LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Aluehallintoviraston riskienhallinnan nykytila

Vilkki, Juha

2014 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Aluehallintoviraston riskienhallinnan nykytila

Juha Vilkki 1001930
Turvallisuusosaamisen
koulutusohjelma
Opinnäytetyö
Lokakuu 2014

Laurea-ammattikorkeakoulu
Laurea Leppävaara
Turvallisuusosaamisen koulutusohjelma

Tiivistelmä

Juha Vilkki

Aluehallintoviraston riskienhallinnan nykytila

Vuosi 2014 Sivumäärä 133

Valtionhallinnon organisaatioille kohdistuu alati korostuva tuloksellisuuden vaade. Toiminnan tuloksellisuus edellyttää siihen liittyvien riskien hallitsemista. Valtion viraston ja laitoksen riskienhallinnalla tarkoitetaan menettelyjä, joilla tunnistetaan, arvioidaan ja hallitaan valtion ja sen organisaation tavoitteiden saavuttamista heikentäviä uhkia sekä avautuneiden toimintamahdollisuuksien menettämistä. Valtion virastossa ja laitoksessa riskienhallinta on tavoitteiltaan perusprosesseihin integroitunut laaja-alainen näkökulma organisaation toimintaan.

Opinnäytetyön tavoitteena oli selvittää valtion aluehallinnon viraston riskienhallinnan nykytila siihen liittyvine rakenteineen ja menettelyineen. Nykytilan arvioimiseksi selvitettiin myös kohdeorganisaation riskienhallinnalle kohdistetut odotukset. Selvityksen pohjalta tarkoituksena oli sekä esittää toimenpiteitä riskienhallinnan kehittämiseksi että laatia kohdeorganisaatiolle riskienhallinnan periaatteiden muodostamista tukeva ohje. Tutkimus on strategialtaan tapaustutkimus ja sen tutkimusmenetelmänä käytettiin teorialähtöistä dokumenttianalyysiä.

Tutkimuksen teoreettinen viitekehys muodostui aluehallintovirastosta sekä sen ohjaamisen ja johtamisen menettelyistä sekä riskienhallinnan käsitteestä piirteineen ja elementteineen. Erikseen tarkastellaan riskienhallinnan erityispiirteitä ja ilmenemisestä valtionhallinnossa. Lisäksi luodaan katsaus riskienhallintaan liittyviin säädösvelvoitteisiin sekä riskienhallinnan ja erilaisten turvallisuuden johtamisen käsitteiden yhteyteen. Tutkimuksen empiirinen aineisto muodostui kohdeorganisaation ohjausasiakirjoista, toiminnan ja tuloksellisuuden raporteista sekä muista organisaation toiminnasta kertovista valmiista aineistoista.

Johtopäätöksinä voidaan todeta, että riskienhallinta on kohdeorganisaatiossa tunnistettu käsitteenä ja kehittämiskohteena, ja sen voidaan katsoa täyttäneen riskienhallinnan järjestämiselle kohdistetut odotukset ja velvoitteet. Riskienhallintaa toteutetaan organisaatiossa lähinnä eri organisaatioturvallisuuden osa-alueilla tehtyjen toimenpiteiden kautta. Menettelyissä painottuvat valtion organisaation keskeisten toimintaedellytysten suojaaminen. Nykytilassa ilmenneet puutteet liittyvät sekä yksittäisin riskienhallintamenettelyihin riskienhallintaprosessin eri vaiheissa että kokonaisvaltaisen riskienhallinnan periaatteiden toteutumiseen. Vaikka valittu tutkimusmenetelmä paljasti kohdeorganisaation riskienhallinnan keskeiset rakenteet, jätti se avoimiksi joitakin riskienhallinnan toteutumiseen liittyviä konkreettisia seikkoja.

Nykyiset menettelyt, organisaation johdon suhtautuminen ja sisäisen valvonnan tila muodostavat kokonaisvaltaisen riskienhallinnan kehittämiselle vahvan perustan. Toimenpidesuosituksina esitetään kokonaisvaltaisen riskienhallinnan periaatteiden muodostamista sekä menettelyjen yhteensovittamista valtion aluehallinnon virastojen kanssa. Suosituksen tueksi luotiin riskienhallinnan periaatteiden muodostamista tukeva tutkimuksen teoreettiseen viitekehykseen ja tutkimustuloksiin perustuva ohje.

Asiasanat: riskienhallinta, valtionhallinto, aluehallintovirasto

Laurea University of Applied Sciences
Laurea Leppävaara
Master´s Degree in Security Management

Abstract

Juha Vilkki

Current state of risk management in a State Administrative Agency

Year 2014 Pages 133

Government organisations are subjected to the increasing efficiency requirements. Operational efficacy requires the management of related risks. The risk management for state agencies refers to procedures that identify, assess and manage the risks to objectives of the state and its organizations and loss of emerging opportunities. For state agencies risk management should be a wide-ranging approach to the activities of the organization which is integrated into the fundamental processes of the organisation.

Aim of this study was to assess the current state of a Regional State Administrative Agency risk management and the associated structures and procedures. In order to assess the current state the expectations of risk management for target organization were also determined. The objective of the assessment was to present actions that would improve risk management in the target organisation and develop guidance to support the formation of risk management principles for the organisation. The strategic approach to the research is a case study, and the research method used was theory-driven document analysis.

The theoretical framework consisted of the Regional State Administrative Agency and it's guidance and management procedures, as well as the concept of risk management. Special features and the occurrence of risk management in the state administration is also reviewed. An overview of risk management related to regulatory requirements and risk management associated with safety and security management concepts is also undertaken together. The empirical data consisted of the target organisation's official procedures, operational and performance reports and other documents describing the activities of the organisation.

It can be concluded that risk management is identified in the target organisation as a concept and as a subject of development. The target organisation can be considered to have met the expectations and requirements of risk management. Risk management in the target organisation is carried out mainly via measures taken in various elements of organisational safety and security. The procedures taken focus on protecting the fundamental operational capabilities of the organisation. The current defficiencies are associated with both individual risk management procedures at different stages of the risk management process and with the implementation of the principles of enterprise risk management. Although the choice of research method revealed the target organisation's risk management structures, it left un answered some of the concrete facts about the implementation of risk management.

The target organisations current procedures, the approach of the organisation's management and the status of internal controls forms a strong foundation for developing the target organisations enterprise risk management. Recommendations for action are presented to both form the principles of enterprise risk management and to coordinate the formed policies and procedures with the risk management of other Regional State Administrative Agencies. In addition instructions based on the theoretical framework and the research results of the study were created to support the target organisation form the principles of risk management.

Key words: risk management, state administration, State Administrative Agency

Sisällys

1 Johdanto

Kaikkeen toimintaan liittyy riskejä. Riskin määritelmiä on useita, mutta usein sillä tarkoitetaan tavoitteiden saavuttamista uhkaavaa tapahtumaa tai tekijää. Määritelmän mukaan erilaisista vaaroista ja uhkista tulee riskejä vasta, kun ne ovat tavoitteiden kannalta oleellisia (Ilmonen, Kallio, Koskinen & Rajamäki 2013, 98; Mäkinen 2007, 106). Riskienhallinnalla käsitetään tavallisimmin organisaation toiminnan suojaamista ei-toivotuilta tapahtumilta, jolloin keskeisenä tavoitteena nähdään toiminnan häiriöttömyyden ja jatkumisen, toimintavarmuuden, turvallisuuden ja laadun kaltaiset asiat. Toisaalta riskillä on myös positiivinen ulottuvuus – kun riskin ottaminen tapahtuu harkitusti ja hallitusti, saadaan mahdollisuus esimerkiksi liikevoittoon. Näin tarkasteltuna riskienhallinnan tarkoitukseksi voidaan katsoa organisaation päätöksenteon tukeminen siten, että johto ymmärtää toimintaan ja tehtäviin päätöksiin liittyvät riskit. (Ilmonen ym. 2013, 5, 10, 15, 69.)

Toiminnan ja tavoitteiden suojaamisen lisäksi organisaatioilla on myös lakisääteisiä henkilöstön, omaisuuden ja ympäristön turvallisuuteen liittyviä velvoitteita, joiden täyttäminen edellyttää riskienhallinnaksi katsottavia toimenpiteitä. Riskienhallinnan voidaan katsoa olevan myös organisaation eettisen ja yhteiskunnallisen vastuun kantamista (Sosiaali- terveysministeriö 2011, 8). Kokonaisvaltaisella riskienhallinnalla tarkoitetaan organisaation toiminnan kaikille osa-alueille ulottuvaa riskienhallintaa (Mäkinen 2007, 106). Riskienhallinnassa ja erityisesti siihen liittyvässä kokonaisvaltaisessa lähestymistavassa korostuvat riskienhallinnan sitominen organisaation perusprosesseihin, kaikille tasoille ja kulloisenkin päätöksenteon yhteyteen.

Valtion viraston ja laitoksen riskienhallinnalla tarkoitetaan menettelyjä, joilla tunnistetaan, arvioidaan ja hallitaan valtion ja sen organisaation tavoitteiden saavuttamista heikentäviä uhkia sekä avautuneiden toimintamahdollisuuksien menettämistä. Riskejä muodostuu tällöin tavoitteiden saavuttamisen kannalta epäedullisista tapahtumista tai menetetyistä mahdollisuuksista, ja ne liittyvät erityisesti tuloksellisuuteen, lain ja talousarvion noudattamiseen sekä hyvän hallinnon arvojen ja periaatteiden toteutumiseen. Myös valtion virastossa ja laitoksessa riskienhallinta on laaja-alainen näkökulma organisaation toimintaan, joka toteutuu tehokkaimmin ollessaan täysin integroitunut organisaation toimintoihin. (Valtiovarain controller –toiminto 2005, 11-12.)

Valtiontalouden heikentyvä tilanne heijastuu valtion organisaatioiden toimintaan erityisesti rajallisempina voimavaroina ja siten edelleen tuloksellisuuden haasteina. Tuloksellisuudella tarkoitetaan valtionhallinnossa yhteiskunnallisen vaikuttavuuden, toiminnallisen tehokkuuden sekä henkisten voimavarojen hallinnan ja kehittymisen muodostamaa kokonaisuutta (Valtiovarain controller –toiminto 2005, 9). Valtiovarainministeriö on todennut useita vuosia ennen nykyisen taloudellisen laskusuhdanteen alkua julkiseen toimintaan kohdistuvan jatkossa

aikaisempaa voimakkaampi tuloksellisuuden vaade (Valtiovarainministeriö 2004a,4). Tuloksellisuuden haasteet näyttäytyvät sekä yhteiskuntapolitiikan lohkojen muodostamalla tasolla että yksittäisten julkisten organisaatioiden ja niiden yksittäisten tehtävien muodostamalla tasolla.

Tuloksellisuuteen liittyviä tavoitteita ei voi saavuttaa ottamatta riskejä esimerkiksi tehokkaampien toimintatapojen muodossa. Toisaalta organisaation toimintaan kohdistuvat häiriöt heikentävät toiminnan tehokkuutta ja vaarantavat tulostavoitteiden saavuttamisen ilman nykyistä mittavampaa riskinottoakin. Toimintaan kohdistuvien ja tuloksellisuutta heikentävien riskien hallitseminen edellyttää tietoisia valintoja ja toimenpiteitä. Tuloksellisemman toiminnan vaateiden lisäksi julkisen organisaation kykyyn suoriutua tehtävistään kaikissa olosuhteissa liittyy sekä odotuksia että velvoitteita. Yhteiskunnan toimivuuden kannalta on ensiarvoisen tärkeää, että sekä viranomaiset että muut poikkeusolojen toiminnan näkökulmasta keskeiset toimijat ovat varmistaneet kykynsä toimia kaikissa oloissa (Parmes (toim.) 2007, 36). Toimintaan liittyvien riskien hallitseminen on keskeistä erityisesti aikana, jolloin julkisen hallinnon säästöpaineet ovat kovat eikä voimavarojen vähentyessä särkymävaraa ole.

Valtion virastoille ja laitoksille on annettu suositus sisäisen valvonnan ja riskienhallinnan lähestymistavoista sekä toimivuuden arvioinnista. Suositus kuvaa valtionhallinnon hyvää käytäntöä ja sen tarkoituksena on tukea sisäisen valvonnan ja riskienhallinnan asianmukaisuuden ja riittävyyden arviointia sekä tähän liittyvien keskeisten kehittämistarpeiden tunnistamista. Suositus perustuu kansainvälisesti käytettyyn kokonaisvaltaisen riskienhallinnan coso-erm –malliin. (Valtiovarain controller –toiminto 2005, 3.)

Opinnäytetytön kohdeorganisaationa olevan aluehallintoviraston riskienhallinnan nykytilaa on arvioitu valtiovarain controller –toiminnon laatiman suosituksen pohjalta vuosittain organisaation toimintakertomukseen sisältyvän sisäisen valvonnan ja riskienhallinnan vahvistuslausuman laadinnan yhteydessä. Vahvistuslausuman mukaan sisäisen valvonnan ja riskienhallinnan arviointikokonaisuuden puutteet liittyvät nimenomaan riskienhallinnan osuuteen. Kohdeorganisaatio on vahvistuslausuman yhteydessä itse todennut välttämättömäksi, että aluehallintovirastoille muodostettaisiin riskienhallinnan periaatteet.

Riskienhallintaa kehitettäessä on riskienhallinnan periaatteiden muodostaminen esimerkiksi riskienhallintapolitiikan muodossa työn ensimmäinen vaihe (Ilmonen ym. 2013, 54-57; Juvonen, Korhonen, Ojala, Salonen & Vuori 2005, 38). Aluehallintovirastojen yleishallinnollisesta ohjauksesta vastaava valtiovarainministeriö on asettanut tavoitteeksi aluehallintovirastojen riskienhallinnan ja sen menettelyjen kehittämisen jo joitakin vuosia sitten. Keskeisenä toimenpiteenä aluehallintovirastojen odotetaan laativan virastojen yhtenäisen riskienhallintapolitiikkamallin. Tavoitteen toteuttamista on aluehallintovirastojen strategisen ohjauksen asia-

kirjoissa siirretty. (Etelä-Suomen aluehallintoviraston…2013, 24; Itä-Suomen aluehallintoviraston…2013, 26; Lapin aluehallintoviraston…2013, 24; Lounais-Suomen aluehallintoviraston…2013, 24; Länsi- ja Sisä-Suomen aluehallintoviraston…2013, 27; Pohjois-Suomen aluehallintoviraston…2013, 27.)

1.1 Opinnäytetyön tavoite ja toteutus

Opinnäytetyön tavoitteena oli tutkimuksen keinoin selvittää kohdeorganisaation riskienhallinnan nykytila siihen liittyvine rakenteineen ja menettelyineen. Selvityksen pohjalta tarkoituksena oli sekä esittää toimenpiteitä riskienhallinnan kehittämiseksi että laatia kohdeorganisaatiolle riskienhallinnan periaatteiden muodostamista ja riskienhallinnan järjestämistä tukeva ohje. Toimenpide-ehdotusten ja ohjeen tarkoituksena on tukea riskienhallinnan kehittymistä kohdeorganisaatiossa. Tarkoituksena on lisäksi tukea kohdeorganisaation riskienhallintaan liittyvän tiedon ja osaamiseen lisäämistä tarjoamalla jäsennetty katsaus aihekokonaisuuteen.

Riskienhallinnan nykytilaa tarkasteltiin suhteessa muodostettuun riskienhallinnan viitekehykseen, mutta myös suhteessa kohdeorganisaation riskienhallinnan toteuttamiseen kohdistuviin odotuksiin. Viitekehyksen vertailukohdat muodostuivat riskienhallinnan yleisestä teoriasta, valtionhallinnon riskienhallinnan periaatteista ja menettelyistä sekä riskienhallintaan liittyvistä säädösvelvoitteista. Odotuksia katsottiin puolestaan muodostuvan strategisen ohjauksen ja tulosohjauksen kautta.

Kohdeorganisaation riskienhallinnan nykytilan ja siihen liittyvien menettelyjen ja rakenteiden sekä riskienhallinnan toteuttamiseen kohdistuvien odotusten selvittäminen oli keskeistä paitsi nykytilan arvioimiseksi, myös riskienhallinnan periaatteiden muodostamiseen ja järjestämiseen liittyvän ohjeen laatimiseksi. Tämä siksi, että riskienhallinnan periaatteiden muodostamisen lähtökohtana toimivat riskienhallinnalle jo osoitetut sisäiset ja ulkoiset vaatimukset, joista ensiksi mainittuja muodostuu muun muassa organisaatiossa jo kirjatuista menettelytavoista ja jälkimmäisiä erityisesti säädöksistä ja sopimuksista. (Ilmonen ym. 2013, 18-20.) Valtionvarain controller –toiminnon näkemyksen (Valtiovarain controller –toiminto 2005, 20-22, 25) mukaan virastossa ja laitoksessa riskienhallintaa kehitettäessä tulee pyrkiä selkeisiin ja yksinkertaisiin menettelyihin, huomioida olemassa olevat toiminnan rakenteet sekä välttää erillisprosesseja ja ylimääräistä dokumentointia. Ohje ei siten saisi olla ristiriidassa organisaation nykyisten menettelyiden eikä sille kohdistettujen odotusten kanssa.

Tutkimus oli luonteeltaan laadullinen. Tutkimusstrategiana käytettiin tapaustutkimusta ja menetelmänä dokumenttianalyysiä. Empiirinen aineisto muodostui kohdeorganisaation sisäisen valvonnan ja riskienhallinnan vahvistuslausumista ja niiden antamiseksi kerätystä kyselyaineistosta, muista organisaation toiminnasta kertovista dokumenteista sekä organisaation

strategisen ohjauksen ja tulosohjauksen asiakirjoista. Empiirisenä aineistona toimivat dokumentit on aineiston kuvailun sekä tulosten ja johtopäätösten yhteydessä nimetty sellaisin nimin ja koodein, ettei kohdeorganisaatio tule dokumenttien nimistä ilmi. Oletuksena oli, että riskienhallinnan kokonaisuuteen liittyviä menettelyitä toteutetaan organisaatiossa esimerkiksi yksittäisten turvallisuuden osa-alueiden yhteydessä, ja että ohjaavissa asiakirjoissa organisaatiolta odotetaan tuloksellisuutta varmistavia toimenpiteitä.

Kohdeorganisaation riskienhallinnan kehittämistarpeiden katsottiin tässä opinnäytetyössä muodostuvan siitä, etteivät riskienhallinnan järjestämiseen liittyvät keskeiset säädösten tai strategisen ohjauksen ja tulosohjauksen velvoitteet ja odotukset olisi täyttyneet. Kehittämismahdollisuuksia katsottiin puolestaan havaittavan vertaamalla riskienhallinnan nykytilaa muodostettuun riskienhallinnan kehykseen. Tarkastelun näkökulmana oli kokonaisvaltainen riskienhallinta, johon sisältyväksi katsottiin kuuluvan myös kohdeorganisaation yksittäisillä turvallisuuden osa-alueilla tapahtuva toiminta. Riskienhallinta toteutuu organisaatioissa usein juuri turvallisuuden osa-alueiden kautta (Ilmonen ym. 2013, 44; Leppänen 2008, 61, 204). Opinnäytetyössä esitetään toimenpide-ehdotuksia kohdeorganisaation riskienhallinnan kehittämiseksi. Lisäksi annetaan opinnäytetyön teoreettiseen ja empiiriseen aineistoon perustuva kohdeorganisaation riskienhallinnan periaatteiden muodostamista tukeva ohje.

1.2 Rajaukset

Tutkittavan aihekokonaisuuden laajuudesta johtuen jouduttiin tekemään useita rajauksia. Tarkastelu rajattiin koskemaan kohdeorganisaatiota eikä sitä kokonaisuutta, jonka se muodostaa yhdessä lukuisien tulosohjaavien ministeriöiden ja muiden sidosryhmien kanssa. Vaikka rajausta on pidettävä selviönä on sen toteaminen siksi oleellista, että viime kädessä valtiontalous ja koko valtionhallinto muodostaa yhden kokonaisuuden (Valtiovarain controller –toiminto 2005, 12). Strategisen ja toiminnallisen tason tarkastelussa opinnäytetyössä pysyttiin toiminnallisella tasolla, sillä strategisen tason tarkastelussa olisi väistämättä kohdattu edellä mainittu kohdeorganisaation ja sitä ohjaavien ministeriöiden kokonaisuus.

Menetelmällisesti työ rajattiin dokumenttianalyysiin. Rajaus tehtiin käytännön aikataulullisista syistä. Menetelmällinen valinta puolestaan tehtiin perustuen siihen oletukseen, että asiakirjat paljastaisivat kohdeorganisaation riskienhallinnan tilasta asioita, joita haastatteluissa ei mahdollisesti tulisi esille. Toisaalta oletettiin, että haastateltavien vastaukset voisivat olla asiakirjojen esitystapaa yleisluontoisempia.

Empiirisen aineiston ulkopuolelle jouduttiin jättämään sellaiset asiakokonaisuuteen liittyviksi arvioidut asiakirjat, joita ei pyynnöistä huolimatta saatu käyttöön. Organisaatiota ohjaavalla taholle tehtyä sähköpostikysely ei myöskään uusittu, vaikka siihen ei saatu vastausta. Riskien-

hallinnan järjestämiseen liittyvien säädösten perustelutekstejä ei käyty läpi. Säädösten osalta tyydyttiin luomaan katsaus teoreettisen viitekehyksen yhteydessä esille nousseisiin lakeihin ja asetuksiin sen sijaan, että olisi pyritty löytämään kaikki asiakokonaisuuteen liittyvät säädösvelvoitteet. Myöskään ei tehty selvitystä siitä, onko kohdeorganisaatiolle tai sen osille osoitettu säädösten tai ohjausasiakirjojen lisäksi riskienhallintaan liittyviä odotuksia esimerkiksi sopimuksin. Kohdeorganisaation riskienhallinnalle kohdistuvien ulkoisten vaatimusten selvittäminen rajattiin siten katsaukseen säädösvelvoitteisiin ja valtiovarain controller –toiminnon antamaan suositukseen sekä strategisen ohjauksen ja tulosohjauksen asiakirjojen analysointiin.

Yksittäisten turvallisuuden osa-alueiden tilaa tarkasteltiin ainoastaan siltä osin, mitä näiden toteuttamiseen liittyviä menettelyjä analysoidut asiakirjat paljastavat. Työssä ei myöskään tarkasteltu organisaation sisäisen valvonnan nykytilaa, vaikka sisäinen valvonta ja riskienhallinta ovatkin toisiinsa kytkeytyviä toimintoja. Toisaalta kohdeorganisaation sisäisen valvonnan tilaan saatiin katsaus sitä kartoittaneen valmiin aineiston kautta.

Kohdeorganisaation riskienhallinnan toteuttamisen tarkastelunäkökulmaksi valittiin organisaation johdon näkökulma. Valittavissa olisi ollut myös esimerkiksi organisaatiota ohjaavien ministeriöiden näkökulma, organisaation muiden työntekijöiden näkökulma tai muiden sidosryhmien ja organisaation palveluja saavien näkökulma. Organisaation johdon näkökulma valittiin siksi, että vaikka organisaation tavoitteiden saavuttaminen ja toiminnan häiriöttömyys on kaikkien edellä todettujen tahojen intressi ja osin sidoksissa ohjaavien ministeriöiden toimenpiteisiin, on toiminnan tavoitteiden saavuttaminen ja turvallisuuteen liittyvien velvoitteiden toteuttaminen kohdeorganisaation ja viime kädessä sen johdon velvollisuus. Kohdeorganisaation tulee jo säädösten velvoittamana tarkastella omaa toimintaansa sekä sitä uhkaavia asioita ja ryhtyä toimenpiteisiin niiden vaikutusten vähentämiseksi.

Opinnäytetyön tarkoituksena ei ollut selvittää toteutuuko valtiovarain controller –toiminnon antama suositus ja sen myötä kokonaisvaltaisen riskienhallinnan malli kohdeorganisaatiossa, sillä organisaation riskienhallinnan tilaa suhteessa suositukseen on jo vuosittain arvioitu. Organisaation riskienhallinnan nykytilaa ja edelleen kehittämismahdollisuuksia ja toimenpideehdotuksia tarkasteltiin kuitenkin suosituksen taustalla olevan kokonaisvaltaisen riskienhallinnan viitekehyksessä. Riskienhallinnan kehittämistarpeita voitaisiin katsoa osoittavan myös se, ettei kohdeorganisaatio saavuttaisi tulostavoitteitaan tai se kohtaisi muita sen suojattaviin arvoihin kohdistuvia ei-toivottuja tapahtumia, mutta tämä tarkastelu rajattiin työn ulkopuolelle.

Tehtyjen rajausten vuoksi kohdeorganisaatiolle itselleen jää riskienhallinnan periaatteita muodostaessaan tehtäväksi joitakin selvityksiä. Toisaalta opinnäytetyön tuotoksena muodos-

tettu ohje on ainoastaan riskienhallinnan periaatteiden muodostamista tukeva ohje, ja kohdeorganisaatio joutuu siinä yhteydessä muutoinkin tekemään linjauksia ja päätöksiä sekä itsenäisesti että vuorovaikutuksessa organisaatiota ohjaavien tahojen kanssa. Tehdyt rajaukset muodostavat myös aiheita jatkotutkimuksille.

1.3 Tutkimuksen teoreettinen viitekehys

Teoreettinen viitekehys muodostuu tässä opinnäytetyössä toisaalta aluehallintovirastosta sekä sen ohjaamisen ja johtamisen menettelyistä, ja toisaalta riskienhallinnan kokonaisuudesta piirteineen ja elementteineen. Yleisen riskienhallinnan teorian lisäksi tarkastellaan riskienhallinnan erityispiirteitä ja ilmenemisestä valtionhallinnossa. Oma katsauksensa luodaan valtion virastoille ja laitoksille annettuun suositukseen sisäisen valvonnan ja riskienhallinnan toteuttamiseksi sekä aihepiiriin liittyviin säädösvelvoitteisiin. Lopuksi käsitellään lyhyesti riskienhallinnan ja turvallisuusjohtamisen sekä näihin läheisesti liittyvien käsitteiden yhteyttä.

Teoreettisella viitekehyksen kautta perehdyttiin riskienhallinnan toteuttamisen kokonaisuuteen. Viitekehyksen kokoamisen yhteydessä muodostetaan käsitys siitä mitä riskienhallinta on, millaisista elementeistä se muodostuu ja millaisin periaattein sitä tulisi toteuttaa. Edelleen viitekehyksen avulla perehdyttiin siihen, kuinka riskienhallintaa on lähestytty valtionhallinnossa ja millaista tukea valtionhallinto tarjoaa alaistensa organisaatioiden riskienhallinnan toteuttamiselle. Viitekehyksen tarkoituksena on mahdollistaa riskienhallinnan nykytilan arvioiminen ja edelleen kehittämiskohteiden löytäminen vertaamalla organisaation nykyistä toimintaa riskienhallinnan teoriaan ja organisaatioon kohdistuviin odotuksiin. Teoriaosuus on myös tarkoitettu tarjoamaan kohdeorganisaatiolle mahdollisuus aihekokonaisuuteen perehtymiseen.

Riskienhallintaa on tutkittu ja sitä koskevaa kirjallisuutta on melko runsaasti. Tutkittu on myös yksittäisten valtion organisaatioiden riskienhallinnan kehittämistä. Valtion organisaatioissa on myös toteutettu riskienhallintaa, ja sitä kuvaavaa aineistoa on saatavilla. Juuri aluehallintovirastojen riskienhallintaa koskevaa tutkimusta ei kuitenkaan ole. Myöskään ei ole selvityksiä aluehallintovirastojen riskienhallinnan kohdistetuista odotuksista. Opinnäytetyön lähdeaineistona toimii ensisijaisesti riskienhallintaan ja turvallisuusjohtamiseen liittyvä kirjallisuus. Teoriapohjaa täydentävät erilaiset näihin liittyvät sekä eri yksityisten että julkisten organisaatioiden julkaisut ja internet-sivut, ammattikorkeakoulujen ja yliopistojen opinnäytetyöt, säädökset, pöytäkirjat ja muistiot. Viitekehystä muodostettaessa käytiin lisäksi tarkentavia puhelinkeskusteluja joidenkin valtionhallinnon organisaatioiden edustajien kanssa. Keskustelujen tarkoituksena oli tarkentaa valtionhallinnon organisaatioiden riskienhallinnalle kohdistuvia odotuksia, meneillään tai suunnitteilla olevia kehittämistoimenpiteitä tai kehittämisen avuksi tarjolla olevia palveluja ja välineitä.

Ennen opinnäytetyön tavoitteiden ja opinnäytetyön näkökulman täsmentymistä harkittiin keskeiseksi käsitteeksi riskienhallinnan ohella myös muun muassa turvallisuusjohtamista tai organisaatioturvallisuutta. Kirjallisuuteen perehtymällä pyrittiin aluksi päättämään minkä käsitteen kautta lähestyä sitä toimintaa, millä kohdeorganisaation häiriötöntä toimintaa, arvoja ja tavoitteiden toteutumista pyritään suojaamaan sekä huolehtimaan turvallisuuteen liittyvistä velvoitteista. Riskienhallinnan käsitteeseen on lopulta päädytty ennen kaikkea mielleyhtymän kautta - vaikka esimerkiksi turvallisuusjohtamisen tavoitteet ja menetelmät ovat pääosin yhteneviä riskienhallinnan kanssa, viittaa käsitteen sävy vahinkojen ja vaarojen hallitsemiseen kokonaisvaltaisen tavoitteiden suojaamisen, ei-toivottujen tapahtumien välttämisen ja mahdollisuuksien hyödyntämisen sijaan.

Tässä työssä riskienhallinnalla tarkoitetaan toimintaa, jolla tunnistetaan, arvioidaan ja hallitaan organisaation tavoitteita, toimintaa ja muita organisaation suojattavia arvoja uhkaavia seikkoja tai menetettyjä mahdollisuuksia. Kokonaisvaltaisella riskienhallinnalla tarkoitetaan organisaation toiminnan kaikille tasoille ja osa-alueille ulottuvaa prosessia, jolla suojataan organisaatiota tunnistamalla siihen vaikuttavia tapahtumia ja mahdollistetaan hallittu riskinotto. Muuta riskienhallinnan ja siihen läheisesti liittyvää käsitteistöä on avattu erillisessä taulukossa (liite 1).

Aluehallintovirastolla tarkoitetaan aluehallintovirastoista annetun lain tarkoittamia monialaisia perusoikeuksien ja oikeusturvan toteutumista, peruspalvelujen saatavuutta, ympäristön kestävää käyttöä ja ympäristönsuojelua, terveellistä ja turvallista elin- ja työympäristöä sekä sisäistä turvallisuutta edistäviä valtion aluehallinnon virastoja. Kohdeorganisaatiolla tarkoitetaan tässä työssä tarkastelun kohteena olevaa tiettyä aluehallintovirastoa. Kyseistä aluehallintovirastoa ei yksilöidä.

1.4 Raportin rakenne

Johdannon jälkeisessä luvussa käsitellään aluehallintovirastoja niiden tehtävien sekä toiminnan ohjaamisen ja johtamisen kautta. Aluehallintovirastoja käsitellään sekä yleisesti että kohdeorganisaation tapauksessa. Kolmannessa luvussa muodostetaan opinnäytetyön teoreettisen viitekehyksen keskeinen osa riskienhallinnan tarkoituksen ja ominaisuuksien sekä riskienhallintaprosessin vaiheiden kautta. Lopuksi tarkastellaan riskienhallintaan liittyväksi katsottuja säädösvelvoitteita sekä riskienhallinnan, tuvallisuusjohtamisen ja muiden näihin läheisesti liittyvien käsitteiden yhteyttä. Neljännessä luvussa luodaan katsaus riskienhallinnan piirteisiin ja toteutumiseen valtionhallinnossa, jonka lisäksi esitellään valtiovarainministeriön antama suositus sisäisestä valvonnasta ja riskienhallinnasta valtion virastossa, laitoksessa ja rahastossa.

Tutkimusaineisto ja tutkimuksen toteuttaminen esitellään raportin viidennessä luvussa. Luvussa on eritelty aineiston hankinta sekä aineiston luokittelu ja analysoiminen. Tutkimustulokset esitellään kuudennessa luvussa. Tuloksina esitellään ensin kohdeorganisaation riskienhallinnan nykytilaa koskevat tulokset ja tämän jälkeen kohdeorganisaation riskienhallinnalle kohdistuvia odotuksia koskevat tulokset. Riskienhallinnan nykytilaa verrataan sekä sille kohdistettuihin odotuksiin että muodostettuun riskienhallinnan viitekehykseen johtopäätöksissä raportin seitsemännessä luvussa. Johtopäätösten yhteydessä vedetään yhteen kohdeorganisaatiossa toteutuvat riskienhallintaan liittyvät nykyiset menettelyt ja rakenteet. Johtopäätöksinä esitetään lisäksi toimenpide-ehdotuksia kohdeorganisaation riskienhallinnan kehittämiseksi. Toimenpide-ehdotukset on annettu kokonaisvaltaisen riskienhallinnan näkökulmasta ja ne koskevat riskienhallinnan määrittelemistä, toteuttamista ja jalkauttamista. Johtopäätösten lopuksi arvioidaan opinnäytetyötä tehtyjen valintojen ja saavutettujen tulosten kautta. Lisäksi esitetään aiheita jatkotutkimuksille.

Raportin lopussa ovat lähde-, kuvio- ja taulukkoluettelot sekä liitteet. Liitteinä ovat riskienhallintaan liittyvää käsitteistöä sisältävä taulukko, valtiovarain controller –toiminnon antaman suosituksen sisäisen valvonnan ja riskienhallinnan suppea arviointikehikko, tutkimuksen empiirisen aineiston esittelevä taulukko, dokumenttianalyysin analyysirunko, tutkimustulosten ja johtopäätösten yhteydessä viitatut empiirisen aineiston sisältämät kuviot sekä opinnäytetyön tuotoksena laadittu ohje riskienhallinnan periaatteiden muodostamiseksi kohdeorganisaatiossa.

2 Aluehallintovirastot

Aluehallintovirastot muodostettiin valtion aluehallintouudistuksen yhteydessä 1.1.2010. Aluehallintovirastot hoitavat aiempien lääninhallitusten, ympäristölupavirastojen, alueellisten ympäristökeskusten ja työsuojelupiirien tehtäviä. Osa palveluista siirtyi samaan aikaan perustettuihin elinkeino-, liikenne- ja ympäristökeskuksiin, joiden nimestä käytetään lyhennettä ELY-keskus. (Aluehallinto 2014.) Virastoja on Manner-Suomessa kuusi ja niiden toimialueet koostuvat yhden tai useamman maakunnan alueesta. Ahvenanmaalla aluehallintoviranomaisena toimii Ahvenanmaan valtionvirasto. (Aluehallintovirastot 2014.)

Tässä luvussa esitellään aluehallintovirastojen tehtävät ja organisointi. Lisäksi luodaan katsaus aluehallintovirastojen ohjaamisen ja johtamisen menettelyihin sekä todetaan joitakin aluehallintovirastojen toimintaa koskettavia meneillään olevia tai mahdollisia tulevia muutoksia.

2.1 Aluehallintovirastojen tehtävät

Virastojen tehtävänä on edistää toimialueellaan perusoikeuksien ja oikeusturvan toteutumista, peruspalvelujen saatavuutta, ympäristön kestävää käyttöä ja ympäristönsuojelua, terveellistä ja turvallista elin- ja työympäristöä sekä sisäistä turvallisuutta. Virastot hoitavat lainsäädännön toimeenpano-, ohjaus- ja valvontatehtäviä alueillaan. Aluehallintovirasto myös ohjaa, valvoo ja kehittää maistraattien toimintaa. Virasto on ministeriöiden edustaja ja se toteuttaa niiltä saamiaan tehtäviä toimialueellaan. (Aluehallintovirastot 2014.)

Aluehallintovirastoista annetun lain (Laki aluehallintovirastoista 896/2009, 4 §) mukaan aluehallintovirastot hoitavat niille erikseen säädettyjä tehtäviä sosiaali- ja terveydenhuollon, ympäristöterveydenhuollon, koulutus- ja muun sivistystoimen, oikeusturvan edistämisen ja toteuttamisen, ympäristönsuojelun- ja vesilainsäädännön alaan kuuluvien lupa- ja muiden hakemusasioiden, pelastustoimen, työsuojelun valvonnan ja kehittämisen, työssä käytettävien tuotteiden tuotevalvonnan sekä työsuojelulainsäädännön noudattamisen valvonnan ja kuluttaja- ja kilpailuhallinnon toimialoilla.

Edellisen lisäksi aluehallintovirastojen tehtävänä on peruspalvelujen alueellisen saatavuuden arviointi ja maistraattien ohjaus sekä näiden valvonta ja kehittäminen. Yhteiskunnan varautumiseen liittyvinä tehtävinä aluehallintovirastolla on varautumisen yhteensovittaminen toimialueellaan ja siihen liittyvän yhteistoiminnan järjestäminen, valmiussuunnittelun yhteensovittaminen, alueellisten maanpuolustuskurssien järjestäminen, kuntien valmiussuunnittelun tukeminen, valmiusharjoitusten järjestäminen sekä alue- ja paikallishallinnon turvallisuussuunnittelun edistäminen. Viraston tehtävänä on lisäksi viranomaisten johtaessa turvallisuuteen liittyviä tilanteita alueella tukea toimivaltaisia viranomaisia ja tarvittaessa sovittaa yhteen toimintaa niiden kesken. (Laki aluehallintovirastoista 896/2009, 4 §)

Aluehallintovirastojen ydinprosessit ovat tasa-arvoinen yhteiskunta – oikeusturvaprosessit, hyvinvoiva yhteiskunta – hyvinvointiprosessit sekä turvallinen yhteiskunta - turvallisuusprosessit. Oikeusturvaprosessit liittyvät perusoikeuksiin ja oikeusturvaa, hyvinvointiprosessit peruspalvelujen saatavuuteen ja tasoon ja turvallisuusprosessit asuin-, työ- ja elinympäristön terveellisyyteen ja turvallisuuteen. Ydinprosessit leikkaavat virastojen kaikkien vastuualueiden läpi. (Aluehallintovirastojen tulosohjaustyöryhmä 2011, 14.)

