korjaaminen. (Hopkin 2012, 238–239.)




Kuvio 5. Riskienhallintakeinot (Hopkin 2012, 239).

Riskinhallintakeinoja valittaessa tulee kiinnittää huomiota kustannustehokkuuteen. Jos riskinhallintakeinojen kustannukset nousevat korkeammaksi, kuin riskin realisoitumisesta aiheutuvat kustannukset on arvioitava riskinhallintakeinojen kannattavuutta. Riskit on kuitenkin huomioitava laajasti muun muassa yhteiskuntavastuun, maineen ja henkilöturvallisuuden kannalta, jolloin riskin toteutumiselle on vaikeaa määritellä tarkkaa kustannusta. Riskin hallintaan käytetty rahasumma ja riskinkäsittelytoimenpiteiden tehokkuus eivät välttämättä ole suoraan verrannollisia, vaan organisaation on tunnistettava kustannustehokkaat kontrollit ja vältettävä ylimitoitettuja turvallisuusratkaisuja. (Hopkin 2012, 246.)

## 4.4 Seuranta ja katselmointi

Riskienhallintaprosessiin kuuluu jatkuvan kehittämisen mallin mukaisesti seuranta ja katselmointi, jonka tulee olla suunniteltu ja integroitu riskienhallintaprosessiin. Seurannan ja katselmoinnin vastuut ja velvollisuudet tulee olla määriteltynä ja sen toteuttaminen tulee olla järjestelmällistä ja organisaation muiden toimintojen kanssa yhteneväistä. Organisaation tulisi kehittää arviointiprosessi, jolla johto voi tunnistaa riskienhallinnan ja organisaation heikkoudet ja vahvuudet, sekä määrittää käsittelytapa, joilla tulevaisuuden toiminnasta aiheutuviin uusiin riskeihin varaudutaan ja suhtaudutaan. Riskienhallinnan tulisi olla ensisijaisesti etupainotteista, ennakoivaa aloitteellista toimintaa, joilla riskejä hallitaan niiden alkulähteillä ennen niiden toteutumista. Myös tapahtumien jälkitarkastelu on tärkeää ja organisaatiolla tulisi olla riittävät suunnitelmat realisoituneiden riskien käsittelyyn. Riskienhallinnan seurannan ja katselmoinnin toimenpiteillä saadaan organisaation johdolle ajantasainen ja tarkka kuva riskikentästä, jolloin riskien huomioiminen päätöksenteossa osana organisaation toimintaa on mahdollista. Seurantaa ja katselmointia tulee suorittaa riskienhallinnan jokaisella tasolla, osana jatkuvan kehittämisen prosessia. (Smith & Politowski 2013, 121–122.)

Riskienhallinnan seurannalla ja katselmoinnilla pyritään varmistamaan, että riskienhallinta on koko organisaation kattavaa ja hallintakeinot ovat riittäviä ja niillä pystytään vaikuttamaan merkittäviksi havaittuihin riskeihin. Tehokas seuranta tuottaa lisätietoa, jota voidaan käyttää riskienhallinnan kokonaisvaltaisessa kehittämisessä ja sillä saatetaan löytää uusia riskejä, joita tulee käsitellä organisaation riskienhallintaprosessien mukaisesti. Riskienhallinta vaikuttaa sisäiseen ja ulkoiseen toimintaympäristöön ja nämä muutokset ovat osana katselmointia. Seurannan ja katselmoinnin tuloksia voidaan käyttää hyväksi, kun riskienhallinnan puitteita suunnitellaan uudelleen. (SFS-ISO 31000:2009, 46.)

Johdon tärkeimmiksi työkaluiksi seurannassa ja katselmoinnissa nousee erityisesti riskienhallinnan jokaisessa vaiheessa tehdyt dokumentit ja tallenteet. Dokumentointi helpottaa sisäisten auditointien toteuttamista ja antaa johdolle mahdollisuuden analysoida erilaisia tapahtumia, mahdollisuuksia, onnistumisia ja epäonnistumisia. Organisaatio noudattaa määrittele-

määnsä riskienhallintasuunnitelmaa ja yksi katselmoinnin työkaluista onkin verrata suoritettuja riskienhallintatoimenpiteitä riskienhallintasuunnitelmaan ja – politiikkaan. Johto tarkastelee esimerkiksi onko suunnitelma kokonaisuudessaan otettu käyttöön suunnitellulla tavalla ja ovatko tavoitteet saavutettu ja edelleen sopivia. Riskienhallinnan tehokkuutta arvioidaan yleisellä tasolla ja erityisesti merkittävien riskien hallintakeinojen tehokkuuteen kiinnitetään huomiota. (Smith & Politowski 2013, 121–122.)

Seurantaan on olemassa erilaisia keinoja, joista osa on etupainotteisia, eli ennakoivia ja osa painottuu tapahtumien jälkitarkasteluun. Etupainotteisia seurannan työkaluja ovat esimerkiksi henkilöstökyselyt, joilla selvitetään työntekijöiden asenteita, läheltäpiti – tilanteiden tutkinta, johdon tarkastuskierrokset, tallenteiden ja laitteiden tarkastukset ja työntekijöiden koulutus, sekä sen tehokkuuden arviointi. Reaktiivisia keinoja ovat muun muassa tapahtumien tutkinta, suorituskyvyn mittaaminen ja sidosryhmien valitusten tarkkailu. Riskienhallinnan puitteissa määritellyt riskienhallinnan tehokkuuden mittarit ovat johdon työkaluja seurannassa ja katselmuksessa ja niistä saadaan tietoa siitä, mikä on organisaation nykytila ja miten se on kehittynyt riskienhallintaprosessin käyttöönoton jälkeen. (Smith & Politowski 2013, 121-127.)

### 4.5 Riskienhallintaprosessin tallenteet

Riskienhallintaprosessin todentamiseksi ja jäljitettävyyden takaamiseksi tulee siitä laatia riittävät tallenteet. Tallenteet luovat perustan myös riskienhallinnan jatkuvalle kehittämiselle. Minimivaatimuksena riskienhallinnan tallenteille on viranomaisten ja lain asettamat vaatimukset, mutta tallenteiden laatu ja määrä vaihtelee organisaation toiminnan mukaan. Organisaation tulee arvioida tallenteiden luomisesta ja ylläpidosta aiheutuvat kustannukset, sekä määrittää tallenteiden säilytysaika ja arkaluontoisuus. Organisaatio määrittä kuinka ja kuka tallenteita pääsee tarkastelemaan ja mitä tallennusvälineitä kunkin tallenteen luomiseen käytetään. (ISO 31000:2009, 46.)

ISO 31000–standardi esittää laadittavaksi seuraavanlaiset dokumentit:

- Riskienhallinnan puitteet
- Riskienhallintasuunnitelma
- Riskienhallinnan puitteiden toteuttamisen aikataulu ja strategia
- Riskienhallintapolitiikka
- Riskienhallinnan tavoitteet
- Sisäisen ja ulkoisen toimintaympäristön määrittäminen
- Viestintää ja tiedonvaihtoa koskeva suunnitelma
- Riskienhallinnan puitteiden seuranta ja katselmointi

- Riskienhallintaprosessin toimintaympäristön määritteleminen
- Riskikriteerien määritteleminen
- Riskien tunnistaminen
- Riskianalyysi

ISO 31000:2009-standardin mukaan riskienhallintaa toteuttavan organisaation tulisi kuitenkin huomioida, että riskienhallinnasta laadittavat dokumentit eivät ole itseisarvo, eivätkä hyvin laaditut dokumentit takaa toimivaa riskienhallintajärjestelmää. Dokumenttien tulee kuvata olemassa olevia prosesseja ja luoda realistisia suuntalinjoja organisaation riskienhallinnan kehittämiselle. ISO 31000:2009:n mukainen kokonaisvaltainen riskienhallinta vaikuttaa organisaation jokaisella tasolla ja sen vaikuttavuus varmistetaan johdon sitoutumisella. Riskienhallinnalle tulee määrittää vastuutahot ja riskeille omistajat, joilla on riittävät valtuuden riskienhallintatoimenpiteiden toteuttamiseen.

Organisaation henkilöstön suhtautuminen riskienhallintaan ja riskin omistajuus on kannattavaa valita työnkuvan ja valtuuksien mukaan, jolloin henkilön roolissa organisaatiossa ja riskienhallinnassa ei ilmene ristiriitaa. Organisaation ylimmän johdon vastuulla on riskienhallinnan strategia ja riskienhallinnan perustan luominen. Ylimmän johdon tulee huomioida merkittävimmät riskit päätöksenteossa ja johtamisessa, jolloin riskienhallintaa on helpompaa ulottaa organisaation jokaiselle tasolle. Kun ylin johto asettaa selkeät tavoitteet ja strategian riskienhallinnan toteuttamiselle on linjajohdon mahdollista toteuttaa ja kehittää riskienhallintaa omassa toimintaympäristössään. Linjajohto toimeenpanee ylemmän johdon asettamia riskienhallinnan toimenpiteitä ja laatii toimintaohjeita henkilöstölleen. Linjajohdon tulee myös kerätä tietoa henkilöstöltä ja viestiä siitä ylemmälle johdolle.

Riskienhallintajärjestelmää voidaan soveltaa mihin tahansa organisaatioon ja sen toimintoihin niiden osiin. Yksi riskienhallinnan perusperiaatteista on, että sen tulee tuottaa organisaatiolle lisäarvoa. Lisäarvon tuottaminen riskienhallinnan kautta on mahdollista monella eri tavalla. Hyvin toteutettu riskienhallinta lisää organisaation toimintavarmuutta, auttaa toipumaan kriisistä ja lisäksi se voi olla kilpailuetu. Kun organisaatioon kohdistuviin uhkiin pystytään varautumaan ja mahdollisuuksia pystytään hyödyntämään, ovat puitteet toiminnan jatkuvuudelle kohdallaan.

# 5 Yhteenveto ja tuotokset

Kirjallisuuskatsausten yhteenvetona laadittiin seuraavissa kappaleissa esitetyt tuotokset, jotka käsittelevät organisaation toimia uudistetun standardin käyttöönotossa. Tarkasteltaessa velvoittavia riskienhallinnan vaatimuksia ISO 9001:2015:n mukaisen laadunhallintajärjestelmän viitekehyksessä, nousee esiin toimintaympäristön määrittelyn keskeisyys sekä laadunhal-

lintajärjestelmän että riskienhallinnan lähtökohtana. Kappaleessa 5.1 kuvataan yleisellä tasolla organisaation toimia laadunhallintajärjestelmää uudistaessa, ja kappaleessa 5.2 ohjataan toimintaympäristön määritettely PESTLE ja SWOT-menetelmiä yhdistävän työkalun avulla.

## 5.1 Siirtymävaiheen toimenpiteet ISO 9001:2008:sta

ISO 9001:2015:een siirtyminen edellyttää organisaatiolta kykyä tunnistaa laadunhallintajärjestelmänsä aukot uuteen revisioon peilaten ja laatia näiden täyttämiseen toteutussuunnitelma. Laadunhallintajärjestelmän tavoite on tuottaa asiakastyytyväisyyttä ja vaatimusten mukaisia lopputuotteita. Tätä samaa tavoittelee jo organisaation olemassa oleva ISO 9001:2008:n mukainen laadunhallintajärjestelmä, mutta riskienhallinnan keinoilla voidaan löytää uusia keinoja tavoitteen varmempaan ja ennustettavampaan saavuttamiseen.

Organisaation on tunnistettava, suunniteltava ja toteutettava sidosryhmien ja henkilöstön koulutus- ja tiedotustarpeet muutoksia koskien. Tämä koskee myös kaikkia organisaation muita johtamisjärjestelmiä, mikäli niillä on kytköstä laaduntuotantokykyyn. ISO 9001:2015 on ensimmäisiä uudistettua hallintajärjestelmärakennetta noudattavia standardeja (Croft 2012) ja on siten entistä yhteensopivampi ja linjakkaampi muiden ISO-tuoteperheen hallintajärjestelmästandardien kanssa. Eri järjestelmien integraatio helpottuu, kun velvoittavat vaatimukset ovat kohdakkain jo sisällysluettelotasolla.

Riskienhallintaa koskettavat velvoittavat vaatimukset ISO 9001:2015:n viitekehyksessä on esitetty taulukossa 3. Vaatimuksissa korostuu toimintaympäristön määrittelyn tärkeys.

| Lausake | Otsikko | Vaatimus |
|---|---|---|
| 4 | Toimintaympäristö | Organisaation on määritettävä toimintaympäristöön ja sen muutoksen liittyvät riskit. |
| 5 | Johtajuus | Organisaation johdon on sitouduttava edellisen lausakkeen toimeenpanoon. |
| 6 | Laadunhallintajärjestelmän suunnittelu | Organisaation on laadunhallintajärjestelmän suunnittelussa tunnistettava ja huomioitava riskit ja mahdollisuudet. |

| | | |
|---|---|---|
| 8 | Toiminta | Organisaation on jalkautettava prosessit riskien ja mahdollisuuksien tunnistamiseksi toiminta-prosesseissa. |
| 10 | Parantaminen | Organisaation on kehityttävä vastaamalla riskeissä tapahtuviin muutoksiin. |

Taulukko 3. Riskienhallinnan velvoittavat vaatimukset ISO/DIS 9001:2014:n mukaan.

ISO 9001:2015:n edellyttämät muutokset voidaan saattaa organisaatiossa voimaan jatkuvan parantamisen silmukan kautta, mutta usein eriävät prosessien kiertoajat puoltavat muutosten johtamista erillisenä hankkeena. Loogisena alkupisteenä muutostyölle on kappaleessa 5.2 yksityiskohtaisesti kuvailtu toimintaympäristön määrittely sekä johdon sitouttaminen riskienhallintaprosesseihin. Tämä lähtökohta on tarkoituksenmukaista sisällyttää sekä laatupolitiikkaan että riskienhallintapolitiikkaan.

Käytännössä tämä tarkoittaa että organisaatio tunnistaa laadunhallinnan prosessin kriittiset pisteet ja omistajat. Tämä on tehty jo ISO 9001:2008 prosessikuvauksia laatiessa, mutta saattaa olla hedelmällistä tarkastella niitä uudestaan riskiperustaisesta näkökulmasta. Viime kädessä johto vastaa siitä että organisaation kaikilla tasoilla joko on tai niille luodaan resurssit riskiperustaisen lähestymistavan ulottamisesta toimintaprosesseihin, niiden suunnitteluun ja mittaamiseen. Tällä voidaan osaamispohjasta riippuen tarkoittaa esimerkiksi tiedottamista, kouluttamista tai kolmannen osapuolen osoittamista riskienhallintaan.

Kullakin toiminnan tasolla laaditaan riskienhallintasuunnitelma, joka vastaa riskeihin myös laadunhallintajärjestelmän näkökulmasta. Tällöin ei ole perusteltua rajata työtä vain laadunhallinnan riskeihin, vaan käyttää hyödyksi laadittuja prosesseja kokonaisvaltaisen riskienhallinnan näkökulmasta. Täten voidaan parhaassa tapauksessa vapauttaa resursseja ja eliminoida päällekkäisiä prosesseja, joiden rajaus ja tuotos olisi periaatteessa sama mutta erot näkökulmassa. Onnistuminen tässä edellyttää hyvää koordinaatiota, mutta voi vahventaa sekä laatuajattelua että riskiperustaista ajattelua organisaatiossa.

Liitteessä 3 on lueteltu pelkistetysti ISO 9001:2015:n mukaisen laadunhallintajärjestelmän dokumentaation vähimmäisvaatimukset, joihin organisaatio voi peilata nykyisen laadunhallintajärjestelmänsä dokumentaatiota ja tunnistaa muutoksia vaativat osa-alueet.

## 5.2 Organisaation toimintaympäristön määrittely

Sekä ISO 9001 että ISO 31000-standardit vaativat organisaation viitekehyksen määrittelemistä riskienhallinnan ja laadunhallinnan järjestelmien integroimiseksi olemassa oleviin prosesseihin ja organisaation osiin. Organisaation viitekehyksellä tarkoitetaan kaikkia niitä tekijöitä, jotka vaikuttavat organisaation toimintaan ja joihin organisaatio voi toiminnallaan vaikuttaa. Organisaation viitekehyksen määrittäminen on hyvä lähtökohta kaikkeen organisaation toimintamenetelmien uudistamista koskevaan työhön, sillä se auttaa ymmärtämään uudistusten vaikutukset ja hallitsemaan niistä aiheutuvia riskejä. Organisaation toimintaympäristö ja sidosryhmät ovat jatkuvasti muuttuvia tekijöitä, joiden huomioiminen on osa organisaation hyvää johtamistapaa. Näiden tekijöiden tarkkailu ja arviointi tulisi olla jatkuvaa riittävän vaikuttavan huomioimisen takaamiseksi.