Aluehallintovirasto on organisoitunut kuuteen vastuualueeseen, joiden lisäksi virastossa on sen hallintopalveluja hoitava vastuuyksikkö. Vastuualueet ovat peruspalvelut, oikeusturva ja luvat -vastuualue, opetus- ja kulttuuritoimi -vastuualue, ympäristölupavastuualue, työsuojelun vastuualue sekä pelastustoimi ja varautuminen -vastuualue. (Valtioneuvoston asetus aluehallintovirastoista 906/2009, 2 §.) Kaikkia vastuualueita ei kuitenkaan ole kaikissa aluehallin-

tovirastoissa, vaan yksi vastuualue voi hoitaa tehtäviä useamman aluehallintoviraston toimialueella. Kaikissa aluehallintovirastoissa on kuitenkin peruspalvelut, oikeusturva ja luvat sekä pelastustoimi ja varautuminen –vastuualueet. (Valtioneuvoston asetus aluehallintovirastoista 906/2009, 3 §; Organisaatio 2014a.) Kohdeorganisaatiossa on kaikki edellä mainitut vastuualueet, ja se hoitaa joitakin tehtäviä useamman viraston alueella (Toimialueet 2014). Kohdeorganisaation vastuulla on myös valtakunnallisia erikoistumistehtäviä (Valtioneuvoston asetus aluehallintovirastoista 906/2009).

Hallintopalvelujen vastuuyksikön tehtävän on huolehtia virastojen yleisistä hallinnollisista tehtävistä liittyen taloushallintoon, toiminta- ja taloussuunnitteluun, henkilöstöhallintoon, tietopalveluun ja viestintään. Yksiköllä voi olla myös erikseen määrättyjä tehtäviä ja muita viraston sisäisen toiminnan tukemiseen liittyviä tehtäviä. (Valtioneuvoston asetus aluehallintovirastoista 906/2009, 5 §.)

Valtiovarainministeriö on syksyllä 2013 asettanut projektin valmistelemaan aluehallintovirastojen hallinnollisten palvelujen kokoamista. Hallinnolliset palvelut käsittävät hallintopalvelujen vastuuyksiköiden lisäksi aluehallintovirastojen yhteiset erikoistumisyksiköt. Projektilla tavoitellaan hallinnollisiin tehtäviin liittyvän henkilöstötarpeen vähentämistä sekä toiminnan yhtenäistämistä. Hallinnollisten tehtävien kokoaminen pyritään toteuttamaan vuoden 2015 alusta siten, että tehtävät kootaan yhden aluehallintoviraston alaisuuteen perustettavalle aluehallintovirastojen hallinto- ja kehittämispalvelut -vastuualueelle. Vastuualueen henkilöstö kuitenkin työskentelisi hajautettuna eri aluehallintovirastoihin. (Aluehallintovirastojen hallinnollisten tehtävien…2014, 9, 49.)

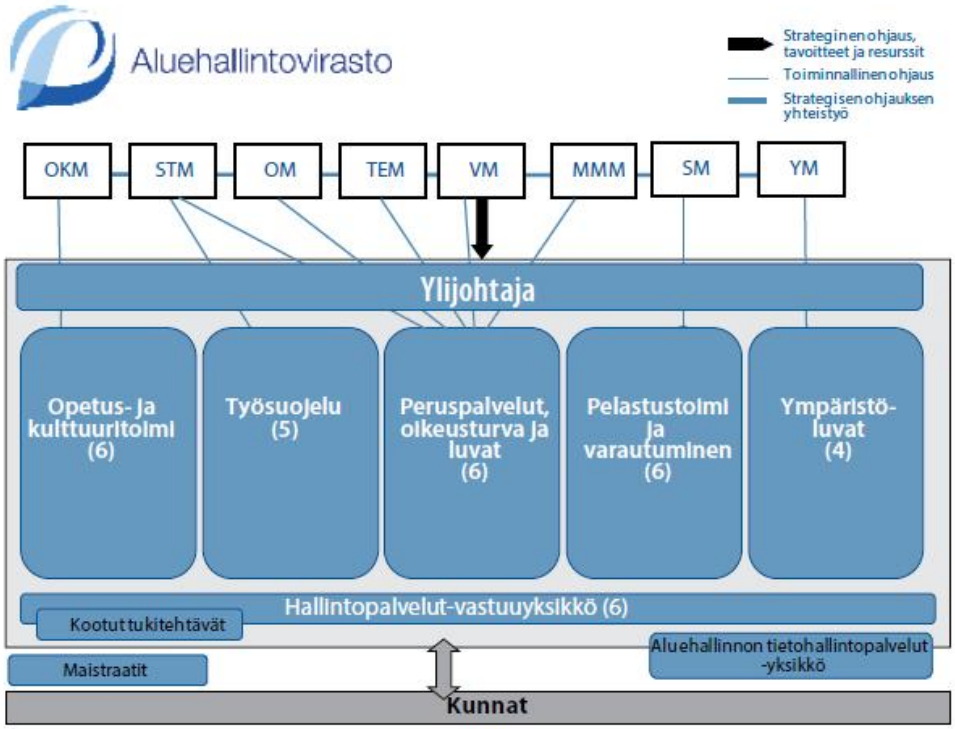
Hallinnollisten palvelujen kokoamishankkeen myötä aluehallintovirastojen erilliset hallintopalvelujen vastuuyksiköt lakkautettaisiin. Yhteisen aluehallintovirastojen hallinto- ja kehittämispalvelut –vastuualueen lisäksi jokaiseen aluehallintovirastoon perustettaisiin viraston johdon tuki –toiminto turvaamaan viraston johdon toimintaedellytykset. Toiminnon henkilöresurssi olisi projektin esityksen mukaan hyvin pieni. Tehtäviin kuitenkin sisältyisi muun muassa viraston ylijohtajan sihteerin tehtävät ja ylijohtajan määräämät viraston johtamista ja toiminnan kehittämistä tukevat tehtävät, strategisen tulossopimuksen valmistelu, koordinointi ja seuranta sekä tuloksellisuusraportointi, toimintaympäristön analysointi, alueellinen ja sidosryhmäyhteistyö sekä viraston sisäiseen turvallisuuteen ja varautumiseen liittyvät tehtävät ja viraston sisäisen valvonnan koordinointi. (Aluehallintovirastojen hallinnollisten tehtävien…2014, 57.)

Esillä on ollut myös valtion aluehallinnon toimijoiden mahdollinen yhdistäminen tai muu toimintojen järjestäminen uudelleen. Valtiovarainministeriö on vuonna 2014 asettanut keskus- ja aluehallinnon virastoselvitys –hankkeen, jonka tavoitteet ovat sekä keskushallinnon että

aluehallinnon osalta lukuisia (Valtiovarainministeriö 2014a, 1-3). Keskeinen tavoite on selkeä yhtenäinen valtionhallinto. Hankeen yleisesittelyssä esiintyy mahdollisina valtion aluehallinnon rakenneuudistusvaihtoehtoina myös aluehallintovirastojen, ELY-keskusten, maistraattien ja TE-keskusten yhdistäminen (Valtiovarainministeriö 2014b, 22).

2.2 Aluehallintovirastojen toiminnan ohjaaminen ja johtaminen

Aluehallintovirastolla on haasteena lukuisten toimialojen tehtävien hoitaminen, ja siten usean ohjaavan ministeriön ohjauksessa toimiminen. Suoran ohjauksen lisäksi virastolle kohdistuu odotuksia lukuisilta sidosryhmiltä. Aluehallintovirastojen toimintaa ohjaavat omilla toimialoillaan oikeusministeriö, sisäasiainministeriö, valtiovarainministeriö, sosiaali- ja terveysministeriö, opetus- ja kulttuuriministeriö, maa- ja metsätalousministeriö, työ- ja elinkeinoministeriö, ympäristöministeriö sekä se keskushallinnon virasto, jonka tehtäväksi ohjaus on erikseen säädetty. Aluehallintoviraston yhteisiä toimintoja ja muita viraston yhtenäisen toiminnan kannalta tarpeellisia toimenpiteitä koskevasta toiminnallisesta ohjauksesta huolehtii valtiovarainministeriö (kuvio 1). Myös aluehallintovirastojen yleishallinnollinen ohjaus on valtiovarainministeriön tehtävä. (Laki aluehallintovirastoista 896/2009, 7 §, 10 §.)



Kuvio 1: Aluehallintoviraston organisaatio ja ohjaus (Aluehallintovirastojen ja elinkeino-, liikenne- ja ympäristökeskusten ohjausjärjestelmän kehittämistyöryhmä 2014, 17).

Valtiovarainministeriö vastaa lisäksi aluehallintovirastojen strategisen suunnittelun ja ohjauksen järjestämisestä ja koordinoinnista sekä siitä, että virastoille laaditaan strategia-asiakirjat ja strategiset tulostavoiteasiakirjat (Valtioneuvoston asetus aluehallintovirastoista 906/2009, 14 §). Tätä tukemaan on asetettu aluehallintovirastojen ohjausryhmä sekä sille käsiteltävät asiat valmisteleva aluehallintovirastojen tulosohjausryhmä (Valtiovarainministeriö 2013, 1-2).

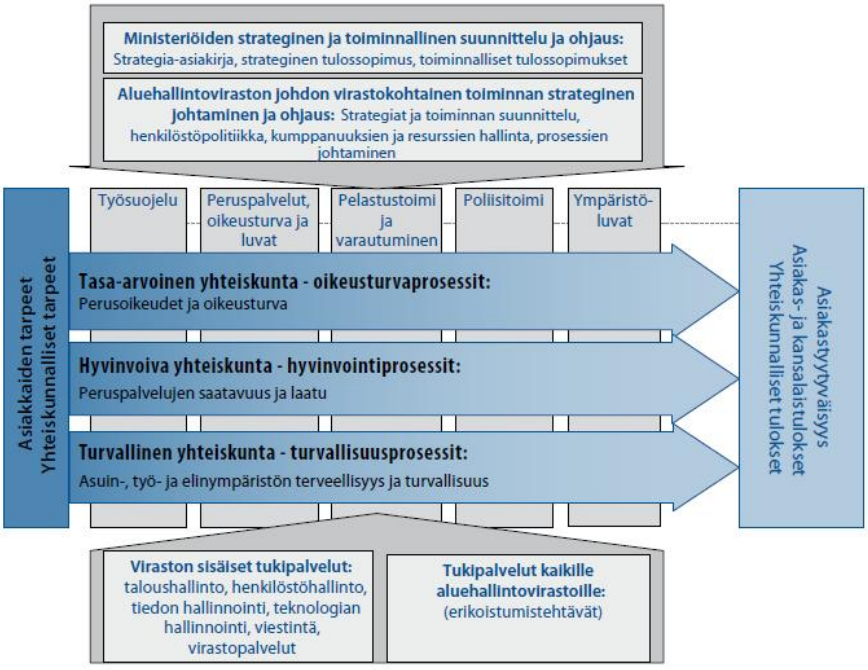
Strategia-asiakirjassa esitetään muun muassa hallitusohjelmasta ja toimintaympäristön muutostekijöistä johdettavat aluehallintovirastojen yhteiset strategiset tavoitteet. Asiakirja muodostetaan ministeriöiden ja aluehallintovirastoja ohjaavien keskushallinnon viranomaisten yhteistyössä näkemykseksi siitä, kuinka valtakunnalliset tavoitteet jalkautetaan aluehallintovirastojen alueelliseen toimintaan. Tarkoituksena on sovittaa yhteen eri hallinnonalojen tavoitteita ja parantaa näin aluehallinnon toimintaedellytyksiä. Strategia-asiakirja on aluehallintovirastoille yhteinen. Se laaditaan hallituskaudeksi ja sen sisältö tarkistetaan tarvittaessa vuosittain. Nykyinen strategia-asiakirja on laadittu vuosille 2012-2015. (Aluehallintovirastojen tulosohjaustyöryhmä 2011, 5.)

Strateginen tulostavoiteasiakirja laaditaan erikseen kullekin aluehallintovirastolle. Myös tämä asiakirja laaditaan hallituskaudeksi, mutta sitä tarkistetaan vuosittain. (Laki aluehallintovirastoista 896/2009, 8 §.) Tulostavoiteasiakirjan sisältö johdetaan strategia-asiakirjasta. Lisäksi asiakirjan sisältöön vaikuttavat maakuntaohjelmat toteuttamissuunnitelmineen. Asiakirjassa määritellään virastolle keskeiset toimintalinjat ja tulostavoitteet, yhteistyökysymykset ja hallinnonalakohtaiset määrärahapuitteet sekä valtion kanta maakuntaohjelmien toteuttamissuunnitelmien mukaisten hankkeiden toteuttamiseen. (Valtioneuvoston asetus aluehallintovirastoista 906/2009, 14 §.)

Aluehallintovirastojen toiminnallisesta ohjauksesta ja siitä, että virastoille laaditaan tarvittaessa toiminnalliset tulostavoiteasiakirjat vastaa toimialaa ohjaava ministeriö tai keskushallinnon virasto. Toiminnallisissa tulosasiakirjoissa määritetään toimintasektorikohtaiset vuosittaiset tai muut lyhyen aikavälin toimintaa koskevat tulostavoitteet sekä näihin kohdistetut taloudelliset resurssit toimintavuodeksi. Asiakirjaa valmisteltaessa tulee ohjaavan ministeriön tai keskushallinnon viraston neuvotella kyseisen aluehallintoviraston, jotta saavutettaisiin yhteinen näkemys toimintavuoden tulostavoitteista ja tarvittavista voimavaroista. (Valtioneuvoston asetus aluehallintovirastoista 906/2009,15 §.)

Aluehallintovirastoa johtaa viraston johtaja, joka vastaa viraston toiminnan tuloksellisuudesta ja viraston yhteisten tulostavoitteiden saavuttamisesta. Viraston vastuualueita johtavat vastuualueiden päälliköt, jotka vastaavat vastuualueen toiminnan tuloksellisuudesta ja tulostavoitteiden saavuttamisesta. Viraston johtajan nimikkeenä on ylijohtaja ja vastuualueiden sekä hallintopalvelujen vastuuyksikön päälliköiden nimikkeinä johtajat (Valtioneuvoston asetus

aluehallintovirastoista 906/2009, 4 §). Aluehallintoviraston johtoryhmä huolehtii viraston toimintojen yhteensovittamisesta. Johtoryhmän muodostavat puheenjohtajana toimiva viraston johtaja sekä viraston työjärjestyksessä määrätyt henkilöt. Virastolla tulee olla työjärjestys, josta päättää viraston johtaja. Myös vastuualueilla voi tarvittaessa olla työjärjestys. Vastuualueen työjärjestyksestä päättää vastuualueen päällikkö. (Laki aluehallintovirastoista 896/2009, 11 §, 13 §.) Kohdeorganisaatiossa johtoryhmän muodostavat viraston ylijohtaja, vastuualueiden ja hallintopalvelujen vastuuyksikön johtajat sekä viestinnän vastuuhenkilö asiantuntijana ja henkilöstön edustus. Aluehallintovirastojen ohjausasiakirjojen, vastuualueiden ja ydinprosessien yhteys voidaan esittää myös rakennekaaviona (kuvio 2).



Kuvio 2: Aluehallintovirastojen ohjausasiakirjat, vastuualueet ja ydinprosessit (Aluehallintovirastojen tulosohjaustyöryhmä 2011, 14).

Aluehallintovirastojen ja ELY-keskusten ohjausjärjestelmää ollaan kehittämässä. Valtiovarainministeriö on asettanut vuonna 2013 työryhmän virastojen ohjausjärjestelmän kehittämiseksi. Ohjausmallia on tarkoitus selkeyttää ja yksinkertaistaa siirtymällä kaksiportaiseen ohjaus- ja suunnittelujärjestelmään. Työryhmän raportin mukaan sekä aluehallintovirastojen että ELY-keskusten ohjausjärjestelmää tulisi kehittää strategisemmaksi, kevyemmäksi, poikkihallinnollisemmaksi ja yhtenäisemmäksi. (Aluehallintovirastojen ja elinkeino-, liikenne- ja ympäristökeskusten ohjausjärjestelmän kehittämistyöryhmä 2014, 13, 39.) Ohjausjärjestelmän kehittäminen juontaa hallitusohjelmaan. Hallitusohjelman mukaisesti on myös tarkoitus vahvistaa valtion aluehallinnon toiminnan yhdenmukaisuutta maan eri osissa (Valtiovarainmisiteriö 2013, 1).

3 Riskienhallinnan viitekehys tässä tutkimuksessa

Riskienhallinnan käsite ei ole täysin vakiintunut (Kerko 2001, 12). Useimmiten siinä on kuitenkin kysymys organisaation toiminnan varmistamisesta. Yritystoiminnassa riskienhallinnalla on rooli omistajien ja rahoittajien tuottoon liittyvien odotusten täyttämisestä, siihen liittyvien epävarmuuksien hallinnasta ja sijoitusten turvaamisesta. Riskienhallinta on siten osa organisaation strategisten tavoitteiden saavuttamista ja ylipäätään sen johtamista. (Ilmonen ym. 2013, 5, 36.) Suomisen (2003, 27) mukaan riskienhallinnalla on perinteisesti tarkoitettu yritystä uhkaavien vaarojen torjumiseen ja niistä aiheutuvien menetyksien minimoimiseen käytettävää prosessia. Sosiaali- terveysministeriön (2011, 8) mukaan riskienhallinta on myös organisaation eettisen ja yhteiskunnallisen vastuun kantamista. Valtiovarain controller –toiminto (2005, 11) puolestaan määrittelee riskienhallinnan olevan toimintatapoja, rakenteita ja prosesseja, joilla tunnistetaan ja arvioidaan sekä hallitaan organisaation tavoitteiden saavuttamista uhkaavia riskejä sekä avautuneiden toimintamahdollisuuksien menettämistä.

Riskienhallinnan tarkoituksena on tukea liiketoimintaan liittyvää päätöksentekoa siten, että johto ymmärtää toimintaan ja tehtäviin päätöksiin liittyvät riskit. Tavallisimmin riskienhallinnalla käsitetään organisaation toiminnan suojaamista ei-toivotuilta tapahtumilta. Keskeisenä tavoitteena nähdään tällöin toiminnan häiriöttömyyden ja jatkumisen, toimintavarmuuden, turvallisuuden ja laadun kaltaiset asiat. Riskienhallinnan keskeisimpiä perusasioita on se, että riskillä on myös toinen puoli. Riskien olemuksen ymmärtämiseksi tulee huomata sen kaksoismerkitys; riski ja sen hallinta laajasti nähtynä sisältää myös mahdollisuuden toivottuun tapahtumaan, kuten liikevoittoon. Kaikkeen liiketoimintaan liittyy riski, ja yritystoiminnassa onkin lopulta aina kysymys riskien ottamisesta. Riskienhallinta tässä yhteydessä tavoittelee tilannetta, jossa riskien ottaminen on hallittua toimintaa. Sen lähestyminen ainoastaan negatiivisten riskien kautta ei hyödynnä riskienhallinnan kokonaisvaltaisia mahdollisuuksia. (Ilmonen ym. 2013, 5, 10, 15, 69.)

Riskienhallinnan luonteeseen liittyy myös käsitys siitä, että havaituista uhkista ja vaaroista tulee riskejä vasta kun ne ovat relevantteja yrityksen toiminnan kannalta (Ilmonen ym. 2013, 98). Myös Mäkisen (2007, 106) mukaan riskin tulee vaikuttaa haitallisesti asetettujen tavoitteiden saavuttamiseen.

Riskienhallinnan tavoitteet ovat ajan kuluessa muuttuneet. Muutos on ollut seurausta alan kehittymisestä, mutta myös ulkoa osoitetuista uusista vaatimuksista liittyen esimerkiksi yritysten talousprosesseihin. Yritysmaailmassa riskienhallinnasta on tuloissa myös kilpailutekijä erityisesti aloilla, joilla toiminnan luotettavuutta korostetaan. Näiden alojen toimijat soveltavat itse riskienhallinnan standardeja ja edellyttävät prosesseihinsa liittyviltä muilta toimijoilta samaa. Globaalien taloudellisten kriisien jälkeen myös omistajat ja sijoittavat ovat alka-

neet vaatimaan parempaa tietoa yrityksen riskeistä. (Ilmonen ym. 2013, 34, 42.) Suomisen (2003, 153) mukaan yritystoiminnassa kiinnitetään nykyisin runsaasti huomiota toiminnan varmuuteen ja laatuun, ja laatuun liittyvät ratkaisut voidaan katsoa riskienhallinnan sukulaiseksi. Laadukas häiriötön toiminta on koko tuotantoketjun intressi tuotteen valmistajasta asiakkaaseen.

Yrityksen omistajien osalta liiketoiminnan riskissä on kysymys erityisesti siitä, että he menettävät sijoituksensa. Yrityksen johdolla ei välttämättä ole tätä riskiä, mutta sen tekemiin liiketoimintaan liittyviin päätöksiin liittyy riski esimerkiksi työpaikkojensa menetyksistä. Yrityksen omistajilla ja sen johdolla on jo tätä kautta yhteinen intressi toiminnan ja tavoitteiden suojaamisessa ja sitä koskevissa pelisäännöissä. (Ilmonen ym. 2012, 30.)

Riskienhallinnan avulla organisaatio pystyy toimimaan myös poikkeavissa tilanteissa. Jos toiminnan jatkuvuuden varmistaminen on laiminlyöty, eivät hyvin laaditut strategiatkaan auta. Ilman riskienhallintaa yritys tulisi toimeen ainoastaan sellaisissa ihanneolosuhteissa, jossa sillä olisi täydellinen toimintavarmuus ja käytössään kaikki tieto. Tällaisia olosuhteita ei ole mahdollista järjestää, jolloin riskienhallinnan merkitys kasvaa keinona sietää epävarmuutta. (Suominen 2003, 195, 205.)

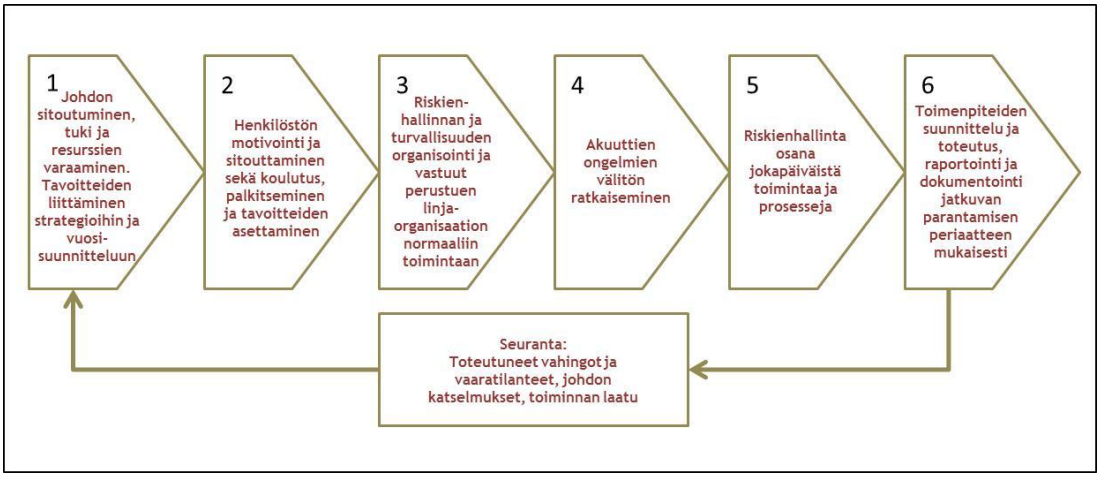
Tavallisesti organisaatioissa tapahtuu riskienhallintaa huomaamattakin toteutettaessa lainsäädännön osoittamia velvoitteita esimerkiksi työsuojeluasioissa. Järjestelmällisestä riskienhallinnasta on kuitenkin kysymys vasta silloin, kun päätöksistä perusteluineen ja niiden mahdollisista seurauksista puhutaan systemaattisella tavalla. Systemaattisessa riskienhallintatyössä keskeisessä asemassa on sitä varten synnytetty dokumentaatio. (Ilmonen ym. 2013, 61.)

Riskienhallinnan toteutumiseen eri turvallisuuden osa-alueiden yhteydessä viittaa myös Leppänen (2008, 59, 61, 203-204), jonka mukaan riskienhallintatoimenpiteet toteutetaan organisaatioturvallisuuden osa-alueiden avulla. Organisaatioturvallisuus on sisällöltään yritysturvallisuutta vastaava käsite. Organisaatioturvallisuuden käsite on tarpeen, sillä turvallisuusjohtamista toteutetaan nykyisin yritysten lisäksi monissa muissakin organisaatioissa, kuten julkisen hallinnon virastoissa ja kunnissa. Elinkeinoelämän keskusliitto EK:n sekä sen jäsenliittojen ja -yritysten yhteistyöorganisaationa toimiva Yritysturvallisuuden neuvottelukunta määrittelee yritysturvallisuuden osa-alueiksi henkilöturvallisuuden, kiinteistö- ja toimitilaturvallisuuden, pelastustoiminnan, rikosturvallisuuden, tietoturvallisuuden, tuotannon ja toiminnan turvallisuuden, työturvallisuuden, ulkomaantoimintojen turvallisuuden, ympäristöturvallisuuden ja valmiussuunnittelun (Yritysturvallisuus 2014).

3.1 Kokonaisvaltainen riskienhallinta

Kokonaisvaltainen riskienhallinta, englanniksi enterprise risk management, on Mäkisen (2007, 106) mukaan organisaation kaikille osa-alueille ulottuvaa riskienhallintaa, ja se eroaa siten perinteisestä taloudellisiin kysymyksiin keskittyneestä riskienhallinnasta. Kokonaisvaltaisessa riskienhallinnassa tarkastelun kohteena on tavallisesti organisaation strategisten tavoitteiden saavuttaminen estämällä siihen kohdistuvat uhat ja hyödyntämällä siihen liittyvät mahdollisuudet. Kokonaisvaltaisen riskienhallinnan toteuttaminen ei tarkoita jonkin tietyn kokonaisvaltaisen riskienhallinnan standardin toteuttamista - kokonaisvaltaisuus tarkoittaa lähestymistapaa riskienhallinnan organisointiin, ei tiettyä tapaa toimia. (Ilmonen ym. 2013, 16, 43.)

Useat lähteet korostavat tarvetta sitoa riskienhallinta osaksi organisaation johtamista ja päivittäistä toimintaa. Juvosen, Korhosen, Ojalan, Salosen ja Vuoren (2005, 145) mukaan tarkasteltaessa riskienhallintaa osana johtamista, havaitaan sen yhteys jokapäiväiseen toimintaan, ja riskienhallinnan onkin ulotuttava strategiasuunnittelusta arkirutiineihin. Myös sosiaali- ja terveysministeriön (2011, 7) mukaan riskienhallinta ja sen suunnittelu sekä seuranta sisältyvät normaaliin johtamiseen, ohjaukseen ja päätöksentekoon (kuvio 3). Samaa korostavat myös esimerkiksi Suominen (2003, 28) ja valtiovarain controller –toiminto (2005, 12): tehokas riskienhallinta on integroitu osaksi yrityksen liikkeenjohtojärjestelmää, ja linjajohdon tulee omaksua riskienhallintaan kuuluvat toimintamallit ja viedä niitä kaikille organisaatiotasoille. Myös Ilmosen (2013, 39) mukaan riskienhallinnan sisällyttäminen perusprosesseihin on keskeistä.



Kuvio 3: Riskienhallinnan järjestäminen sosiaali- ja terveysministeriön (2011, 20) mukaan.

Riskienhallintaa ei tule nähdä kerran tai ajoittain toteutettavan projektina, vaan toiminnan jatkuvaan kehittämiseen tähtäävänä prosessina. Kokonaisvaltaista riskienhallintaa järjestettäessä tulee keskeisenä tavoitteena olla riskienhallintaprosessin mutta erityisesti riskiraportoinnin ja riskienhallintatoimenpiteiden sovittamien ja integroiminen osaksi liiketoimintaa.

On tärkeää miettiä kuinka riskienhallinta sidotaan strategia- ja vuosisuunnitteluprosessiin ajallisesti ja prosessuaalisesti. Riskienhallinnan kytkeminen suunnitteluprosessiin on kaikkein tärkein suunniteltava asia riskienhallintaa kehitettäessä. Kytkennän onnistuessa riskienhallinta muodostuu normaalin johtamisen ja suunnitteluprosessin luontevaksi osaksi. Riskienhallinnan integroiminen kaikkeen johtamiseen myös helpottaa keskittymistä organisaation tavoitteiden kannalta oleellisiin asioihin. (Ilmonen ym. 2013, 16, 74, 84, 87.)

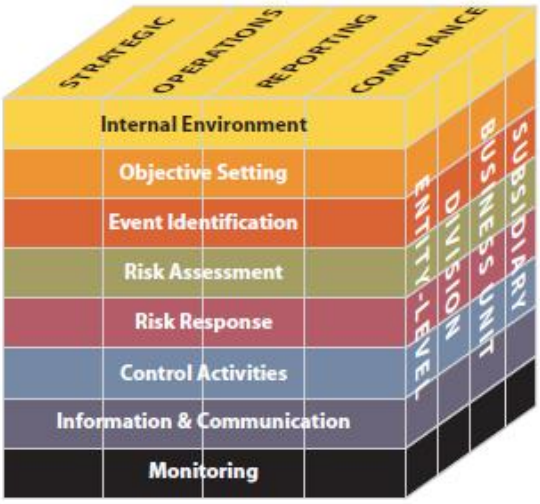
Johtamiseen ja päivittäiseen toimintaan kytkemisen lisäksi keskeistä on tarkastella riskienhallintaa suhteessa organisaation tavoitteisiin. Organisaation johdon tulee johtamisessaan sekä strategian ja tavoite- ja toimintasuunnitelmien käsittelyn yhteydessä tunnistaa ja analysoida riskit ja sellaiset tapahtumat, joilla on merkitystä organisaation tavoitteiden saavuttamiselle ja sen toiminnan jatkuvuudelle. (Sosiaali- ja terveysministeriö 2011, 10.) Myös Suomisen (2003, 31) mukaan tulee yrityksen koosta riippumatta korostaa riskienhallinnan liittämistä yrityksen tavoitteisiin. Tämä senkin vuoksi, että riskienhallinnan jäädessä irralliseksi toiminnokseen, jää se helposti liian vähälle huomiolle.

Vaikka riskienhallinta tulisi sitoa osaksi prosesseja, täytyy se mieltää tukiprosessin asemaan. Se tulisi pitää mahdollisimman yksikertaisena ja selkeänä, jottei se siirrä huomiota pois siitä varsinaisesta tekemisestä, jota varten organisaatio on olemassa. Tavoitteena on syytä olla käytännöllinen lähestymistapa. Monimutkaistuessaan riskienhallinta voi alkaa tuntua taakalta ja sen tuoma lisäarvo unohtua. (Ilmonen ym. 2013, 39.)

Kokonaisvaltaisesta riskienhallinnasta puhuttaessa mainitaan usein COSO-ERM –malli kokonaisvaltaisen riskienhallinnan viitekehyksenä. COSO-ERM –mallin mukaan riskienhallinta on organisaation kaikille organisaation osa-alueille ja tasoille ulottuva prosessi, jolla tavoitellaan kohtuullista varmuutta organisaation tavoitteiden saavuttamisesta. Prosessilla tunnistetaan organisaatioon kohdistuvia potentiaalisia tapahtumia ja pidetään riskit riskinottohalukkuuden rajoissa. Riskienhallinta tarkoittaa strategian ja riskinottohalukkuuden yhdenmukaistamista, tehokkaampaa riskeihin vastaamista, toiminnallisten yllätysten ja tappioiden vähentämistä, monitahoisten ja koko organisaatiota koskevien riskien tunnistamista ja hallintaa, tilaisuuksiin tarttumista sekä tehokkaampaa pääoman käyttöä. (Committee of Sponsoring Organizations of the Treadway Commission 2004, 1-2.)

Organisaation tavoitteiden ja sen riskienhallinnan osa-alueiden suhdetta on kuvataan COSO-ERM –mallissa kolmiulotteisena kuutiomatriisina. Matriisin yhden sivun muodostavat tavoitealueet, jotka mallissa muodostavat strategiset, toiminnalliset, raportointia koskevat sekä vaatimustenmukaisuutta koskevat tavoitteet (kuvio 4).

Matriisin toisella sivulla on kuvattu riskienhallinnan kahdeksan osa-aluetta. Riskienhallinta koostuu mallin mukaan kahdeksasta kiinteästi organisaation johtamisprosessiin liittyvästä osa-alueesta, jotka ovat muun muassa organisaation riskienhallintafilosofian ja –halukkuuden muokkaama sisäisen valvontaympäristö, organisaation tavoitteiden asettaminen, asetettujen tavoitteiden saavuttamiseen liittyvien riskejä ja mahdollisuuksia koskevien sisäisten ja ulkoisten tapahtumisen tunnistaminen, tunnistettujen riskien arvioimien niiden toteutumistodennäköisyyteen ja vaikutuksiin perustuen, riskeihin vastaaminen organisaation johdon määrittelemin toimenpitein, päätetyt valvontamenettelyt, tehtävien hoitamiseen tarvittavan tiedon vertikaalinen ja horisontaalinen viestintä, sekä riskienhallinnan toteutumiseen liittyvä seuranta ja arviointi. (Committee of Sponsoring Organizations of the Treadway Commission 2004, 3-4.)



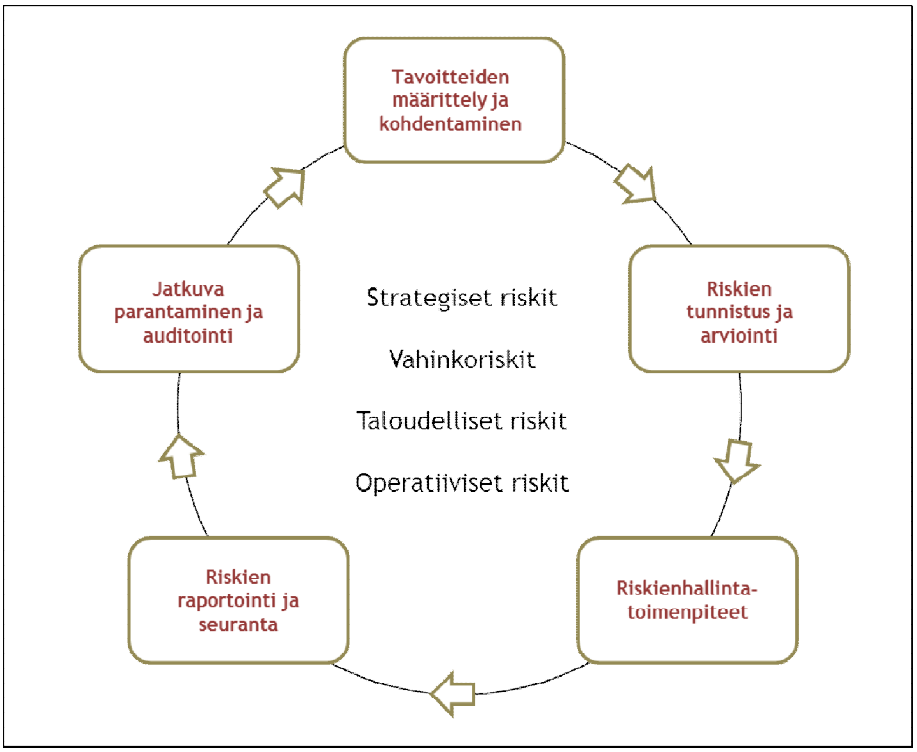
Kuvio 4: Organisaation riskienhallinnan kokonaisuus COSO-ERM –mallin mukaan (Committee of Sponsoring Organizations of the Treadway Commission 2004, 5).

Valtiovarain controller –toiminto on antanut COSO-ERM-malliin pohjautuvan suosituksen valtion viraston ja laitoksen sekä rahaston sisäisestä valvonnasta ja riskienhallinnasta (Valtiovarain controller –toiminto 2005). Malliin pohjautuvat myös Liikennevirastossa (Liikennevirasto 2012, 7) ja Viestintävirastossa (Arnell 2010, 30) toteutettava riskienhallinta.

Erityisesti yrityksissä kokonaisvaltainen riskienhallinta on myös myyntiargumentti; perusprosesseihin viety riskienhallinta välittää ajan myötä sidosryhmille kuvaa hyvin hallitusta organisaatiosta. Toisaalta organisaation riskienhallinnan tila tulee ulkopuolisten tietoisuuteen tavallisimmin sellaisten ei-toivottujen tapahtumien yhteydessä, jotka paljastavat ettei riskienhallinta ollut kunnossa. (Ilmonen 2013, 7, 17.) Kokonaisvaltainen riskienhallinta on leviämässä sekä julkisyhteisöihin että yrityksiin, ja valtaosassa suuria yrityksiä on jo toteutettuna erilaisia kokonaisvaltaisen riskienhallinnan hankkeita. Riskienhallinnan rooli on nousemassa yrityksissä yhä merkittävämmäksi, ja useimmissa yrityksissä turvallisuusyksiköiden toimenkuva ja tehtävät on muutettu tukemaan kokonaisvaltaista riskienhallintaa. (Juvonen ym. 2005, 3.)

3.2 Riskienhallintaprosessi

Riskienhallinnan perussääntö on, että ensin riskit tunnistetaan, sen jälkeen tunnistetut riskit arvioidaan, ja lopuksi arvioiduille riskeille kohdistetaan mahdolliset riskienhallintatoimenpiteet. Kokonaisuudessaan riskienhallintaprosessi on tätä laajempi kokonaisuus: se on systemaattinen tapa riskien arvioimiseksi, hallitsemiseksi ja raportoimiseksi. Yksikertaisimmillaan riskienhallintaprosessin voidaan nähdä koostuvan kolmesta vaiheesta: riskien tunnistamisesta ja arvioinnista, riskienhallintapäätöksen tekemisestä ja sen mukaisten toimenpiteiden toteuttamisesta, sekä riskienhallintatoimenpiteiden arvioinnista, seurannasta ja tarkastamisesta. Jotta riskienhallintaprosessi huomioisi kaikki tavoitteellisen johtamisen elementit, on prosessi hyvä jakaa viiteen vaiheeseen. Tällöin riskienhallintaprosessi muodostuisi tavoitteiden määrittelystä ja kohdentamisesta, riskien tunnistamisesta ja arvioimisesta, riskienhallintatoimenpiteiden päättämisestä ja toteuttamisesta, riskien raportoimisesta ja seuraamisesta sekä jatkuvasta parantamisesta ja auditoinnista (kuvio 5). Esitetty jako sisältää riskienhallintastandardien yleisimmin noudatteleman perusrungon elementit. (Ilmonen ym. 2013, 84-85, 113.)