### 5.2.1 Toimintaympäristön ymmärtäminen ja määritteleminen

Organisaatioilla on erilaisia ulkoisia ja sisäisiä toimintaympäristöjä, jotka tulee huomioida ISO 9001 ja ISO 31000-standardien käyttöönotossa. Toimintaympäristöt muuttuvat jatkuvasti ja organisaation on tärkeää havaita kehityssuunnat ja reagoida niihin, jotta muutoksesta johtuvat riskit saadaan hallittua. Toimintaympäristöjen määrittelemisessä auttaa ulkoisten ja sisäisten sidosryhmien tunnistaminen ja hallinta. Yrityksen toimintaympäristön määrittelemisessä voidaan käyttää niin kutsuttua PESTLE-analyysiä. PESTLE on akronyymi sanoista political, economical, social, technological, legal ja environmental. Toimintaympäristön tarkastelussa huomioidaan siis poliittiset, taloudelliset, sosiaaliset, teknologiset, lainsäädännölliset ja ympäristön näkökulmat. (Pestleanalysis 2015.)

Poliittisella toimintaympäristöllä tarkoitetaan ensisijaisesti sitä hallintoa, jonka alaisuudessa organisaatio toimii. Verotus, tulli ja kaupparajoitukset ovat tekijöitä, jotka ohjailevat vahvasti organisaation toimintaa ja joiden muutoksiin vastaaminen on yrityksen kannalta tärkeää. Esimerkkinä poliittisen toimintaympäristön muutoksesta voidaan pitää vuonna 2014 EU:n Venäjään kohdistamia pakotteita, jotka vaikuttivat myös Suomessa toimiviin yrityksiin Venäjän viennin osalta (Ulkoministeriö 2014a). Venäjän asettamat vastapakotteet ja esimerkiksi EU:n alueelta tulevien elintarvikkeiden tuontikielto aiheutti suomalaisille yrityksille mittavia sopeutumistoimenpiteitä (Ulkoasiainministeriö 2014b). Poliittinen toimintaympäristö voi vaikuttaa merkittävästi taloudelliseen toimintaympäristöön. Sisäisessä toimintaympäristössä poliittinen näkökulma voi tarkoittaa esimerkiksi hallintotapaa ja organisaatiorakennetta. Kenellä on vastuu mistäkin osa-alueesta ja mitkä ovat organisaation toimintaperiaatteet. (Pestleanalysis 2015; SFS-ISO 31000:2009, 28.)

Taloudellisella toimintaympäristöllä PESTLE-analyysissä tarkoitetaan taloudellisia tekijöitä jotka vaikuttavat suoraan organisaation toimintaan. Talouskasvu, inflaatio, deflaatio, valuuttakurssit ja korkotaso ovat talouden tekijöitä ja ilmiöitä jolla saattaa olla pitkäkestoisia vai-

kutuksia organisaatioiden ja kuluttajien ostovoimaan, sekä kysyntään ja tarjontaan. Sisäisen toimintaympäristön määrittelyssä taloudellisia näkökulmia on esimerkiksi resursseihin ja tietämykseen liittyvät asiat. Sosiaalisen toimintaympäristön määrittelemisessä otetaan huomioon muun muassa trendit ja muoti. Sosiaaliseen toimintaympäristöön liittyy myös erilaiset sesongit, sekä yhteiskunnan ja erityisesti organisaation sidosryhmien sosiaalisen rakenteen määrittely. Esimerkiksi asiakaskohderyhmien ja alihankkijoiden arviointi on tavallista, mutta organisaatio voi hyötyä myös sisäisten sidosryhmien tarkastelusta. Teknologia kehittyy jatkuvasti ja muutokset tuovat sekä uhkia, että mahdollisuuksia organisaatioille. Riippuvuus teknologiasta on organisaatiokohtaista. Vaikka organisaatio ei olisi vahvasti riippuvainen teknologiasta, on hyödyllistä selvittää mitä hyötyä teknologian kehittymisestä voisi organisaation toiminnalle olla. Sisäisessä toimintaympäristössä teknologianäkökulma voi tarkoittaa esimerkiksi tietojärjestelmiä ja käytössä olevia laitteita. (Pestleanalysis 2015; SFS-ISO 31000:2009, 28.)

Lainsäädännön näkökulma sisältää ulkoisen ja sisäisen sääntelyn näkökulmat. Organisaatio toimii lain, asetusten ja viranomaismääräysten vaikutuksen alaisuudessa, mutta sillä saattaa olla myös sisäisiä sääntöjä ja vaatimuksia, joiden määritteleminen kuuluu toimintaympäristön määrittelyyn. Sisäisessä toimintaympäristössä sääntely voi ilmetä sopimuksissa, käyttöönotetuissa standardeissa ja ohjeissa. Ympäristönäkökulma huomioi ekologisuuden, ilmastonmuutoksen, saasteet ja muut luonnonsuojeluun liittyvät asiat, mutta ei kuitenkaan rajoitu siihen. Ympäristöön kuuluu myös rakennettu ympäristö, lähialueen ihmiset ja muut tekijät, joihin organisaation toiminta vaikuttaa tai jotka voivat suoraan vaikuttaa organisaatioon. (Pestleanalysis 2015; SFS-ISO 31000:2009, 28.)

PESTLE-analyysi toteutetaan keräämällä organisaation toimintaa tuntevilta henkilöiltä ajatuksia jokaiseen näkökulmaan. Ajatukset voidaan kerätä työryhmässä post-it lapuilla, joita jaotellaan PESTLE-analyysin osa-alueiden mukaisesti. Näkökulmissa saattaa olla päällekkäisyyksiä ja yhteneväisyyksiä, joten irrallisilla lapuilla olevien ajatusten uudelleen jaottelusta ja ryhmittelystä on hyötyä organisaation toimintaympäristön määrittelemisessä. Työryhmän on syytä ottaa kantaa myös siihen, liittyvätkö löydetyt tekijät sisäiseen vai ulkoiseen toimintaympäristöön.

Ajatus PESTLE ja SWOT menetelmiä yhdistelevästä toimintaympäristön määrittelytyökalusta syntyi Hopkinin teoksessa mainitusta tavasta jaotella riskejä hyödyntämällä näitä kahta työkalua tai niiden yhdistelmää (Hopkin 2011, 157). Samaa työkalua voitaisiin käyttää toimintaympäristön ymmärtämiseksi tarkemmin toteuttamalla SWOT-analyysi PESTLE-analyysin osa-alueista. Nelikenttäisessä SWOT-analyysissä arvioidaan tarkasteltavan kohteen sisäisiä vahvuuksia (strengths), heikkouksia (weaknesses), ulkoisia mahdollisuuksia (opportunities) ja uhkia (threats). Nelikenttäisen SWOT-analyysin löydettyjä vahvuuksia, heikkouksia, mahdollisuuksia ja uhkia voidaan toimintaympäristön määrittelyvaiheessa käsitellä määrittelemällä

keinoja jolla organisaatio voi hyödyntää vahvuuksia ja mahdollisuuksia, varautua uhkiin, korjata heikkouksia, sekä välttää ja torjua ulkoisista uhkien ja sisäisten heikkouksien yhdistelmiä. (Kuvio 6.) Näin toimintaympäristöstä saadaan tarkka ja kattava kuva, jota voidaan hyödyntää sekä laadun, että riskien hallintaan liittyvissä kysymyksissä ja määrittelyissä. Liitteessä 1 on kuvattuna tapa hyödyntää nelikenttäistä SWOT-analyysiä organisaation toimintaympäristön määrittelyssä. (Koskinen 2006, 74-76.)

| | Hyödylliset | Haitalliset |
|---|---|---|
| **Sisäiset** | Vahvuudet | Heikkoudet |
| **Ulkoiset** | Mahdollisuudet | Uhat |

| | Vahvuudet | Heikkoudet |
|---|---|---|
| **Mahdollisuudet** | Hyödynnä | Korjaa/kehitä |
| **Uhat** | Varaudu/ennakoi | Vältä/torju |

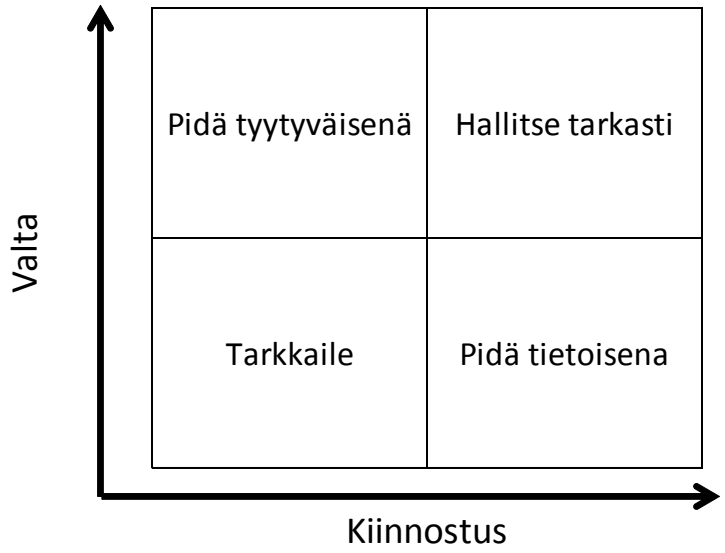
Kuvio 6. SWOT – analyysi (Koskinen 2006, 74-76).

### 5.2.2 Sidosryhmät

Organisaation tulee selvittää tärkeimmät sidosryhmänsä ja tiedottaa riskienhallinnasta ja sen eduista. SFS-ISO 31000 (2009, 16) määrittelee sidosryhmän tahona, joka voi vaikuttaa organisaation toimintoihin tai joihin organisaation toiminta voi vaikuttaa. Standardi huomioi myös, että vaikka organisaatio ei todellisuudessa vaikuta tiettyyn tahoon suoraan, voi tämä henkilö tai organisaatio kokea olevansa toiminnan vaikutuksen piirissä. Hopkin (2012, 284) jakaa tyypillisen organisaation sidosryhmät kuuteen ryhmään; asiakkaat, henkilökunta, rahoittajat, tuotteiden ja palveluiden toimittajat, sääntelijät ja yhteiskunta. Organisaation kannalta sidosryhmät voivat olla toivottuja tai ei-toivottuja riippuen siitä, mikä suhde sidosryhmällä on organisaatioon ja sen toimintaan. Näiden eri sidosryhmälajien tunnistaminen on hyödyllistä ja auttaa arvioimaan sidosryhmistä johtuvia ja niihin kohdistuvia riskejä. Riskienhallinnasta ja sen eduista tiedottaminen sidosryhmille lisää avoimuutta ja toimintojen läpinäkyvyyttä.

Osa sidosryhmistä tunnistetaan organisaation toimintaympäristön määrittelyssä. Jos sidosryhmiksi katsotaan kaikki ihmiset ja organisaatiot, joihin oma organisaatio tai sen toiminnot voivat vaikuttaa, kasvaa sidosryhmien piiristä usein liian suuri ja vaikeasti hallittava. Organisaation kannalta on siis tärkeää rajata sidosryhmien tarkkailua ja löytää tärkeimmät sidosryhmät tarkasteltavan osa-alueen kannalta. Sidosryhmiä voidaan tarkastella koko organisaation kannalta, tietyn projektin kannalta tai käyttäen hyväksi PESTLE-analyysiä. Tärkeintä on tunnistaa sidosryhmät, joilla on eniten valtaa vaikuttaa organisaation toimintaan. Lisäksi on huomioita-

va sidosryhmät, joilla ei ole välttämättä suurta valtaa, mutta jotka ovat kiinnostuneet organisaation toiminnasta.




Kuvio 7. Sidosryhmien luokittelu (Mindtools 2015).

Kuvio 8 kuvaa tapaa luokitella sidosryhmien tärkeyttä ja ohjata organisaation suhtautumista niihin. Alhaisimmalla merkittävyyden tasolla ovat sidosryhmät, jotka eivät ole kovinkaan kiinnostuneita organisaatiosta ja joilla on vain vähäistä valtaa organisaatiota kohtaan. Näitä sidosryhmiä on hyvä tarkkailla, mutta niitä ei tarvitse hallita kovinkaan tarkasti. Organisaation on hyvä tiedostaa näiden sidosryhmien olemassaolo, jotta näiden tahojen osallistamiseen käytetyt resurssit voidaan ohjata tärkeämpien sidosryhmien huomioimiseen. Näille sidosryhmille viestiminen on syytä pitää vähäisenä. Sidosryhmät joilla on vähäistä valtaa, mutta jotka ovat kiinnostuneita organisaatiosta, ovat tiedottamisen ja viestinnän kannalta tärkeitä. Näitä sidosryhmiä voivat olla esimerkiksi pienet yksittäiset osakkeenomistajat ja potentiaaliset asiakkaat. Organisaatio voi viestiä toiminnastaan näille sidosryhmille erilaisia kanavia käyttäen. On tärkeää huomata, että sidosryhmien sijainti kuvaajassa voi muuttua nopeastikin. Esimerkiksi jos potentiaalisen yritysasiakkaan kanssa tehdään tärkeä sopimus, sen valta organisaatioon nähden voi kasvaa merkittävästi. (Mindtools 2015.)

Sidosryhmät joilla on paljon valtaa mutta vähäinen kiinnostus on kuvaajassa määritettynä tyytyväisenä pidettäväksi sidosryhmäksi. Tällaisia sidosryhmiä voivat olla esimerkiksi tietyt viranomaiset tai asiakkaat. Nämä tahot saattavat vaatia vain vähäisen määrän viestintää ja ovat kiinnostuneita organisaatiosta vain tietyissä tapauksissa. Näiden sidosryhmien huomioiminen on kuitenkin tärkeää, sillä niillä on valtaa vaikuttaa organisaation toimintaan. Merkittävimmät sidosryhmät ovat niitä, joilla on paljon valtaa ja jotka ovat myös erittäin kiinnostuneita organisaatiosta. Näitä sidosryhmiä voivat olla muun muassa media, suuret asiakkaat se-

kä tärkeät osakkeenomistajat. Näille ryhmille viestiminen ja tiedonanto on erittäin tärkeää. Organisaation tulee hallita nämä ryhmät tarkasti ja olla tietoinen niiden olemassaolosta ja vaikutuksista organisaatioon. (Mindtools 2015.)

### 5.2.3 Toimintaympäristön määrittelytyökalun käyttö

Koska ISO 9001:2015 ja ISO 31000-standardit vaativat kumpikinen organisaation toimintaympäristön määrittelemistä, on se luonnollinen lähtökohta laadunhallintajärjestelmän päivittämiselle. Organisaatio kokoaa työryhmän jolla on mahdollisimman laaja-alainen näkemys ja kokemus organisaation toiminnasta ja sen vaikutuksista toimintaympäristöön. Toimintaympäristön määrittelemiseen ja tarkasteluun käytetään PESTLE-analyysin ja SWOT-analyysin yhdistelmää (Liite 1). Näin saatu kuva toimintaympäristöstä ja sen luomista uhista ja mahdollisuuksista saadaan tarkasteltua organisaation vahvuuksien ja heikkouksien viitekehyksessä. SWOT-analyysiä voidaan jatkoarvioida tutkimalla tekijöitä joita organisaation tulee hyödyntää, kehittää tai välttää ja niitä tekijöitä, joihin organisaation tulee varautua (Liite 2). Opinnäytetyötä varten kehitellyt taulukkomuotoiset mallipohjat on tarkoitus tulostaa A3 kokoiselle paperiarkille. Toimintaympäristön työkalun ohjeistus on laadittu opiskelijoiden toimesta ja perustuu kirjallisuuskatsaukseen sekä Hopkinin teoksessa mainittuun riskien luokittelutapaan. (Hopkin 2011, 157.)

Työryhmä aloittaa aivoriihimäisen työskentelyn keräämällä ajatuksia esimerkiksi irrallisilla uudelleenliimattavilla paperilapuilla liitteessä 1 kuvattuun analyysikenttään. Paperilappujen etuna on niiden siirreltävyys ja mahdollisuus jäsennellä niitä uudelleen. Ideoita voidaan kerätä liittyen johonkin PESTLE:n osa-alueeseen tai taulukon ulkopuolelle jatkotarkastelua varten. Näin saadaan tunnistettua erilaisia tekijöitä yrityksen toimintaympäristöön liittyen. Ensimmäisessä vaiheessa pyritään keräämään mahdollisimman paljon ideoita, eikä niiden jäsentäminen ole ensisijaista. Aivoriihityöskentelyssä esiin tulleita ajatuksia ei myöskään kritisoida vaan kaikki otetaan huomioon seuraaviin vaiheisiin siirryttäessä.

Seuraavassa vaiheessa kerättyjä ajatuksia jäsennellään ja ryhmitellään tarkemmin. Työryhmä pyrkii löytämään tekijöitä, jotka sopivat yhteen tai useampaan PESTLE-SWOT-taulukon (liite 1) alueisiin. Uusia lappuja voidaan kirjoittaa edelleen. Seuraavassa vaiheessa hyödynnetään liitteessä 2 esiteltyä taulukkoa, jossa organisaation vahvuus ja heikkoustekijöitä tarkastellaan ulkoisia uhkia ja mahdollisuuksia vasten. Työryhmä etenee ruudukko kerrallaan ja määrittelee yhteneväisyyksiä ja vaikutussuhteita eri tekijöiden välillä. Työryhmä vastaa muun muassa seuraaviin kysymyksiin: miten mahdollisuuksia voidaan hyödyntää organisaation vahvuuksien avulla? Miten ulkoisia mahdollisuuksia voidaan käyttää organisaation heikkouksien parantamiseen ja kehittymiseen? Miten organisaatioon kohdistuviin uhkiin voidaan varautua organisaation

vahvuuksia hyödyntäen? Minkälaisia vältettäviä tilanteita ulkoiset uhat ja organisaation heikkoudet voivat aiheuttaa?