Kuvio 5: Riskienhallintaprosessi Ilmosen ym. (2013, 85) mukaan.

Harringtonin ja Niehausin (1999) mukaan (ks. Suominen 2003, 31) riskienhallinta etenee suunnitelmallisena vaiheittaisena prosessina, jonka vaiheet muodostavat merkittävien riskien tunnistaminen, todennäköisyyden ja vakavuuden arviointi, riskienhallintamenetelmien kehittäminen ja sopivien menetelmien valitseminen, riskienhallintapäätökset ja toteutettujen toimenpiteiden arviointi. Suominen (2003, 38) laajentaa edellä mainittuja vaiheita riskien tun-

nistamiseen, turvallisuustekijöiden tarkistamiseen, jäljelle jäävien riskien arviointiin ja raportointiin, riskien seurausten kuvaamiseen ja tarkempaan esittelyyn euroina, tarvittavien riskienhallintatoimien järjestämiseen ja vastuuttamiseen sekä toimenpiteiden toteutukseen, seurantaan ja päivitykseen. Myös Juvosen ym. (2005, 23-24) esittämät riskienhallinnan neljä vaihetta ovat vastaavat: riskien tunnistaminen, riskien arvioiminen, riskienhallintamenetelmien valinta ja riskien tarkkailu. Usein käsitteenä mainittu riskianalyysi kattaa Bergin (1996, 73) mukaan riskien tunnistamisen, vahinkotaajuuden selvittämisen ja riskin suuruuden määrittämisen.

Riskienhallinnan järjestämiseksi on olemassa yleisesti hyväksyttyjä riskienhallintastandardeja, joiden tarkoituksena on kattaa riskienhallinnan osa-alueet mahdollisimman laajasti. Ne ovat ohjeellisia ja organisaatioiden eroista johtuen niitä kannattaa käyttää soveltuvin osin. Kokonaisuuden kattamisen lisäksi standardien merkittävin hyöty on siinä, että niiden kautta syntyy sekä yhteinen kieli keskeisten käsitteiden määrittymisen kautta, että yhteisesti ymmärretty metodi riskienhallinnan toteuttamiseksi. Nämä yhdessä tukevat riskienhallinnan prosessimaisuutta mahdollistamalla jatkuvan ja toistettavissa olevan lähestymistavan ja menettelyn. Etenkin suurissa organisaatioissa riskien ja niiden hallinnan yhteismitallisuus edellyttää jonkin yhdessä sovitun järjestelmän käyttöönottoa. Tunnetuimpia riskienhallinnan standardeja edellä esitellyn COSO-ERM –mallin lisäksi esimerkiksi Australia ja uusi-Seelanti AS/NZS 4360:2004, Business Continuity BS25999, ISO/DIS 3100, ISO/IEC 27005:2008 sekä ISO/IEC 17799:2005 ja ISO 27001, A.14.1. (Ilmonen ym. 2013, 27-29.)

Australia ja uusi-Seelanti AS/NZS 4360:2004 on COSO ERM:in ohella laajimmin käytetty. Se sisältää COSO ERM:iä enemmän käytännön ohjeita riskienhallinnan järjestämiseksi. Business Continuity BS25999 määrittelee jatkuvuussuunnitteluprosessin periaatteet ja terminologian, ja on jatkuvuussuunnittelussa laajimman kannatuksen saanut standardi. ISO/DIS 3100 on ensimmäinen kaikkiin yrityksiin sovellettavissa oleva kansainvälinen riskienhallintastandardi. Se kokoaa yhteen kokonaisvaltaisen riskienhallinnan yleisesti hyväksytyn sanaston, viitekehyksen ja toimintatavan. Standardi korostaa sitä, että riskillä voi olla sekä positiivinen että negatiivinen ulottuvuus. ISO/IEC 27005:2008 on tietoturvallisuuden riskienhallintajärjestelmän standardi ja ISO/IEC 17799:2005 sekä ISO 27001, A.14.1. jatkuvuussuunnittelun ISO-standardeja. (Ilmonen ym. 2013, 27-29.)

Useista riskienhallinnan standardeista ja menetelmistä huolimatta ne kaikki noudattavat pääsääntöisesti samaa perusrunkoa, jossa 1) määritetään riskienhallinnan tavoitteet, 2) tunnistetaan riskit, 3) arvioidaan riskien vaikuttavuus ja todennäköisyys, 4) suunnitellaan ja toteutetaan riskienhallintatoimenpiteet, 5) varmistetaan raportointi ja kommunikointi, sekä 6) arvioidaan säännöllisesti riskienhallinnan onnistuminen ja taso (Ilmonen 2013, 27).

3.3 Riskienhallinnan määritteleminen organisaatiossa

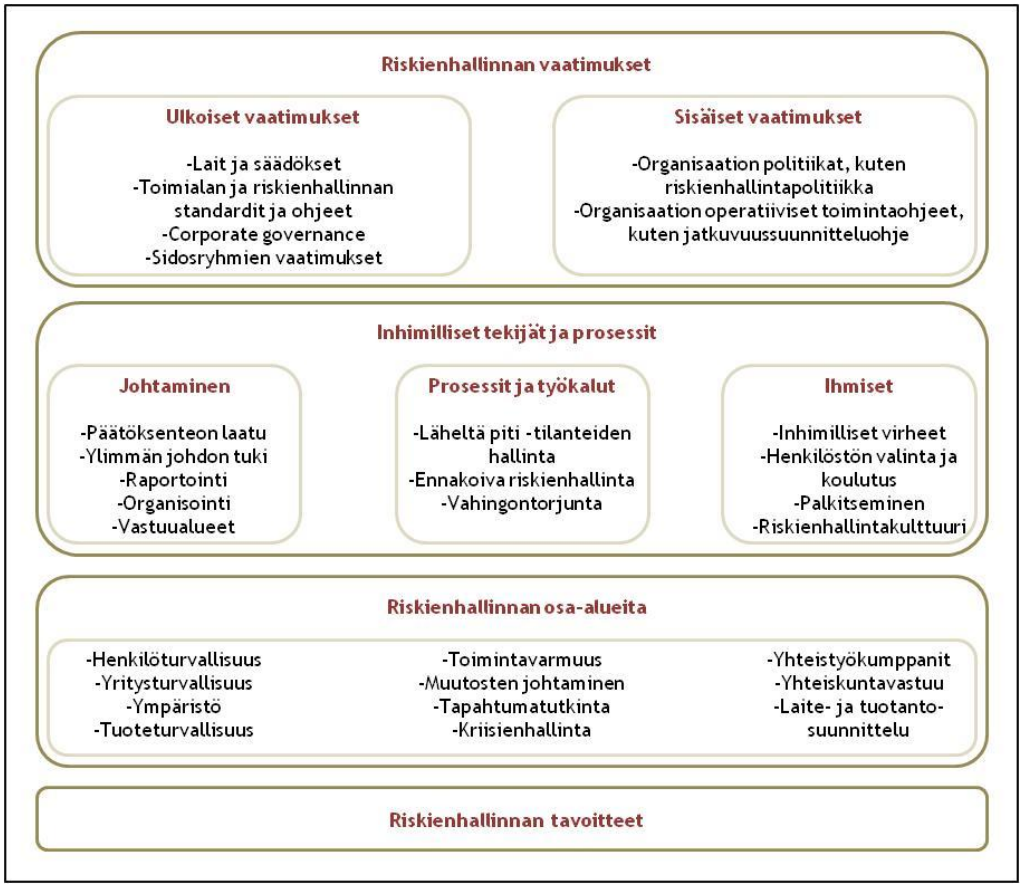
Ei ole olemassa tiettyä vakiintunutta määrittelyä sille, mitä kaikkea riskienhallinta kattaa. Laajimmillaan riskienhallinnan voidaan katsoa käsittävän muun muassa yritysturvallisuuden osa-alueet, jatkuvuussuunnittelun ja kriisienhallinnan, ja suppeimmillaan esimerkiksi ainoastaan riskiluetteloiden laatimisen. Se voidaan käsittää asiaksi, jota tehdään ainoastaan ylimmän johdon toimesta ja vuosisuunnittelun yhteydessä, tai se voidaan viedä osaksi organisaation koko henkilöstöä ja kaikkia prosesseja. Organisaatio voi pyrkiä kokonaisvaltaiseen riskienhallintaan, tai päättää keskittyä ainoastaan joihinkin riskeihin. Riskienhallintatyöhön ryhtyessään organisaation on lopulta itse määriteltävä mitä se riskienhallinnalla tarkoittaa, mitä se merkitsee sekä mistä osa-alueista ja tekijöistä se koostuu ja mitkä ovat näiden väliset suhteet. Tämä korostuu organisaatiossa, jossa riskienhallinta on uusi asia ja työhön ollaan vasta ryhtymässä.. Varsinaisen riskienhallintatyön aloittaminen on mahdollista vasta kun yrityksen johto ja omistajat ovat sopineet toiminnan ja tavoitteiden suojaamisesta ja sitä koskevista pelisäännöistä. (Ilmonen ym. 2013, 30, 38.)

Riskienhallinta saa luonnostaan erilaisia painotuksia jo toimialasta riippuen. Esimerkiksi teollisuudessa huomio kiinnittyy prosesseihin ja finanssialalla taloudellisiin riskeihin. Organisaation toimialaan liittyvien erilaisten riskienhallinnan painotusten lisäksi myös riskienhallinnan menetelmät ja sisältö muuttuvat toiminnan luonteen myötä. Määrittelystä riippumatta oleellista on kuitenkin edelleen se, että riskienhallinta sidotaan osaksi johtamista ja vuosisuunnittelua. (Ilmonen ym. 2013, 35, 44.) Myös Suomisen (2003, 196) mukaan yritysten riskienhallintaan liittyvät tarpeet ovat toimialasidonnaisia.

Osana riskienhallintatyön käynnistämistä ja keinona määritellä organisaation riskienhallinta tulee muodostaa riskienhallinnan periaatteet. Ne toimivat johdon ja yrityksessä omistajien tahdon osoituksena organisaation riskienhallinnasta. Niiden tarkoituksena on myös antaa tukea riskienhallintatyölle auttamalla johdon eri tasoja riskienhallinnan toteuttamisessa. Käytännössä riskienhallinnan periaatteilla tulee määritellä riskienhallinnan tarkoitus, tavoitteet, vastuut, keinot, seuranta ja raportointi sekä terminologia. Periaatteet voidaan kuvata myös riskilajikohtaisesti, esimerkiksi tietoturvallisuusperiaatteina ja projektiriskien hallinnan periaatteina. Organisaatio voi riskienhallinnan periaatteiden lisäksi laatia myös riskienhallintapolitiikan, joka kokoaa yhteen riskienhallinnan periaatteet. Periaatteiden tulee kuitenkin aina olla kuvattuna lyhyesti, eivätkä niissä kuvatut tavoitteet eivät saa olla irrallisia suhteessa organisaation käytännön arkeen. Huomiota tulee kiinnittää myös siihen, ettei asiakirjojen keskinäisissä suhteissa ole epäselvyyksiä, ja että henkilöstö perehdytetään niihin ja niiden yhteyteen omiin työtehtäviin. (Ilmonen ym. 2013, 54-57; Juvonen ym. 2005, 38.)

Sosiaali- ja terveysministeriön (2011, 9) mukaan ”riskienhallintapolitiikka on johdon strategisesta näkökulmasta laatima periaatedokumentti, joka kuvaa johdon sitoutumista ja tahtoa riskienhallinnan toteuttamiseksi ja turvallisuuskulttuurin kehittämiseksi”. Politiikkaa voidaan tarvittaessa täydentää erillisillä esimerkiksi tietoturvallisuus- tai varautumispolitiikka-asiakirjoilla. Politiikka-asiakirjojen lisäksi tarvitaan sellaisia asiantuntijoiden laatimia tavoite-, toimenpide- tai vastaavia ohjelmia, joiden avulla toteutetaan ja tehostetaan turvallisuuteen, valmiuteen ja riskienhallintaan liittyviä menettelyjä.

Riskienhallinnan kokonaisuutta ja tavoitetilaa määriteltäessä tulee tarkasteluun ottaa riskienhallinnan asetettavat vaatimukset ja tavoitteet. Riskienhallinnan tavoitetilan määritteleminen edellyttää riskienhallinnan kokonaiskuvan sisäistämistä ja yhteisen ymmärryksen saavuttamista. Inhimillisten tekijöiden, prosessien ja riskienhallinnan osa-alueiden huomioiminen auttaa kokonaisuuden hahmottamisessa ja määrittelyssä (kuvio 6). Alkuvaiheessa ei kuitenkaan ole tarkoituksenmukaista syventyä yksittäisiin riskityyppeihin, vaan muodostaa riskienhallinnan viitekehys käsitteiden määrittelyineen, vastuuttamisineen, tavoitteineen ja mittareineen sekä perehdyttää osallistuvat henkilöt tähän kokonaisuuteen. (Ilmonen ym. 2013, 35-36, 74.)



Kuvio 6: Riskienhallinnan määrittelyn kokonaisuutta Ilmosen ym. (2013) mukaan.

Riskienhallinnan tavoitetilan asettamisen lähtökohtana ovat sille osoitetut vaatimukset. Organisaation riskienhallinnalle on määritettävissä sekä ulkoisia että sisäisiä vaatimuksia. Ulkoiset vaatimukset ovat nimensä mukaisesti vaatimuksia tai suosituksia riskienhallinnan toteuttamisesta. Ne ovat karkeasti jaettavissa lainsäädännön ja muun viranomaissäätelyn osoittamiin vaatimuksiin sekä sidosryhmiin ja toimialaan liittyviin sopimusperusteisiin vaatimuksiin. Ulkoisten vaatimusten lähteitä ovat siten esimerkiksi lait ja säädökset, toimialan standardit ja ohjeet sekä asiakasvaatimukset. Useissa säädöksissä edellytetään riskianalyysin tekemistä. (Ilmonen 2013, 18-19.)

Sisäiset vaatimukset ovat asioita, joista on sovittu organisaation visiossa, arvoissa ja strategioissa, tai joita riskienhallinnasta on jo kirjattu esimerkiksi organisaation politiikoissa tai toimintaohjeissa. Riskienhallinta ei ole organisaation muusta toiminnasta erillinen toiminto, vaan sen perustana toimivat juuri organisaation visio, arvot ja strategia. On huomattava, että organisaation omien arvojen lisäksi myös yhteiskunnan asenteet ja arvostukset voivat vaikuttaa riskienhallintaan kohdistuviin vaatimuksiin. Yleisimmin riskienhallinnalle asetettavat tavoitteet on kirjattu organisaation politiikkoihin ja ohjeisiin, kuten riskienhallintapolitiikkaan tai esimerkiksi jatkuvuussuunnitteluohjeisiin, mutta niitä saatetaan kirjata jo sen strategiaan. (Ilmonen 2013, 19-20, 30.)

Myös valtionhallinnon organisaatiossa sisäinen toimintaympäristö ja organisaation toiminnan rakenteet luovat perustan riskienhallinnalle ja sisäiselle valvonnalle. Valtion virastossa ja laitoksessa puitteet muodostuvat muun muassa hallintosäännöksillä ja työjärjestyksillä tehdyistä organisaatioratkaisuista sekä muusta töiden järjestämisestä. Sisäistä toimintaympäristöä muodostavat myös sekä viraston johdon että virastoa ohjaavien elimien riskinottoon ja valvontaan liittyvät asenteet ja toimenpiteet. Toimintaympäristön tekijöitä ovat lisäksi johdon ja henkilöstön arvot sekä pätevyys. (Valtiovarain controller –toiminto 2005, 25.)

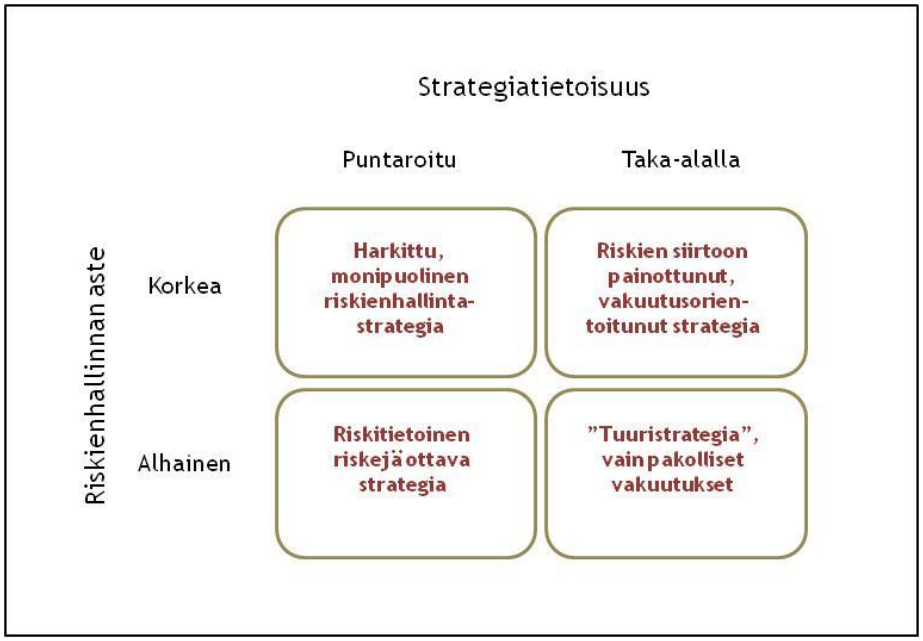
Valtion virastoissa riskienhallinnan määrittelyä on tehty esimerkiksi Viestintävirastossa, Liikennevirastossa ja ELY-keskuksissa. Viestintäviraston riskienhallintapolitiikassa kuvataan viraston riskienhallinnan tarkoitus ja tavoite, käytetyt määritelmät, riskienhallintaorganisaatio, riskienhallintaprosessi, riskien tunnistamisen, arvioinnin ja hallintakeinojen valinnan periaatteet, seurannan ja raportoinnin menettelyt sekä organisaatiossa toteutettava riskienhallintaan liittyvä koulutus. (Arnell 2010.)

Liikennevirasto on laatinut riskienhallintapolitiikan ja riskienhallinnan menettelytapaohjeet. Riskienhallintapolitiikassa kuvataan viraston riskienhallinnan päämäärät, riskinoton pääperiaatteet, riskienhallintamenettelyt ja vastuut. Riskienhallinnan menettelytapaohjeissa käsitellään viraston riskienhallintamalli, viraston riskien luokittelu, riskienhallintaan liittyvät vas-

tuut, riskienhallinnan osa-alueet ja periaatteet riskienhallinnan kehittämiseksi. (Liikennevirasto 2012.)

ELY-keskuksille on laadittu virastojen yhteiset sisäisen valvonnan ja riskienhallinnan toimintaperiaatteet. Asiakirjassa on kuvattu sisäisen valvonnan perusta määritelmineen. Sisäisen valvonnan ja riskienhallinnan periaatteissa on kuvattu osa-alueet, riskienhallinnan periaatteet, riskien tunnistamisen ja arvioinnin menettelyt sekä lausuttu riskienhallinnan lisäarvosta virastolle. Erikseen on kuvattu muun muassa toimenpiteet sisäisen valvonnan ja riskienhallinnan järjestämiseksi, soveltamiseksi ja arvioimiseksi. (Työ- ja elinkeinoministeriö 2011.)

Riskienhallinnan kokonaisuutta määriteltäessä on mahdollista tehdä riskienhallintaan liittyviä strategisia valintoja, jotka Suomisen (2003, 160) mukaan näyttäytyvät konkreettisimmin organisaation suhtautumisessa tunnettuihin riskienhallintakeinoihin. Nämä valinnat kuvastavat riskienhallinnan asemaa organisaatiossa. Suominen kuvaa strategisten valintojen muuttujiksi puntaroidun tai taka-alalla olevan strategiatietoisuuden ja alhaisen tai korkean riskienhallinnan asteen (kuvio 7). Valinnan johtavat parhaimmillaan harkittuun ja monipuoliseen riskienhallintastrategiaan, tai heikoimmillaan menettelyyn, jossa riskienhallinta toteutuu ainoastaan pakollisten vakuutusten ottamisena.



Kuvio 7: Riskienhallinnan perusstrategiat Suomisen (2003, 160) mukaan.

Riskienhallinnalle asetettujen sisäisten ja ulkoisten vaatimusten huomioiminen täysimääräisestikään ei takaa sitä, että riskit todella ovat hallinnassa. Organisaation riskienhallintakulttuuri ja inhimilliset tekijät ovat merkittävimmässä asemassa riskienhallinnalle asetettujen tavoitteiden toteutumisen kannalta. Riskienhallintaan liittyvien tavoitteiden asettaminen,

tavoitteiden jalkauttaminen käytännön toimintaan sekä toiminnan johtaminen ja mittaaminen ovat merkittävimmät riskienhallinnan onnistumiseen vaikuttavat asiat. Näihin vaikuttaa moni asia, joista keskeisimpiä ovat organisaation johdon toteuttama tavoitteellinen johtaminen ja tuki riskienhallintatyölle, riskienhallinnan organisointi selkeine vastuineen, riskien järjestelmällinen raportointi, konkreettinen toiminta operatiivisella tasolla, jossa yksittäisten ihmisten teot vaikuttavat riskien toteutumiseen ja toteutumatta jäämiseen, sekä henkilöstön valinta, koulutus ja palkitseminen riskienhallintakulttuurin kehittymisen tukijoina. (Ilmonen ym. 2013, 26.)

Riskienhallintaa määriteltäessä tulee huomata riskienhallinnan olevan pitkäaikaista, huolellista ja kärsivällistä sitoutumista ja panostusta vaativaa toimintaa (Suominen 2003, 195). Riskienhallinta tulee nähdä pitkän aikavälin vaiheittaisena kehitystyönä. Eteneminen hitaasti ja harkiten auttaa luomaan oman organisaation soveltuvan, järkevän ja mahdollisimman yksinkertaisen mallin riskienhallinnan toteuttamiseksi. Koska riskienhallinnan tulee myös kehittyä ajan saatossa on selvää, ettei kerralla valmista ratkaisua ole edes olemassa. Tulee myös pitää mielessä, että kehittymiskelpoiselta organisaatioltakin voi kestää useita vuosia, ennen kuin systemaattinen riskienhallintatyö alkaa osoittaa hyötyjään. Riskienhallintaprosessille kannattaa muodostaa sekä lyhyen että pitkän tähtäimen konkreettisia kehitystavoitteita. (Ilmonen ym. 2013, 37, 55, 86.) Myös valtiovarain controller –toiminto (2005, 21) korostaa riskienhallinnan kehittämisen olevan monivuotinen priorisointia edellyttävä prosessi.

Riskienhallinnan kehittäminen ja kokonaisvaltaisen riskienhallinnan käyttöönotto on sidoksissa organisaation johtamisen kypsyyteen. Voi olla perusteltua aloittaa toiminnan kehittäminen pienin, yksinkertaisin askelin perusasioiden kuntoon saattamiseksi ja keskittyä ainoastaan negatiivisiin riskeihin ja saattamaan riskienhallinta osaksi organisaation vuosisuunnittelua. Erityisesti riskien ja mahdollisuuksien huomioiminen yhdellä kertaa voi olla liian suuri kokonaisuus omaksuttavaksi. Riskienhallintatyön laajentaminen ja syventäminen voidaan tehdä seuraavissa vaiheissa. (Ilmonen ym. 2013, 41, 43.)

Keskeisenä riskienhallintatyölle asetettavana tavoitteena tulee olla se, että riskienhallinta muodostuu osaksi organisaation normaalia toimintaa. Tämä tukee ajan myötä riskitietoisuuden kehittymistä ja vaikuttaa siten organisaatiokulttuuriin riskienhallintaa tukevasti. Lopulta riskienhallinta muodostuu luontaiseksi osaksi organisaation jokaisen työtekijän roolia. (Ilmonen ym. 2013, 37.)

3.4 Riskienhallinnan vastuut ja organisointi

Riskienhallinnan johtamista ja siihen liittyvää hallintotapaa on ohjattu säädöstasoisesti suhteellisen vähän. Yritysten osalta riskienhallinnan johtamista määrittelevät esimerkiksi, osake-

yhtiö-, tilintarkastus-, kirjanpito- ja arvopaperimarkkinalait sekä tilinpäätösdirektiivi. Johdon merkitys on joka tapauksessa keskeinen, sillä riskienhallinta on pohjimmiltaan laadukasta johtamista. Sitä ei voi siten kehittää ilman johdon antamaa mandaattia ja tukea sekä todellista sitoutumista. (Ilmonen ym. 2013, 20, 37.)

Yrityksessä lopullisen vastuun riskienhallinnasta kantavat yrityksen hallitus ja toimitusjohtaja. Muut riskienhallintaan liittyvät vastuut, kuten raportointi ja valvonta, kannattaa osoittaa yksiselitteisesti jo työn alkuvaiheissa. Riskienhallinnan pääperiaatteisiin kuuluu se, että riskit omistetaan ja hallitaan operatiivisella tasolla. Siten johdon vastuulla on toiminnan järjestäminen ja valvonta, toimiva linja vastaa konkreettisista riskienhallintatoimista, ja yksittäisen työntekijän vastuulla voi puolestaan olla esimerkiksi riskien havainnointi, sovittujen toimintatapojen noudattaminen ja raportointi. Tästä huolimatta ylimmässä johdossa tulee olla yksiselitteisesti riskienhallinnasta vastaava henkilö. Jos tähdätään kokonaisvaltaiseen riskienhallintaan ja sen sitomiseen osaksi kaikkea toimintaa, voi jokaisella organisaation jäsenellä olla vastuuta tässä kokonaisuudessa. (Ilmonen 2013, 20, 35, 40, 51, 53.)

Esimerkkinä riskienhallinnan vastuiden jakautumisesta yrityksessä todettakoon Rautaruukki Oyj, jossa riskienhallintaan liittyvät vastuut noudattavat edellä Ilmosen ym. esittämää jakoa (taulukko 1). Johdon vastuita on jaettu useaan portaaseen, jonka lisäksi vastuu konsernin riskienhallinnan arvioimisesta on osoitettu sisäiselle tarkastukselle.

Hallitus	Vastaa konsernin riskienhallintapolitiikasta ja valvoo sen toteutumista. Hyväksyy riskienhallintapolitiikan.
Toimitusjohtaja	Vastaa siitä, että riskienhallinta on asianmukaisesti järjestetty.
Johtaja, yrityssuunnittelu	Vastaa riskienhallinnan toimintamallista ja raportoinnista.
Johtoryhmä	Osallistuu riskien tunnistamiseen, arviointiin, vastuuttamiseen sekä kontrolloimiseen.
Liiketoiminta-alueiden ja tukitoimintojen johtajat	Vastaavat omaan alueeseensa liittyvien riskien tunnistamisesta ja hallinnasta sekä riskienhallinnan kehitystoimenpiteiden toteutuksesta ja raportoinnista.
Konsernin riskienhallintapäällikkö	Vastaa liiketoiminta-alueiden ja muiden toimintojen tukemisesta riskienhallinnassa ja riskienhallinnan kehittämisestä sekä riski-informaation ylläpidosta.
Sisäinen tarkastus	Arvioi konsernin riskienhallintaa.
Jokainen työntekijä	Vastaa omaan työhönsä liittyvien ja muutoin havaitsemiensa riskien tunnistamisesta, arvioinnista ja raportoimisesta esimiehelle.

Taulukko 1: Riskienhallinnan vastuut Rautaruukki Oyj:ssä (Riskienhallinnan organisointi 2013).

Myös valtion virastoissa ja laitoksissa johdon rooli on keskeinen paitsi riskienhallinnan myös siihen läheisesti kytkeytyvän sisäisen valvonnan toteuttamisessa ja organisoinnissa (Valtiovarain controller –toiminto 2005, 13). Kuten organisaation tavoitteiden saavuttamisesta ja sen edellyttämän toiminnan järjestämisestä muutenkin, on ylimmällä johdolla vastuu myös sisäisen valvonnan järjestämisestä ja johtamisesta. Valtion virastoissa ylimmällä johdolla tarkoitetaan ylintä johtavaa virkamiestä, kuten ylijohtajaa, sekä ylintä päätös- ja johtovaltaa käyttävää monijäsenistä hallintoelintä, kuten johtokuntaa. Ylimmän johdon kokonaisvaltaista vastuuta sisäisen valvonnan ja riskienhallinnan järjestämisestä ei voi delegoida, mutta sen tulee delegoida näiden toteuttamiseen liittyviä tehtäviä. Ylimmän johdon tulee näyttäytyä uskottavasti sitoutuneena sisäiseen valvontaan ja riskienhallintaan. (Valtiovarain controller –toiminto 2005, 13-14.)

Valtion virastossa ja laitoksessa sisäisen tarkastuksen roolina on systemaattisin menetelmin arvioida sisäisen valvonnan toimivuutta ja tehokkuutta. Sen tulee myös asiantuntijana tukea muuta organisaation riskienhallinnan toteuttamisessa. Viraston sisäisten toimintayksiköiden johto vastaa oman vastuualueen toiminnan suunnittelusta sekä siihen liittyvästä riskien tunnistamisesta, hallitsemisesta, viestinnästä ja raportoinnista. Jokaisella valtionhenkilökuntaan kuuluvalla on puolestaan velvollisuus tiedostaa sisäisen valvonnan ja riskienhallinnan merkitys omien tavoitteiden ja työtehtävien näkökulmasta. Koko henkilöstön tulee hoitaa sisäiseen valvontaan ja liittyvät menettelyt sekä pitää omalta osaltaan yllä hyvää sisäistä toimintaympäristöä. (Valtiovarain controller –toiminto 2005, 14-15.)

Valtiovarain controller- toiminnon esittämää riskienhallintaan liittyvää vastuunjakoa noudattaa myös sosiaali- ja terveysministeriön sosiaali- ja terveydenhuollon johdolle ja turvallisuusasiantuntijoille antama ohje (Sosiaali- ja terveysministeriö 2011, 12-13). Erona ohjeessa on se, ettei siinä osoiteta vastuita sisäiselle tarkastukselle (taulukko 2).

Organisointiin ja vastuisiin liittyvä tavallinen ongelma on se, että riskienhallinnan kehittämisestä vastaavan henkilön ja johdon asiaan liittyvien vastuiden rajat hämärtyvät (Ilmonen ym. 2013, 40). Suominen (2003, 28) kuitenkin toteaa, että erityisesti pienissä yrityksissä riskienhallintatyö sisältyy normaaliin päivittäiseen työntekoon, sillä erillisiä riskienhallinnan resursseja ei ole. Vastuu riskienhallinnasta ei Suomisen (2003, 30) mukaan myöskään saisi jäädä vain yhdelle henkilölle. Tähän liittyy avainhenkilöriski sekä vaara siitä, että riskienhallinta eriytyy liiaksi omaksi irralliseksi toiminnokseen. Ilmonen ym. (2013, 71) huomauttavat, että riskienhallinnan organisointiin, käytännön toteutukseen ja työvälineisiin liittyy keskeisesti se, minkä tyyppisiä riskejä pyritään hallitsemaan. Nämä ovat esimerkiksi strategiaa uhkaavien riskien ja tietyn työskentely-ympäristön työtapaturmariskien osalta aivan toiset.

Ylin johto	- Tekee toimintapolitiikkoihin liittyvät päätökset, linjaa riskienhallinnan ja turvallisuustoiminnan tavoitteet sekä seuraa, ohjaa ja valvoo niiden toteutumista - Huolehtii keskijohdon/esimiesten riskienhallintaan ja turvallisuuteen liittyvästä pätevyydestä, työterveyshuollon toteutumisesta sekä organisaation resursseista - Sitoutuu ja sitouttaa henkilöstön tehtäviinsä - Raportoi organisaation ulkopuolelle ja vastaa viranomaisyhteistyöstä
Keskijohto/esimiehet	- Vastaa riskienhallinnasta ja turvallisuudesta oman yksikön osalta ja huolehtii näihin liittyvien toimenpiteiden toteuttamisesta - Huolehtii tarvittavien resurssien varaamisesta sekä henkilöstön kouluttamisesta ja motivoinnista
Riskienhallinta- ja turvallisuusasiantuntijat	- Toimivat johdon asiantuntijoina ja tukena - Kouluttavat, ohjeistavat ja konsultoivat - Arvioivat, seuraavat ja mittaavat riskien, riskienhallinnan ja turvallisuusasioiden tilaa sekä raportoivat ylimmälle johdolle - hoitavat vakuuttamisen, ellei toisin sovittu.
Jokainen työntekijä	- Osallistuu riskien tunnistamiseen ja arviointiin sekä työpaikkaselvityksiin - Edistää turvallisuutta omassa toiminnassaan ja valinnoissaan - Noudattaa annettuja ohjeita ja osallistuu koulutuksiin - Raportoi havaitsemistaan turvallisuuteen liittyvistä poikkeamista ja ilmoittaa kehittämiskohteista

Taulukko 2: Riskienhallinnan ja turvallisuuden organisoiminen ja vastuut sosiaali- ja terveysministeriön (2011, 12-13) mukaan.

Riskienhallintaprosessien synnyttämiseksi on sisäinen tarkastus joutunut joskus laajentamaan toimintaansa riskienhallinnan suuntaan. Sisäisen laskennan ei kuitenkaan tule vastata organisaation riskienhallinnasta, vaan sen tulee päinvastoin toimia riskienhallinnan riippumattomana arvioijana. (Ilmonen ym. 2013, 44.)

3.5 Riskien tunnistaminen

Riskien tunnistamisen tarkoituksena on tunnistaa mitä sellaista voi tapahtua, millä on merkitystä organisaation tavoitteiden saavuttamisen kannalta. Onnistuminen siinä on riskienhallintaprosessin keskeisimpiä vaiheita. Riskien tunnistaminen voidaan tehdä vasta, kun riskienhallinnan asema ja tehtävä on määritelty. (Ilmonen ym. 2013, 5, 99.)

Organisaation on harvoin niin pieni, että sen kannattaisi pyrkiä tunnistamaan ja analysoimaan kaikki riskinsä kerralla. Jos toimintoja tai osastoja on useampia, kannattaa keskittyä kerrallaan niistä yhteen. Kun organisaatio on päättänyt aloittaa systemaattisen riskienhallinnan, tulisi fokuksen aluksi olla siinä, että organisaatiossa pyritään tunnistamaan ja hallitsemaan strategisten tavoitteiden ja vuositavoitteiden toteutumista uhkaavat riskit. Riskit tulee tunnistaa suhteessa strategisiin tavoitteisiin aina kun se on mahdollista. (Ilmonen ym. 2013, 72, 173.)

Kokonaisvaltaisen riskienhallinnan näkökulmasta riskien tunnistaminen tulee liittää osaksi organisaation vuosikelloa, strategiakierrosta tai muuta vastaavaa suunnittelumenettelyä. Tavoitteita laadittaessa arvioidaan samalla niiden toteutumista uhkaavat riskit. Kokonaisvaltaiselle riskienhallinnan on myös tyypillistä, että vapaasta riskienhallinnasta on luovuttu, ja riskien tunnistaminen tapahtuu suhteessa organisaation tavoitteisiin. (Ilmonen 2013, 87-88.) Myös valtiovarain controller –toiminto korostaa riskien tunnistamista tavoitteiden asettamisen yhteydessä. Tavoitteita uhkaavien riskien tunnistamisen edellytys on, että organisaation toiminnan suunnittelu, seuranta, ohjaus ja näihin liittyvä tavoitteiden määrittely on johdonmukaista. (Valtiovarain controller –toiminto 2005, 27.)

Riskien tunnistamiseen on olemassa erilaisia menetelmiä, joista Ilmonen ym. (2013, 99-100) mainitsevat toteutuneisiin riskeihin perustuvan tunnistamismenetelmän, tarkistuslistoihin perustuvan tunnistamismenetelmän, ryhmätyönä tehtävän riskien tunnistamisen ja induktiivisen päättelyn riskien tunnistamisen menetelmänä. Kullakin menetelmällä on etunsa ja puutteensa, joten useamman menetelmän käyttäminen on suositeltavaa.

Riskien tunnistamisessa on tarpeen lähteä niiden luokittelemisesta. Riskien luokittelemiseksi on olemassa lukuisia vaihtoehtoja; riskit voidaan jakaa esimerkiksi sisäisiin ja ulkoisiin riskeihin, jolloin sisäisen riskin lähde on organisaation omassa toiminnassa, kuten laadunvarmistuksen pettämisessä, ja ulkoinen riski realisoituu esimerkiksi kriittisen yhteistyökumppanin toiminnan häiriintymisestä ja sen vaikutuksista omaan organisaatioon. Edelleen luokittelu voidaan tehdä sen mukaan voidaanko riskiin vaikuttaa vai ei, onko riski vakuutettava vai ei, on riski tietoinen vai tiedostamaton, tai onko riski välitön vai välillinen. (Ilmonen ym. 2013, 35, 69-70.)

Juvonen ym. (2005, 16-17) jakavat riskit niihin joita voi vakuuttaa ja niihin joita ei. Vakuutettavilla riskeillä tarkoitetaan tässä määritelmässä puhtaita vahinkoriskejä, joihin ei sisälly mahdollisuutta voiton tavoitteluun. Muut riskit ovat liiketoimintariskejä. Niihin sisältyy mahdollisuus voittoon, ja niitä ei voi vakuuttaa. Edelleen riskit voidaan jakaa sen mukaan, miten niihin on varauduttu. Tällöin riski voi olla joko luonnollinen, eli riskiin ei ole vielä puututtu, tai se voi olla kontrolloitu tai poistettu. Ilmosen (2013, 65-70) mukaan vakiintuneimpia tapoja

riskien jaotteluun on jako neljään riskikategoriaan, jolloin riskit ovat joko strategisia, operatiivisia, taloudellisia tai vahinkoriskejä. Näin jaotelleen riskit on jaettu toisaalta niiden lähteen ja toisaalta niiden tyypin mukaan. Kaikissa luetelluissa riskeissä voidaan edelleen tehdä luokittelu riskin lähteen, vakuutettavuuden, tietoisuuden ja välittömyyden mukaan.

Strategiset riskit, joita toisinaan kutsutaan myös liiketoimintariskeiksi, liittyvät organisaation pitkän aikavälin strategisiin tavoitteisiin. Sisäisinä riskeinä ne liittyvät esimerkiksi strategian toimeenpanon epäonnistumiseen kyvyn puuttuessa tai epäoleellisuuksiin keskityttäessä. Ulkoisina riskeinä niiden lähde on esimerkiksi erilaisissa toimintaympäristön muutoksissa. (Ilmonen ym. 2013, 65-66.) Mäkisen (2007, 114) mukaan strategiset riskit liittyvät sekä organisaation strategiaprosessiin että strategisiin valintoihin, ja edelleen sekä strategian laaditaan että sen jalkauttamiseen.

Operatiiviset riskit liittyvät organisaation päivittäisiin toimintoihin, ja ovat luonteeltaan välittömien tai välillisten vahinkojen tai maineen riskejä. Niiden lähteenä on prosesseihin, henkilöstöön tai järjestelmiin liittyvä epäonnistuminen tai riittämättömyys. Operatiiviset riskit liittyvät merkittävästi toiminnan häiriintymiseen ja keskeytymiseen esimerkiksi ulkoisten palveluntuottajien toiminnan häiriintymisen tai omien tuotannollisten tekijöiden häiriintymisen kautta. Osa sisäisistä operatiivisista riskeistä on hyvin lähellä strategisia riskejä. (Ilmonen ym. 2013, 66-67.) Sosiaali- ja terveysministeriön (2011, 11) mukaan operatiivisten riskien hallinta tukee strategisten riskien hallintaa. Juvosen ym. (2005, 93) mukaan toiminnan keskeytyminen on useimmiten seurausta yrityksen johtoon tai muuhun avainhenkilöön tai yrityksen omaisuuteen kohdistunut vahinko. Keskeytyminen voi olla seurausta myös riippuvuusriskin toteutumisesta.

Taloudelliset riskit liittyvät organisaation rahaprosessia uhkaaviin tekijöihin. Rahoitusriskit koskevat erityisesti yritystoimintaa, ja niissä voi olla kysymys esimerkiksi yrityksen maksuvalmiudesta, korkoriskeistä rahoituskuluihin liittyen tai valuuttariskeistä toimittaessa usealla valuutalla. Vahinkoriskit ovat puolestaan tyypillisesti esimerkiksi työtapaturmiin tai muutoin työkyvyttömyyteen tai alentuneeseen työkykyyn liittyvät riskit. Vahinkoriskeihin luetaan myös ympäristöriskit. Tämä riskityyppi mielletään usein riskeihin perehtymättömien keskuudessa helpoiten. (Ilmonen ym. 2013, 68-69.)

Suominen (2003, 32-33) luokittelee riskit samoin neljään luokkaan, joista omaisuusriskit, henkilöriskit sekä vastuu- ja keskeytysriskit koskevat kaikkia yrityksiä toimialasta riippumatta. Neljäs luokka painottuu yrityksen toimialalle ja yritykselle ominaisiin riskeihin, esimerkiksi tietoriskeihin. Juvonen ym. (2005, 44-45) jakavat riskit henkilöriskeihin, tietoriskeihin, liiketoimintariskeihin, toiminnan riskeihin ja omaisuusriskeihin. Berg (1996, 24-26) puolestaan jakaa riskit ainoastaan liiketaloudellisiin ja vahinkoriskeihin, joista ensin mainittu otetaan

liikevoiton saamiseksi. Vahinkoriskit aiheuttavat taloudellista vahinkoa esimerkiksi onnettomuuden tai rikoksen seurauksena, eikä niiden ottamiseen sisälly voiton mahdollisuutta.

Juvonen ym. (2005, 48-50, 53) käsittelee henkilöriskiä yksilön, organisaation ja yhteiskunnan kannalta. Tässä määritelmässä yksilön kannalta riski liittyy toimeentulon hankkimiseen, terveyteen ja toimintakykyyn, ja yhteiskuntaan liittyvä henkilöriski työtä tekevän väestön määrään ja osaamiseen. Organisaation kannalta henkilöriskeihin liittyy henkilöstön työskentelyyn ja toimintaan liittyvien riskien lisäksi keskeisesti avainhenkilön työpanoksen menettäminen. Esimerkiksi osaaminen ja ammattitaito, suhteet ja kontaktit sidosryhmiin, ohjelmistoihin ja laitteistoihin liittyvä asiantuntemus, esimiestaidot sekä neuvottelu- ja yhteistyötaidot voivat tehdä henkilöstö avainhenkilön.

Ilmonen ym. (2013, 69) huomauttavat, että ”eri ryhmiin kuuluvat riskit voivat olla läheistä sukua keskenään – raja on usein hiuksenhieno. Monet riskit ovat myös saman ilmiön tai asian ilmenemismuotoja eri tasoilla, jolloin periaatteessa samaan asiaan liittyy sekä strateginen että operatiivinen taso. Riskien luokittelu helpottaa riskien analysointia ja riskien keskinäisten suhteiden löytämistä”. Suomisen (2003, 202) mukaan yritykset tarvitsevatkin tulevaisuudessa riskienhallintaan lähestymistavan, jossa liike- ja vahinkoriskejä ei erotella toisistaan. Riskilajien integrointi vahvistaisi myös riskienhallinnan asemaa. Myöskään Bergin (1996, 24) mukaan riskiryhmien välinen raja ei ole täysin selvä.

Riskien syntymiseen ja kehittymiseen liittyvien hiljaisten signaalien kerääminen on tärkeää. Hiljaiset signaalit ovat lähteestä riippuen esimerkiksi huolenaiheita tai pieniä toistuvia tapahtumia joita ei ole vielä osattu yhdistää varsinaiseen syyhyn. Tämä korostuu erityisesti silloin, kun riskinarviointi toteutetaan esimerkiksi ainoastaan kerran vuodessa, sillä toiminta keskittyy tuolloin suuren kokonaisuuden kartoittamiseen ja ymmärtämiseen pienten havaintojen kustannuksella. Hiljaisten signaalien lähteitä ovat henkilökunta, sidosryhmät ja organisaation muut tukitoiminnot kuten sisäinen tarkastus. (Ilmonen ym. 2013, 108-110.)

3.6 Riskien arvioiminen

Riskien tunnistamisen jälkeen ne tulee arvioida. Arvioinnilla tarkoitetaan arviota riskin vaikutuksista ja sen toteutumisen todennäköisyydestä. (Ilmonen ym. 2013, 88, 100; sosiaali- ja terveysministeriö 2011, 11.) Keskeistä riskien arvioimisessa on pyrkimys mahdollisimman tarkkaan analyysiin riskin juurisyystä, sen toteutumisen vaikutuksista sekä toteutumisen todennäköisyydestä. Riskien keskinäinen vertailu on mahdollista ainoastaan ymmärtämällä toteutumisen todennäköisyydet ja vaikutukset. Arvioinnin tuloksena kyetään erottamaan esimerkiksi kohtalokkaat riskit, merkittävää vahinkoa aiheuttavat riskit sekä seurauksiltaan pienet mutta kiusallisen usein erottuvat riskit. (Ilmonen ym. 2013, 79.) Myös Juvonen ym. (2005, 11) koros-

tavat, että yksittäisten pienten ja merkityksettömiltä tuntuvien riskien yhteisvaikutus voi olla merkittävä, jonka vuoksi arvioinnissa tarvitaan kokonaisvaltaisuutta ja toimintojen laajaa tuntemusta. Riskin vakavuutta arvioitaessa tulee välittömien vaikutusten arvioimisen lisäksi huomioida sen aiheuttamat seurannaisvaikutukset.

Myös Suomisen (2003, 11) ja valtiovarain controller –toiminnon (2005, 31) mukaan tunnistetut riskit tulee saada laajuutensa ja seurausvaikutustensa suhteen jonkinlaiseen tärkeysjärjestykseen. Seurausvaikutuksia tulee arvioida nimenomaan suhteessa toiminnan tavoitteisiin. Valtion virastossa ja laitoksessa riskit tulee suhteuttaa lisäksi organisaatiota koskevaan lainsäädäntöön sekä ohjaavien ministeriöiden ja valtioneuvoston asettamiin linjauksiin sekä näiden puitteissa organisaation omaan riskinottokykyyn ja –halukkuuteen. (Valtiovarain controller –toiminto 2005, 32.)

Riskien arviointi voidaan riskin luonteesta riippuen toteuttaa monella tavalla. Arvio voi olla laadullinen, määrällinen tai näiden yhdistelmä. Riskin vaikuttavuuden laadullisessa arvioinnissa riskin toteutumisen aiheuttamia seurauksia kuvataan sanallisesti, mutta pyritään lisäksi antamaan arvio vaikuttavuudesta jollakin valitulla asteikolla, esimerkiksi väliltä 1-5. Havainnollistamisen helpottamiseksi voidaan asteikon numeroita kuvata esimerkiksi siten, että arvo yksi tarkoittaa olematonta haittaa, ja arvo viisi pysäyttää organisaation toiminnan. (Ilmonen ym. 2013, 100.)

Tavanomaisesti riskin suuruus tai merkittävyys on sen seurausten vakavuuden ja todennäköisyyden tulo (Ilmonen ym. 2013, 101; Suominen 2003, 10). Juvosen ym. (2005, 9-10) mukaan riskienhallintatyössä tulee kuitenkin kiinnittää huomioita ensisijaisesti riskien seurausten vakavuuteen. Tällöin riskin todennäköisyydellä ei tulisi olla yhtä suurta painoarvoa kuin sen toteutumisen aiheuttamilla vaikutuksilla, kuten on perinteisessä riskin suuruuden määrittävässä laskentakaavassa riski = todennäköisyys x vakavuus. Juvosen ym. mukaan riskin suuruus tulisi määritellä kaavalla riski = todennäköisyys x vakavuus^2, jolloin seurausten vaikutus korostuu. Tällöin tunnistetut riskit voidaan asettaa tärkeysjärjestykseen sen mukaan, mihin niistä ensisijaisesti tulisi varautua.

Myös Mäkinen viittaa Juvosen edellä mainittuun edistyneeseen riskin suuruutta määrittävään kaavaan. Kolmantena laskentatapana Mäkinen esittää todennäköisyyden ja vakavuuden summan, jolloin riski = todennäköisyys + vakavuus. Mäkisen mukaan kaikki matemaattiset riskin suuruutta kuvaavat määritelmät ovat kuitenkin ainoastaan osatotuuksia ja arvioita. Vähäisiltä vaikuttavien riskien toteutumisen yhteisvaikutus voi olla merkittävä. (Mäkinen 2007, 111.)

Riskin arvioimisen kaavasta seuraa, ettei riskin suuruutta voida määritellä, ellei toteutumisen todennäköisyyttä kyetä arvioimaan. Tästä seuraava epävarmuus johtaa yli- tai alilyönteihin

valittaessa toimenpiteitä riskin hallitsemiseksi. (Limnéll, Majewski & Salminen 2014, 108.) Todennäköisyyden arviointiin on olemassa erilaisia menetelmiä, jonka valintaan vaikuttavat käytettävissä olevat tiedot, riskin tekijöiden luonne ja valittu tarkastelujakso. Usein todennäköisyyden arviointi perustuu kuitenkin historiatietoon. Historiatietoon perustuva arvio muuttuu luotettavammaksi, jos sen yhteydessä kyetään huomioimaan suhdanne- ja kausivaihtelu sekä epäsäännöllisen vaihtelun mahdollisuus. Myös riskin todennäköisyyden arvioinnissa voidaan myös käyttää lukuarvoa kuvaamaan todennäköisyyttä. Yksinkertaisimmillaan voidaan jälleen käyttää asteikkoa 1-5-, jolloin arvolla yksi tapahtuma on tarkastelujaksolla erittäin epätodennäköinen, ja arvolla viisi erittäin todennäköinen. (Ilmonen ym. 2013, 101-102.)

Juvosen ym. (2005, 9) mukaan riskin merkittävyys on aina sidoksissa yrityksen riskinkantokykyyn. Riskinkantokyvyllä tarkoitetaan sitä, kuinka paljon taloudellisia menestyksiä yritys tietyssä ajassa kestää. Riskinkantokyvyn määritteleminen on tärkeää siksi, että se auttaa havaittujen riskien merkittävyyden arvioinnissa. Liiketoiminnassa tähän läheisesti liittyvä käsite on riskinottohalu, jolla määritellään vielä hyväksyttävissä oleva taloudellisen menetyksen määrä yrityksen tavoitellessa lisää kassavirtaa tai uusia liiketoimintamahdollisuuksia. (Ilmonen 2013, 10-12.)

Eräs tapa riskien suuruuden arviointiin on riskin vuosialtistuksen laskeminen, jolloin riskin suuruus muodostuu riskin euromääräisen vaikutuksen ja riskin vuotuisen toteutumisen todennäköisyyden tulosta. Jos arvioitu euromääräinen vahinko on esimerkiksi 100 000 euroa ja todennäköisyys toteutumiselle tarkasteltavana vuonna 20 %, realisoituu organisaatiolle riskistä vuodesta 20 000 euroa. Kun sama tarkastelu tehdään koko organisaation riskisalkulle, saadaan yhteenlaskettu vuotuinen riskialtistus. Sen jälkeen voidaan arvioida vuotuisen riskialtistuksen ja organisaation riskikantokyvyn tai –halun suhdetta. (Ilmonen ym. 2013, 175.)

Riskien arviointi kannattaa tehdä järjestelmällisesti samalla riskirekisteriä muodostaen. Riskit kirjataan riskirekisteriin niiden todennäköisyyden ja vaikutusten perusteella. Apuna voidaan myös käyttää erilaisia riskitunnistusmatriiseja. Matriisit luodaan organisaatiokohtaisesti määrittelemällä pääriskiluokat ja niille yksittäisiä riskikokonaisuuksia. Matriisin tarkoituksena on esittää ne organisaation tavoitteita uhkaavat merkittävimmät riskit, joihin seuranta ja riskienhallintatoimenpiteet tulee ensisijaisesti kohdistaa. Riskit voidaan esittää esimerkiksi kaaviossa väreillä organisaation toiminnan tekijöittäin. Tunnistettujen riskien arvioinnissa annettujen numeeristen arvojen tarkoituksena on kyetä hahmottamaan riskit riskimatriisiin. Mikäli organisaatiossa on tunnistettu ja kuvattu sen kriittiset prosessit, voidaan riskit kiinnittää suoraan niihin. Prosessikaavioihin voidaan myös lisätä riskejä koskevaa tietoa. Organisaation prosessimainen toimintamalli palvelee riskienhallintaa muutenkin, sillä eri yksiköiden välinen vuoropuhelu tuo luonnostaan esille organisaation toiminnan epäkohtia ja edelleen uhkia ja niistä arvioituja riskejä. (Ilmonen ym. 2013, 88-89, 94, 100.)

Arvio riskistä voidaan esimerkiksi riskimatriisissa tai prosessikaavion yhteydessä esittää Ilmosen ym. (2013, 97) mukaan toteamalla riskin nimi ja yleiskuvaus, riskin luokittelu esimerkiksi henkilö- tai tietoriskeihin, riskien toteutumisen aiheuttamat tappiot, riskin toteutumisen syyt, käytössä olevat riskienhallintatoimenpiteet, riskin toteutumisen todennäköisyys jollakin tarkastelujaksolla sekä vaikutuksiin ja todennäköisyyteen perustuva riskin merkittävyys.

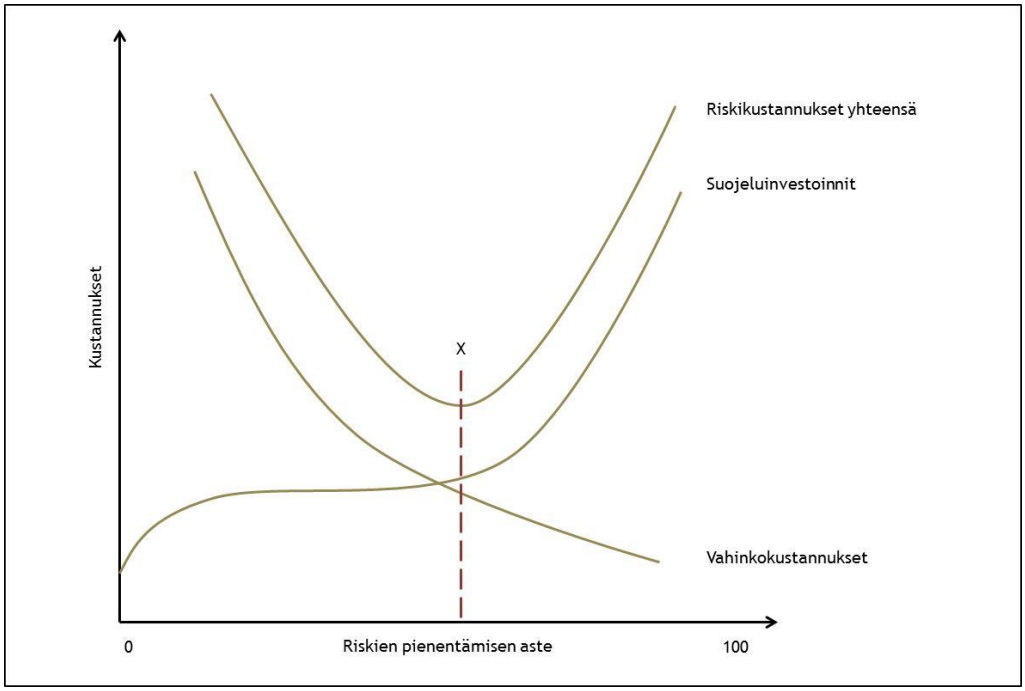
Riskien arvioiminen on käsitteellistä ja vaikeaa. Yhteisen kielen muodostaminen on keskeistä myös riskienhallinnan tässä vaiheessa. Riskien absoluuttisen suuruuden ja arviointi on siitä huolimatta käytännössä mahdotonta eikä täydelliseen arvon määritykseen tulekaan pyrkiä. Tähän liittyvä ilmiö on myös se, että arvioon riskistä vaikuttaa usea tekijä. Arvioitsijan ja tämän henkilökohtaisten näkemyksien ja kokemuksien, vaaratyyppiin sekä riskin sosiaalisten tekijöiden mukaan riskiä arvioidaan todennäköisyyttä tai seurausta korostaen. Tämän vuoksi riskienhallinnan asiantuntijoiden ja kokeneempien arvioitsijoiden käyttäminen arviointivaiheessa on hyödyllistä. (Ilmonen ym. 2013, 79-82, 103.) Myös Juvonen ym. (2005, 13) tuovat esille tämän riskin hahmottamisen eron maallikoiden ja asiantuntijoiden välillä.

3.7 Riskien hallitseminen

Riskien tunnistamisen ja arvioinnin tarkoitus on riskien priorisoiminen ja siten hallintatoimenpiteiden kohdistamiseen liittyvän päätöksenteon tukeminen. Riskienhallinnan pääpainon tulee olla nimensä mukaisesti juuri riskien hallinnassa, ei niiden listaamisessa. On tavallista, että riskienhallintatyössä koetaan päästyn valmiiksi esimerkiksi perusprosessien jalkauduttua ja raportoinnin vakiinnuttua. Varsinaisen riskienhallintatyön voidaan kuitenkin katsoa alkavan vasta tästä. (Ilmonen ym. 2013, 41.)

Kaikkiin riskeihin ei voida kohdistaa riskienhallintatoimenpiteitä, eikä se aina ole tarkoituksenmukaistakaan. Toimenpiteet tulee kohdistaa organisaation kannalta kriittisimpiin riskeihin. Kriittisillä riskeillä voidaan esimerkiksi niin kutsuttuja nollatoleranssiriskejä kuten henkilöturvallisuutta vaarantavia riskejä, vahingoiltaan euromääräisesti suurimpia riskejä, tai merkittävimpiä organisaation strategian toteutumista uhkaavia riskejä. Tulee huomata, että kriittistenkään riskien täydellinen hallinta ei aina ole tarkoituksenmukaista, sillä lähtökohtana tulee olla kustannus- ja hyötyanalyysiin perustuva riskienhallinta organisaation riskinkantokyvyn puitteissa. Esimerkiksi yrityksessä täydellinen riskien poistaminen tulee varmuudella niin kalliiksi, että se vaikuttaa yrityksen kannattavuuteen. Riskienhallinnan tarkoitus on päinvastainen. (Ilmonen ym. 2013, 117, 158.) Myös Leppäsen (2008, 61, 204) mukaan riskienhallintatoimenpiteiden tulee kohdistus organisaation tavoitteiden saavuttamisen kannalta elintärkeiden asioiden suojaamiseen.

Riskienhallinnan keskeisimpiä tavoitteita onkin käytettyjen resurssien ja tavoiteltujen hyötyjen välisen suhteen optimitason löytäminen - riskienhallinnan kustannukset eivät saisi olla yli- tai alimitoitettuja suhteessa realisoituviin riskeihin. Yrityksessä kaikkien riskien poistaminen olisi jopa vierasta liiketoiminnan logiikalle. (Ilmonen 2013, 10, 16.) Myös Suominen (2003, 116) kuvaa riskikustannusten optimointia riskeiltä suojautumisen investointien ja vahinkokustannusten välisen optimitason löytämisenä. Valtiovarain controller –toiminto (2005, 32) kuvaa asiaa siten, että lainsäädännön vaatimusten ja arvioitujen riskienhallintamenettelyjen kustannusten suhde riskienhallinnalla saatuihin hyötyihin auttaa linjaamaan mitä riskejä otetaan ja miten riskejä hallitaan. Menettelyjen on perustuttava kustannus/hyöty –arviointiin. Riskien pienentämisen ja riskikustannusten välistä suhdetta voidaan kuvata viivakaaviona (kuvio 8).

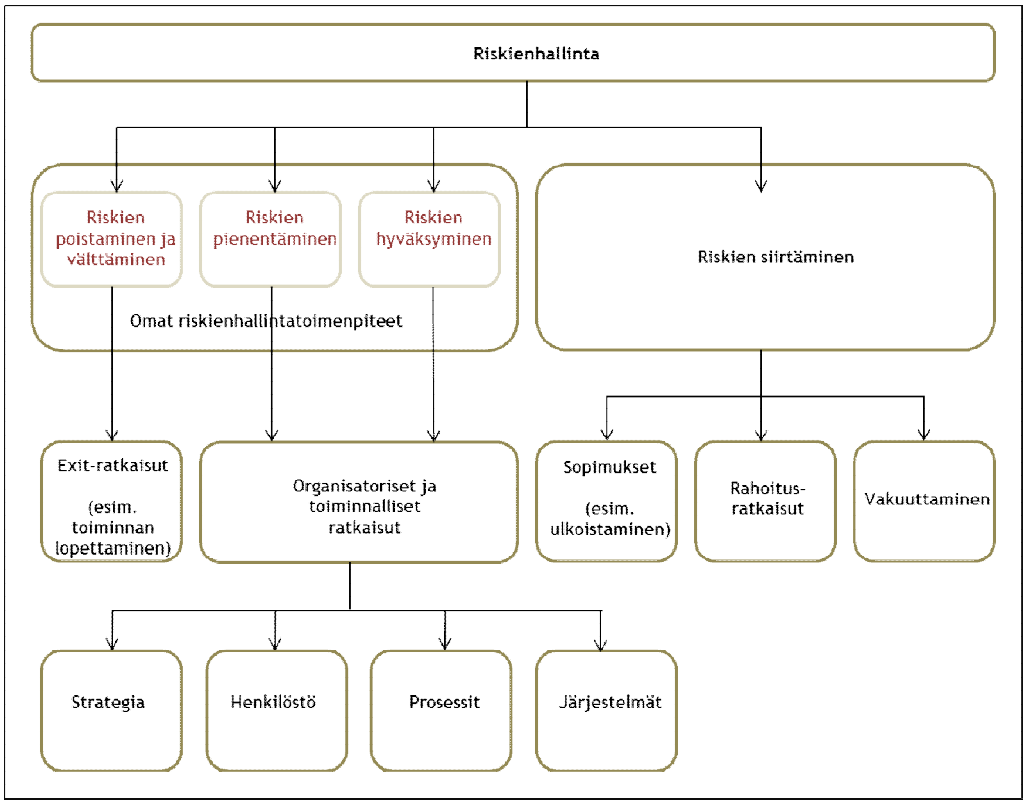


Kuvio 8: Riskikustannusten optimointi Suomisen (2003, 117) mukaan.

Historiatieto on tärkeää paitsi riskejä arvioitaessa myös riskienhallintatoimia valittaessa. Tapahtuneiden poikkeamien ja vahinkojen listaamisen ja analysoinnin kautta löydetään keinoja vastaavien tapahtumien ja niiden vaikutusten ehkäisemiseksi. (Ilmonen ym. 2013, 117, 118.) Juvonen ym. (2005, 25) lähestyvät asiaa siten, että riskin kolme mahdollista alkulähdettä ovat esimerkiksi luonnonvoimiin tai ihmisiin liittyvä kontrollin puute, epätäydelliseen tietoon ja tulevaisuuden ennustamattomuuteen liittyvä tiedon puute, tai ajan puutteeseen liittyvä kiireinen päätöksenteko. Ilmosen ym. (2013, 90) mukaan riskien juurisyyn tunnistaminen on olennaista, sillä riskienhallintatoimenpiteet tulee pyrkiä kohdistamaan niihin. Tunnistettuja riskejä voidaan mallintaa sekä niiden juurisyiden että aiheutuvien seurausten löytämiseksi ja arvioimisen sekä hallintatoimenpiteiden löytämisen avuksi. Mallintamisen menetelmiä ovat esimerkiksi vikapuu- ja tapahtumapuu-menetelmät, joiden avulla pyritään kuvaamaan kaikki

mahdolliset riskiin johtavat ja siitä aiheutuvat tapahtumaketjut. (Berg 1996, 99-100.) Muita juurisyyanalyysin apuvälineitä ovat esimerkiksi juurisyytaulukko tai perhospuuanalyysi (Ilmonen ym. 2013, 90).

Riskienhallintatoimenpiteiden valintaa helpottaa tunnistamisvaiheessa tehty luokittelu, mutta toimenpiteiden valintaa voidaan määritellä jo organisaation riskienhallintapolitiikassa. Riskienhallintatoimenpiteet ovat karkeasti jaettavissa omiin riskienhallintatoimenpiteisiin ja riskien siirtämiseen (kuvio 9). Organisaation omat toimenpiteet pyrkivät kontrolloimaan riskiä vaikuttamalla sen toetutumisen todennäköisyyteen ja seurausten vakavuuteen, ja näiden tulee lähtökohtaisesti olla ensisijaisia riskienhallinnan menettelyjä. Jos omat toimenpiteet eivät riitä, voidaan joitakin riskejä siirtää muille sopimuskumppaneille, vakuutusyhtiöille tai rahoituslaitoksille. (Ilmonen ym. 2013, 116-117.)



Kuvio 9: Riskienhallintatoimenpiteet Ilmosen ym. (2013, 116) mukaan.

Organisaation omat riskienhallintatoimenpiteet voidaan edelleen jakaa riskien poistamiseen, pienentämiseen ja hyväksymiseen. Nollatoleranssi riskille on usein ainoa tavoite puhuttaessa henkilöihin ja ympäristöön kohdistuvista turvallisuusriskeistä. Tällöin riskienhallintatoimenpiteillä tähdätään riskin poistamiseen. Toimintatavan muuttaminen tai tietyn toiminnan lopettaminen liian suuren riskin vuoksi ovat riskin poistamisen menetelmiä. On huomattava, että täysin poistettavia riskejä on vähän, ja että tietyn riskin poistaminen voi synnyttää jonkin muun uuden riskin. (Ilmonen ym. 2013, 119.)

Riskien pienentyminen tapahtuu sen vaikutuksia tai toteutumisen todennäköisyyttä pienentämällä. Näiden pienentymiseen päästään esimerkiksi henkilöresurssien lisäämisellä, koulutuksella tai teknisillä suojaustoimenpiteillä. Riskin pienentäminen on mahdollista useimpien riskien kohdalla. Riskien hyväksyminen on puolestaan vaihtoehto erityisesti silloin, kun riskin vaikutusten ja todennäköisyyden arvioidaan olevan hyvin pieniä. Näidenkin riskien osalta tulee kuitenkin huomioida niiden mahdolliset riippuvuudet ja kerrannaisvaikutukset. Pientenkin riskien hyväksymisellä on lisäksi yhteys organisaation riskinkantokyvyn ja –halun muutoksiin. Organisaatiossa on syytä sopia siitä, kuka seuraa ja raportoi pienten tunnistettujen riskien toteutumisesta ja kehittymisestä. (Ilmonen ym. 2013, 118-119.)

Työterveys- ja työturvallisuusjohtamisjärjestelmien vaatimuksia koskevan OHSAS 18001-standardin mukaan vaaran ja riskin vähentäminen toteutetaan järjestyksessä vaaran ja riskien poistaminen, menettelyn korvaaminen toisella, vaaran vähentäminen teknisellä toimenpiteellä, lisäämällä kylttejä, varoituksia ja ohjeita, ja viimeiseksi käyttämällä henkilösuojaimia (Tuominen & Moisio 2008, 30-31).

Sopimuksilla, rahoitusratkaisuilla tai vakuutuksilla voidaan siirtää riskejä toisen kannettavaksi. Riskin siirtäminen sopimuksin voi tarkoittaa esimerkiksi tietyn toiminnon ulkoistamista tai erilaisia rahastoivia ratkaisuja, mutta yleensä riskin siirtämisen menetelmänä on kuitenkin vakuuttaminen. Vakuutus voidaan ottaa organisaation riskinkantokyvyn ylittäville ja katastrofiriskeille taloudellisten menetysten kattamiseen. On tärkeää huomata, ettei vakuuttaminen tai muu riskin siirtämisen menettely siirrä riskienhallintaa tai kyseistä riskiä koskevaa vastuuta pois organisaatiosta, ja että vakuutus korvaa ainoastaan taloudellisia menetyksiä. Riskin toteutuminen voi lisäksi aiheuttaa esimerkiksi viivästymisiä toiminnan häiriintyessä, maineen menetystä tai ylimääräisestä työstä aiheutuvia kuluja sekä omavastuukuluja. Vakuuttaminen ei estä vahinkojen syntymistä eikä siten poista tarvetta muille riskienhallintatoimenpiteille. On kuitenkin olemassa myös lakisääteisiä vakuutuksia. (Ilmonen ym. 2013, 120, 130.) Mäkisen (2007, 119) mukaan tutkimustulokset osoittavat, ettei vakuutusturva suojaa yrityksen osakekurssia yritystä kohtaavissa katastrofitilanteissa. Vakuuttamiseen perustuva strategia ei korvaa korkealaatuista kokonaisturvallisuuden, riskienhallinnan ja jatkuvuussuunnittelun kokonaisuutta.

Juvonen ym. (2005, 19) jakavat riskienhallintatoimenpiteet pääpiirteissään samoin. Heidän mukaansa riskienhallintatoimenpiteet voidaan jakaa karkeasti kontrollointiin, jonka keinoja ovat riskin pienentäminen, välttäminen, jakaminen ja siirtäminen sekä rahoittamiseen, jolloin riski pidetään omalla vastuulla tai siirretään vakuuttamalla. Suominen (2003, 99) luokittelee riskienhallintatoimenpiteet tämän kanssa lähes identtisesti.

Organisatoristen ja toiminnallisten ratkaisujen yhteydessä riskienhallintatoimenpiteet voidaan jakaa esimerkiksi teknisiin riskienhallintatoimenpiteisiin sekä varautumiseen riskin realisoitumisen varalle. Osa varautumista on jatkuvuussuunnittelu. Jatkuvuussuunnittelulla parannetaan organisaation valmiuksia kohdata yllättäviä häiriöitä ja pienennetään siten niiden organisaation toiminnalle aiheuttamia vaikutuksia. Sen tavoitteena on estää organisaation toiminnan keskeytyminen suojaamalla kriittisiä prosesseja merkittäviltä onnettomuuksilta ja muilta häiriöiltä. Suunnitelmat laaditaankin muutamien valittujen organisaation olemassaolon vaarantavien riskiskenaarioiden varalle. Prosessien suojaamista tukee tässäkin yhteydessä se, että prosessit on kuvattu ja jaettu hallittaviin ja tarkoituksenmukaisiin osiin. (Ilmonen ym. 2013, 147-148.) Juvosen ym. (2005, 129) määritelmän mukaan jatkuvuussuunnittelulla varaudutaan turvallisuuden pettämiseen.

Myöskään jatkuvuussuunnitteluun liittyvä käsitteistö ei ole täysin vakiintunut, ja samassa yhteydessä puhutaan usein esimerkiksi kriisienhallintasuunnitelmista, varautumis- ja valmiussuunnitelmista, pelastussuunnitelmista ja toipumissuunnitelmista. Erityisesti jatkuvuus- ja toipumissuunnitelmilla on pitkä historia it-toiminnoissa. Jatkuvuussuunnittelun nykytilaa organisaatiossa - ja siten jatkuvuussuunnittelun sisältöä - voidaan arvioida sen kautta, onko organisaatiossa on laadittu kirjalliset ohjeet henkilöstön pelastamisen ja omaisuuden turvaamisen varalle onnettomuuden tapahtuessa ja onko ohjeita on harjoiteltu, onko poikkeusolojen tehtävät on määritelty, onko organisaatiota uhkaavat suurimmat riskit on listattu systemaattisesti ja säännönmukaisesti, onko kriittiset prosessit ja resurssit on listattu ja niitä varten on laadittu jatkuvuus- tai valmiussuunnitelmat, onko organisaatiossa on määritelty kriisiorganisaatio, jolla on selkeät vastuut ja valtuudet toimia kriisitilanteessa, onko toimenpiteet kriisiorganisaation hälyttämiseksi sekä jatkuvuussuunnitelman mukaisen toiminnan käynnistämiseksi on kuvattu ja kaikkien tiedossa, onko kriisitiedottaminen sekä sisäisen että ulkoisen viestinnän osalta on vastuutettu ja harjoiteltu, ja onko jatkuvuussuunnitelmien päivittämisen menettelyt on määritelty ja vastuutettu. (Ilmonen ym. 2013, 152.)

Sosiaali- ja terveysministeriön (2011, 12) mukaan organisaatiossa toteutettu strateginen ja operatiivinen riskienhallinta mahdollistavat tilanteen hallitsemisen ja haitallisten seurausten minimoimisen tilanteissa, joissa kohdataan poikkeama- tai häiriötilanne. Normaalioloissa toteutettu riskienhallintatyö muodostaa perustan organisaation toiminnan jatkuvuudelle missä tahansa oloissa.

Toimintojen ulkoistaminen tuo mukanaan merkittäviä riippuvuusriskejä. Yhteistyökumppanien toimitusvarmuus on kriittistä organisaation oman toiminnan häiriöttömyydelle. Ulkoistamisen yleistyessä on riippuvuusriskien tunnistaminen ja hallitseminen jatkuvasti tärkeämpää. Organisaatiossa on syytä pohtia mitä toimintavaihtoehtoja sillä on tilanteessa, jossa sopimuskumppani ei toimitakaan siltä odotettua palvelua. Tähän vaikuttaa oleellisesti se, toimittaako

sopimuskumppani helposti korvattavaa standardipalvelua vai organisaation tarpeisiin räätälöityä palvelua. Sopimusriskien hallinta ja hyvä tiedonvälitys ovat riippuvuusriskienhallinnassa keskeisiä, jonka lisäksi niitä voidaan paikoin vakuuttaa keskeytysvakuutuksilla. (Ilmonen ym. 2013, 118, 125.) Juvosen ym. (2005, 96) mukaan alihankkijoihin ja toimittajiin liittyvää riskiä kannattaa aina jakaa käyttämällä useaa palveluntuottajaa.

Vaikka organisaation strategian toteutumista uhkaavat sekä organisaation sisäisiin prosesseihin että liiketoimintaympäristöön liittyvät riskit, lähtevät strategian toteutumisen esteet useimmiten organisaatiosta itsestään. Tähän liittyvien riskien hallinta liittyy organisaation johdon päivittäiseen toimintaan, ja on toteutettavissa vastuuttamisen ja valvonnan keinoin. (Juvonen ym. 2005, 151, 186.) Valtion viraston ja laitoksen sisäistä valvontaa ja riskienhallintaa koskeva suositus korostaa (Valtiovarain controller –toiminto 2005, 35) toimivan tiedonkulun, raportoinnin ja muun vuorovaikutuksen merkitystä, jotta organisaation johto ja muu henkilöstö sekä sidosryhmät saisivat käyttöönsä oikea-aikaista ja olennaista tietoa organisaation toimintaan vaikuttavista tekijöistä.

Vastuu riskienhallintatoimenpiteiden toteuttamisesta ja raportoinnista on usein operatiivisella tasolla, sillä riskit sijaitsevat yleensä siellä. Vastuuhenkilön nimeäminen toimenpiteiden käytännön toteuttamiselle on tärkeää. Organisaation johdolla on vastuu toteutuksen ja vaikutusten valvonnasta. (Ilmonen ym. 2013, 117.)

3.8 Riskienhallinnan seuranta, raportointi ja jatkuva parantaminen

Riskienhallintaprosessin viimeiset vaiheet muodostuvat riskien ja riskienhallintatoimenpiteiden seurannasta ja arvioinnista sekä siihen liittyvästä raportoinnista. Näiden tulee edelleen johtaa riskienhallinnan kehittämiseen organisaatiossa. Juvosen ym. (2003, 30) mukaan havaittuja ja hallittuja riskejä tulee tarkkailla systemaattisesti ja säännöllisesti, sillä riskienhallinnan tulisi olla jatkuvaa tietoista toimintaa.

Valtion virastossa ja laitoksessa seuranta on keino sisäisen valvonnan ja riskienhallinnan tehokkuuden arvioimiseksi ja kehittämiseksi. Se voidaan jakaa jatkuvaan seurantaan sekä sisäiseen ja ulkoiseen arviointiin. Jatkuva seuranta on tavanomaiseen toimintaan liittyvää seurantaa, joka toteutetaan esimerkiksi poikkeamaraporttien, operatiivisten raporttien, asiakas- ja henkilöstöpalautteiden ja mahdollisten itsearviointien kautta. Sisäinen arviointi on organisaation säännöllisesti toteuttamaa sisäisen valvonnan ja riskienhallinnan tilaa tarkastelevaa toimintaa esimerkiksi tilinpäätöksen ja toimintakertomuksen yhteydessä. Ulkoisen arvioinnin välineitä ovat esimerkiksi valtiontalouden tarkastusviraston vuosiyhteenvedot ja ministeriön tilinpäätöskannanotot toteutetaan. Organisaatio käsittelee ulkopuolisten arvioitsijoiden ha-

vainnot ja huomioi ne toimenpidesuunnitelmissaan. (Valtiovarain controller –toiminto 2005, 37.)