Edellä mainittuihin kysymyksiin vastataan poliittisen, taloudellisen, sosiaalisen, teknologisen ja lainsäädännöllisen toimintampäristön, sekä ympäristön näkökulmista. Ajatuksia kerätään edelleen liikuteltaville ja jäsenneltäville lapuille. Kun työryhmä on saanut riittävän laajan kuvan kustakin PESTLE-analyysin osa-alueesta, siirrytään tutkimaan syy- ja seuraussuhteita ja tapoja joilla eri toimintaympäristön tekijät vaikuttavat toisiinsa. Työryhmä laatii työskentelystään raportin, joka voidaan liittää osaksi ISO 9001:2015 ja ISO 31000-standardien mukaista toimintaympäristön määrittelyä.

# 6 Johtopäätökset ja itsearviointi

Laadunhallintajärjestelmän voidaan todeta toimivan organisaatiossa ennaltaehkäisevänä työkaluna (ISO/DIS 9001:2014, 45), kuten riskienhallinnankin. Yksi ISO 9001:2015–uudistuksen keskeisistä muutoksista on systemaattinen lähestymistapa riskeihin, kun taas edellisissä versioissa riskejä on käsitelty erillisenä osa-alueena. Riskejä tulee hallita koko prosessin ajan ja riskienhallinnan vaikuttavuutta tulee seurata ja parantaa hyödyntämällä jatkuvan parantamisen periaatetta. Riskienhallinta, kuten laadunhallintakaan ei saa olla erillinen saareke, vaan se tulee integroida kaikkiin organisaation toimintoihin.

Riskienhallintaa ei ISO 9001:2015:n näkökulman mukaan katsota tukiprosessiksi tai laadunhallintajärjestelmän ulkopuolikseksi vaikuttajaksi; se on sisällytetty kategorisesti kaikkeen organisaation tekemiseen, joka koskettaa laatua. Organisaation on ymmärrettävä paitsi sidosryhmien odotukset laadulle, sen on myös tunnistettava ja hallittava sidosryhmistä riippuvaiset omaan laaduntuotankokykyyn kohdistuvat riskit. ISO 9001:2015 edellyttää organisaatiolta systemaattista riskienhallintaa, jonka keinoin voidaan varmistua laadunhallintajärjestelmän kyvystä saavuttaa ja ylläpitää siltä edellytetty laaduntuotantokyky, eli vastata organisaation asettamiin laatutavoitteisiin.

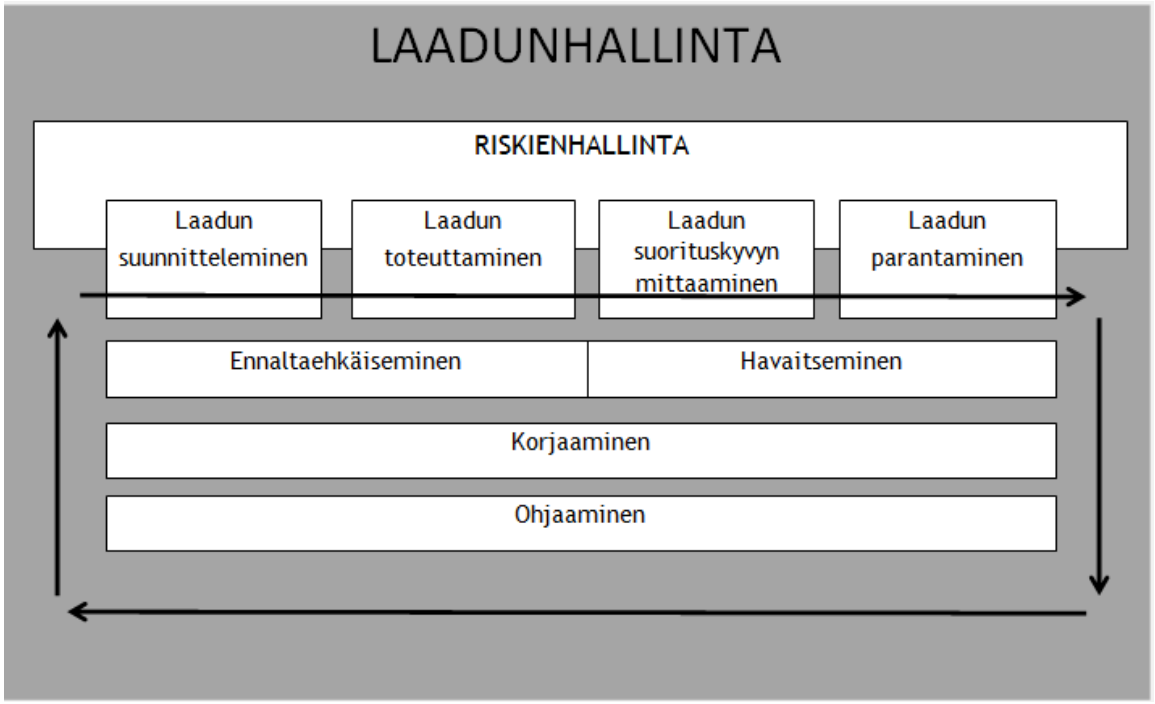
ISO 9001–standardin vuonna 2008 julkaistu versio on suosittu, laajalle levynnyt ja hyvin tunnettu tapa kehittää organisaation laadunhallintaa. Vuosina 2012 ja 2013 ISO 9001-sertifikaatteja myönnettiin globaalisti eri organisaatioille yli kaksi miljoonaa kappaletta vuosittain (ISO 2015). Maailmanlaajuisesti tunnetusta standardista on etua, kun ollaan tekemisissä ulkomaisten asiakkaiden tai muiden sidosryhmien kanssa. Laatusertifikaatti luo luotettavan kuvan organisaatiosta ja sen tuotteista tai palveluista. ISO 9001:2008-sertifikaatit vanhentuvat kolmen vuoden kuluttua uuden ISO 9001:2015 revision julkaisemisen jälkeen, joten laatuhallintajärjestelmäsertifioitujen organisaatioiden on lähitulevaisuudessa pohdittava voimassa olevan sertifikaatin merkitystä toiminnalle (IAF 2015). ISO 9001:2015:n tehokkaalla käyttöön-

otolla pystytään lisäämään asiakastyytyväisyyttä laadun parantamisen kautta ja sen vaikutuksesta liiketoiminnan positiivisena kehittymisenä ja kannattavuuden parantumisena on myös tutkimuksellista näyttöä (Knowles 2011, 39).

Riskienhallinnan tulee integroitua laadunhallintajärjestelmän toimintaprosesseihin, ja sen suorituskykyä on kyettävä arvioimaan. Riskienhallinnan vaikuttavuuden takaamiseksi se on hyödyllistä tehdä ISO 31000:n vaatimusten mukaisesti, jolloin riskienhallinnasta saadaan myös dokumenttinäyttöä ja sitä pystytään mittaamaan ja tarkkailemaan. Jos ISO 31000:2009 :n mukaista riskienhallintajärjestelmää tarkastelee itsenäisenä osana johtamisjärjestelmää, sen yhdeksi tärkeimmäksi vahvuudeksi nousee väistämättä sen sovellettavuus; sitä voidaan hyödyntää julkisten ja yksityisten yritysten, järjestöjen, ryhmien ja yksittäisten henkilöiden tarpeisiin. ISO 31000:2009:n mukaista riskienhallintaa voidaan käyttää hyödyksi näiden organisaatioiden päätöksenteossa, toimenpiteissä, prosesseissa, projekteissa, tuotteissa, palveluissa sekä organisaation voimavarojen hallinnassa. (Moeller 2011, 331–334; SFS-ISO 31000 2009, 4-12.) Kuten ISO 9001-standardi, myös ISO 31000 on globaalisti tunnettu ja sen käyttöönotosta voi olla kilpailuetua niin kotimaan markkinoilla, kuin kansainvälisestikin. Organisaation jokaisella tasolla toteutettu riskienhallinta lisää organisaation luotettavuutta ulkoisten sidosryhmien tarkastelussa ja luo organisaatiolle ja sen toiminnan jatkuvuudelle vakaan pohjan.

Riskienhallinta tulee ISO 9001:2015:n mukaan huomioida laadunhallintajärjestelmän soveltamisalan mukaisten prosessien suunnittelussa. Riskienhallinnan ulottaminen jokaiseen toimintaprosessiin vahvistaa entuudeestaan organisaation laaduntuotantokykyä ja parhaimmillaan myös sen jatkuvuutta. Riskienhallinta laadunhallintajärjestelmän osana vapauttaa resursseja ja eliminoi päällekkäisiä prosesseja, joiden rajaus ja tuotos saattaisi olla periaatteessa sama mutta erot näkökulmassa. Onnistuminen tässä edellyttää hyvää koordinaatiota, mutta voi vahventaa sekä laatuajattelua että riskiperustaista ajattelua organisaatiossa. Kun riskiperustainen näkökulma on tietoisesti läsnä ja sitä edellytetään kaikissa prosesseissa, se on mahdollistanut ”Ennaltaehkäisevät ja korjaavat toimenpiteet”-kappaleen poistamisen standardista; sen konsepti ilmentyy riskiperustaisen näkökulman kautta.