Eräs keino arvioida organisaation riskienhallintaa on skenaariotyöskentely. Tällöin muodostetaan tapahtumakuvauksia organisaation kriittisimpiä toimintoja uhkaavista tilanteista kuvailemalla tapahtuman syyt, kulku ja niiden aiheuttamat välittömät ja välilliset seurausvaikutukset organisaation toiminnalle. Tällaiset tapahtumakuvaukset paljastavat organisaation riskienhallinnan vahvuuksia ja heikkouksia. Skenaariotyöskentely on lisäksi hyvä jatkuvuussuunnittelun menetelmä. Tällaisen analysoinnin yhteydessä tulee muistaa, että samanaikaisesti voi toteutua valitun skenaarion lisäksi muitakin riskejä. (Ilmonen ym. 2013, 174.)

Riskienhallinnan johtamiseen liittyy siitä raportointi. Riskienhallinnan raportointi on olennainen osa johdolle tehtävää ja johdon tekemää raportointia. Raportointitapa ja sen aikataulu ttaminen voidaan linjata organisaation riskienhallintapolitiikassa, mutta se on suositeltavaa liittää osaksi organisaation johtamis- ja strategiaprosessia. Tällöin myös raportointi tapahtuu määrävälein. Raportoinnin säännöllinen aikataulu ja rakenne ovat johtamisen kannalta tärkeitä. Esimerkiksi kuukausi, neljännesvuosi- ja vuosiraportit voivat kuitenkin olla tarkoitukseltaan ja siten sisällöltään erilaisia. (Ilmonen ym. 2013, 177.)

Riskienhallintaa koskeva raportointi on jaettavissa sisäiseen ja ulkoiseen raportointiin. Ulkoinen raportointi tarkoittaa tällöin julkista ja sidosryhmäraportointia, ja sisäinen organisaatiolle itselleen tehtävää kokonaisvaltaista riskiraportointia ja muuta sisäistä riskienhallintaan liittyvää raportointia. Riskiraportoinnin laajuus ja sisältö vaihtelee raportin kohderyhmän mukaan. Raportti voi olla pelkistetty sisäinen raportti, seikkaperäinen yrityksen johdolle annettava raportti tai hallitukselle annettava yrityksen riskiprofiilia ja kriittisimpien riskien kehitystrendejä kuvaava kooste. Oman yksikön asioita tarkasteleva yksikkötasoinen riskiraportointi voi olla laaja ja yksityiskohtainen, jolloin keskiössä ovat riskienhallintatoimenpiteiden suunnittelu, toteutuksen vastuutus ja seuranta. Yksikkötason raportointi voi tapahtua esimerkiksi viikoittain. (Ilmonen ym. 2013, 176, 178.)

Riskiraportoinnin painopiste on nykyisin riskienhallintatoimenpiteiden ja niiden vaikuttavuuden seurannassa sekä riskien kehityssuuntia arvioinnissa ja tulevaisuuden ennakoinnissa. Johdon riskiraportoinnissa pääpaino tulee olla strategisissa riskeissä, sillä niiden merkitys on tavallisesti kaikkein suurin. Yksikkötason riskiraportoinnissa korostuvat enemmän operatiiviset riskit. Käytännössä johdon raportissa on lukumääräisesti huomattavasti vähemmän riskejä. (Ilmonen ym. 2013, 177, 179.)

Riskeistä raportointia auttaa keskeisten tunnistettujen riskien kokoaminen organisaation riskisalkuksi. Siihen kannattaa koota esimerkiksi 10-15 merkittävintä riskiä, jotka on asetettu

riskiluvultaan suuruusjärjestykseen. Tämä määrä riittää organisaation johdolle raportoitaessa, mutta kohderyhmästä riippuen voi olla tarpeen käsitellä riskejä tätä tarkemmalla tasolla. Riskisalkun tulee painottua valittujen riskienhallinnan tavoitteiden tavoin, jolloin keskeisessä osassa voivat olla esimerkiksi organisaation strategisten tavoitteiden saavuttamista uhkaavat riskit. Operatiiviset ja taloudelliset riskit ovat tavallisesti seuraavaksi suurimmat ryhmät, ja vahinkoriskien osuus on tässä yhteydessä pienin. Tulee kuitenkin huomata, että painotus riippuu esimerkiksi organisaation koosta ja toimialasta. (Ilmonen ym. 2013, 172-173.)

Kokonaisvaltaisessa riskienhallinnassa jatkuvalla parantamisella on merkittävä rooli. Jatkuvan parantamisen tavoitteet määritellään organisaatio- ja vuosikohtaisesti, mutta sen tavoitteena voi olla esimerkiksi organisaation antaman ohjeistuksen toteutuminen, toimintojen suoritustason ja yhdenmukaisuuden todentaminen ja riskienhallinnan kattavuuden varmistaminen. Riskienhallinnan nykytilan ja kypsyysasteen tulee olla tiedossa, jotta organisaation riskienhallinnalle voidaan asettaa realistisia ja konkreettisia tavoitteita aikatauluineen. (Ilmonen ym. 2013, 86, 94-95.)

Ilmonen ym. (2013, 45-46) mainitsevat viisi kehitysvaihetta yrityksen matkalla kohti organisaation päivittäiseen toimintaan ja johtamiseen integroitua riskienhallintaa. Ensimmäinen kehitysvaihe on vahinkokeskeinen riskienhallintatyö, jolloin riskit tulevat esille ainoastaan vakuutusyhtiöiden tarjotessa tuotteitaan. Riskejä ei pyritä tunnistamaan yrityksen omista lähtökohdista. Toisessa vaiheessa yrityksen johto on tiedostanut tarpeen riskienhallinnan kattavalle koordinoinnille kaikissa toiminnoissaan, ja laaditaan riskienhallintapolitiikat ja tarvittavat ohjeistukset. Organisaation toimintojen johtajien tueksi perustetaan mahdollisesti erillinen riskienhallinnan tukitoiminto. Tässä vaiheessa riskien arviointi on tavallisesti vielä projektiluontoista toimintaa.

Kehitysvaiheiden kolmannessa ja neljännessä vaiheessa riskienhallintatoiminnolle alkaa muodostua liiketoimintaa neuvova rooli, ja on mahdollisesti perustettu tietyn riskityypin hallintaan keskittyviä tukitoimintoja. Yrityksen yhteisiä riskejä on myös alettu kuvaamaan matriisimaisesti, riskienhallintakeskustelu päätöksenteossa on aikaistunut, ja riskienhallintaan liittyvä raportointi ylimmälle johdolle on muodostunut hyvin suoraksi. Kypsimmässä vaiheessa riskienhallinta on integroitunut johtamiseen siten, että varsinaisesta riskienhallintatoiminnosta on tullut näennäisesti tarpeeton. Tulee kuitenkin huomata, että toimintaympäristön kokonaisuuden muutokset ovat jatkuvia ja niin moninaisia, ettei kehittyvää ja ajantasaista riskienhallintajärjestelmää tule tuolloinkaan hylätä. (Ilmonen ym. 2013, 45-46.)

Olennainen riskienhallinnan osa-alue on organisaation suunnitellun toiminnan poikkeamista ja kohdatuista vahingoista oppiminen. Tämä edellyttää riskien, poikkeamien ja vahinkojen kirjaamista ja analysointia sen tämän kautta tapahtumien perussyiden löytämistä. Tuloksia voi-

daan hyödyntää teknisten ratkaisujen ja toimintatapojen kehittämisessä ja niihin liittyvässä koulutuksessa. On syytä tiedostaa, että ei-toivotun tapahtuman perimmäiset syyt voivat olla syvemmällä organisaation kulttuurissa. (Ilmonen ym. 2013, 170.)

Riskienhallintakulttuurin juurtuakseen organisaation toimintaan tulee joidenkin organisaatioteorioiden mukaan pyrkiä vaikuttamaan kaikkiin kolmeen yrityskulttuurin tasoon: 1) organisaation jokaisen työntekijän kokemat konkreettiset, jokaiseen työpäivään vaikuttavat menettelyt, joilla riskienhallintatoimenpiteet näkyvät, 2) Dokumentoidut, helposti saatavilla olevat ja ääneen sanotut periaatteet, jotka ilmaisevat johdon tahtotilan riskienhallinnan suhteen, sekä 3) yksilölliset käsitykset siitä asioiden tilasta ja siitä kuinka tulisi toimia. (Ilmonen ym. 2013, 77.)

3.9 Riskienhallintaan liittyviä säädösvelvoitteita

Valtion viraston sisäisen valvonnan ja riskienhallinnan järjestämisestä säädetään laissa (423/1988) ja asetuksessa (1243/1992) valtion talousarviosta. Laki valtion talousarviosta (423/1988, 24 b§) edellyttää viraston huolehtivan siitä, että sisäisen valvonta on asianmukaisesti järjestetty sen omassa toiminnassa sekä toiminnassa, josta se vastaa. Vastuu sisäisen valvonnan järjestämisen johtamisesta ja sen asianmukaisuudesta ja riittävyydestä on viraston ja laitoksen johdolla. Tarkemmat säännökset sisäisen valvonnan järjestämisestä annetaan asetuksella valtion talousarviosta.

Talousarvioasetuksen (1243/1992, 69 §) mukaan sisäisellä valvonnalla tarkoitetaan menettelyjä, joilla varmistetaan viraston ja laitoksen talouden ja toiminnan laillisuuden ja tuloksellisuus, viraston ja laitoksen hallinnassa olevien varojen ja omaisuuden turvaaminen sekä viraston ja laitoksen johtamisen ja ulkoisen ohjauksen edellyttämät oikeat ja riittävät tiedot viraston ja laitoksen taloudesta ja toiminnasta. Menettelyiden on käsitettävä myös ne viraston ja laitoksen toiminnot ja tehtävät, jotka se on antanut toisten virastojen ja laitosten, yhteisöjen tai yksityisten tehtäväksi tai joista se muuten vastaa.

Kirjanpitoyksiköllä tulee myös olla taloussääntö, jolla on annettava tarkemmat määräykset muun muassa vahvistettujen tulostavoitteiden toimeenpanosta, tuloksellisuuden ja johdon laskentatoimen sekä muun seurantajärjestelmän järjestämisestä ja menettelystä havaittaessa virheitä tai väärinkäytöksiä taloudenhoidossa. Taloussäännön on yhdessä virastojen ja laitosten hallinnosta annettujen säädösten ja niiden nojalla annettujen työjärjestysten kanssa antaa riittävät perusteet sisäisen valvonnan menettelyille. (Asetus valtion talousarviosta 1243/1992, 69 §.)

Valtion tiliviraston tilinpäätökseen kuuluvan toimintakertomuksen tulee sisältää muun muassa arviointi sisäisen valvonnan ja siihen sisältyvän riskienhallinnan asianmukaisuudesta ja riittävyydestä. Toimintakertomuksen tulee lisäksi sisältää edelliseen perustuva lausuma sisäisen valvonnan tilasta ja olennaisimmista kehittämistarpeista. Toimintakertomuksen tulee lisäksi sisältää muun muassa kuvaus toiminnallisesta tuloksellisuudesta ja yhteiskunnallisesta vaikuttavuudesta sekä näiden kehityksestä. (Asetus valtion talousarviosta 1243/1992, 63 §, 65 §.)

Valtion virastoille ja laitoksille osoitettujen sisäisen valvonnan ja riskienhallinnan järjestämisvelvoitteen lisäksi on riskienhallintaan ja turvallisuuteen liittyviä velvoitteita osoitettu säädöksin kaikille organisaatioille. Säädökset liittyvät erityisesti työntekijöiden terveyteen ja turvallisuuteen ja velvoittavat ensisijaisesti työnantajaa. Seuraavassa on luotu esimerkinomainen katsaus säädösvelvoitteisiin, jotka osoittavat organisaatiolle velvollisuuksia erilaisten uhkien tunnistamiseen ja arviointiin sekä ehkäiseviin toimenpiteisiin ryhtymiseen.

Työturvallisuuslain (738/2002) mukaan työnantaja on velvollinen huolehtimaan työntekijöiden turvallisuudesta ja terveydestä työssä. Laki velvoittaa työantajia selvittämään, tunnistamaan ja arvioimaan työntekijöiden terveydelle ja turvallisuudelle aiheutuvat haitat. Laki velvoittaa työantajaa myös laatimaan työsuojelun toimintaohjelman. Työterveyshuoltolain (1383/2001) tarkoituksena on muun muassa edistää työnantajan, työntekijän ja työterveyshuollon yhteistoimin työhön liittyvien sairauksien ja tapaturmien ehkäisyä sekä työn ja työympäristön terveellisyyttä ja turvallisuutta. Lain mukaan työterveyshuollon sisältöön kuuluu työn ja työolosuhteiden terveellisyyden ja turvallisuuden selvittäminen ja arviointi.

Laki työsuojelun valvonnasta ja työpaikan työsuojeluyhteistoiminnasta (44/2006) pyrkii varmistamaan työsuojelua koskevien säännösten noudattamisen sekä työsuojelun viranomaisvalvonnan ja työnantajan sekä työntekijöiden yhteistoiminnan avulla parantamaan työympäristöä ja työolosuhteita. Laki edellyttää työantajan ja työntekijöiden ylläpitävän ja parantavan työturvallisuutta toimintayksiköissä. Lain mukaan työturvallisuuteen vaikuttavia tekijöitä ja tehtyjen toimenpiteiden vaikuttavuutta tulee seurata. Valtioneuvoston asetuksen kemiallisista tekijöistä työssä (715/2001) tarkoituksena on työntekijöiden suojeleminen työssä esiintyvien kemiallisten tekijöiden aiheuttamilta vaaroilta ja haitoilta. Asetuksen mukaan työnantajan tulee tunnistaa työssä esiintyvien kemiallisten tekijöiden aiheuttamat vaarat ja arvioida niistä työntekijöille aiheutuvat riskit.

Lain yksityisyyden suojasta työelämässä (759/2004) tarkoituksena on toteuttaa työelämässä perusoikeuksia, jotka liittyvät yksityiselämän suojan ja muun yksityisyyden suojan turvaamiseen. Laki käsittelee työntekijälle tehtäviä testejä ja tarkastuksia sekä työntekijää koskevien henkilötietojen käsittelyä. Laissa viranomaisten toiminnan julkisuudesta (621/1999) säädetään oikeudesta saada tieto viranomaisten julkisista asiakirjoista, viranomaisen vaitiolovelvol-

lisuudesta, asiakirjojen salassapidosta ja muista välttämättömistä rajoituksista liittyen tietojen saantia koskevien yleisten ja yksityisten etujen suojaamiseen. Laissa säädetään myös viranomaisten velvollisuuksista lain tarkoituksen toteuttamiseksi. Laki asettaa salassapitovelvoitteita ja velvoittaa hyvään tiedonhallintatapaan.

Pelastuslain (379/2011) mukaan rakennuksen omistajan ja haltijan sekä toiminnanharjoittajan tulee muun muassa osaltaan ehkäistä tulipalojen syttymistä ja muiden vaaratilanteiden syntymistä, varautua henkilöiden, omaisuuden ja ympäristön suojaamiseen vaaratilanteissa sekä tulipalojen sammuttamiseen ja muihin sellaisiin pelastustoimenpiteisiin, joihin ne omatoimisesti kykenevät. Edellä mainituilla tahoilla on myös velvollisuus laatia pelastussuunnitelma, jossa käsitellään havaitut vaarat ja riskit sekä niiden hallintaan liittyvät toimenpiteet. Pelastuslaki osoittaa lisäksi yleiset kaikkia koskevat huolellisuus- ja toimintavelvoitteet.

Valmiuslain (1552/2011) mukaan valtioneuvoston, valtion hallintoviranomaisten, valtion itsenäisten julkisoikeudellisten laitosten, muiden valtion viranomaisten ja valtion liikelaitosten sekä kuntien, kuntayhtymien ja muiden kuntien yhteenliittymien tulee valmiussuunnitelmin ja poikkeusoloissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muilla toimenpiteillä varmistaa tehtäviensä mahdollisimman hyvä hoitaminen myös poikkeusoloissa.

Organisaation toiminnan luonne sanelee sen velvollisuutta ottaa vakuutuksia. Yleensä vakuuttamisvelvoite on kuitenkin selkeä. Lakisääteisiä vakuutuksia ovat työeläkevakuutus ja tapaturmavakuutus, jonka lisäksi työ- ja virkaehtosopimusperusteisesti otetaan ryhmähenkivakuutuksia työ- ja vapaa-ajan kuolintapausten varalta. Vakuutusyhtiöt keräävät myös veroluonteista työttömyysvakuutusmaksua. Liikennevakuutusten järjestämisestä on puolestaan säädetty liikennevakuutuslaissa, ja potilasvahinkolaissa sairaanhoitotoimintaa harjoittavien velvollisuudesta ottaa potilasvakuutus. Lakisääteisiä vakuutuksia ovat lisäksi esimerkiksi ympäristövahinkovakuutus ja lääkevahinkovakuutus. (Ilmonen ym. 2013, 133.)

3.10 Riskienhallinnan ja turvallisuuden johtamisen yhteydestä

Organisaatioiden suojatessa toimintaansa ja pyrkiessä varmistamaan tavoitteidensa saavuttamisen käytetään tätä tukevista menettelyistä sekä riskienhallintaan että turvallisuuteen liittyvää käsitteistöä. Usein toistuvia ja sisällöltään hyvin lähellä toisiaan olevia käsitteitä ovat riskienhallinnan ohella turvallisuusjohtaminen, yritysturvallisuus, organisaatioturvallisuus ja kokonaisturvallisuus. Myös jatkuvuudenhallinnalla tavoitellaan riskienhallinnan kaltaisia asioita. Riskien ja niiden hallinnan sekä turvallisuuden välistä yhteyttä voidaan tarkastella niistä annettujen määritelmien kautta.

Sekä riskienhallinnan (Ilmonen ym. 2013, 20; Juvonen ym. 2005, 18, 20-21) että mainittujen turvallisuuteen liittyvien käsitteiden (Leppänen 2006, 59; Kerko 2001, 21; Mäkinen 2007, 155) määrittelyssä tavoitteina toistuvat toiminnan jatkuvuuden ja häiriöttömyyden varmistaminen. Riskienhallinnan määritelmissä tuodaan lisäksi esille riskikustannusten optimointi (Juvonen ym. 2005, 20-21), riskin positiivinen ulottuvuus mahdollisuuksien hyödyntämisenä (Riskienhallinta 2014) sekä riskinkantokyvyn ja –halun huomioiminen (Ilmonen ym. 2013, 20). Näihin viittaa kuitenkin myös Mäkisen (2007, 155) kokonaisturvallisuuden määritelmä. Mäkisen (2007, 155) mukaan kokonaisturvallisuuden tavoitteena on lisäksi liiketoiminnan jatkuvuuden varmistaminen kaikissa tilanteissa ja olosuhteissa. Tältä osin kokonaisturvallisuuden käsite vastaa puolestaan jatkuvuussuunnittelun (Ilmonen ym. 2013, 194) ja varautumisen (Parmes (toim.) 2007, 31) käsitteiden määritelmiä. Turvallisuuteen liittyvissä määritelmissä korostuu puolestaan henkilöstön, omaisuuden ja muiden arvojen suojaaminen (Leppänen 2006, 59; Kerko 2001, 21; Reiman & Oedewald 2008, 435).

Leppänen (2008, 13, 21) rinnastaa riskienhallinnan ja turvallisuusjohtamisen: Riskienhallinta ja turvallisuusjohtaminen ovat organisaation toimintaa uhkaavien riskien kokonaisvaltaista hallintaa ja johtamista, jolla tavoitellaan organisaation häiriötöntä toimintaa ja sen strategian toteutumista. Organisaation turvallisuusjohtamisen ja riskienhallinnan tulee tukea sen ydinprosesseja.

Erityisesti riskienhallinta sekä yritysturvallisuus ja sen johtaminen kulkevatkin useissa lähteissä rinnakkain. Yhteinen näkemys näiden käsitteiden välisestä suhteesta on etenkin siinä, että organisaation riskienhallinta toteutuu käytännössä turvallisuuden osa-alueiden kautta. Esimerkiksi Ilmosen ym. (2013, 44) mukaan organisaation riskienhallintatoiminto voi olla huomaamattakin jo järjestetty esimerkiksi yritysturvallisuustoiminnon kautta. Riskienhallintaa voidaan käytännössä toteuttaa organisaatiossa esimerkiksi työsuojelun, jatkuvuudenhallinnan, yritysturvallisuuden, tietoturvallisuuden ja sisäisen laskennan menetelmin. Myös Leppäsen (2008, 61, 204) mukaan riskienhallinta toimenpiteet toteutetaan organisaatioturvallisuuden osa-alueiden avulla. Toimenpiteet kohdistetaan niihin organisaation määrittelemiin asioihin, jotka ovat elintärkeitä sen tavoitteiden saavuttamiselle. Turvallisuutta Leppänen (2008, 54) luonnehtii tunnetilaksi, joka on riskien ja vahingoittumattomuuden välissä.

Samaa kokonaisuutta tarkoittavista käsitteistä huolimatta eri näkemyksiä on kuitenkin usein siitä, onko esimerkiksi yritysturvallisuus tai organisaatioturvallisuus osa organisaation riskienhallintaa vai riskienhallinta osa turvallisuutta. Suomisen (2003, 28) mukaan riskienhallinta lähtee turvallisuusajattelusta, ja sen tulee yltää kaikille yritysturvallisuuden osa-alueille. Suominen (2003, 163) pitää turvallisuutta käsitteellisesti riskienhallintaa laajempana, vaikka ei perustelekaan asiaa. Ilmonen ym. (2013, 77) puolestaan näkevät yritysturvallisuuden johtamisen toteutettavan osana riskienhallintaa. Ilmonen ym. (2013, 38) kuitenkin huomautta-

vat, ettei riskienhallinnan sisällölle ole vakiintunutta määritelmää, ja että laajimmillaan riskienhallinnan voidaan katsoa käsittävän muun muassa yritysturvallisuuden osa-alueet, jatkuvuussuunnittelun ja kriisienhallinnan.

Juvosen ym. (2005, 3) mukaan riskienhallinnan rooli on nousemassa yrityksissä yhä merkittävämmäksi, ja useimmissa yrityksissä turvallisuusyksiköiden toimenkuva ja tehtävät on muutettu tukemaan kokonaisvaltaista riskienhallintaa. Ilmosen ym. (2013, 77) mukaan yritysturvallisuuden johtaminen on nykyisin riskipohjaista toiminnan kehittämistä sekä keskeytysriskien hallintaa varautumalla ennakoimattomiin tapahtumiin. Yritysturvallisuuden kehittämisen tulee pohjautua riskiarvioihin. Osa yritysturvallisuuteen liittyvästä toiminnasta on kuitenkin perinteistä turvallisuuspalvelujen tarjontaa kuten toimitilaturvallisuutta tukevaa vartiointitoimintaa. Se on siten osa organisaation tarvitseman peruspalvelun tuottamista eikä sellaisena tarvitse päivittäistasolla riskienhallinnan ohjausta.

Keskenään erilaisista ja sisällöltään sekä yhtenevistä että ristiriitaisista käsitteistä johtuen korostuu organisaatiossa käytettävän yhtenäisen kielen ja käsitteiden määrittelyn merkitys. Lanne (2007, 30) on todennut, että riskienhallinnan ja turvallisuusjohtamisen käsitteellistä suhdetta turvallisuuden hallinnan kontekstissa on vaikea kuvata ja ymmärtää käsitteiden väljyydestä ja yleisluonteisesta määrittelystä johtuen (ks. Rusanen 2009, 40-41).

4 Riskienhallinta valtionhallinnossa

Valtiokonsernin ohjauksen kokonaisuuden osana käytetään tulosohjausta, joka on sopimukseen perustuva ohjausmalli. Sen tavoitteena on voimavarojen ja niillä saavutettavien tulosten saattaminen tasapainoon. Samalla varmistetaan palvelujen kustannuksiltaan tehokas toteuttaminen ja kehitetään niiden laatua. Tulosohjaus pohjautuu hallitusohjelmassa asetettuihin tavoitteisiin. Keskeisenä tulosohjauksen asiakirjana toimii valtion talousarvio. Talousarviossa todetaan määrärahojen käyttötarkoitusta perustelevia alustavia tulostavoitteita, joiden pohjalta ministeriöt neuvottelevat ja sopivat alaistensa virastojen ja laitosten kanssa tulostavoitteista ja niiden toteuttamisen edellyttämistä voimavaroista. Tulostavoitteiden toteutumisesta virastot ja laitokset raportoivat tilinpäätökseen kuuluvien toimintakertomustensa yhteydessä. Ministeriöt raportoivat edelleen koko toimialansa tuloksellisuudesta valtion tilinpäätöskertomuksessa. (Tulosohjaus 2014.)

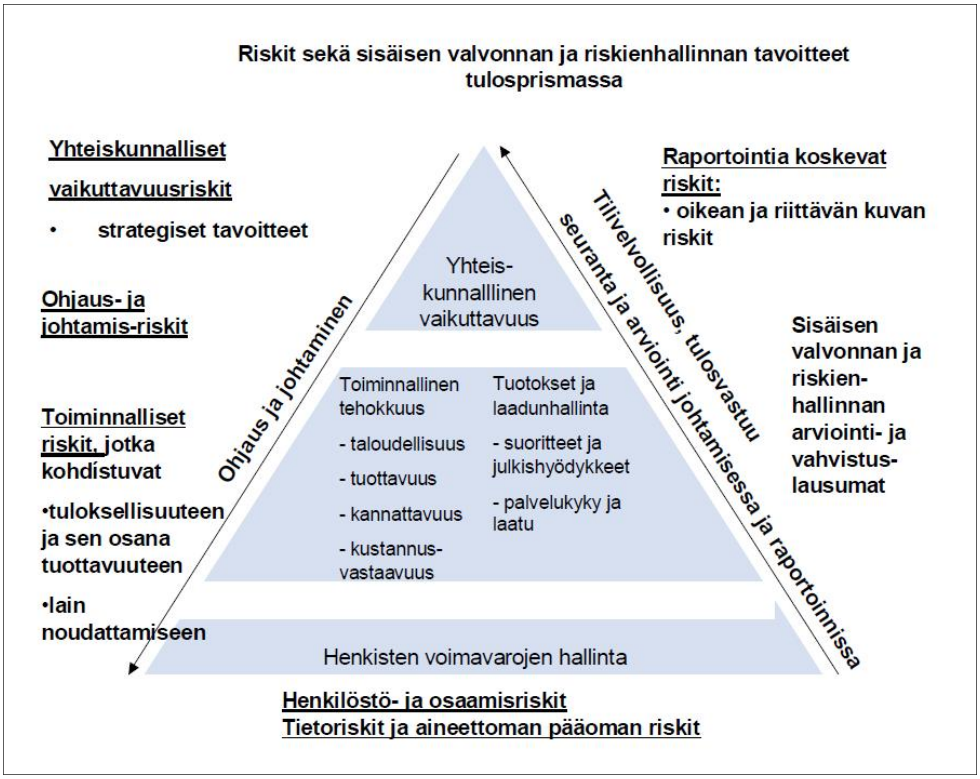
Tulostavoitteiden asettamisessa käytettävät tuloksellisuuden peruskriteerit muodostuvat yhteiskunnallisesta vaikuttavuudesta ja toiminnallisesta tuloksellisuudesta. Tämä jako tuotettuja hyötyjä ja aikaansaatuja vaikutuksia kuvaaviin vaikuttavuustavoitteisiin sekä konkreettisiin välittömiin suoritteisiin on tulosohjausajattelun keskeisiä lähtökohtia. Toiminnallisen tuloksellisuuden tekijöitä ovat toiminnallinen tehokkuus, tuotokset ja laadunhallinta sekä henkisten

voimavarojen hallinta ja kehittäminen. Toiminnallinen tehokkuus sisältää toiminnan taloudellisuutta tuottavuutta ja maksullisen palvelutoiminnan osalta myös kannattavuutta. Tuotoksiin ja laadunhallintaan liittyvät suoritteiden ja julkishyödykkeiden määrä ja toiminnan palvelukyky sekä laatu. Henkisten voimavarojen hallintaan ja kehittämiseen sisältyy puolestaan henkilöstömäärää ja –rakennetta koskeva tieto, henkilöstökulut, työhyvinvointi sekä osaaminen ja muu aineeton pääoma. Toiminnallisen tavoitteiden saavuttamiseen virasto voi vaikuttaa omin toimenpitein. Yhteiskunnallisten vaikuttavuustavoitteiden saavuttaminen on puolestaan viraston toimintaan nähden välillistä ja sen saavuttaminen siten vaikeammin todennettavissa. Niiden saavuttaminen on usein sidoksissa myös muiden toimijoiden samansuuntaisia tavoitteita ja toimintaa. (Salminen 2005, 24-25.)

Valtionhallinnon organisaatioissa riskit liittyvät erityisesti tuloksellisuuteen, lain ja talousarvion noudattamiseen, hyvän hallinnon periaatteiden ja arvojen toteutumiseen sekä valtion ja sen vastuulla olevien varojen ja omaisuuden turvaamiseen. Valtion virastojen ja laitosten keskeisiä toimintaedellytyksiä ja voimavaroja ovat henkiset voimavarat sekä informaatio ja tieto. Henkiset voimavarat liittyvät tässä yhteydessä henkilöstön määrään, osaamiseen, työmotivaatioon ja työhyvinvointiin. Keskeinen osa riskienhallintaa valtion virastossa ovat siten henkilöstöön ja osaamiseen sekä tiedon laatuun ja tietoturvallisuuteen liittyvä riskien hallinta. Mahdollisuuksien menettämisellä tarkoitetaan tässä yhteydessä sitä, että menetetään tilaisuus tehokkaampaan ja tuloksellisempaan toimintaan. (Valtiovarain controller –toiminto 2005, 11.) Edellisen perusteella voidaan riskien katsoa olevan valtion virastossa jaettu yleisesti toiminnan tuloksellisuuteen liittyviin riskeihin, toiminnan laillisuuteen liittyviin riskeihin, hyvän hallinnon toteutumista uhkaaviin riskeihin, varoja ja omaisuutta koskeviin riskeihin, henkisiin voimavaroihin liittyviin riskeihin sekä tietoriskeihin. Riskityyppien liittyminen valtionhallinnon tulosohjaukseen valtiovarain controller –toiminnon (2005, 12) mukaan on esitetty tulosprismassa (kuvio 10).

Valtiovarain controller-toiminto on määritellyt valtion ja sen toimintayksikön riskienhallinnan tarkoittavan yleisesti menettelyitä, joilla tunnistetaan, arvioidaan ja hallitaan tavoitteiden saavuttamista heikentäviä uhkia, niiden todennäköisyyksiä sekä avautuneiden toimintamahdollisuuksien menettämistä. Riskienhallinta on valtionhallinnossa kokonaisvaltainen näkökulma organisaation toimintaan, ja se toteutuu tehokkaimmillaan ollessaan täysin integroituna toimintayksikön tavanomaisiin toimintoihin – myös valtiovarain controllerin mukaan riskienhallinnan tulee olla osa organisaation tavanomaista johtamista ja muita prosesseja. Riskien tunnistaminen, arviointi ja ratkaisut niiden hallitsemiseksi toteutetaan kulloinkin käsillä olevan päätöksenteon yhteydessä. Sisäinen valvonta ja riskienhallinta eivät saa muodostua raskaaksi erillisprosessiksi, vaan ne on integroitava erottamattomaksi ja saumattomaksi osaksi tulosohjausta, johtamista ja toimintayksikön perustoimintoja. Valtion viraston riskienhallintapolitiikkaa voi siten sisältyä tulostavoiteasiakirjoihin, toiminta- ja taloussuunnitelmiin ja tietoturval-

lisuussuunnitelmiin sen sijaan, että laadittaisiin erillinen dokumentti riskienhallintapolitiikkaa varten. (Valtiovarain controller –toiminto 2005, 11-12, 20, 22.)



Kuvio 10: Valtionhallinnon riskityyppien liittyminen tilivelvollisuuteen ja tulosohjaukseen valtiovarain controller –toiminnon (2005, 12) mukaan.

Sisäisellä valvonnalla on keskeinen rooli valtionhallinnon riskienhallinnan toteuttamisessa. Talousarvioasetuksen (1243/1992) mukaan valtion viraston ja laitoksen johdon on huolehdittava siitä, että organisaatiossa noudatetaan sellaisia asianmukaisia menettelyjä, joilla varmistetaan viraston ja laitoksen talouden ja toiminnan laillisuus ja tuloksellisuus, sen hallinnassa olevan omaisuuden ja varojen turvaaminen sekä johtamisen ja ulkoisen ohjauksen tarvitsemat oikeat ja riittävät tiedot viraston ja laitoksen toiminnasta ja taloudesta. Sisäisellä valvonnalla pyritään hallitsemaan näihin tavoitteisiin kohdistuvia riskejä. Lisäksi se parantaa toimintayksikön tuloksellisuutta ja hallinnon tilivelvollisuuden toteutumista. (Valtiovarain controller –toiminto 2005, 8-9, 12-13.) Riskienhallinnalla puolestaan tunnistetaan, arvioidaan ja pyritään hallitsemaan näihin liittyvien tavoitteiden saavuttamista uhkaavia tekijöitä. Riskienhallinnan ja sisäisen valvonnan tavoitteet ovat samat. (Sisäinen valvonta ja riskienhallinta 2013.)

Sisäisen valvonnan ja riskienhallinnan lähestymistavoista ja toimivuuden arvioinnista valtion virastoille ja laitoksille annettu suositus toteaa, että tehokas sisäisen valvonnan ja riskienhallinnan toteuttaminen edellyttää näitä koskevan järjestelmän ja menettelyjen pitämistä mahdollisimman yksinkertaisina, ja että riskeissä ja kontrolleissa keskitytään olennaisimpiin seik-

koihin laajojen ja monimutkaisten kartoitusten sijaan. Ylimitoitettua dokumentaatiota tulee välttää: työjärjestys, taloussääntö ja johdon antamat ohjeet kirjoitetaan lyhyinä ja selkeinä dokumentteina. Myös riskejä tulee käsitellä tiiviisti ja olennaisimmilta osiltaan. Menettelyt on sisällytettävä suoraan työjärjestyksillä ja muilla vastaavilla ohjaavilla menettelyillä osaksi tavanomaisia toimintatapoja. Sisäisen valvonnan ja riskienhallinnan tehokkuus ja kattavuus edellyttää myös sitä, että organisaation johto saa sekä talous- ja hallintojohdon että tulos-alueiden ja muiden yksiköiden tuen. Vaikka riskienhallinnan järjestämiseen liittyvät tarpeet vaihtelevat valtion virastojen kesken hyvin paljon, on erillinen on riskienhallintaprosessin tai –yksikön järjestäminen hyvin harvoin tarkoituksenmukaista. (Valtiovarain controller –toiminto 2005, 6, 12, 20-22.)

Valtion virastossa sisäisen valvonnan ja riskienhallinnan kehittäminen tulee nähdä monivuotisena priorisointia vaativana prosessina, joka aloitetaan saattamalla perusasiat kuntoon. Kehittämiskohteita priorisoitaessa tulisi ensin keskittyä sisäisen valvonnan perusasioihin ennen näkökulmien laajentamista yleisemmin riskienhallintaan. Huomionarvoista valtion viraston ja toimintayksikön riskienhallinnassa on se, että ne ovat osa valtiontalouden ja valtioneuvoston alaisen hallinnon muodostamaa konsernia. Tästä syystä riskejä ja niiden hallintaa tulisi tarkastella valtiokonsernin kokonaisuuden ja tavoitteiden näkökulmasta. (Valtiovarain controller –toiminto 2005, 12, 20-21.)

4.1 Katsaus riskienhallinnan toteutumiseen valtionhallinnossa

Riskienhallinnan koordinointi valtionhallinnossa kuuluu osaksi valtiovarainministeriön strategiaa sen konserniohjaustehtävän kautta (Valtiovarainministeriö 2011, 2). Valtiovarainministeriön yhteydessä toimii sisäisen valvonnan ja riskienhallinnan neuvottelukunta, jonka tehtävänä on toimia ”ministeriöiden virkamiesjohdon ja valtiontalouden tarkastusviraston yhteisenä foorumina sisäisen valvonnan ja riskienhallinnan kysymyksissä” (Sisäisen valvonnan ja riskienhallinnan neuvottelukunta 2014). Valtioneuvoston asetuksen talousarviosta (254/2004, 71 §) mukaan neuvottelukunta muun muassa seuraa ja arvioi sisäisen valvonnan ja sen osana olevan riskienhallinnan järjestämisen tilaa, menettelyitä ja yleistä kehitystä valtionhallinnossa, sekä tekee aloitteita sisäisen valvonnan ja sen osana olevan riskienhallinnan kehittämiseksi. Neuvoston puheenjohtajana toimii valtiovarainministeriön yhteydessä toimiva valtioneuvoston controller, joka on valtioneuvoston yhteinen tulos- ja valtiovarainvalvoja. Toiminto palvelee valtioneuvostoa ja ministeriöiden johtoa muun muassa ylimmän johdon neuvonantajana ja hallinnon ohjaajana valtion talouden ja toiminnan ohjaus- ja raportointijärjestelmien laadun varmistamisessa ja kehittämisessä. Valtiovarain controller –toiminnon tehtäviin kuuluu myös huolehtia sisäisen valvonnan ja riskienhallinnan ohjauksesta, yhteensovittamisesta ja kehittämisestä. (Valtiovarain controller –toiminto 2013.)

Neuvottelukunta on todennut muun muassa tarpeesta kartoittaa sisäisen valvonnan ja riskienhallinnan menettelyt valtion virastoissa ja laitoksissa. Tietojärjestelmien on todettu olevan nykyisin hyvin keskeinen osa riskienhallintaa. (Valtiovarainministeriö 2008a,4.) Neuvottelukunnan asialistalla on vuonna 2008 ollut myös aluehallinnon uudistus sisäisen valvonnan ja riskienhallinnan näkökulmasta (Valtiovarainministeriö 2008b,4). Myös kokonaisvaltaisesta riskienhallinnasta on keskusteltu. Tällöin on tuotu esille muun muassa se, että yksityisen ja julkisen sektorin samasta riskienhallinnan viitekehyksestä huolimatta löytyy näiden välillä kuitenkin eroja. Julkisella sektorilla on esimerkiksi poliittisella viitekehyksellä merkittävä rooli, ja yksityisellä puolella riskin euromääräistä hintaa on helpompi arvioida. Myös neuvottelukunnassa on korostettu ylimmän johdon sitoutumisen merkitystä sekä sitä, että riskienhallinnan jalkautetaan koko organisaatioon ja nivotaan saumattomasti organisaation vuosikelloon. Riskienhallinnan tulisi sisältyä omana osanaan jo päätösasiakirjoihin. (Valtiovarainministeriö 2009a,2-3.)

Sisäisen valvonnan ja riskienhallinnan neuvottelukunta on myös keskustellut roolistaan ja tehtäviensä toteuttamisesta. Löyhän keskustelufoorumin sijasta on pidetty tarpeellisena tehokkaasti toimivaa neuvottelukuntaa, joka voisi toimia hyvien käytäntöjen ylläpitäminen ja suositusten antaminen. Neuvottelukunta on todennut, että sisäinen valvonnan koordinoimiseksi tarvittaisiin vahvaa konserniohjausta ja kokonaisuuden hallintaa. Esimerkiksi sisäisen valvonnan käsite on neuvottelukunnan käsityksen mukaan vuonna 2010 edelleen ymmärretty hyvin eri tavoin. (Valtiovarainministeriö 2010,2.) Toimikauden 6.3.2008–15.3.2011 toiminut neuvottelukunta totesi viimeisessä muistossaan, että neuvottelukunnan työn vaikuttavuutta ja suunnitelmallisuutta tulee tehostaa, ja sen tulisi löytää toiminnalleen selkeät vaikuttamiskanavat. Esimerkkeinä mainittiin suositusten saattaminen toimivaltaiselle viranomaiselle jatkotoimenpiteitä varten ja informaatiotilaisuuksien järjestäminen esimerkiksi riskienhallintaa koskien. (Valtiovarainministeriö 2011,4-5.)

Vuonna 2011 neuvottelukunta on todennut riskienhallinnan nykytilan keskeisiksi ongelmiksi valtionhallinnossa heikon yleiskäsityksen riskienhallinnan tilasta, epäselvyyden riskienhallinnan tarkoituksesta ja käsitteistä sekä riskienhallintatoimenpiteiden erillisyyden päivittäisestä johtamisesta. Toimintatapojen todettiin olevan hajanaiset. Ongelmien keskeiseksi syyksi nimettiin riskienhallinnan määrittelemättömyys valtion virastoissa harvoja poikkeuksia lukuun ottamatta. Kehitettävää on erityisesti riskikustannustietoisuudessa sekä riskien seurannassa ja tilastoinnissa. (Valtiovarainministeriö 2011,4.)

Neuvottelukunta on todennut samankaltaiset ongelmat valionhallinnossa jo yli kuusi vuotta aikaisemmin (Valtiovarainministeriö 2004b,2). Tuolloin on katsottu riskienhallinnan edustavan osin uutta näkökulmaa julkisessa hallinnossa, vaikka useissa virastoissa ja laitoksissa sekä erillisissä toiminnoissa onkin jo pitkään sovellettu systemaattiseen riskien analysointiin ja

arviointiin sekä riskienhallintaan liittyviä menettelyjä (Valtiovarainministeriö 2004a,4). Neuvottelukunta on todennut olevan perusteltua ryhtyä toimenpiteisiin systemaattisen riskienhallintapolitiikan kehittämiseksi valtionhallinnossa, ja että riskienhallinnan kehittäminen on tarkoituksenmukaista aloittaa keräämällä tietoa siitä mitä riskienhallinta on, mitä sillä tavoitellaan ja mitkä sen nykyiset toteutustavat ovat. Riskienhallintapolitiikan tulisi kattaa konsernitaso, jolla viitataan valtiontalouden ja –toiminnan kokonaisuuteen ja erityisesti yhteiskuntapolitiikan strategiseen tasoon sekä hallinnonalataso ja virastojen ja laitosten taso. Hallinnontasolla kyse olisi hallinnonalakohtaisista riskienhallinnan periaatteista. Virasto- ja laitostasolla tavoitteena olisivat virasto-, laitos-, liikelaitos- ja rahastokohtaiset riskienhallintapolitiikat sekä niitä toteuttavat välineet. (Valtiovarainministeriö 2004b,1.)

Valtiokonttorissa oli jo vuonna 2004 tehty pidempään systemaattista kehitystyötä riskienhallinnan palvelujen tarjoamiseksi valtionhallinnolle. Valtiokonttorin vakuutustoimialalla oltiin tuolloin kehittämässä vahinkoriskien hallintaa sekä kartoitettu valtion liikelaitosten riskejä tavoitteena tukea riskienhallintapolitiikan laatimista. Neuvottelukunta totesi kokouksessaan valtiokonttorissa tehtävän riskienhallinnan kehittämistyön ja palveluiden kehittämisen olevan tarkoituksenmukaista ottaa järjestelmällisesti osaksi neuvottelukunnan kautta tehtävää yleisempää riskienhallinnan kehittämistyötä. (Valtiovarainministeriö 2004b,1-2.)

Kuluneen kymmenen vuoden aikana sisäisen valvonnan ja riskienhallinnan neuvottelukunnan tarpeelliseksi toteamaa tukevaa ja kehittävää työtä on myös tehty. Vuosina 2004-2008 Valtiokonttori on selvittänyt valtionhallinnon organisaatioiden riskienhallinnan tilaa vuosittaisilla kyselyillä. Valtiokonttorissa on myös yhteistyössä VTT:n Tuotteet ja tuotanto –yksikön kanssa luotu valtionhallinnon erityispiirteet huomioiva Kaiku-luotain –väline kokonaisvaltaiseen riskienarviointiin ja dokumentointiin. (Ks. Rusanen 2009, 29-31.) Yhteinen riskienhallintapolitiikka on laadittu, mutta ainoastaan valtion liikelaitoksille (Suoninen 2014). Sisäisen valvonnan ja riskienhallinnan neuvottelukunta ja sen alainen sisäisen tarkastuksen jaosto on puolestaan laatinut valtion virastoille ja laitoksille edellä esiteltyyn COSO-ERM-malliin pohjautuvan suosituksen sisäisen valvonnan ja riskienhallinnan lähestymistavoista sekä toimivuuden arvioinnista (Valtiovarain controller –toiminto 2005).

Lupaavasti käynnistynyt valtionhallinnon riskienhallintaa tukeva ja kehittävä työ on kuitenkin sekä Valtiokonttorin että valtiovarain controllerin osalta tämän jälkeen hiipunut. Sisäisen valvonnan ja riskienhallinnan neuvottelukunta ei ole luonut työtään edistäviä vakioituja informointi ja vaikuttamiskanavia (Valtiovarainministeriö 2011, 2). Valtiokonttorin riskienhallintapalveluihin liittyvä tuki ja kehitystyö on päättynyt (Suoninen 2014). Kaiku-luotain –välinettä ei myöskään enää jaeta käyttöön, ja Valtiokonttorin Kaiku-palvelu liittyy nykyisin ainoastaan työhyvinvoinnin tukemiseen Kaiku-rahalla ja pienimuotoisella konsultointipalvelulla (Takkinen 2014). Valtiovarain controller –toiminnon laatiman suosituksen jälkeen ei ole luotu uusia tu-

kevia välineitä, eikä valtiovarainministeriössä ole meneillään akuuttia valtionhallinnon riskienhallinnan kehittämiseen tai tukemiseen liittyvää palvelua tai kehittämistyötä (Helkiö 2014). Valtionhallinnon virastoille ja laitoksille ei siten ole tarjolla kokonaisvaltaista riskienhallintaa tukevia palveluja tai työvälineitä valtiovarain controller –toiminnon laatiman suosituksen lisäksi. Sisäisen valvonnan ja riskienhallinnan neuvottelukunnan lisäksi ei myöskään ole olemassa muuta valtionhallinnon konsernitasolla asiakokonaisuutta koordinoivaa elintä (Valtiovarainministeriö 2011, 3).

Valtionhallinnon organisaatioissa on kuitenkin ollut käytössä lukuisia erillisiä riskienhallinnan ja turvallisuuden osa-alueita koskevia riskienhallinnan välineitä. Työsidonnaisten riskien hallitsemiseen on sosiaali- ja terveysministeriön ja valtion teknillisen tutkimuskeskuksen yhteistyönä laadittu riskien tunnistamisen ja arvioinnin soveltuva Riski-Arvi. Turvallisuusjohtamisen tueksi on valtion työpaikoille kehitetty työturvallisuusriskeihin perustuva RIMA, jonka avulla voidaan täyttää työturvallisuuslain (738/2002) asettamat riskien arviointia koskevat vaatimukset. Käytössä on myös ollut yleisen järjestyksen ja siisteyden kontrollointiin kehitetty TUTTA-VA-menetelmä sekä kemikaaliriskejä käsittelevä Kemi-Arvi-menetelmä. Valtionhallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen toimielin VAHTI on puolestaan merkittävästi ohjeistanut tietoturvallisuuteen liittyvää riskienhallintaa. (Herrainsilta 2006, 55-56.)

Merkittävä valtion johdolla luotu turvallisuuteen ja riskienhallintaan liittyvä väline on Kansallinen turvallisuusauditointikriteeristö KATAKRI. KATAKRI:n päätavoitteena on yhtenäistää viranomaistoimintoja viranomaisen toteuttaessa yrityksessä tai muussa yhteisössä kohteen turvallisuustason todentavan tarkastuksen. KATAKRI:n on tarkoitettu toimivan välineenä yrityksen tai muun auditoitavan kohteen turvallisuustason varmentamiseen. Tarve turvallisuustason varmentamiselle syntyy joko valtionhallinnon salassa pidettävää tietoa sisältävissä hankkeissa tai kansainvälisen pyynnön seurauksena. Kansainvälisen pyynnön taustalla on se, että päästäkseen osallistumaan kansainväliseen tarjouskilpailuun tulee yrityksen täyttää hankeen turvallisuuteen liittyvät vaatimukset. Jos arvioinnin kohteena oleva taho täyttää kriteeristön vaatimukset tarvittavalla tasolla, voi toimivaltainen viranomainen myöntää tästä todistuksen. Kriteeristön toinen päätavoite on auttaa yrityksiä ja yhteisöjä omassa sisäisessä turvallisuustyössään. KATAKRIn taustalla on vuodelta 2008 olevaan järjestyksessään toiseen sisäisen turvallisuuden ohjelmaan kirjattu toimenpide, jonka tarkoituksena oli luoda viranomaisille ja yrityksille yhteinen turvallisuuskriteeristö yhteisöturvallisuusmenettelyjen yhtenäistämiseksi ja omavalvonnan sekä auditoinnin parantamiseksi. Toimenpiteen toteuttaminen osoitettiin puolustusministeriön johtovastuulle ja se valmistui vuoden 2009 lopussa laajan viranomais-, järjestö- ja yrityskentän toimijoiden joukon yhteistyönä. (Puolustusministeriö 2011, 2-4.)

Kriteeristöstä julkaistiin vuonna 2011 toinen versio. Ensimmäisen version tavoin se on jaettu neljään hallinnollisen turvallisuuden eli turvallisuusjohtamisen, henkilöstöturvallisuuden,

fyysisen turvallisuuden ja tietoturvallisuuden pääosioon. Kriteeristön pääosiot on jaettu edelleen osiosta riippuen kolmesta yhdeksään osa-alueeseen, joista kukin sisältää kolmesta jopa yhdeksääntoista tarkasteltavaa asiaa. (Puolustusministeriö 2011, 3, 8-117, 123.) Riskienhallinnan kokonaisuudesta tuttuja elementtejä käsitellään kriteeristön hallinnollista turvallisuutta koskevassa osiossa, jonka osa-alueita ovat muun muassa turvallisuuspolitiikka, turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt, turvallisuuden tavoitteiden määrittely, riskien tunnistus, arviointi ja kontrollit, turvallisuusorganisaatio ja vastuut, turvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen, turvallisuuden vuotuinen toimintaohjelma, sekä raportointi ja johdon katselmukset. (Puolustusministeriö 2011, 3, 8-46.)

Nykyisin tietoista organisaation toimintaa tukevaa riskienhallintaa toteutetaan useissa valtion virastossa ja laitoksissa. Tästä esimerkkinä Liikennevirasto (Liikennevirasto 2012) ja Viestintävirasto (Arnell, 2010). Viestintävirastossa riskienhallinnalla tuetaan viraston tavoitteiden saavuttamista ja varmistetaan toiminnan jatkuvuus - Viestintävirastossa toteutettava ”kokonaisvaltainen riskienhallinta on osa viraston toiminnanohjausjärjestelmää ja siten oleellinen osa viraston johtamista. Viraston riskienhallinta koostuu viraston tavoitteiden saavuttamisen turvaamisesta, organisaatioturvallisuudesta sekä toiminnan jatkuvuuden varmistamisesta.” (Riskienhallinnalla tuetaan viraston…2013.) Esimerkkinä voidaan mainita myös Kansaneläkelaitos, jossa Sisäisen valvonnan ja riskienhallinnan neuvottelukunnan mukaan toteutetaan hyvin kehittynyttä ja jäsentynyttä riskienhallintaa (Valtiovarainministeriö 2009b, 2).

Riskienhallintaa on ryhdytty toteuttamaan myös toisessa valtion aluehallinnon keskeisessä toimijassa: Elinkeino-, liikenne- ja ympäristökeskuksille on laadittu yhteinen riskienhallintapolitiikka, jota toimeenpannaan ELY-keskuskohtaisin kaksivuotisin toimenpideohjelmin. Jokaisessa ELY-keskuksessa toimii sisäisen valvonnan ja riskienhallinnan kehittämistä ja toimeenpanoa tukeva työryhmä, jonka lisäksi on muodostettu ELY-keskusten ja niitä ohjaavan työ- ja elinkeinoministeriön välinen muun muassa riskienhallinnataa edistävä ja kehittävä yhdyshenkilöverkosto. Riskienhallintatyö ELY-keskuksissa on käynnistynyt virastoja ohjaavan Työ- ja elinkenoministeriön toimesta. (Tolonen 2013, 20-23.) ELY-keskuksille laaditut riskienhallinnan periaatteet pohjautuvat valtiovarain controller –toiminnon antamaan suositukseen (Työ- ja elinkeinoministeriö 2011, 12).

4.2 Valtiovarainministeriön suositus sisäisestä valvonnasta ja riskienhallinnasta

Valtioneuvoston asettama sisäisen valvonnan ja riskienhallinnan neuvottelukunta ja sen alainen sisäisen tarkastuksen jaosto on laatinut valtion virastoille ja laitoksille suosituksen sisäisen valvonnan ja riskienhallinnan lähestymistavoista sekä toimivuuden arvioinnista. Valtion viraston ja laitoksen sekä rahaston sisäinen valvonta ja riskienhallinta – Valtionhallinnon hyvä käytäntö ja sen toteutumisen arviointi valmistui vuonna 2005. (Sisäinen valvonta ja riskienhal-

linta 2013.) Suositus kuvaa valtionhallinnon hyvää käytäntöä, ja sen tarkoituksena on tukea sisäisen valvonnan ja riskienhallinnan asianmukaisuuden ja riittävyyden arviointia sekä tähän liittyvien keskeisten kehittämistarpeiden tunnistamista. Erityisesti suosituksen tarkoituksena on tukea valtion virastojen ja laitosten johtoa laadittaessa talousarvioasetuksen (1243/1992 ,65 §) tarkoittamaa sisäisen valvonnan arviointi- ja vahvistuslausumaa. Arviointi- ja vahvistuslausuman edellyttämät arvioinnit tehdään tavanomaisten tulossuunnittelu- ja johtamisprosessien osana. (Valtiovarain controller –toiminto 2005, 3, 6, 20.)

Sisäisen valvonnan ja riskienhallinnan neuvottelukunnan antaman suosituksen keskeinen osa on arviointikehikko, johon organisaatio voi verrata omaa sisäisen valvonnan ja riskienhallinnan järjestelmäänsä ja tunnistaa niihin liittyviä kehittämistarpeita. Kehikon sisältö ei totea sisäistä valvontaa ja riskienhallintaa koskevia vähimmäisvaatimuksia, vaan on luonteeltaan kuvaus ideaalitilanteesta ja toimii tarkistuslistana. Kehikko ei siten ohjaa käytettäväksi arvioissa tiettyjä numeerisia arvoja. Arviointikehikko perustuu kokonaisvaltaisen riskienhallinnan COSO-ERM –malliin, mutta on muokattu mahdollisimman helposti valtion virastoissa, laitoksissa ja rahastoissa käytettäväksi. Kehikossa sisäinen valvonta ja riskienhallinta on jaettu COSO-ERM –mallin mukaisesti kahdeksaan osa-alueeseen, jotka ovat sisäinen toimintaympäristö ja toimintarakenteet, tavoitteiden asettaminen, riskien tunnistaminen, riskien arviointi, riskeihin vastaaminen, valvontatoimet eli kontrollit, informaatio ja tiedonkulku sekä seuranta. (Valtiovarain controller –toiminto 2005, 18-19.)

Neuvottelukunnan sisäisen tarkastuksen jaosto on lisäksi laatinut arviointikehikosta suppeamman version käytettäväksi virastoissa ja laitoksissa sisäisen valvonnan käynnistämiseksi minimivaatimusten täyttämisellä. Arviointikehikon suppeampi versio on osa-alueiltaan sama, mutta osa-alueiden sisältämiä arvioitavia kohteita on karsittu. Suppea suositus ohjeistaa arvioimaan kunkin arviointikohteen numeerisesti välille 1-4. (Valtiovarain controller -toiminto ja sisäisen tarkastuksen jaosto 2009.) Aluehallintovirastojen toimintakertomusten yhteydessä annetut sisäisen valvonnan arviointi- ja vahvistuslausumat perustuvat edellä mainitulla suppealla arviointikehikolla tehtyyn arviointiin.

Virasto tai laitos voi käyttää sisäisen valvonnan ja riskienhallinnan toimivuutta arvioidessaan myös muita yleisesti hyväksyttyjä arviointikehikkoja, kuten COSO:a, COSO-ERM:ia tai CoCo:a, mutta käytettävä kehikko tulee aina sopeuttaa vastaamaan viraston tarpeita. (Sisäinen valvonta ja riskienhallinta 2013.) Valtioneuvoston controller kuitenkin suosittelee valtion tilivirastoina toimivien sellaisten virastojen ja laitosten, joille ministeriö on suoraan asettanut tulostavoitteet, käyttävän suositusta ja sen sisältämää arviointikehikkoa sisäisen valvonnan ja riskienhallinnan kehittämisessä. Lisäksi on huomattava, että joidenkin valtion tehtävien ja toimintojen sekä eräiden riskien osalta on perusteltua käyttää kyseistä riskityyppiä tai toimin-

toa koskevia erityisiä riskienhallintavälineitä. (Valtiovarain controller –toiminto 2005, 6.) Suositukset eivät kuitenkaan erittele mitä nämä toiminnot tai riskityypit ovat.

Valtionvarainministeriön antama suositus arvio, että sen laatimaa arviointikehikkoa käytettäessä kohdataan useassa virastossa uusia esimerkiksi riskien tunnistamiseen ja hallintaan sekä riskienhallintapolitiikkaan liittyviä asioita, joita ei ennen ole ollut tarkastelussa. Suositus kuitenkin korostaa, että ennen näkökulmien laajentamista riskienhallintaan tulisi huolehtia sisäisen valvonnan perusasioista. Perusasioita tässä yhteydessä ovat ne, että hallintosäädökset sekä työjärjestykset ovat ajantasaisia, taloussääntö on päivitetty vastaamaan talousarvioasetuksen 69 b §:n säännöksiä ja perustuu viraston talousprosessin ja siihen liittyvien olennaisimpien riskien kohtuulliseen hallintaan, perustehtävien ja prosessien määrittelyt ovat yleisesti ottaen kunnossa ja ottavat huomioon lainsäädännön vaatimukset, hankintatoimi ja tietojärjestelmät sekä muut kriittiset ja riskiherkät toiminnot on analysoitu ja tuloksellisuutta ja lainmukaisuutta turvaavat järjestelyt sekä henkilöstön koulutus on toteutettu, tavoitteenasettelu vastaa tulosohjaus- ja tilivelvollisuusuudistuksen asettamia vaatimuksia, ja että tuloksellisuuden ja johdon laskentatoimi sekä muu seurantajärjestelmä vastaa talousarvioasetuksen 55 §:n vaatimuksia. (Valtiovarain controller –toiminto 2005, 21.)

Sisäisen valvonnan ja riskienhallinnan neuvottelukunta on kuitenkin todennut, etteivät kehikot saa olla itsetarkoituksellisia, vaan niiden merkitys käytännön kannalta tulee ymmärtää ja sisäistää (Valtiovarainministeriö 2008,4). Kuten edellä todettu, toteuttavat valtiovarain controller –toiminnon suosituksen mukaisia menettelyjä riskienhallintansa järjestämisessä esimerkiksi Liikennevirasto (Liikennevirasto 2012, 6) ja ELY-keskukset (Työ- ja elinkeinoministeriö 2011, 12).

5 Tutkimusaineisto ja menetelmät

Tämä opinnäytetyö on lähestymistavaltaan laadullinen tutkimus ja sen tutkimusstrategiana tapaustutkimus. Tapaustutkimuksessa tutkimuksen kohteena on yksittäinen tapaus tai tilanne tai tapausten joukko. Sen tavoitteena on useimmiten ilmiöiden kuvailu tai kartoitus ja mielenkiinnon kohteena prosessit. Tapaustutkimukselle on tyypillistä se, että aineistoa kerätään useita menetelmiä käyttäen. (Hirsjärvi, Remes & Sarajärvi 1998, 130, 136.) Anttilan (1996, 250) mukaan tavoitteena on tutkimuskohteen ominaispiirteiden systemaattinen, tarkka ja totuudenmukainen kuvailu, ei niinkään ilmiöiden välisten yhteyksien selittäminen, ennusteiden tekeminen tai hypoteesien testaaminen (ks. Saaranen-Kauppinen & Puusniekka 2006d). Tapaustutkimus on kirjava käsite – se ei rajoita menetelmävalintoja, ja monet projektit ja kehittämis- tai arviointitutkimukset voidaan lukea tapaustutkimuksiksi (Saaranen-Kauppinen & Puusniekka 2006d).

Tässä opinnäytetyössä tutkimuksen kohteena oli tapaustutkimukselle tyypillisesti yksittäinen virasto ja tavoitteena riskienhallinnan toteutumisen kartoitus ja kuvailu. Empiirinen aineisto muodostui kuitenkin ainoastaan valmiista aineistoista sen sijaan, että aineistoa olisi kerätty usein menetelmin. Tutkimusmenetelmänä käytettiin dokumenttianalyysia. Dokumenttianalyysissä pyritään Ojasalon, Moilasen ja Ritalahden (2009, 121) mukaan tekemään päätelmiä kirjalliseen muotoon saatetusta aineistosta. Aineistoihin voidaan lukea kaikki tutkittavaan ilmiöön liittyvä kirjoitettu, kuvattu ja puhuttu materiaali, kuten www-sivut, raportit ja vuosikertomukset, lehtiartikkelit ja tekstiksi muutetut haastattelut. Menetelmän tarkoituksena on informaatioarvon lisääminen järjestämällä aineisto selkeäksi ja tiiviiksi. Dokumenttianalyysi toimii vaihtoehtoisena menetelmänä sille, että tieto kerättäisiin esimerkiksi haastatteluin ja kyselyin (Dokumenttianalyysi 2013). Virallisia dokumentteja valtion viraston turvallisuudenhallinnan nykytilan arvioimisen välineenä on käyttänyt myös Rusanen (2009, 67).

Opinnäytetyö sisältää myös konstruktiiviselle tutkimukselle tyypillisiä elementtejä. Konstruktiivista tutkimusta käytetään lähestymistapana muun muassa silloin, kun tavoitteena on luoda esimerkiksi suunnitelma, mittari tai malli. Kokonaan uudella tai aikaisempaa paremmalla rakenteella pyritään tietyn ongelman ratkaisemiseen käytännönläheisellä ja teoreettisesti perustellulla tavalla. Konstruktiivista tutkimusta kuvaillaan tutkimustietoon pohjautuvaksi uudenlaisen todellisuuden rakentamiseksi, ja se muistuttaa lähestymistapana innovaatioiden tuottamista. Konstruktiivisella tutkimuksella on yhteistä myös toimintatutkimuksen kanssa, sillä kummassakin pyritään muuttamaa organisaation toimintaa ja käytänteitä. (Ojasalo ym. 2009, 65-66.)

Konstruktiivisessa tutkimuksessa on oleellista, että kyseessä oleva ongelma ja sen ratkaisu kytketään teoreettiseen tietoon. Keskeistä on myös se, että luotu rakenne osoittautuu toimivaksi paitsi kohdeorganisaatiossa, mahdollisuuksien mukaan myös sen ulkopuolella. Käytännön ongelman ratkaisemisen lisäksi konstruktiivisen tutkimuksen tulisi myös tuoda uutta tietoa tiedeyhteisöön. Konstruktiivisen tutkimuksen piirre on myös se, että tutkimuksen toteuttajien ja hyödyntäjien keskinäinen vuorovaikutus korostuu. Kohdeorganisaation johdon tai muiden kehittämisen kohteeseen käytännössä liittyvien toimijoiden tuleekin olla tutkimuksen toteuttamisessa aktiivisesti mukana. (Ojasalo ym. 2009, 65-66.)

Opinnäytetyön tuotoksena laadittiin teoreettiseen tietoon ja kohdeorganisaatiossa tunnistetun ongelman ratkaisemiseen tähtäävä ohje. Konstruktiivisen tutkimukselle keskeiset ominaisuudet eivät kuitenkaan muilta osin täyty, sillä kohdeorganisaation johto ja organisaation sidosryhmät eivät osallistuneet aktiivisesti tutkimusprosessiin. Myöskään konstruktiivisen tutkimuksen vaiheet eivät tässä opinnäytetyössä toteudu. Konstruktiivisen tutkimuksen prosessin vaiheet muodostuvat mielekkään ongelman etsimisestä, tutkimuksen ja kehittämisen kohdetta koskevan teoreettisen ja käytännöllisen tiedon hankkimisesta sekä ratkaisujen laatimises-

ta, ratkaisun toimivuuden testaamisesta ja oikeellisuuden osoittamisesta, ratkaisussa käytettyjen teoriakytkentöjen näyttämisestä ja ratkaisun uutuusarvon osoittamisesta sekä ratkaisun soveltamisalueen laajuuden tarkastelusta (Ojasalo ym. 2009, 67-68). Tässä opinnäytetyössä ei toteutettu ratkaisun laatimista seuraavia vaiheita, vaikkakin tämä on opinnäytetöiden yhteydessä työläydestä ja aikataulusyistä yleistä (Ojasalo ym. 2009, 68).

5.1 Aineiston hankinta

Tässä opinnäytetyössä empiirinen aineisto muodostui valmiista aineistoista. Järvinen ja Järvinen (2004, 156) jakavat valmiit kirjalliset materiaalit dokumentteihin ja arkistoihin, joista ensiksi mainitut sisältävät esimerkiksi muistioita, organisaatiokarttoja, pöytäkirjoja, raportteja ja tutkimuksia. Arkistoihin puolestaan luetaan tilastoja, budjetteja, katsausaineostoja ja muita jollain tapaa järjestettyjä tiedostoja. Dokumenttiaineistoa ovat myös esimerkiksi 1) lait, asetukset, hallinnolliset päätökset, viralliset kirjeet, viranomaisten ohjeet, 2) hakuteokset, muu kirjallisuus, aikakauslehdet, sanomalehdet, vuosikertomukset, sekä 3) yhdistysten, yritysten, laitosten yms. tiedotusmateriaali, pöytäkirjat ja historiikit (Anttila 1998). Tutkimusaineistona käytettävä kirjallinen materiaali voidaan jakaa myös yksityisiin dokumentteihin ja arkistoihin. Tällöin yksityiset dokumentit muodostuvat esimerkiksi puheista, kirjeistä, muistelmista ja sopimuksista. Joukkotiedotteiksi luetaan esimerkiksi sanomalehdet ja elokuvat sekä radio- ja tv-ohjelmat. (Tuomi & Sarajärvi 2009, 84.)

Valmis aineisto muodostui organisaation sisäisen valvonnan ja riskienhallinnan vahvistuslausumista ja niiden antamiseksi kerätystä kyselyaineistosta sekä muista organisaation toiminnasta kertovista dokumenteista. Vahvistuslausumat ja niihin liittyvä valmis kyselyaineisto käsittelevät organisaation riskienhallinnan nykytilaa suhteessa valtiovarain controller –toiminnon antamaan suositukseen sisäisen valvonnan ja riskienhallinnan toteuttamisesta valtion virastossa ja laitoksessa. Kysely on toteutettu käyttämällä valtiovarain controller -toiminnon suppeaa arviointikehikkoa (liite 2), joka on keskeisiltä osin kokonaisvaltaisen riskienhallinnan COSO-ERM –mallin mukainen. Kyselyn toteuttamiseksi arviointikehikko on laadittu WebroPol-kyselyn muotoon, ja siihen ovat vastanneet organisaation ylijohtaja, kaikkien vastuualueiden johtajat ja hallintopalvelujen vastuuyksikön johtaja. Vahvistuslausuman antaminen on toteutettu tällä menettelyllä koko aluehallintovirastojen toiminnan ajan.

Vahvistuslausuman antamiseksi laaditussa kyselyssä tarkastellaan toimintakulttuuria, tavoitteiden asettamista, riskien tunnistamista, arviointia ja hallintaa, kontrolleja, tiedonkulkua ja informaation käytettävyyttä sekä seurantaa. Kukin arviointikohteista sisältää alaotsikoita ja näiden alla arvioitavia asioita, joista kullekin annetaan numeroin 0-4 arvoksi ei sovellettavissa, heikosti, kohtuullisesti, melko hyvin tai hyvin ja järjestelmällisesti. Osa-aluekohtaisten tulosten lukuarvot ovat alakohtiensa keskiarvoja, jotka edelleen kaikkien vastaajien keskiar-

voja. Kuhunkin arvioitavaan asiaan on vastannut kuusi henkilöä, jotka arviointi- ja vahvistuslausuman mukaan ovat viraston johdon edustajat.

Tähän liittyvänä aineistona oli käytössä kohdeorganisaation tuloksellisuusraportteihin liitetyt kunkin toimintavuoden sisäisen valvonnan arviointi- ja vahvistuslausumat, .xls-muotoinen kyselytulokset kokoava ja osa-aluekohtaiset kesiarvot sisältävä tiedosto sekä vuotta 2013 koskevan arvioinnin osalta .mht-muotoinen tiedosto, joka sisälsi kaikki kysytyt asiat ja vastaajien niihin antamat numeroarviot. Vahvistuslausumat saatiin tuloksellisuusraporttien yhteydestä, ja kyselyaineisto sähköpostitse organisaation hallintopalvelujen vastuuyksiköltä. Kyselyaineistoon sisältyvät kuviot esitetään tässä tutkimuksessa siltä osin, kuin niihin on viitattu tutkimustulosten ja johtopäätösten yhteydessä (liite 5).

Hirsjärven ym. (1998, 185, 188) mukaan tutkimusongelman joihinkin osiin voi saada vastauksen jo olemassa olevien valmiiden aineistojen pohjalta, eikä tällaisen sekundääriaineiston käyttämisellä ole vaikutusta esimerkiksi opinnäytetytön arvoon. Aikaisempien tutkimusten materiaalia voi käyttää esimerkiksi vertailumateriaalina tai omaa aineistoa täydentävänä materiaalina. Kaikkeen olemassa olevaan materiaaliin on kuitenkin suhtauduttava kriittisesti.

Muut organisaation toiminnasta kertovat dokumentit muodostuivat strategisen ohjauksen ja tulosohjauksen asiakirjoista, toiminnan raportoinnin asiakirjoista ja muista organisaation toimintaan liittyvistä dokumenteista ja tiedostoista. Nämä muodostivat aineiston määrällisesti suurimman osan. Tämän aineiston tarkoituksena oli selvittää sekä riskienhallinnan ilmenemismuodot ja käytetyt menettelyt että organisaation riskienhallinnalle kohdistetut odotukset. Nämä asiakirjat koskevat vuosia 2010-2013, eli aikaa jolloin aluehallintovirastot ovat toimineet. Dokumentit olivat sähköisiä .pdf-muotoisia ja niitä oli yhteensä 39 kappaletta. Asiakirjoiksi valittiin organisaation strategia-asiakirjat ja strategiset tulossopimukset, strategia, toiminnalliset tulossopimukset, työjärjestykset, toimintaa ja tuloksellisuutta koskevat raportit sekä muut organisaation tuottamat dokumentit, joiden kautta arvioitiin voitavan muodostaa käsitystä riskienhallinnan toteutumisesta kohdeorganisaatiossa. Näitä olivat esimerkiksi työhyvinvointisuunnitelmat, valmiussuunnitelma ja toimitilojen pelastussuunnitelma.

Dokumentit saatiin pääosin kyseisen aluehallintoviraston intranet-sivuilta. Aineistoon kuuluvia oletettavia puuttuvia asiakirjoja, kuten joitakin tulosohjauksen asiakirjoja sekä vahvistuslausuman antamiseksi tehtyyn kyselyyn liittyvät muut tiedostot kysyttiin ja saatiin lisäksi kohdeorganisaation hallintopalvelujen vastuuyksiköltä, sillä asiakirjoja ei löytynyt valtion raportointipalvelu Netran sivuilta. Netra on julkinen palvelu, joka sisältää ajankohtaista tietoa valtion toiminnasta, resursseista ja tuloksellisuudesta. Palveluun on koottu valtion ohjauksen kannalta keskeinen informaatio, kuten tuloksellisuus-, talous- ja henkilöstöraportointia sekä toiminnan ja tuloksellisuuden asiakirjoja. (Valtion raportointipalvelu Netra 2013.) Ohjausasiakirjoja

ja tuloksellisuusraportteja lukuun ottamatta tutkimuksen empiirinen aineisto koostuu asiakirjoista ja tiedostoista, jotka eivät ole julkisesti saatavilla.

Kvalitatiivisessa tutkimuksessa on tavoitteena tutkimuskohteen ymmärtäminen. Tällöin kohdataan kysymys tutkimusaineiston koosta ja edustavuudesta. Aineiston riittävyyden yhteydessä käytetään saturaation käsitettä. Haastatteluaineiston yhteydessä aineisto on riittävä ja saturaatio tapahtunut, kun haastatteluissa alkavat kertautua samat asiat. (Hirsjärvi ym. 1998, 178-181.) Voidaan arvioida myös aineiston validiteettia, jolloin tarkasteluun tulee ottaa aineiston kattavuus ja se vastaako aineisto tutkittavaa ilmiötä tai vastaako aineiston kokoamistapa valittua analyysimenetelmää (Anttila 1998).

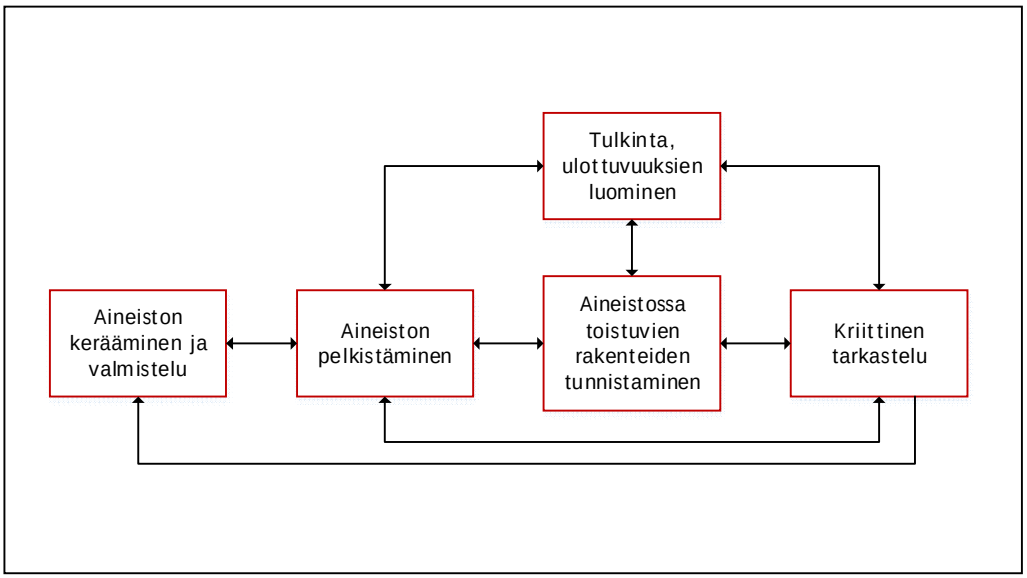
Tässä tutkimuksessa aineiston valintaa pidettiin perusteltuna, sillä valtion organisaatioille osoitetaan odotuksia juuri strategisen ohjauksen ja tulosohjauksen asiakirjoin. Riskienhallinnan nykytilaa taas arvioidaan vahvistuslausuman antamisen yhteydessä, sitä toteutetaan usein turvallisuuden osa-alueiden kautta, ja toimintaa organisoidaan muun muassa työjärjestyksin. Kerättyä aineistoa pidettiin myös riittävänä, sillä ohjausasiakirjat, vahvistuslausumat ja niiden antamiseksi kerätty kyselyaineisto sekä toiminnan raportit käsittivät organisaation koko toiminnan ajan ja yksittäisiä poikkeuksia lukuun ottamatta sen kaikki vastuualueet. Aineisto käsitti myös organisaation työjärjestykset ja kohdeorganisaation kontekstissa keskeisiin turvallisuuden osa-alueisiin liittyvät dokumentit.

5.2 Aineiston analysointi

Kerättyä aineistoa voidaan analysoida usealla eri tavalla. Kehittämistehtävä määritteleekin tilanteeseen sopivan analyysin. Siten ennen analyysiä on päätettävä muun muassa se analysoidaanko aineiston piiloviestejä vai ainoastaan ilmisisältöä. Dokumenttianalyysin päävaiheita kuvaa hyvin laadullisen tutkimuksen yleinen malli, jonka vaiheita ovat aineiston kerääminen ja valmistelu, aineiston pelkistäminen ja aineistoissa toistuvien rakenteiden tunnistaminen (kuvio 11). Kaikkiin vaiheisiin liittyy lisäksi kriittinen tarkastelu tarkoituksenaan vaiheiden toteutuksen ja tulosten mahdollisten virheiden tunnistaminen ja korjaaminen. (Ojasalo ym. 2009, 122-123.) Poimittaessa tietoja dokumenteista tulee huomata, ettei näitä dokumentteja ole tehty tutkimusta varten, vaan niiden tarkoituksena on ollut välittää tietoa tai tukea dokumentin käyttäjän muistia. On myös epävarmaa kuvaavatko dokumentin tiedot todellisuutta. (Järvinen ja Järvinen 2004, 156; Dokumenttianalyysi 2013.)