Kuviossa 8 esitettyjen laadunhallinta- ja riskienhallintajärjestelmien integraatio on organisaatiolle hyödyllistä, sillä ne kumpikin hyödyntävät samaa prosessien vuorovaikutusmallia ja perustuvat Demingin ympyrän mukaiseen PDCA-malliin. Opinnäytetyössä esitetty tapa luokitella riskienhallintakeinoja ennaltaehkäiseviin, korjaaviin, ohjaaviin ja havaitseviin keinoihin on mahdollista liittää luontevasti myös laadunhallintajärjestelmän prosesseihin, ja osaltaan riskiperustainen näkökulma mahdollistaa organisaatiolle joustavamman ja mukautuvamman laadunhallintajärjestelmän toteuttamisen, sillä se on ISO/DIS 9001:2014 mukaan vähentänyt ohjailevien vaatimusten määrää, ja siirtänyt painotusta suorituskykyperustaisten vaatimusten suuntaan.




Kuvio 8. ISO 9001:2015 laadunhallintajärjestelmän ja ISO 31000:2009 riskienhallinnan prosessien integraatio.

Sekä laadunhallinnan että riskienhallinnan näkökulmasta osoittautui oleelliseksi toimintaympäristön seikkaperäinen ja kattava määrittely. Riskienhallintaa integroiva, prosessiajatteluun perustuva laadunhallintajärjestelmä hyötyy organisaation pyrkimyksistä ylläpitää ajanmukaista ja ajoittain rohkean ennakoivaakin toimintaympäristön tilannekuvaa.
Hyvin koordinoidut ja mahdollisimman saumattomasti toteutetut riskienhallinnan ja laadunhallintajärjestelmän ratkaisut osana organisaation johtamisjärjestelmää tukevat toisiaan ja ilmentävät kokonaisvaltaisen riskienhallinnan ydinajatusta.

Laadun- ja riskienhallintajärjestelmien laaja ymmärrys auttaa organisaatiota viemään toimintojaan suuntaan, jossa nämä johtamisjärjestelmän osatekijät ovat saumattomasti integroituna organisaation kaikkiin prosesseihin. Opinnäytetyöhön valitut standardit antavat hyvän perusrungon näiden järjestelmien luomiselle ja vapautta toteuttaa järjestelmien käyttöönotto organisaation erityispiirteisiin parhaiten sopivalla tavalla. Ne eivät kuitenkaan ole ainut tai edes välttämättä paras tapa hoitaa organisaation laadun- ja riskienhallinnan tarpeita. ISO-standardien käytössä etuna on kuitenkin se, että ne ovat laajalti käytössä ja tunnettuja. Tämä edesauttaa organisaation toimintojen yhtenäistämistä monien muiden organisaatioiden kanssa.

Itsearviointi

Opinnäytetyö eteni suunnitelman mukaisesti pääasiassa aikataulussa ja yhteistyö opiskelijoiden välillä oli tehokasta. Työn tekemisessä hyödynnettiin opiskelijoiden yhdessä määrittele-

miä välipalautuksia, jotka jaksottivat työn kulkua. Alkuperäisessä suunnitelmassa ei kuitenkaan osattu ottaa huomioon kirjallisuuskatsauksen vaatimaa aikaresurssia, vaan aihealueen kirjallisuuteen tutustumiseen ja tiedonhakuun kului huomattavan paljon aikaa. Tämä johtui osaltaan siitä, ettei opiskelijoilla ollut alussa laajaa kokemusta standardien käytöstä, eikä vankkaa tietämystä laadunhallinnan ja riskienhallinnan erityispiirteistä. Lisäksi aihealueesta on olemassa paljon erilaista ja vaihtelevalla laadulla tuotettua kirjallisuutta, jonka läpi käyminen ja hyödyntämiskelpoisten lähteiden löytäminen oli aikaa vievää.

Opiskelijat tutustuivat kumpikin tarkemmin ennalta määritettyihin osa-alueisiin ja perehdyttivät toisensa riittävällä tasolla oman tutkimusalueensa kysymyksiin yhtenäisen ja tehokkaan työskentelyn varmistamiseksi. Työhön saatiin ohjausta sekä Laurea ammattikorkeakoulun että työelämän edustajan tahoilta, mutta erityisesti Laurean tarjoamaa ohjausmahdollisuutta olisi voinut hyödyntää nykyistä tehokkaammin. Työelämän edustajalta saatu palaute ohjasi työn toteuttamista ja työstä saatu palaute on ollut rakentavaa. Opinnäytetyön viimeistelyvaiheessa työ koettiin työelämäkumppanin toimesta hyödyntämiskelpoiseksi ja sen puitteissa tehtyä tutkimustyötä ja tuotoksia hyödynnetään opinnäytetyön tekijöiden ja työelämän kumppanin yhteisessä oppikirjaprojektissa opinnäytetyön valmistumisen jälkeen. Tärkeimpänä työtä ohjaavana tekijänä pidettiin työn edetessä opinnäytetyön varsinaista tavoitetta, eli tekstin tuottamista julkaistavaa oppikirjaa varten, sekä työelämän edustajalta saatuja kommentteja.

Laadun- ja riskienhallinnan kentät todettiin työn edetessä niin laajoiksi kokonaisuuksiksi, että työn tarkemmasta rajauksesta alkuvaiheessa olisi ollut hyötyä. Rajaaminen oli kuitenkin hankalaa, sillä opiskelijoilla ei ollut selkeää kuvaa kummankaan osa-alueen laajuudesta tai ydinasioista. Työn edetessä opiskelijat ovat joutuneet kirjallisuuskatsauksen ja toimintakenttään perehtymisen pohjalta määrittelemään mitkä asiat ovat opinnäytetyön ja tulevan oppikirjaprojektin kannalta olennaisia, jotta työssä ei lähdetä sivuraiteille.

Opinnäytetyölle olisi ollut eduksi, jos sitä olisi voitu tarkastella osana valmista oppikirjaa, kuten suunnitelmavaiheessa nähtiin mahdolliseksi. Prosessi ei tältä osin kuitenkaan edennyt odotettua vauhtia, ja kirjoitustyön aikana jouduttiin tekemään päätöksiä joilla mahdollistettiin opinnäytetyölle asetettujen kriteerien täyttyminen oppikirjasta irrallisena. Tämä aiheutti rakenteessa muutoksia, joilla oli selkeästi negatiivinen vaikutus raportin eheyteen ja luettavuuteen. Tätä pyrittiin parantamaan aina viime metreille asti. Opinäytetyöltä jäätiin kirjoittajien näkökulmasta kaipaamaan määrällisesti lisää tuotoksia ja tässä suhteessa tuntemus on se, että suunniteltu aikataulu saattoi sittenkin olla liian tiukka suhteessa tavoitteeisiin.

Kokonaisuudessaan opinnäytetyöprosessi koettiin haastavana ja ennen kaikkea opettavaisena. Opinnäytetyön aihealueiden tarkastelussa pyrittiin uudenlaisiin näkökulmiin ja uusien toimin-

tamallien kehittämiseen, joka sopii Laurea ammattikorkeakoulun Learning by Developing-malliin.

Jatkosuunnitelmat

Opinnäytetyö toteutettiin työelämälähtöisenä kehittämishankkeena, jonka tavoitteena oli tutkia laadunhallintaa ja riskienhallintaa, sekä näiden välisiä yhtymäkohtia syksyllä 2015 julkaistavaa oppikirjateosta varten. Opinnäytetyö tehtiin työelämän yhteistyökumppanin, Suomen turvallisuusosaaminen Oy:n tarpeisiin ja vastaamaan tulevan oppikirjan rakennetta. Kirjallisuuskatsaus ja opinnäytetyön teoreettinen osuus on pyritty pitämään käytännönläheisenä ja helposti lähestyttävänä erilaisten esimerkkien avulla.

Oppikirjaa varten on aikomuksena kesän 2015 aikana laatia lisää tämän opinnäytetyön tuotosten kaltaista ohjemateriaalia. Ohjeiden tueksi laaditaan case-esimerkkejä kuvitteellisen yrityksen laadun- ja riskienhallinnan prosesseista, käytänteistä ja mahdollisista ongelmatilanteista. Oppikirjan aihealueesta on suunnitteilla laatia koulutuspaketti ja elektronista materiaalia, joilla voidaan helpottaa laatujärjestelmiään päivittäviä organisaatioita hyödyntämään oppikirjan tietoperustaa. Mahdollisuutena nähdään myös oppikirjan kääntäminen englanniksi, jos kysyntää on.

Erään lisähaasteen opinnäytetyöhön toi se, että uudesta ISO 9001:2015 standardista on olemassa tätä kirjoittaessa vasta luonnosversio. Vaikka luonnosversio onkin todennäköisesti hyvin lähellä lopullista standardia, ovat muutokset vielä mahdollisia. Tästä syystä mahdollisia muutoksia standardin luonnokseen tulee seurata ja lopulta tarkastaa mahdolliset muutokset kun standardi julkaistaan.

Yhteistyökumppanin edustaja Jyri Paasonen  ilmaisi palautteessaan tyytyväisyyden työn kirjoitusasuun ja olevansa vakuuttunut siitä, että työn pohjalta voidaan laatia erinomainen kirja.

Lähteet

Chandra, M. J. 2001. Statistical Quality Control. Boca Raton: CRC Press.

Hirsjärvi, S. R. 2011. Tutki ja kirjoita. Helsinki: Tammi.

Hopkin, P. 2012. Fundamentals of Risk Management: understanding, evaluating and implementing effective risk management. Philadelphia: KoganPage.

ISO. 2012. Quality management principles. Geneve: ISO Central Secretariat.

ISO/DIS 9001:2014 International Organization for Standardization. 2014. Draft International Standard ISO/DIS 9001. Quality management systems — Requirements. Geneve: ISO.

ISO-IEC 27000 Suomen standardoimisliitto SFS. 2006. ISO-IEC 27000: Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen standardoimisliitto.

Juvonen, M., Korhonen, H., Ojala V.M., Salonen, T. & Vuori, H. 2005. Yrityksen riskienhallinta. Helsinki: Yliopistopaino.

Koskinen, K. 2006. Johda yrityksesi osaamista – näkökulmia pk-yritykselle. Turku: Yritystoiminnan tutkimus- ja koulutuskeskus.

Kuluttajaturvallisuuslaki 920/2011.

Kuusela, H., Ollikainen, R. 2005. Riskit ja Riskienhallinta: Riskit ja riskienhallinta-ajattelu. Tampere:Tampere University Press.

Kvist, H-H., Arhomaa, S., Järvelin, K. & Räikkönen J. 1995. Asiakasprosessit: Miten parannat tulosta prosesseja kehittämällä?. Jyväskylä:Gummerus.

Lecklin, O. 2006. Laatu yrityksen menestystekijänä. 5. painos. Helsinki: Talentum.

Leino, M., Steiner M.-L., Wahlroos, J. 2005. Riskit ja riskienhallinta: Corporate Governance ja riskienhallinta. Tampere: Tampere University Press.

Moeller, Robert R. 2011. Coso Enterprise Risk Management : establishing effective governance, risk, and compliance processes. Hoboken: John Wiley & Sons, Inc.

Owen, F. & Maidment, D. 1996. Quality Assurance: A Guide to the Application of ISO 9001 to process plant projects. Warwickshire: Institution of Chemical Engineers.

Pelastuslaki 379/2011

Pesonen, H.2007. Laatua! Asiantuntijaorganisaation laatuopas. Helsinki: Infor.

Pöyry, O. 2008. Kokonaisvaltainen riskienhallinta (ERM) – jalkauttamisen avaintekijät ja haasteet. Tampere: Tampereen yliopisto

Roper, Carl. A. 1999. Risk Management for Security Professionals. Burlington: Elsevier Science

Sallis, E. 2002. Total Quality Management in Education. Lontoo: Kogan Page.

Salminen, A. 2011. Mikä kirjallisuukatsaus? Vaasa: Vaasan yliopisto

SFS-EN ISO 9000:2000. 2001. Laadunhallintajärjestelmä. Standardikokoelma. Helsinki: Suomen standardoimisliitto.

SFS-EN 31010 Suomen standardoimisliitto SFS. 2011. SFS-EN 31010: Riskien hallinta. Riskien arviointimenetelmät. Helsinki: Suomen standardoimisliitto.

SFS-ISO 31000:2009 Suomen standardoimisliitto SFS. 2011. SFS-ISO 31000: Riskienhallinta. Periaatteet ja ohjeet. Helsinki: Suomen standardoimisliitto.

Silén, T. 1998. Laatujohtaminen. Porvoo: WSOY.

Slack, N., Chambers, S. & Johnston, R. 2010. Operations Management. 6. painos. Harlow: Pearson Education Limited.

Sousa V.D. 2012. Risk Management Framework for the Construction Industry According to the ISO 31000:2009 Standard. Lisbon: Atlantis Press

Työturvallisuuslaki 738/2002.

Croft, N. H. 2012. ISO 9001:2015 and beyond - Preparing for the next 25 years of quality management standards. International Organization for Standardization. Viitattu 17.2.2015; 13.4.2015.
http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1633

Elinkeinoelämän keskusliitto. 2015. Yritysturvallisuus. Viitattu 24.3.2015. http://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/

ISO. 2008. ISO 9000 Introduction and Support Package: Guidance on the Documentation Requirements of ISO 9001:2008. Viitattu 14.4.2015.
http://www.iso.org/iso/02_guidance_on_the_documentation_requirements_of_iso_9001_2008..pdf

ISO. 2015. The ISO Survey of Management System Standard Certifications. 2013 Executive summary. Viitattu 27.4.2015.
http://www.iso.org/iso/iso_survey_executive-summary.pdf

Knowles, G. 2011. Quality Management. Ventus Publishing. Viitattu 20.4.2015.
https://books.google.fi/books?id=ruSJEcNWf2sC

Martincic, C. J. 1997. A Review of ISO 9000. University of Pittsburgh. Viitattu 13.4.2015
http://www.sis.pitt.edu/~mbsclass/standards/martincic/iso9000.htm

Mindtools. 2015. Shareholder analysis. Viitattu 21.4.2015.
http://www.mindtools.com/pages/article/newPPM_07.htm

Pestleanalysis. 2015. Viitattu 15.4.2015 http://pestleanalysis.com/what-is-pestle-analysis/

Suomen riskienhallintayhdistys. 2012a. Riskin luokittelu. Viitattu 24.3.2015.
http://www.pk-rh.fi/index.php?page=riskien-luokittelu

Suomen riskienhallintayhdistys. 2012b. Riskienhallintaprosessi. Viitattu 24.3.2015.
http://www.pk-rh.fi/index.php?page=riskienhallintaprosessi

Terveyden ja hyvinvoinnin laitos. 2014. Liukastumis ja kaatumistapaturmat. Viitattu 25.3.2015. https://www.thl.fi/fi/web/tapaturmat/tietoa-tapaturmista/tapaturmista-aiheittain/liukastumis-ja-kaatumistapaturmat

Terveyden ja hyvinvoinnin laitos. 2015. Kaatumiset ja putoamiset. Viitattu 25.3.2015.
https://www.thl.fi/fi/web/tapaturmat/tietoa-tapaturmista/tilastot/tilastokatsaukset/kaatumiset-ja-putoamiset

Ulkoasiainministeriö. 2014a. EU:n Venäjä-pakotteet laajenivat – muutosten pääsisältö. Viitattu 19.3.2015. http://formin.finland.fi/public/default.aspx?contentid=310108

Ulkoasiainministeriö. 2014b. Hallitus selvityttää Venäjän vastapakotteiden vaikutukset. Viitattu 19.3.2015. http://www.formin.finland.fi/public/default.aspx?contentid=310455&contentlan=1&culture=fi-FI

Vanguard Consulting LLC. 2012. A brief history of ISO 9000. Viitattu 13.4.2015. http://www.systemsthinking.co.uk/3-1-article.asp

Kuviot

Taulukot

Liitteet

Liite 1. Työkalu organisaation toimintaympäristön määrittelemiseen.

POLIITTINEN

| | Hyödylliset | Haitalliset |
|---|---|---|
| Sisäiset | Vahvuudet<br>S | Heikkoudet<br>W |
| Ulkoiset | Mahdollisuudet<br>O | Uhat<br>T |

TALOUDELLINEN

| | Hyödylliset | Haitalliset |
|---|---|---|
| Sisäiset | Vahvuudet<br>S | Heikkoudet<br>W |
| Ulkoiset | Mahdollisuudet<br>O | Uhat<br>T |

SOSIAALINEN

| | Hyödylliset | Haitalliset |
|---|---|---|
| Sisäiset | Vahvuudet<br>S | Heikkoudet<br>W |
| Ulkoiset | Mahdollisuudet<br>O | Uhat<br>T |

TEKNOLOGINEN

| | Hyödylliset | Haitalliset |
|---|---|---|
| Sisäiset | Vahvuudet<br>S | Heikkoudet<br>W |
| Ulkoiset | Mahdollisuudet<br>O | Uhat<br>T |

LAINSÄÄDÄNNÖLLINEN

| | Hyödylliset | Haitalliset |
|---|---|---|
| Sisäiset | Vahvuudet<br>S | Heikkoudet<br>W |
| Ulkoiset | Mahdollisuudet<br>O | Uhat<br>T |

YMPÄRISTÖ

| | Hyödylliset | Haitalliset |
|---|---|---|
| Sisäiset | Vahvuudet<br>S | Heikkoudet<br>W |
| Ulkoiset | Mahdollisuudet<br>O | Uhat<br>T |

Liite 2. PESTLE-SWOT –analyysin jatkoarviointi.