Laadullisen aineiston analyysissä erotellaan usein tutkimuksessa käytetyn päättelyn logiikan mukaisesti deduktiivinen, eli yleisestä yksittäiseen, ja induktiivinen, eli yksittäisestä yleiseen -analyysi. Jaottelu on tieteellisesti kuitenkin ongelmallinen, ja Eskola (ks. Tuomi & Sarajärvi 2009, 95) on esittänyt jaotteluksi aineistolähtöisen, teoriasidonnaisen ja teorialähtöisen ana-

lyysin. Jako huomioi analyysiä ohjaavat tekijät deduktiivinen/induktiivinen –jakoa paremmin. Analyysimuotojen erot liittyvät tutkittavaan ilmiöön liittyvän teorian ohjaavuuteen aineistoa hankittaessa, analysoitaessa ja raportoitaessa. Käsitettä teoriasidonnainen vastaa käsite teoriaohjaava. (Tuomi & Sarajärvi 2009, 95, 98.)



Kuvio 11: Laadullisen tutkimuksen yleinen malli Ojasalon ym. (2009, 123) mukaan.

Aineistolähtöisessä analyysissä aikaisemmilla tiedoilla ja teorialla ei pitäisi olla vaikutusta itse analyysin tulokseen eikä lopputulokseen. Tätä analyysitapaa pidetään ongelmallisena siksi, että tutkija vaikuttaa väistämättä tuloksiin jo käyttämiensä käsitteiden ja tutkimusasetelman kautta. Teoriaohjaavassa analyysissä aikaisemman tiedon vaikutus on tunnistettavissa, mutta tarkoituksena ei ole testata aikaisempaa teoriaa. Analyysi voi tällöin alkaa aineistolähtöisesti, mutta se loppuvaihetta ohjaa esimerkiksi teoriasta johdettu luokittelu. Teorialähtöinen analyysi nojaa olemassa olevaan tietoon, ja analyysiä ohjaa jokin valmis kehys. Tämä analyysityyppi liittyy tutkimukseen, jossa testataan aikaisempaa teoriaa. Aineisto analysoidaan teoriaosuudessa hahmotettuihin kategorioihin suhteutetusti. (Tuomi & Sarajärvi 2009, 95-98.)

Dokumenttianalyysissä on erotettavissa eri analyysitapoina sisällön erittely ja sisällön analyysi. Erittelyllä tekstin sisältöä kuvataan määrällisesti esimerkiksi numeroin. Sisällön analyysissä aineiston sisältöä puolestaan kuvataan sanallisesti tavoitteena tekstin merkitysten etsiminen ja tunnistaminen. Menetelmät eivät kuitenkaan sulje toisiaan pois, ja myös sisällön analyysissä voidaan tuottaa määrällisiä tuloksia esimerkiksi laskemalla tietyn sanan esiintymistä analysoitavassa aineistossa. (Ojasalo ym. 2009, 122; Tuomi & Sarajärvi 2009, 106-107.) Tuomi & Sarajärvi (2009, 107) toteavatkin, että sisällön analyysi voi käsitteenä tarkoittaa sekä sisällön analyysiä että sisällön erittelyä.

Kvalitatiivinen tutkimusote ei myöskään sulje pois laskemisen kaltaista määrällisen menetelmän käyttöä, ja määrällisen analyysin käyttäminen laadullisen aineiston analyysissä voi joskus olla käyttökelpoinen ratkaisu aineiston hahmottamisen ja päätelmien tekemisen tueksi. Esimerkiksi sanojen esiintymistä laskettaessa tulee kuitenkin huomioida konteksti – haettu sana voi esiintyä erilaisissa yhteyksissä, eikä pelkästään sanoja laskemalla saada luotettavia tuloksia. (Saaranen-Kauppinen & Puusniekka 2006a; Saaranen-Kauppinen & Puusniekka 2006b.) Tämän opinnäytetyön kohdeorganisaation osalta tämä korostuu siksi, että organisaation toiminnan ohjauksen asiakirjoissa sekä tuloksellisuusraporteissa turvallisuus, uhka ja riski esiintyvät lukuisissa sellaisissa aluehallintoviraston ydintehtäviin liittyvissä yhteyksissä, jotka koskevat turvallisuuden edistämistä yhteiskunnassa.

Tässä tutkimuksessa dokumenttianalyysin analyysimuotona käytettiin teorialähtöistä analyysia, ja siinä analysoitiin ainoastaan ilmisisältöä. Analyysi toteutettiin sekä sisällön analyysinä että sisällön erittelynä.

Aineiston keräämisen jälkeen seuraava aineiston valmistelu selkeäksi analysointia varten voi tarkoittaa esimerkiksi aineiston saattamista digitaaliseen muotoon valokuvia skannaamalla tai haastatteluaineiston litteroimista. Myöhempänä tehtävän viittaamisen helpottamiseksi aineisto kannattaa numeroida. Aineiston tallentaminen eri tiedostoiksi on myös suositeltavaa. (Ojasalo ym. 2009, 123-124; Saaranen-Kauppinen & Puusniekka 2006e.)

Tässä opinnäytetyössä tutkimuksen empiirinen aineisto muodostui valmiista erillisistä sähköisistä dokumenteista ja tiedostoista. Aineiston valmistelun yhteydessä kullekin dokumentille tai tiedostolle annettiin numerotunnus (liite 3). Tunnuksen antamisen yhteydessä aineisto luokiteltiin samalla sen mukaan, onko dokumentti tai tiedosto luonteeltaan kohdeorganisaatiolle kohdistettuja odotuksia kuvaavaa vai kohdeorganisaation toimintaa kuvaavaa. Analyysivaihetta edeltävää luokittelua pidettiin aineiston hankinnan yhteydessä tehtyjen valintojen ja aineiston luonteen vuoksi perusteltuna. Aineiston pääluokiksi nimettiin tällä perusteella kohdeorganisaation riskienhallinnan nykytilaa kuvaavat dokumentit ja kohdeorganisaation riskienhallinnan järjestämiseen liittyviä odotuksia kuvaavat dokumentit. Riskienhallinnan järjestämiseen liittyviä odotuksia kuvaavat dokumentit jaettiin edelleen strategisen ohjauksen asiakirjoihin ja tulosohjauksen asiakirjoihin.

Riskienhallinnan nykytilaa kuvaavat dokumentit jaettiin sisäisen valvonnan ja riskienhallinnan vahvistuslausumiin ja niiden antamiseksi kerättyyn kyselyaineistoon sekä muihin kohdeorganisaation riskienhallinnan nykytilaa kuvaaviin dokumentteihin. Erilaisten aineistomuotojen ohella tätä jakoa pidettiin tarkoituksenmukaisena erityisesti siksi, että vahvistuslausumat ja niihin liittyvä kyselyaineisto on alun perin muodostettu tässä tarkastelun kohteena olevan ilmiön arviointiin ja raportointiin, ja muut dokumentit ovat pääsääntöisesti laadittu muuhun käyttö-

tarkoitukseen. Vahvistuslausumat ja niihin liittyvä kyselyaineisto jaettiin nimensä mukaisesti vuosikohtaisiin vahvistuslausumiin ja kyselytuloksiin. Muut kohdeorganisaation riskienhallinnan nykytilaa kuvaavat dokumentit jaettiin edelleen strategioihin, toiminnan ja tuloksellisuuden raportteihin, työjärjestyksiin, turvallisuuden osa-alueiden järjestämiseen liittyviin asiakirjoihin ja muihin asiakirjoihin.

Aineiston valmistelun jälkeen teorialähtöisen analyysin ensimmäinen vaihe on analyysirungon muodostaminen. Analyysirunko voi olla hyvin väljä tai hyvin yksityiskohtainen, mutta aikaisempaa teoriaa tai käsitejärjestelmää testattaessa käytetään yleensä yksityiskohtaista eli strukturoitua analyysirunkoa. Rungon sisälle muodostetaan erilaisia luokituksia ja kategorioita. Teorialähtöisessä analyysissa aineistosta voidaan poimia sekä muodostetun analyysirungon sisälle kuuluvat että sen ulkopuolelle jäävät asiat. (Ojasalon ym. 2009, 126.) Tässä opinnäytetyössä analyysirunko muodostettiin puolistrukturoiduksi teoreettisesta viitekehyksestä johdettujen riskienhallinnan keskeisten ilmenemismuotojen ja sisältötekijöiden mukaiseksi. Analyysirunko muodostui viidestä pääkategoriasta, joiksi valittiin riskienhallintaprosessin vaiheet sekä riskienhallinnan toteuttamiseen liittyvä organisointi.

Analyysirungon pääkategoriat muodostivat riskienhallinnan määrittely, riskienhallintamenettelyt, riskien ja riskienhallinnan seuraaminen ja raportointi, riskienhallinnan kehittäminen sekä riskienhallinnan vastuut ja organisointi. Riskienhallintamenettelyillä tarkoitetaan analyysirungossa riskien tunnistamista ja arviointia sekä riskien hallitsemiseksi tehtäviä toimenpiteitä. Kategoriat noudattavat Ilmosen ym. (2013, 85) kuvaamaa riskienhallintaprosessia, joka sisältää riskienhallintastandardien yleisimmin noudatteleman perusrungon elementit. Kategorioiden valinta katsottiin olevan perusteltua muutoinkin: riskienhallinnan määrittely on riskienhallinnan toteuttamisen ensimmäinen vaihe (Ilmonen ym. 2013; Juvonen ym. 2005), ja sen katsottiin olevan tavoitteellisen ja johdonmukaisen riskienhallinnan edellytys. Riskienhallintamenettelyjen lisäksi riskien ja riskienhallinnan seuraamisen ja raportoinnin sekä riskienhallinnan kehittämisen katsottiin ilmentävän riskienhallinnan konkreettista toteuttamista.

Omaksi kategoriaksi nostettiin lisäksi riskienhallinnan vastuut ja organisointi. Riskienhallinnan toteuttamisen yhteydessä korostetaan organisaation johdon vastuuta ja muiden vastuiden nimeämistä (Ilmonen ym. 2013; sosiaali- ja terveysministeriö 2011; Valtiovarain controller –toiminto 2009). Riskienhallintaan liittyvien vastuiden osoittamisen ja organisoinnin katsottiin olevan edellytys riskienhallinnan jalkautumiselle organisaation toimintaan, ja osoittavan osaltaan edellytyksiä riskienhallinnan konkreettiselle toteuttamiselle. Vastuut ja organisointi ovat myös keskeinen osa niitä organisaation riskienhallinnan nykyisiä menettelyjä ja rakenteita, jotka tulee huomioida kohdeorganisaation riskienhallinnan määrittelemiseksi annettavaa ohjetta laadittaessa.

Analyysirunkoa muodostettaessa pohdittiin vaihtoehtoisesti käytettäväksi valtiovarain controller –toiminnon antaman suosituksen suppeaa arviointikehikkoa. Arviointikehikon käyttöä olisi puoltanut se, että kyseessä on valtion virastolle ja laitokselle annettu suositus sisäisen valvonnan ja riskienhallinnan järjestämisestä ja se, että käytössä ollut kyselyaineisto noudattaa kyseistä kehikkoa. Toisaalta nyt käytetty analyysirunko painottuu sille suosituksen osa-alueelle, jolla kyselyaineiston ja niiden pohjalta laadittujen vahvistuslausumien mukaan organisaation nykytilan puutteet ovat. Lisäksi valittu analyysirunko huomioi muun riskienhallinnan teoreettisen kehyksen korostamat keskeiset elementit mainittua arviointikehikkoa selkeämmin.

Pääkategorioiden sisälle analyysirunkoon kirjattiin huomioitaviksi asioiksi yksityiskohtaisempia riskienhallinnan sisältötekijöitä, jotka ilmentävät tarkasteltavaa pääkategoriaa, tai joiden kautta tarkasteltavan pääkategorian toteutumista suhteessa teoriaan on mahdollista tarkastella. Runkoon kirjatut sisältötekijät eivät rajoittaneet pääkategorian yhteyteen kirjattavia havaintoja. Taulukkoon kirjatut sisältötekijät ovat lyhyitä kuvauksia, joiden ilmeneminen dokumentissa ei vielä tarkoita tarkasteltavan asian toteutumista esimerkiksi valtionhallinnon erityispiirteiden, yleisen riskienhallinnan teorian tai kohdeorganisaatiolle kohdistettujen odotusten tai velvoitteiden mukaisesti. Tutkimuksen johtopäätöksiä tehtäessä kutakin pääkategoriaa tai sen sisältötekijää tarkasteltiin suhteessa edellä mainittuihin.

Yleisesti käytettyjä aineiston pelkistämisen välineitä ovat koodaaminen ja teemakortistot. Koodaamisessa tekstin sisään merkitään eri tekstikohtien yhteyteen tulkinta siitä, mitä kyseisessä kohdassa tarkoitetaan. Merkinnöistä syntyy kuvaus siitä, mitä aineistossa tutkijan näkemyksen mukaan käsitellään. Koodien avulla voidaan myöhemmin etsiä tekstistä kohdat, joissa tarkasteltavaa asiaa käsitellään. (Ojasalon ym. 2009, 126.) Koodaaminen helpottaa aineiston käsittelyä, mutta se ei ole välttämätöntä (Saaranen-Kauppinen & Puusniekka 2006f). Koodien avulla kyseiset tekstikohdat voidaan poimia teemakorteiksi, joihin kootaan aineistosta kaikki kyseistä teemaa käsittelevät asiat. Näin syntyvät tiivistelmät helpottavat yleiskuvan muodostamista sekä tulkintojen ja johtopäätösten tekemistä. (Ojasalon ym. 2009, 126-127.)

Tässä opinnäytetyössä koodaamista ja teemakortistoja sovellettiin riskienhallinnan teoreettisesta kehyksestä johdettujen asiasanojen ja taulukkomuotoon laaditun analyysirungon keinoin. Empiirisestä aineistosta etsittiin riskienhallinnan toteuttamista käsittelevää sisältöä asiasanojen avulla. Adobe Acrobat Reader –ohjelman etsi-toiminnolla selvitettiin esiintyykö kussakin dokumentissa sana riski, turvallisuus, jatkuvuus, häiriöttömyys, uhka tai vaara sellaisessa yhteydessä, mikä liittyy riskienhallinnan järjestämiseen kyseisessä organisaatiossa. Hakusanoina olivat riski, turvallis, jatkuvuu, häiriöttöm, uh tai vaar. Jotkut dokumentit olivat skannattuja .pdf-muotoon, jolloin etsi-toimintoa ei voitu käyttää. Nämä dokumentit luettiin läpi tarkasteltavan sisällön löytämiseksi.

Analyysirunko toimi teemakortistona. Analyysirunko laadittiin taulukkomuotoon, jossa pääkategoriat ja niiden alla kuvatut yksityiskohtaisemmat riskienhallinnan sisältötekijät muodostivat vaakarivit (liite 4). Taulukon toiseen sarakkeeseen kirjattiin yksityiskohtaiset sanalliset kuvaukset tarkastellun asian ilmenemisestä dokumenteissa ja kolmanteen sarakkeeseen kyseisen dokumentin yksilöivä koodi. Neljänteen sarakkeeseen kirjattiin tieto siitä, koskeeko havaittu asia koko organisaatiota, jotakin sen vastuualueista tai vastuualueen yksiköstä vai organisaation sidosryhmää. Tämän katsottiin olevan tärkeää siksi, että tieto mahdollistaa useasta organisaatiota ohjaavasta tahosta juontavat mahdolliset ristiriidat. Viidenteen sarakkeeseen kirjattiin pääkategoriakohtainen yhteenveto. Sekä nykytilaa että odotuksia kuvaavien dokumenttien analysointiin käytettiin samaa analyysirunkoa.

Analyysi toteutettiin asiasanojen etsimisen yhteydessä myös sisällön erittelynä (Ojasalo ym. 2009, 122; Tuomi & Sarajärvi 2009, 106-107), jolloin dokumenteista laskettiin tarkastelun kohteena olevissa yhteyksissä esiintyvien asiasanojen määrä ja kirjattiin tämä tieto erilliseen kaiken empiirisen aineiston luetteloivaan taulukoon. Taulukon riveille kirjattiin dokumentit ja asiasanakohtaisiin sarakkeisiin kunkin asiasanan absoluuttinen lukumäärä sekä se, kuinka monessa eri yhteydessä nämä kussakin dokumentissa esiintyivät. Taulukon viimeiseen sarakkeeseen kirjattiin myös yhteenveto tarkastelun kohteena olevan ilmiön esiintymisestä dokumentissa. Tämän katsottiin tarvittaessa mahdollistavan analyysirunkoa helpommin päätelmien tekemisen siitä, minkä tyyppisissä, kenen laatimissa ja mihin ajankohtaan sijoittuvissa dokumenteissa tarkasteltavaa ilmiötä on käsitelty.

Poikkeuksen asiasanojen käyttöön muodostivat sisäisen valvonnan arviointi- ja vahvistuslausumat ja niiden laatimiseksi kerätty kyselyaineisto. Vahvistuslausumat ovat noin kahden sivun mittaisia ja sisältävät taulukon ja kaavion lisäksi organisaation johdon sanallisen arvion sisäisen valvonnan ja riskienhallinnan nykytilasta. Vahvistuslausumat luettiin kokonaisuudessaan. Vahvistuslausumissa ja kyselyaineistossa esiintyvien asiasanojen lukumäärää ei laskettu, sillä tämä aineisto käsitteli yksinomaan riskienhallintaa, eikä sisällön erittelyn nähty tuovan lisäarvoa analyysille.

Kyselyaineisto oli puolestaan valmiiksi kategorisoitu valtiovarain controller –toiminnon antaman suosituksen suppean arviointikehikon (Valtiovarain controller -toiminto ja sisäisen tarkastuksen jaosto 2009) mukaisesti. Kyselyn arviointikohdat vastaavat sisällöltään laajaa arviointikehikkoa ja siten yleisesti käytettyä kokonaisvaltaisen riskienhallinnan COSO-ERM -mallia (Valtiovarain controller –toiminto 2005, 19). Kyselyaineiston vastauksista oli suoraan löydettävissä kuhunkin pääkategoriaan ja yksittäisiin sisältötekijöihin liittyvät kohdeorganisaation johdon arviot tarkasteltavan asian tilasta.

Havainnoista tulee pyrkiä laatimaan keskeiset tulokset kokoavia synteesejä, joiden pohjalta johtopäätökset lopulta laaditaan (Ojasalon ym. 2009, 129). Muodostetusta riskienhallinnan teoriapohjasta johdettuihin pääkategorioihin ja niihin liittyviin sisältötekijöihin perustuvan analyysirungon katsottiin paitsi kokoavan havainnot, myös mahdollistavan riskienhallinnan teorian ja empirian välisen suhteen esittämisen tutkimustuloksina ja edelleen johtopäätöksinä. Tutkimuksen johtopäätöksiä tehtäessä kutakin pääkategoriaa tai sen sisältötekijää tarkasteltiin suhteessa yleiseen riskienhallinnan teoriaan ja riskienhallintaan liittyviin valtionhallinnon erityispiirteisiin sekä kohdeorganisaatiolle kohdistettuihin odotuksiin ja velvoitteisiin.

6 Tulokset

Tuloksina esitellään seuraavassa ensin kohdeorganisaation riskienhallinnan nykytilaan liittyvät tulokset, joina todetaan riskienhallinnan ilmenemismuodot kohdeorganisaation toiminnassa analysoitujen asiakirjojen valossa. Tämän jälkeen esitellään kohdeorganisaation riskienhallinnalle kohdistettuihin odotuksiin liittyvät tulokset. Nykytilaan ja odotuksiin liittyviä tuloksia verrataan toisiinsa johtopäätösten yhteydessä.

6.1 Riskienhallinnan nykytila

Kohdeorganisaation riskienhallinnan nykytilaan liittyvät tutkimustulokset esitetään seuraavassa omina lukuinaan analyysirungon pääkategorioiden mukaisessa järjestyksessä. Luvut käsittelevät riskienhallinnan määrittelyä, riskienhallintamenettelyjä, riskien ja riskienhallinnan seuraamista, arviointia ja raportointia sekä riskienhallinnan vastuita ja organisointia.

6.1.1 Riskienhallinnan määrittely kohdeorganisaatiossa

Kohdeorganisaatiolle ei ole laadittu riskienhallintapolitiikkaa (asiakirja V.2.1). Aluehallintovirastoille yhteiseksi tulostavoitteeksi asetettu aluehallintovirastojen yhtenäisen riskienhallintapolitiikkamallin laadinta on toteutumatta (asiakirja A.2.1.) Organisaatio on todennut näkemyksenään, että riskienhallinnan kehittäminen ja riskienhallintapolitiikan laatiminen valtakunnallisena yhteistyönä on järkevää päällekkäisen työn välttämiseksi (asiakirja V.1.1).

Riskienhallintapolitiikan puuttumisesta huolimatta joitakin riskienhallinnan määrittelyyn liittyviä yksittäisiä sisältötekijöitä on käsitelty muissa asiakirjoissa. Sisäisen valvonnan tarkoitus on määritelty sisäisen valvonnan ja riskienhallinnan vahvistuslauman yhteydessä (asiakirja A.2.3). Riskienhallinnan tarkoitusta ja riskienhallintaprosessia on määritelty kohdeorganisaation päätoimipaikan pelastussuunnitelmassa (asiakirja A.4.2). Samassa dokumentissa on todettu lisäksi organisaation johdon määrittelevän suojelutoiminnan tavoitteet ja turvallisuuspäällikön määrittelevän osaltaan suojelutoiminnan painopistealueet. Lisäksi on määritelty työsuo-

jelun keskeiset vaikuttamisen kohteet valtiosektorilla sekä korostettu henkilöturvallisuuden varmistamisen tärkeyttä (asiakirja A.4.5).

Lisäksi tietoturvallisuuden kokonaisuus on määritelty aluehallintovirastojen yhteisessä tietoturvapolitiikassa. Tietoturvapolitiikassa on määritelty tietoturvatyön tavoitteet ja tietoturvaperiaatteet sekä tietoturvallisuuden merkitys organisaatiolle, tietoturvatoimintaa ohjaavat tekijät ja tietoturvallisuuteen kohdistuvat keskeiset uhkat. Lisäksi on määritelty tietoturvallisuuden toteutumista tukevia käytäntöjä sekä kuvattu tietoturvallisuuden hallintajärjestelmä ja tietoturvavastuut ohjaavien tahojen sekä organisaation ja sen yhteistyökumppanien osalta. Edelleen on avattu tietoturvakoulutusta ja –ohjeita, tietoturvallisuudesta tiedottamista ja tietoturvallisuuden toteutumisen valvontaa sekä käytettäviä käsitteitä. Tietoturvallisuustyön tavoite on muun muassa turvata riittävällä ja tarkoituksenmukaisella tasolla viraston toiminnalle tärkeiden suojattavien kohteiden toiminta ja varmistaa, että viraston sekä yhteistyökumppaneiden henkilöstö voivan suorittaa tehtävänsä niin normaali- kuin poikkeusoloissakin. (asiakirja A.4.7.)

Muillakin turvallisuuden osa-alueilla tehtävien toimenpiteiden tarkoitusta on määritelty. Kohdeorganisaation valmiussuunnitelman tarkoituksena on kuvata, miten aluehallintovirasto toteuttaa sille kuuluvia tehtäviä yhteiskunnan häiriötilanteissa ja poikkeusoloissa. Suunnitelma kuvaa organisaation toiminnan kohdistamista, mutta siinä on lisäksi käsitelty toimintaedellytysten turvaamista. (asiakirja A.4.6.) Pelastussuunnitelman tavoite on viraston turvallisuutta vaarantavien riskitekijöiden kartoittaminen, henkilöturvallisuuden parantaminen sekä onnettomuus- ja vahinkotilanteiden ennaltaehkäisy (asiakirja A.4.2). Asiakirjojen suojelusuunnitelman tarkoituksena on varmistaa kohdeorganisaation toiminnan jatkumisen kannalta välttämättömien sekä tutkimuksellisista, oikeudellisista tai taloudellisista syistä suojeltavien paperimuodossa olevien asiakirjojen ja tietojen säilyminen ja käytettävyys normaaliolojen häiriötilanteissa ja poikkeusoloissa (asiakirja A.4.1).

Kohdeorganisaation työsuojelun toimintaohjelma tavoittelee turvallisuuden ja terveellisyyden edistämistä ja työntekijöiden työkyvyn ylläpitämistä. Tarkoituksena on parantaa työympäristöä ja työoloja työntekijöiden työkyvyn turvaamiseksi ja ylläpitämiseksi. Huomion kohteena ovat työtapaturmien, ammattitautien ja muiden työstä ja työympäristöstä johtuvien fyysisten ja henkisten terveyden haittojen ehkäisy ja torjuminen. (asiakirja A.4.5.) Työhyvinvointisuunnitelmalla tuetaan henkilöstön työhyvinvointia ja varmistetaan viraston perustehtävien ja asiakaspalvelujen sujuminen laadukkaasti. Tavoitteena on työhyvinvoinnin takaaminen muutostilanteissa ja laadukkaiden palveluiden tuottamisen turvaaminen resurssien pienentyessä. (asiakirja A.4.3.)

Riskienhallinnan määrittelyn sisältötekijöitä voidaan katsoa ilmentävän myös se, että riskienhallintaan ja turvallisuuden osa-alueisiin liittyviä yksittäisiä vastuita sekä seurannan, arvioinnin ja raportoinnin menettelyitä samoin kuin riskienhallintamenettelyitä on määritelty useissa analysoiduissa dokumenteissa (asiakirjat A.2.3; A.3.2; A.4.1; A.4.2; A.4.5; A.4.6; A.4.7). Edelleen yksittäisiin riskienhallinnan määrittelyn sisältötekijöihin liittyen dokumentit osoittavat puutteina sen, ettei organisaation johdon arvion mukaan riskien hallintamenettelyjä tai niiden periaatteita eikä riskinottohalukkuutta riskinottokyvyn puitteissa ole määritelty (liite 5).

Määrittelyyn läheisesti liittyviksi asioiksi voidaan lisäksi katsoa organisaation johdon riskienhallintaan ja turvallisuuteen liittyvät lausumat. Kohdeorganisaatio on strategiassaan todennut pitävänsä huolta henkilöstön työhyvinvoinnista sekä pitävänsä työympäristön terveellisenä ja turvallisena sekä toimivansa tietoturvallisuuden periaatteiden ja tavoitteiden mukaisesti (asiakirja A.1.1). Organisaation lausuman mukaan henkilöturvallisuus on varmistettava niin virkapaikalla kuin virkamatkoilla (asiakirja A.4.5). Organisaation johto toteaa riskienhallinnan nousseen vuonna 2012 keskusteluun, ja että työtä on aloitettu tietoturvallisuuden, työturvallisuuden ja toimitilaturvallisuuden puitteissa (asiakirja V.2.2).

6.1.2 Riskienhallintamenettelyt

Riskienhallintamenettelyillä tarkoitetaan tässä riskien tunnistamista ja arviointia sekä riskien hallitsemiseksi tehtäviä toimenpiteitä. Riskienhallintamenettelyihin katsottiin kuuluvaksi myös sellaiset organisaation toimenpiteet, joilla huolehditaan turvallisuuden eri osa-alueista sekä toiminnan jatkuvuuden varmistamisesta. Kohdeorganisaatiossa riskien tunnistamista, arvioimista ja hallitsemista toteutetaan lähinnä yksittäisillä turvallisuuden osa-alueilla. Toimintaa ja tavoitteita uhkaavien ja toiminnan laillisuuteen, tuloksellisuuteen ja raportointiin liittyviin riskien osalta organisaation johto on arvioinut menettelyt riskien tunnistamista lukuun ottamatta hyvin heikoiksi (liite 5).

Organisaation päätoimipaikan pelastussuunnitelma perustuu turvallisuutta vaarantavien riskien kartoittamiseen ja uhkakuvista johdettujen riskien arviointiin. Suunnitelmassa on todettu keskeiset riskit ja suojattavat kohteet sekä riskien tunnistamisen ja arvioinnin periaatteet. Onnettomuus- ja vahinkoriskien kartoittaminen toteutetaan ryhmätyönä, johon on osallistuttava henkilöitä eri työntekijäportaista sekä työnjohdon ja työnantajan edustajista. Keskeisimmiksi aihealueiksi on todettu työturvallisuus, palo- ja henkilöturvallisuus, toimitila- ja tietoturvallisuus sekä ympäristönsuojelu. Riskikartoituksessa huomioidaan omasta toiminnasta aiheutuvien riskitekijöiden lisäksi viraston ulkoiset riskitekijät. Tunnistettujen riskien arviointi tehdään toteutumisen todennäköisyyden ja arvioitujen seurausten tulona. Seurausten tekijöinä huomioidaan eri tarkastelunäkökulmia. (asiakirja A.4.2.)

Asiakirjojen suojelusuunnitelmassa on todettu normaaliolojen häiriötilanteiden ja poikkeusolojen vaikutus ja tilanteet, joissa asiakirjojen suojelutarve korostuu. Tilanteiden todennäköisyyksiä tai vaikutuksia tai menettelyjä näiden arvioimiseksi ei ole esitetty, mutta on todettu, että useimmissa tapauksissa häiriötilanteiden luonteella ei ole vaikutusta asiakirjojen suojeluun. (asiakirja A.4.1.) Aluehallintovirastojen tietoturvapolitiikassa kuvattu tietoturvallisuuden hallintajärjestelmä sisältää tietoturvallisuuteen liittyvän kokonaisuuden kaikki elementit. Politiikassa todettuja riskien tunnistamisen ja arvioinnin menettelyjä tai menettelyjä riskien hallitsemiseksi ei ole kuvattu. Tietoturvallisuuden hallintajärjestelmä kuitenkin sisältää dokumentteja koskien muun muassa riskien arviointia sekä tietoturvakäytäntöjä ja -periaatteita sekä kokonaisuuteen liittyvää ohjeistusta ja koulutusta. (asiakirja A.4.7.)

Työsuojelun toimintaohjelmassa on käsitelty kohdeorganisaatiossa tehtävät toimenpiteet työn ja työympäristön vaarojen ja haittojen selvittämiseksi ja arvioimiseksi. Työ on todettu tehtävän ryhmätyönä, mutta sen yhteydessä käytettäviä menettelyitä ei ole esitetty. On kuitenkin todettu, että henkilöturvallisuus on varmistettava niin virkapaikalla kuin virkamatkoilla, ja että erityisesti tarkastusmatkojen ja – käyntien turvallisuuteen kiinnitetään huomiota. (asiakirja A.4.5.) Tunnistettuja riskejä ei ole todettu, mutta analyysiä tehtäessä ei ollut käytettävissä viimeisintä työsuojelun toimintaohjelmaa. Riskien kartoittamiseksi ja hallitsemiseksi voitaisiin katsoa myös työhyvinvoinnin nykytilan kartoittamiseksi tehdyt säännölliset mittaukset (asiakirja A.4.3).

Kohdeorganisaation johdon arvion mukaan virastossa on kohtuullisesti käytössä menettelyt, joilla tunnistetaan toimintaa ja tavoitteita uhkaavia sekä toiminnan laillisuuteen, tuloksellisuuteen ja raportointiin liittyviä riskejä. Arvion mukaan riskienhallintamenettelyt on organisaatiossa kohtuullisesti kytketty osaksi suunnittelu- ja ohjausprosesseja, mutta dokumentit eivät paljasta mitä nämä menettelyt ovat. Arvion mukaan tunnistettuja riskejä kuitenkin dokumentoidaan heikosti, eikä tunnistettuja riskejä arvioida. Riskejä ei luokitella niiden luonteen mukaisesti eikä priorisoida merkityksen mukaisesti. (liite 5.) Sisäisen valvonnan ja riskienhallinnan vahvistuslausuman antamiseksi toteutetun kyselyn vastauksista ei tule selväksi kattaako niissä tarkoitettu riskien tunnistaminen myös esimerkiksi eri turvallisuuden osa-alueisiin liittyvät riskit. Riskien tunnistamiseen liittyy myös se, ettei kohdeorganisaatiossa ole havaittu varoihin kohdistuneita väärinkäytöksiä (asiakirjat V.1.1; V.1.2; V.1.3).

Tunnistettuihin riskeihin kohdistettuja hallintamenettelyitä tai niiden periaatteita on asiakirjoissa kuvattu hyvin vähän. Pelastussuunnitelmassa on todettu, että toiminnan kannalta sietämättömät riskitekijät on pyrittävä aina poistamaan tai pienentämään ennen toiminnan jatkamista tai aloittamista, minkä lisäksi on todettu toimenpiteitä riskien toteutuessa sekä asiakokonaisuuteen liittyvä henkilöstön kouluttaminen. (asiakirja A.4.2.) Työsuojelun toimintaohjelman kehittämistoimenpiteet liittyvät työturvallisuutta koskevien riskien hallitsemiseen

esimerkiksi sisäisten turvallisuusohjeiden muodossa (asiakirja A.4.5). Valmiussuunnitelmassa on kuvattu toimenpiteet viraston toimintaedellytysten turvaamiseksi (asiakirja A.4.6). Tunnistettujen riskien hallintaan voidaan katsoa kuuluvaksi myös työhyvinvoinnin kehittämistoimenpiteet (asiakirja A.4.3).

Asiakirjojen suojelusuunnitelman mukaan kaikki organisaation toiminnan kannalta kriittiset tietojärjestelmien sisältämät asiakirjat ja tiedot varmuus- ja suojakopioidaan, minkä lisäksi on todettu menettelyt tilanteessa, jossa erityisiin suojelutoimenpiteisiin joudutaan ryhtymään (asiakirja A.4.1). Tietoturvapolitiikassa ei ole kuvattu tunnistettujen riskien hallitsemisen menettelyjä. Politiikka itsessään tähtää tietoturvariskien hallitsemiseen, ja menettelyjä on politiikan mukaan käsitelty muissa tietoturvallisuuden hallintajärjestelmän dokumenteissa (asiakirja A.4.7). Riskin hallitsemiseen voidaan lukea myös se, että organisaation sisäisellä viestinnällä pyritään varmistamaan, että häiriötilanteessa kaikilla on tiedossaan työn tekemisen kannalta oleellinen ja yhdenmukainen tieto tilanteesta ja sen vaikutuksista tehtäviin (asiakirja A.4.6). Yksittäisillä turvallisuuden osa-alueille toteutettavien toimenpiteiden yhteydessä ei ole viittauksia riskikustannusten optimointiin.

Organisaation johdon arvion mukaan toimintaa ja tavoitteita uhkaaviin sekä toiminnan laillisuuteen, tuloksellisuuteen ja raportointiin liittyville tunnistetuille riskeille ei määritellä hallintamenettelyjä, eikä hallintamenettelyjen tuotos-panos –suhdetta siten arvioida. Hallintamenettelyiden periaatteita ei myöskään ole linjattu. (liite 5.) Dokumentit eivät myöskään osoita kohdeorganisaation vastuualueilla toteutettavan riskienhallintamenettelyitä eivätkä sisäisen valvonnan menettelyjä. Erään vastuualueen osalta on kuitenkin todettu vastuualueen toimitusaikatavoitteiden ylitysten osoittavan resurssien haavoittuvuutta tietyllä osa-alueella, ja että ongelmaan on reagoitu toiminnan häiriöttömyyden varmistamiseksi (asiakirja A.2.3).

6.1.3 Riskien ja riskienhallinnan seuraaminen, arviointi ja raportointi

Kohdeorganisaatiossa toteutetaan riskeihin ja riskienhallintaan liittyvää seurantaa, arviointia ja raportointia sekä yksittäisten turvallisuuden osa-alueiden yhteydessä että jossain määrin toimintaa ja tavoitteita uhkaavien ja toiminnan laillisuuteen, tuloksellisuuteen ja raportointiin liittyviin riskien osalta. Organisaation johto on itse arvioinut sisäisen valvonnan ja riskienhallinnan järjestämiseen liittyvistä osa-alueista seurannan sekä tiedonkulun ja informaation käytettävyyden toteutuvan hyvin (liite 5). Jatkuvan seurannan osalta organisaation johto on todennut saavansa säännölliset tiedot poikkeamaseuranasta, ja että yksiköissä hyödynnetään poikkeamaseurannan tietoja. (liite 5.)

Organisaation tietoturvallisuuteen liittyvä seuraaminen ja raportointi muodostuu päivittäisvalvonnasta, edistymisen seurannasta ja raportoinnista, auditointi- ja tarkastustoiminnasta

sekä johdon katselmuksesta. Viraston yleishallinnollisesta ohjauksesta vastaava ministeriö valvoo tietoturvatoimintaa. Aluehallintovirastojen ja ELY-keskusten yhteinen tietoturvaryhmä koordinoi tietoturvallisuuden kehittämissuunnitelman toteutumaseurannan ja raportoinnin. Viraston tietoturvaryhmä ja tietoturvallisuuden vastuuhenkilö vastaavat tietoturvallisuuden seurannasta. Tietoturvallisuuden valvonnan toimenpiteet on määritelty, samoin on todettu kohdeorganisaatiolla olevan sidosryhmiensä kanssa sopimukset valvontatehtävistä. (asiakirja A.4.7.)

Organisaation lausuman mukaan työantajan tulee tarkkailla työturvallisuuteen liittyviä asioita ja toteutettujen toimenpiteiden vaikutusta työn turvallisuuteen ja terveellisyyteen (asiakirja A.4.5). Organisaatiossa myös seurataan työtapaturmien määrää ja tehdään työtyytyväisyyskyselyjä (asiakirjat A.4.5; A.4.3). Työsuojelu- ja työhyvinvointitoimikunta puolestaan koordinoi yhdessä työterveyshenkilöstön, linjajohdon, henkilöstöhallinnon ja kuntoutusyhdyshenkilöiden kanssa työkykyä ylläpitävän toiminnan seurantaa (asiakirja A.4.5).

Kohdeorganisaatiossa johdon ja vastuualueiden esimiesten tulee seurata työhyvinvoinnin kehittämistoimenpiteiden edistymistä (asiakirja A.4.3). Tämä liittyy riskienhallinnan tarkoitukseen oleellisesti siksi, että työhyvinvointi on kohdeorganisaatiossa mielletty keskeiseksi myös tuloksellisuuden kannalta: kohdeorganisaation tavoitteena on työhyvinvoinnin takaaminen organisaation muutostilanteissa ja laadukkaiden palveluiden tuottamisen turvaaminen yhä niukentuvilla resursseilla (asiakirja A.4.3). Riskienhallintaan liittyväksi seurannaksi voidaan katsoa myös se, että työsuojelun toimintaohjelma ja pelastussuunnitelman sisältämä riskikartoitus päivitetään vuosittain, ja että pelastussuunnitelman mukaista turvallisuuskoulutusta seurataan (asiakirjat A.4.5; A.4.2).