POLIITTINEN

| | Vahvuudet | Heikkoudet |
|---|---|---|
| Mahdollisuudet | Hyödynnä | Korjaa / kehitä |
| | | |
| Uhat | Varaudu / ennakoi | Vältä / torju |
| | | |

TALOUDELLINEN

| | Vahvuudet | Heikkoudet |
|---|---|---|
| Mahdollisuudet | Hyödynnä | Korjaa / kehitä |
| | | |
| Uhat | Varaudu / ennakoi | Vältä / torju |
| | | |

SOSIAALINEN

| | Vahvuudet | Heikkoudet |
|---|---|---|
| Mahdollisuudet | Hyödynnä | Korjaa / kehitä |
| | | |
| Uhat | Varaudu / ennakoi | Vältä / torju |
| | | |

TEKNOLOGINEN

| | Vahvuudet | Heikkoudet |
|---|---|---|
| Mahdollisuudet | Hyödynnä | Korjaa / kehitä |
| | | |
| Uhat | Varaudu / ennakoi | Vältä / torju |
| | | |

LAINSÄÄDÄNNÖLLINEN

| | Vahvuudet | Heikkoudet |
|---|---|---|
| Mahdollisuudet | Hyödynnä | Korjaa / kehitä |
| | | |
| Uhat | Varaudu / ennakoi | Vältä / torju |
| | | |

YMPÄRISTÖ

| | Vahvuudet | Heikkoudet |
|---|---|---|
| Mahdollisuudet | Hyödynnä | Korjaa / kehitä |
| | | |
| Uhat | Varaudu / ennakoi | Vältä / torju |
| | | |

Liite 3. ISO 9001:2015:n mukaisen laadunhallintajärjestelmän dokumentaatio.

Otsikkotason numerointi kuten standardissa.
Laadunhallintajärjestelmältä edellytetty dokumentaatio ISO/DIS 9001:2014 mukaan:

**4 TOIMINTAYMPÄRISTÖ**

**4.3 Laadunhallintajärjestelmän soveltamisala**

Laadunhallintajärjestelmän soveltamisalasta, eli rajauksesta ja kattavuudesta on säilytettävä dokumentoitua tietoa, joka ilmaisee:

Laadunhallintajärjestelmän soveltamisalan kattamat tuotteet ja palvelut,
sekä seikkaperäiset selvitykset ja perustellut syyt mikäli niitä on rajattu laadunhallintajärjestelmän ulkopuolelle.

**4.4 Laadunhallintajärjestelmä ja sen prosessit**

Organisaation tulee säilyttää dokumentoitua tietoa siinä määrin kun se on tarpeellista prosessien toiminnan tukemiselle, sekä säilyttää dokumentoitua tietoa prosesseista siinä määrin että voidaan varmistua niiden toimivan suunnitellusti.

**5 JOHTAMINEN**

**5.2 Laatupolitiikka**

Laatupolitiikan on oltava saatavilla dokumentoituna tietona organisaation sisäiseen käyttöön ja tarveharkinnan mukaisesti myös sidosryhmille. Laatupolitiikkan tulee olla organisaatiossa tiedoitettu, ymmärretty ja jalkautettu.

**6 LAADUNHALLINTAJÄRJESTELMÄN SUUNNITTELU**

**6.2 Laatutavoitteet ja toteutussuunnitelmat**

Organisaation on säilytettävä dokumentoitua tietoa laatutavoitteista.

**7 OSAAMINEN**

Organisaation on määritettävä laaduntuottokykyyn vaikuttavien prosessien henkilöstöltä vaadittava osaaminen, ja säilytettävä dokumentoitua tietoa näistä vaatimuksista ja henkilöstönsä osaamisesta.

#### 7.1.5 Mittaaminen ja seuranta

Organisaation on säilytetettävä dokumentoitua tietoa osoittaakseen mittaamisen ja seurannan resurssien riittävyyden tarkoituksenmukaisuudeen. Mikäli tuotteelta tai palvelulta niin edellytetään, on käytettyjen mittalaitteiden vaatimuksenmukaisuudesta ja kalibroinnista säilytettävä dokumentoitua tietoa.

## 8 TOIMINTA

### 8.1 Toiminnan suunnittelu ja ohjaus

Organisaation on säilytettävä dokumentoitua tietoa prosesseista ja niiden ohjauksesta siinä määrin että voidaan varmistua niiden toimivan suunnitellusti ja osoittaa niiden tuotosten olevan yhdenmukaisia niille asetettujen laatuvaatimusten kanssa.

### 8.2 Tuotteille ja palveluille asetettujen vaatimusten määrittely

#### 8.2.3 Tuotteille ja palveluille asetettujen vaatimusten katselmointi

Organisaation on säilytettävä dokumentoitua tietoa tuotteille asetettujen laatuvaatimusten ja niiden määrittelyn katselmoinnista ja niihin kohdistuneista muutoksista.

#### 8.3.5 Suunnitelu- ja kehitystyön tuotokset

Suunnittelu- ja kehitystyön tuotokset on säilytettävä dokumentoituna tietona.

#### 8.3.6 Suunnitelu- ja kehitystyön muutokset

Suunnittelu- ja kehitystyön muutokset on säilytettävä dokumentoituna tietona.

### 8.4 Ulkoisten tuotteiden ja palveluiden ohjaus

Organisaation on varmistettava, että ulkoisesti tuotetut prosessit, tuotteet ja palvelut vastaavat niille asetettuja vaatimuksia. Organisaation on säilytettävä asianmukaista dokumen-

taatiota ulkoisesti tuotettujen prosessien arvioinnista, suorituskyvyn mittaamisesta ja uudelleenarvionnista.

#### 8.5.2 Tunnistettavuus ja jäljitettävyys

Organisaation on säilytettävä dokumentoitua tietoa prosessien tuotosten tunnistettavuudesta ja jäljitettävyydestä mikäli niitä edellytetään.

#### 8.5.6 Muutostenhallinta

Organisaation tulee katselmoida ja hallita suunnittelemattomia muutoksia siinä määrin kun se laaduntuotantokyvyn kannalta on oleellista, ja säilytettävä dokumentoitua tietoa katselmoinneista, muutokset hyväksyneestä tahosta ja tarvittavista toimenpiteistä.

### 8.6 Tuotteiden ja palveluiden julkaiseminen

Tuotteiden ja palveluiden julkaisemista asiakasrajapinnassa ei sallita, kunnes suunnitellut toimenpiteet niiden vaatimuksenmukaisuuden varmentamiseksi on hyväksyttävästi suoritettu, mikäli vastuutahot ja joissain tapauksissa asiakas eivät toisin valtuuta. Tieto valtuuttaneesta henkilöstä on säilytettävä dokumentoituna.

### 8.7 Poikkeavien prosessituotosten, tuotteiden ja palveluiden hallinta

Organisaation on säilytettävä dokumentoitua tietoa prosessien, tuotteiden ja palveluiden poikkeamien hallintaan käytetyistä toimenpiteistä, mahdollisista myönnytyksistä ja henkilöstä tai tahosta joka on tehnyt päätöksen toimenpiteistä poikkeaman hallitsemiseksi.

## 9 SUORITUSKYVYN ARVIOINTI

### 9.1 Seuranta, mittaaminen, analysointi and arviointi

Organisaation on varmistuttava seurannan ja mittaamisen toimenpiteiden vaatimuksenmukaisaesta jalkauttamisesta, ja säilytettävä dokumentoitua tietoa niiden tuloksista.

### 9.2 Sisäiset auditioinnit

Organisaation on säilytettävä dokumentoitua tietoa auditointiohjelmasta ja sen tuloksista.

### 9.3 Johdon katselmus

Organisaation on säilytettävä dokuementoitua tietoa johdon katselmusten tuloksista.

## 10 PARANTAMINEN

### 10.2. Poikkeamat ja korjaavat toimenpiteet

Organisaation on säilytettävä dokumentoitua tietoa poikkeamista, niiden korjaamiseksi suoritetuista toimenpiteistä ja toimenpiteiden tuloksista.