Kohdeorganisaatiossa sisäisen valvonnan ja riskienhallinnan tilaa arvioidaan vuosittain tätä koskevan vahvistuslausuman antamiseksi (asiakirjat V.1.1; V.1.2; V.1.3). Turvallisuuspäällikkö puolestaan arvioi suojelutoiminnan tuloksellisuutta ja raportoi toiminnastaan johdolle (asiakirja A.4.2). Lisäksi kohdeorganisaatiossa on tehty tietoturvallisuuden tasoa kartoittava auditointi, jonka tuloksena aluehallintoviraston hallinnollinen tietoturvallisuus täyttää Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän antaman ohjeen mukaisen tietoturvallisuuden perustason vaatimukset (asiakirja A.2.1). Tietoturvallisuuden arviointia toteutetaan lisäksi määrävälein tehtävin riskianalyysein, tietoturvallisuuden itsearvioinnilla sekä tietoturvallisuutta käsittelevien sopimusten arvioinnilla ja palvelujen auditoinnilla (asiakirja A.4.7).

Organisaation johdon mukaan olennaisiksi koetuista riskeistä raportoidaan viraston johdolle kohtuullisesti tai melko hyvin. Riskeillä viitataan toimintaa ja tavoitteita uhkaaviin sekä toiminnan laillisuuteen, tuloksellisuuteen ja raportointiin liittyviin riskeihin. (liite 5.) Asiakirjat eivät paljasta millaisin menettelyin raportointi tapahtuu, ja ovatko riskit myös jatkuvan seu-

rannan kohteena. Viraston tietoturvallisuudesta vastaava raportoi viraston johdolle sekä tietohallinnolle (asiakirja A.4.7).

Riskienhallinnan ulkoinen raportointi toteutuu organisaation tuloksellisuusraportteihin liitettyjen vahvistuslausumien avulla, mutta raportointi ei käsitä keskeisiä riskejä (asiakirjat A.2.1; A.2.2; A.2.3). Organisaation johdon arvion mukaan virastolla on järjestelmälliset tavat raportoida ja tiedottaa toiminnastaan ja riskeistään ohjaaville tahoille (asiakirja V.2.1). Dokumenteista ei tule ilmi ulkoisten arviontien menettelyjä. Organisaation johdon mukaan ulkoisten arviointien tuloksia kuitenkin käsitellään organisaatiossa säännöllisesti (asiakirja V.2.1).

6.1.4 Riskienhallinnan kehittäminen

Kohdeorganisaation johdon arvion mukaan kaikilla sisäisen valvonnan osa-alueilla on tapahtunut kehitystä ja tilanne on hyvä, mutta riskienhallinnan olevan olennaisimpia kehittämisalueita (asiakirja V.1.1). Johdon arvion mukaan sisäisen valvonnan ja siihen kuuluvan riskienhallinnan menettelyt kuitenkin täyttävät valtion talousarviosta annetun asetuksen 69 §:ssä säädetyt vaatimukset, ja että menettelyillä on kyetty kohtuullisesti varmistamaan aluehallintoviraston toiminnan laillisuus, tuloksellisuus ja omaisuuden turvaaminen sekä raportoinnin oikeellisuus ja riittävyys johtamisen ja ulkoisen ohjauksen tarpeet huomioon ottaen. (asiakirjat V.1.1; V.1.2; V.1.3.)

Tarve riskienhallinnan kehittämiselle on kohdeorganisaatiossa todettu koko sen toiminnan ajan (asiakirjat V.1.2; V.1.3; V.1.4), ja organisaatio on itse todennut välttämättömäksi, että aluehallintovirastoille määriteltäisiin riskienhallinnan menettelyt (asiakirja V.1.4). Aluehallintovirastojen riskienhallintaan liittyvä kehittäminen on asetettu valtakunnalliseksi tavoitteeksi siten, että aluehallintovirastojen yhteiset toiminnan kehittämisyksikkö ja sisäisen tarkastuksen yksikkö kehittävät menettelyitä yhdessä aluehallintovirastojen kanssa (asiakirja B.1.3; B.1.4). Tulostavoitteeksi asetettu aluehallintovirastojen riskienhallinnan menettelyiden kehittäminen on toteutumatta (asiakirja A.2.1). Organisaatio on todennut näkemyksenään, että riskienhallinnan kehittäminen valtakunnallisena yhteistyönä on järkevää päällekkäisen työn välttämiseksi (asiakirja V.1.1).

Kehittämisen menettelyitä on määritelty erityisesti tietoturvallisuuden osalta. Tietoturvallisuuden hallintajärjestelmä sisältää kehittämissuunnitelman sekä todettuina menettelyinä jatkuvan parantamisen ja korjaavat toimet sekä kokemusten, palautteiden ja mittaustiedon keruun (asiakirja A.4.7). Riskienhallintaan liittyväksi voidaan katsoa myös kohdeorganisaation työsuojelun toimintaohjelmaan kirjatut kehittämistoimenpiteet, jotka liittyvät laajasti työsuojelun sisältöön. Toimenpiteille on osoitettu aikataulu, toteutuksen vastuu sekä seuranta. (asiakirja A.4.5.) Tulevat työsuojeluun liittyvät kehittämiskohteet on todettu toteutettavan

riskienhallintaan pohjautuen. Kohdeorganisaation valmiussuunnitelmaa kehitetään valmiusharjoitusten osoittamien kehittämistarpeiden avulla (asiakirja A.4.6).

6.1.5 Vastuut ja organisointi

Kohdeorganisaatiossa on osoitettu riskienhallintaan liittyviä vastuita ja nimetty tähän liittyvää organisointia sekä yleisesti että yksittäisillä turvallisuuden osa-alueille. Sisäisen valvonnan ja riskienhallinnan järjestämiseen liittyvä vastuu on osoitettu viraston johdon edustajille. Aluehallintoviraston sisäisen valvonnan ja riskienhallinnan järjestämistä johtavat ja sen asianmukaisuudesta ja riittävyydestä vastaavat ylijohtaja ja osaltaan vastuualueiden ja hallintopalvelujen vastuuyksikön johtajat (asiakirja V.1.3).

Turvallisuuden osa-alueisiin liittyviä vastuita ja organisointia on osoitettu pelastussuunnitelmassa, tietoturvallisuuspolitiikassa, työsuojelun toimintaohjelmassa, asiakirjojen suojelusuunnitelmassa ja valmiussuunnitelmassa (asiakirjat A.4.2; A.4.7; A.4.5; A.4.1; A.4.6). Vastuut ja nimetyt tehtävät koskevat asiasta riippuen joko viraston johtoa, sen vastuualueita tai yksiköitä, yksittäisiä henkilöitä, perustettuja työ- tai muita ryhmiä tai koko henkilöstöä. Pääosa vastuista on osoitettu henkilön nimen tarkkuudella.

Kohdeorganisaation johto vastaa viime kädessä koko organisaation toiminnasta, mutta yksittäisiä vastuita on osoitettu lukuisia myös sisäisen valvonnan ja riskienhallinnan järjestämisen lisäksi. Aluehallintoviraston johdon tulee omalta osaltaan mahdollistaa pelastussuunnitelman mukainen turvallisuustoiminta (asiakirja A.4.2). Vastuu työsuojelusta on työantajalla (A.4.5). Aluehallintoviraston ylijohtaja vastaa, organisoi ja resursoi tietoturvapolitiikan ja sen mukaisen hallintajärjestelmän toimeenpanoa. Viraston johto vastaa siitä, että tietoturvanäkökohdat otetaan huomioon kaikessa toiminnassa sekä osoittaa riittävät resurssit tietoturvallisuuden toteuttamiselle (asiakirja A.4.7).

Riskienhallinnan keskeiseen tarkoitukseen liittyen aluehallintoviraston ylijohtaja vastaa viraston toiminnan tuloksellisuudesta ja viraston yhteisten tulotavoitteiden saavuttamisesta. Vastuualueen johtaja vastaa vastuualueen toiminnan tuloksellisuudesta ja tulostavoitteiden saavuttamisesta. Vastuualueiden johtajien on myös tiedotettava ylijohtajalle tärkeistä vastuualueen hallintoa, henkilöstöä ja substanssia koskevista asioista ja päätöksistä. (asiakirja A.3.1.) Vastuualueiden johdolla on myös vastuu tietoturvallisuudesta (asiakirja A.4.7). Hallintopalvelujen vastuuyksiölle on osoitettu vastuu viraston toimintaedellytysten turvaamisesta ja aluehallintoviraston vastuualueiden toiminnan tukemisesta häiriötilanteissa erilaisin suunnitelmin (asiakirja A.4.6).

Yksittäisille henkilöille osoitetut vastuut liittyvät erityisesti pelastussuunnitelman tarkoittamaan riskienhallintaan, työturvallisuuteen, tietoturvallisuuteen ja valmiussuunnitteluun. Erikseen on nimetty turvallisuuspäällikkö varahenkilöineen, turvallisuusvalvojat, laitteistojen ja väestönsuojien hoitajat (asiakirja A.4.2), työsuojelupäällikkö ja –valtuutetut varahenkilöineen (asiakirja A.4.5), tietoturvallisuuden vastuuhenkilö, sisäisen riskienhallinnan koordinoinnin vastuuhenkilö, sisäisen valvonnan yhteyshenkilö, taloturvallisuuden vastuita usealle henkilölle (asiakirja A.3.2), valmiussuunnittelun vastuuhenkilö (asiakirja A.3.3) sekä asiakirjojen suojeluun liittyviä vastuita nimetyille henkilöille (asiakirja A.4.1). Pelastussuunnitelman mukaan riskienhallintaa vetää turvallisuuspäällikkö (asiakirja A.4.2).

Erikseen on nimetty riskienhallintaan ja yksittäisiin turvallisuuden osa-alueisiin liittyviä työryhmiä. Turvallisuuspäällikön apuna riskienhallinnassa on työryhmä (asiakirja A.4.2). Lisäksi on nimetty tietoturvaryhmä (asiakirjat A.4.7; A.3.2) sekä työn ja työympäristön vaaroja ja haittoja selvittävä arviointiryhmä (asiakirja A.4.5). Aluehallintovirastoilla on myös ELY-keskusten kanssa yhteinen tietoturvaryhmä, jonka vastuulla ovat voimakkaasti tietoturvallisuuteen liittyvät kehittämistoimenpiteet (asiakirja A.4.7). Ryhmiksi voitaisiin katsoa myös työsuojelutoimikunta ja työsuojeluorganisaatio (asiakirja A.4.5) sekä turvallisuusorganisaatio ja pelastussuunnitelman tarkoittamat yleisryhmät (asiakirja A.4.2) ja viraston kriisijohtamisen johtoryhmä (asiakirja A.4.6).

Jokaiselle henkilökuntaan kuuluvalle on osoitettu vastuita asiakirjojen suojeluun, työhyvinvoinnista huolehtimiseen, tietoturvallisuuteen sekä pelastussuunnitelman mukaiseen turvallisuudesta huolehtimiseen liittyen. Henkilöstön tulee muun muassa perehtyä annettuihin turvallisuusohjeisiin ja toimia niiden mukaan sekä tarvittaessa ehkäistä vahingon syntyminen tai rajoittaa vahingon laajuutta (asiakirja A.4.2). Henkilö on tehtävästä riippumatta omalta osaltaan vastuussa tietoturvallisuudesta ja siihen liittyvien toimintatapojen noudattamisesta (asiakirja A.4.7). Vastuut korostavat henkilöstön roolia turvallisuuskulttuurin muodostamisessa ja ylläpitämisessä.

6.2 Riskienhallintaan liittyvät odotukset

Aluehallintovirastoissa toteutettavan riskienhallinnan periaatteita ei ole määritelty yhteisen strategisen ohjauksen yhteydessä (asiakirjat B.1.1; B.1.2) eikä kohdeorganisaation osalta myöskään virastokohtaisen strategisen ohjauksen tai tulosohjauksen yhteydessä. Ohjausasiakirjoin ei myöskään ole esitetty odotuksia riskien ja riskienhallinnan seuraamisen tai raportointiin tai riskienhallinnan toteuttamisen organisointiin tai tähän liittyviin vastuisiin liittyen. Kohdeorganisaation strategisessa tulossopimuksessa kuitenkin korostetaan toiminnan tuloksellisuutta, henkisistä voimavaroista huolehtimista sen tekijänä ja asetettujen tavoitteiden saavuttamista eräänä mittarina (asiakirja B.1.4).

Kuten edellä on todettu, on aluehallintovirastojen riskienhallinnan määrittelemiselle ja kehittämiselle kohdistettu strategisen tulossopimuksen yhteydessä odotuksia. Aluehallintovirastojen odotetaan laativan virastojen yhtenäisen riskienhallintapolitiikkamallin sekä kehittävän aluehallintovirastojen riskienhallinnan menettelyitä (asiakirja B.1.3). Vastuu toimenpiteistä on aluehallintovirastojen yhteisellä toiminnan kehittämisyksiköllä yhteistyössä yhteisen sisäisen tarkastuksen yksikön ja aluehallintovirastojen kanssa. Tavoitteen mukaan aluehallintovirastot arvioivat vuodesta 2012 alkaen tulosohjausprosessiin kytkeytyen strategisten tavoitteiden toteutumiseen liittyvät riskit ja niiden merkittävyyden sekä määrittelevän olennaisimpien riskien hallintamenettelyt. Tavoitteen toteutuminen on viivästynyt ja sitä on siirretty vuodelle 2013 (asiakirja B.1.4), mutta se on edelleen toteutumatta (asiakirja A.2.1).

Organisaation toiminnalliset tulossopimukset on pääsääntöisesti laadittu ohjaavan ministeriön tai keskusviraston ja kohdeorganisaation tai sen tietyn vastuualueen välisinä. Erään kohdeorganisaation vastuualueen tulossopimuksessa asetetaan tavoitteeksi avainhenkilöriskien kartoituksen perustuva toiminnan jatkuvuudesta huolehtiminen (asiakirja B.2.4). Tulossopimus on aluehallintovirastojen toiminnan aloittamisvuodelta, eikä myöhemmissä sopimuksissa mainintaa enää ole. Lisäksi kyseisen vastuualueen tulossopimuksissa on mainintoja henkilöstön hyvinvoinnista huolehtimisesta osana henkisten voimavarojen hallintaa. (asiakirjat B.2.3; B.2.4).

Riskienhallintaan liittyviksi tavoitteiksi voidaan katsoa myös joitakin yksittäisiä kohdeorganisaatiolle tai sen vastuualueelle osoitettua tulostavoitteita. Eräs kohdeorganisaatiota ohjaavista keskusvirastoista on osoittanut eräälle vastuualueelle tavoitteeksi varautuminen kiireellisiin tehtäviin (asiakirjat B.2.11; B.2.12; B.2.13). Lisäksi yksi ohjaavista ministeriöistä on antanut kohdeorganisaatiolle tavoitteeksi valmiussuunnitelman laatimisen (asiakirjat B.2.14; B.2.15).

Eräs ohjaava keskusvirasto on asettanut kohdeorganisaatiolle tulostavoitteen, jonka mukaan aluehallintoviraston suoritteet ovat riittävän laadukkaita ja täyttävät ohjaavan viraston kanssa sovitut laatukriteerit (asiakirjat B.2.8; B.2.9). Tulossopimuksen mukaan kyseinen ohjaava virasto järjestää koulutusta aluehallintoviraston virkamiehille tavoitteena osaava henkilöstö. Sama keskusvirasto on todennut, että tehtävien priorisointia, prosessien ja toimintatapojen kehittämistä sekä tuottavuuden mittaamista parannetaan (asiakirja B.2.10). Sopimus on laadittu kohdeorganisaation kanssa, mutta se koskettaa ainoastaan yhtä viraston vastuualueista.

7 Johtopäätökset

Johtopäätöksinä tarkastellaan ensin kohdeorganisaation riskienhallinnan nykytilaa ja siinä ilmenneitä puutteita. Riskienhallinnan nykytilaa arvioidaan kolmesta näkökulmasta. Ensin arvioidaan tutkimustulosten mukaisessa järjestyksessä kohdeorganisaatiossa toteutettuja yk-

sittäisiä riskienhallintatoimenpiteitä ja toimenpiteiden kokonaisuutta suhteessa muodostettuun riskienhallinnan viitekehykseen. Tämän jälkeen tarkastellaan riskienhallinnan nykytilaa suhteessa sille kohdistettuihin odotuksiin ja säädösvelvoitteisiin. Kolmanneksi luodaan erikseen katsaus riskienhallinnan toteutumiseen kokonaisvaltaisen riskienhallinnan näkökulmasta.

Nykytilan tarkastelun jälkeen todetaan sellaiset tutkimusaineistosta nousseet kohdeorganisaation riskienhallinnan nykyiset rakenteet ja menettelytavat sekä muut kohdeorganisaation riskienhallinnalle kohdistuvat vaatimukset, jotka on huomioitava riskienhallinnan periaatteiden muodostamisen ja riskienhallinnan järjestämisen tueksi annettavassa ohjeessa. Johtopäätösten lopuksi tehdään yhteenveto kohdeorganisaation riskienhallinnan nykytilasta tutkimustulosten valossa.

7.1 Riskienhallinnan nykytila suhteessa riskienhallinnan viitekehykseen

Kohdeorganisaatiossa toteutettavan riskienhallinnan keskeinen puute on se, ettei organisaatiolla ole riskienhallinnan kokonaisuutta määrittelevää riskienhallintapolitiikkaa (asiakirja V.2.1). Riskienhallintaa järjestettäessä on sitä koskevien määrittelyjen ja periaatteiden muodostaminen työn ensimmäinen vaihe. Riskienhallinnan asemaa ja sisältöä organisaatiossa määriteltäessä tulee ottaa kantaa riskienhallinnan tarkoitukseen, tavoitteisiin, vastuisiin, keinoihin, seurantaan, raportointiin sekä terminologiaan. Menetelmänä määrittelyille toimii tavallisesti riskienhallintapolitiikka tai riskienhallinnan periaatteet. (Ilmonen ym. 2013, 54-57; Juvonen ym. 2005, 38.) Valtionhallinnon organisaatiossa riskienhallintapolitiikkaa voi erillisen politiikka-asiakirjan sijasta sisältyä esimerkiksi tulostavoiteasiakirjoihin ja toiminta- ja taloussuunnitelmiin (Valtiovarain controller –toiminto 2005, 22). Periaatteita voidaan kuvata myös esimerkiksi riskilajikohtaisesti (Ilmonen ym. 2013, 54-57).

Kohdeorganisaatiossa tarvittava määrittely on tehty tietoturvallisuuden osalta (asiakirja A.4.7). Tietoturvapolitiikka vastaa rakenteeltaan riskienhallinnan määrittelyltä odotettuja sisältötekijöitä. Myös sisäisen valvonnan tehtävä on määritelty valtiovarain controller- toiminnon (2005, 8) ja talousarvioasetuksen (1243/1992, 69 §) mukaisesti (asiakirja A.2.3). Joitakin riskienhallinnan määrittelyyn luettavia yksittäisiä tekijöitä on käsitelty muillakin kohdeorganisaation turvallisuuden osa-alueilla - määritelty on vastuita sekä seurannan, arvioinnin ja raportoinnin menettelyitä samoin kuin joitakin riskienhallintamenettelyitä.

Yksittäisistä toteutetuista määrityksistä ja toimenpiteistä voidaan tehdä yksittäisiä havaintoja. Riskienhallinnan tarkoitus on määritelty pelastussuunnitelmassa (asiakirja A.4.2), mutta suunnitelmassa kuvattu riskienhallinnan tarkoitus ”estää ja minimoida erilaisista onnettomuus- ja vahinkoriskeistä yritykselle aiheutuvat menetykset ja turvata siten aluehallintoviraston henkilöstö, asiakkaat ja toiminnan jatkuvuus” ei vastaa valtion virastojen sisäiselle val-

vonnalle ja riskienhallinnalle annettua suositusta (Valtiovarain controller –toiminto 2005, 11) eikä kokonaisvaltaisen riskienhallinnan tarkoituksen määritelmiä (Committee of Sponsoring Organizations of the Treadway Commission 2004, 1-2; ks. myös Ilmonen ym. 2013, 16, 43).

Pelastussuunnitelmassa kuvattu aluehallintoviraston riskienhallintaprosessi ”varsinainen riskien kartoittaminen, niiden hallintamenetelmien harkitseminen ja toteuttaminen sekä toimenpiteet onnettomuus- ja vahinkotilanteiden ennalta ehkäisemiseksi tai niiden seurausten rajoittamiseksi" (asiakirja A.4.2) ei vastaa yleisesti määriteltyä riskienhallintaprosessin kokonaisuutta (Ilmonen ym. 2013, 27; ks. myös Suominen 2003, 38; ks. myös Juvonen ym. 2005, 23-24).

Asiakirjat eivät pelastussuunnitelman käsittelemiä riskejä lukuun ottamatta paljasta konkreettisia menettelytapoja riskien tunnistamiseen ja arviointiin tai hallintamenettelyihin liittyen. Riskienhallintamenettelyistä päätettäessä ei dokumenttien valossa tehdä valtion organisaatioille suositeltua (Valtiovarain controller –toiminto 2005, 32) arvioita riskikustannusten optimoimiseksi, eikä riskien hallintamenettelyjä tai niiden periaatteita eikä riskinottohalukkuutta riskinottokyvyn puitteissa ole määritelty (liite 5). Käytettävissä ei kuitenkaan ollut niitä tietoturvallisuuden hallintajärjestelmään sisältyviä dokumentteja, jotka koskevat riskien arviointia sekä tietoturvakäytäntöjä ja –periaatteita.

Merkittävimmäksi riskienhallinnan menettelyihin liittyväksi puutteeksi on katsottava se, että organisaation johdon arvion mukaan toimintaa ja tavoitteita uhkaaviin sekä toiminnan laillisuuteen, tuloksellisuuteen ja raportointiin liittyville tunnistetuille riskeille ei määritellä hallintamenettelyjä (liite 5). Tähän liittyy kuitenkin ristiriita, sillä toimintaa ja tavoitteita uhkaavia riskejä hallitaan usealla turvallisuuden osa-alueella toteutetuin menettelyin (asiakirjat A.4.1; A.4.2; A.4.3; A.4.6; A.4.7). Aineiston valossa jää epäselväksi, viitataanko johdon arvioilla esimerkiksi organisaation vastuualueilla toteutettaviin riskienhallintamenettelyihin.

Valtion virastossa ja laitoksessa riskienhallintaan liittyvä seuranta voidaan jakaa jatkuvaan seurantaan sekä sisäiseen ja ulkoiseen arviointiin. Jatkuva seuranta on tavanomaiseen toimintaan liittyvää seurantaa, joka toteutetaan esimerkiksi poikkeamaraporttien ja mahdollisten itsearviointien kautta. Sisäinen arviointi on organisaation säännöllisesti toteuttamaa sisäisen valvonnan ja riskienhallinnan tilaa tarkastelevaa toimintaa esimerkiksi tilinpäätöksen ja toimintakertomuksen yhteydessä. Ulkoisen arvioinnin välineitä ovat esimerkiksi valtiontalouden tarkastusviraston vuosiyhteenvedot ja ministeriön tilinpäätöskannanotot. (Valtiovarain controller –toiminto 2005, 37.)

Kohdeorganisaatiossa riskienhallintaan liittyvää seurantaa voidaan katsoa toteutettavan yksitäisillä turvallisuuden osa-alueilla, mutta selvimmin ja kattavimmin tietoturvallisuuden osalta

(asiakirja A.4.7). Myös työturvallisuuteen ja työhyvinvointiin liittyvää seurantaa on tähdennetty (asiakirjat A.4.3; A.4.5). Tältä osin kohdeorganisaation huomio on kiinnittynyt merkittäviltä osin juuri valtiovarain controller –toiminnon (Valtiovarain controller –toiminto 2005, 11) esittämiin valtion viraston keskeisiin riskeihin. Asiakirjoissa ei kuitenkaan suoraan mainita työturvallisuuteen liittyvien menettelyiden sisäistä arviointia. Riskienhallintaan liittyvä ulkoinen arviointi toteutuu asiakirjojen valossa ainoastaan tietoturvallisuuden osalta.

Riskienhallintaan liittyvää seurantaa ja riskienhallinnan kehittymistä tukee oleellisesti se, että organisaation johto saa säännölliset tiedot poikkeamaseuranasta, ja että yksiköissä hyödynnetään poikkeamaseurannan tietoja (liite 5). Ilmosen ym. (2013, 170) mukaan organisaation suunnitellun toiminnan poikkeamista ja kohdatuista vahingoista oppiminen on olennainen riskienhallinnan osa-alue. Tämä edellyttäisi kuitenkin myös muun muassa riskien kirjaamista. Asiakirjat eivät kuitenkaan suoraan osoita tunnistettujen riskien seurantaa esimerkiksi siten, organisaatio pitäisi yllä seurantaa tukevaa riskirekisteriä tai toteuttaisi vastaavia riskitietoa kokoavia menettelyitä. Organisaation johdon arvion mukaan toimintaa ja tavoitteita uhkaavien sekä toiminnan laillisuuteen, tuloksellisuuteen ja raportointiin liittyviä riskejä dokumentoidaan heikosti (liite 5). Havaittuja ja hallittuja riskejä tulisi seurata systemaattisesti ja säännöllisesti, sillä riskienhallinnan tulisi olla jatkuvaa tietoista toimintaa (Juvonen ym. 2003, 30).

Riskienhallinnan raportointi on suositeltavaa liittää osaksi organisaation johtamis- ja strategiaprosessia. Riskienhallintaa koskeva raportointi on jaettavissa sisäiseen ja ulkoiseen raportointiin. Ulkoinen raportointi tarkoittaa julkista ja sidosryhmäraportointia, ja sisäinen organisaatiolle itselleen tehtävää riskienhallintaan liittyvää raportointia. Riskiraportoinnin painopiste on nykyisin riskienhallintatoimenpiteiden ja niiden vaikuttavuuden seurannassa sekä riskien kehityssuuntien arvioinnissa ja tulevaisuuden ennakoinnissa. (Ilmonen ym. 2013, 176-179.)

Kohdeorganisaatiossa toteutetaan sisäistä riskiraportointia kaikkien riskien osalta, mutta asiakirjat eivät osoita tämän tapahtuvan johtamis- ja strategiaprosessin yhteydessä. Raportointiin liittyy myös toinen tutkimusaineistossa ilmenneistä ristiriidoista; organisaation johdon arvion mukaista kohtuullisesti tai melko hyvin tapahtuvaa riskiraportointia (liite 5) haittaa väistämättä tunnistettujen riskien heikko dokumentointi (liite 5). Ulkoinen raportointi toteutuu organisaation tuloksellisuusraportoinnin avulla raporttien sisältämien sisäisen valvonnan ja riskienhallinnan vahvistuslausumien kautta, mutta vahvistuslausumat eivät käsitä keskeisiä riskejä. (asiakirjat V.1.1; V.1.2; V.1.3.) Organisaation johdon arvion mukaan riskeistä raportointi ohjaaville tahoille tapahtuu kuitenkin säännöllisesti ja järjestelmällisesti (liite 5), joten tätä varten lienee olemassa tuloksellisuusraportoinnista erillinen menettely. Asiakirjat eivät osoita, että ulkoinen raportointi koskisi ohjaavien tahojen lisäksi muita sidosryhmiä.

Jatkuvalla parantamisella on riskienhallinnassa merkittävä rooli. Jatkuvan parantamisen tavoitteet määritellään organisaatio- ja vuosikohtaisesti, mutta sen tavoitteena voi olla esimerkiksi organisaation antaman ohjeistuksen toteutuminen, toimintojen suoritustason ja yhdenmukaisuuden todentaminen ja riskienhallinnan kattavuuden varmistaminen. Riskienhallinnan nykytilan ja kypsyysasteen tulee olla tiedossa, jotta organisaation riskienhallinnalle voidaan asettaa realistisia ja konkreettisia tavoitteita. (Ilmonen ym. 2013, 45-46, 86.) Kohdeorganisaatiossa riskienhallinnan yleinen kehittämistarve on tunnistettu ja sen edellyttämät toimenpiteet todettu, mutta ne eivät ole toteutuneet. Kohdeorganisaation lausumaa kehittämisestä valtakunnallisin menettelyin voidaan pitää voimavarojen tarkoituksenmukaisena käyttönä. Riskienhallintaan luettavaa kehittämistä kuitenkin tapahtuu yksittäisillä turvallisuuden osa-alueilla tietoturvallisuuden ja työsuojelun osalta. Riskienhallinnan kehittämiselle on myös edellytykset, sillä riskienhallinnan nykytilan voidaan katsoa olevan tiedossa vuosittaisen arvioinnin tulosten kautta.

Kohdeorganisaatiossa kaikki riskienhallinnan toteuttamiseksi tarvittavat vastuut on osoitettu, ja eri turvallisuuden osa-alueilla toteutettu organisointi tukee tätä kokonaisuutta. Menettelyt noudattavat valtiovarain controller –toiminnon suositusta (Valtiovarain controller –toiminto 2005, 13-14). Riskienhallintaan liittyviksi vastuiksi voidaan katsoa myös työturvallisuussäädösten edellyttämien työsuojelupäällikön, työsuojeluvaltuutetun ja työsuojelutoimikunnan nimeäminen (Laki työsuojelun valvonnasta ja työpaikan työsuojeluyhteistoiminnasta 44/2006, 28 §, 29 §, 30 §). Näihin liittyen kohdeorganisaatiossa toteutetut menettelyt täyttävät myös työturvallisuussäädösten osoittamat velvoitteet. Vastuissa on kuitenkin havaittavissa joitakin yksittäisille henkilöille kasautuvia päällekkäisyyksiä. Riskienhallinnan menettelyjä kehitettäessä tämä tulee huomata siksi, että Suomisen (2003, 30) mukaan vastuu riskienhallinnasta ei saisi jäädä vain yhdelle henkilölle.

Eri turvallisuuden osa-alueilla velvoitteita on kohdistettu myös henkilöstölle, mutta asiakirjojen valossa ei kuitenkaan toimintaa ja tavoitteita uhkaavien sekä toiminnan laillisuuteen, tuloksellisuuteen ja raportointiin liittyvien riskien osalta. Valtion virastossa jokaisella valtionhenkilökuntaan kuuluvalla on velvollisuus tiedostaa sisäisen valvonnan ja riskienhallinnan merkitys omien tavoitteiden ja työtehtävien näkökulmasta. (Valtiovarain controller –toiminto 2005, 14-15.)

Kaiken kaikkiaan kohdeorganisaatiossa toteutettavilla ja vastuutetuilla riskienhallintamenettelyillä käsitellään merkittävää osaa valtion organisaation riskilajeista, vaikka toteutetuissa menettelyissä onkin yksittäisiä puutteita. Valtionhallinnon organisaatioissa riskit liittyvät erityisesti tuloksellisuuteen, lain ja talousarvion noudattamiseen, hyvän hallinnon periaatteiden ja arvojen toteutumiseen sekä valtion ja sen vastuulla olevien varojen ja omaisuuden turvaa-

miseen. Valtion virastojen ja laitosten keskeisiä toimintaedellytyksiä ja voimavaroja ovat henkiset voimavarat sekä informaatio ja tieto. (Valtiovarain controller –toiminto 2005, 11.)

Työsuojelun toimintaohjelmassa, työhyvinvointisuunnitelmassa ja asiakirjojen suojelusuunnitelmassa esitetyin toimenpitein sekä tietoturvapolitiikan mukaisella kokonaisuudella suojataan edellä määriteltyjä keskeisiä toimintaedellytyksiä (asiakirjat A.4.5; A.4.3; A.4.1; A.4.7) ja turvataan siten osaltaan tuloksellista toimintaa. Toiminnan tuloksellisuutta tukevat myös toimintaa ja tavoitteita uhkaavien riskien tunnistaminen, joka organisaation johdon arvion mukaan toteutuu kohtuullisesti (liite 5). Tuloksellisuutta suojaa osaltaan myös pelastussuunnitelman ja valmiussuunnitelman mukainen toiminnan jatkuvuuden turvaaminen (asiakirjat A.4.2; A.4.6). Lain ja talousarvion noudattamiseen, hyvän hallinnon periaatteiden ja arvojen toteutumiseen sekä valtion ja sen vastuulla olevien varojen ja omaisuuden turvaamiseen vastataan puolestaan sisäisen valvonnan menettelyin (asiakirja A.2.3).

Valtion ja sen toimintayksikön riskienhallinta tarkoittaa yleisesti menettelyitä, joilla tunnistetaan, arvioidaan ja hallitaan tavoitteiden saavuttamista heikentäviä uhkia, niiden todennäköisyyksiä sekä avautuneiden toimintamahdollisuuksien menettämistä. Mahdollisuuksien menettämisellä tarkoitetaan tässä yhteydessä sitä, että menetetään tilaisuus tehokkaampaan ja tuloksellisempaan toimintaan. (Valtiovarain controller –toiminto 2005, 11.) Kohdeorganisaatiossa toteutetut menettelyt liittyvät tavoitteiden saavuttamiseen, mutta viitteitä toimintamahdollisuuksien hyödyntämisen ja riskienhallinnan yhteydestä ei analysoiduissa asiakirjoissa ole.

7.2 Riskienhallinnan nykytila suhteessa odotuksiin ja velvoitteisiin

Kohdeorganisaatiolle voidaan katsoa osoitetun sekä riskienhallintaan liittyviä odotuksia strategisella ohjauksella ja tulosohjauksella että riskienhallintaan liittyviä velvoitteita säädöksin. Odotuksia on osoitettu hyvin vähäisissä määrin - valtaosa organisaatiota ohjaavista ministeriöistä tai virastoista ei ole asettanut kohdeorganisaatiolle tai sen yksittäisille vastuualueille riskienhallintaan liittyviä tulostavoitteita. Kohdeorganisaation strategisessa tulossopimuksessa kuitenkin korostetaan toiminnan tuloksellisuutta ja sen yhteydessä henkisistä voimavaroista huolehtimista (asiakirja B.1.4). Kohdeorganisaatiossa toteutetuissa riskienhallintamenettelyissä painottuu henkisistä voimavaroista huolehtiminen.

Yksiselitteisesti kohdeorganisaatiolle voidaan katsoa osoitetun yhtä vastuualuetta koskeva tavoite avainhenkilöriskien tunnistamiseen ja tähän liittyvien riskienhallintatoimenpiteiden toteuttaminen (asiakirja B.2.4), yhtä vastuualuetta koskeva tavoite varautumisesta kiireellisiin tehtäviin (asiakirjat B.2.11; B.2.12; B.2.13) sekä koko virastoa koskeva tavoite valmius-

suunnitelman laatimiseksi (asiakirjat B.2.14; B.2.15). Avainhenkilöriskiä ja valmiussuunnitelman laatimista koskevat tulostavoitteet on toteutettu (asiakirjat A.2.3; A.4.6).

Erään vastuualueen tulossopimuksissa esiintyy lisäksi mainintana henkilöstön hyvinvoinnista huolehtiminen osana henkisten voimavarojen hallintaa (asiakirjat B.2.3; B.2.4). Henkisten voimavarojen hallinta liittyy valtiovarain controller –toiminnon (Valtiovarain controller –toiminto 2005, 11) esittämiin valtion viraston keskeisiin riskeihin, mutta viittausta tähän ei ole. Muita konkreettisiin tuloksellisuutta tai häiriötöntä toimintaa edistäviin toimenpiteisiin viittaavia asioita kohdeorganisaation ohjausasiakirjoissa ei ole. Ohjausasiakirjojen sisältö ei kuitenkaan sulje pois sitä, etteikö aihepiiriä olisi käsitelty näihin liittyvien neuvottelujen yhteydessä.

Tulosohjauksen asiakirjat (asiakirjat B.2.1; B.2.2; B.2.3; B.2.4; B.2.5; B.2.6; B.2.7; B.2.8; B.2.9; B.2.10; B.2.11; B.2.12; B.2.13; B.2.14; B.2.15) osoittavat siten asetetuissa tulostavoitteissa joitakin mutta vähäisiä vastuualuekohtaisia ohjaavasta tahosta riippuvaisia eroja. Asetettuja riskienhallintaan liittyväksi katsottavia tulostavoitteita voi pitää keskenään ristiriidattomina. Kohdeorganisaation ominaisuutena oleva usean tahon ohjauksessa toimiminen (kuvio 1) ei siten tutkimusaineiston valossa ole konkretisoitunut riskienhallinnan yhteensovittamiseen liittyvinä haasteina.

Riskienhallintaan liittyvistä tulostavoitteista keskeisimmät ovat kuitenkin aluehallintovirastojen yleishallinnollisesta ohjauksesta vastaavan valtiovarainministeriön asettamat tulostavoitteet aluehallintovirastojen riskienhallinnan määrittelemiselle ja kehittämiselle. Vastuu kehittämistoimenpiteistä on aluehallintovirastojen yhteisellä toiminnan kehittämisyksiköllä yhteistyössä yhteisen sisäisen tarkastuksen yksikön ja aluehallintovirastojen kanssa (asiakirja B.1.3), joten tulostavoitteen toteuttamista ei odoteta yksittäiseltä aluehallintovirastolta. Tavoitteen toteutuminen on viivästynyt ja sitä on siirretty (asiakirja B.1.4).

Tavoitteeseen sisältyvä täsmennys aluehallintovirastojen yhteisen riskienhallintapolitiikkamallin laatimisesta, strategisten tavoitteiden toteutumiseen liittyvien riskien arvioimisesta sekä olennaisimpien riskien hallintamenettelyjen määrittelemisestä tulosohjausprosessiin kytkeytyen kuvaa riskienhallinnan järjestämisen ja tarkoituksen kannalta olennaisimpia askelia. Riskienhallinnan määrittely on riskienhallinnan toteuttamisen ensimmäinen vaihe (Ilmonen ym. 2013, 54-57; Juvonen ym. 2005, 38), ja riskienhallinnalla tulee suojata erityisesti organisaation tavoitteiden saavuttamisesta (Ilmonen ym. 2013, 5; sosiaali- ja terveysministeriö 2011, 10; Suominen 2003, 31). Aluehallintovirastojen riskienhallinnan kehittymisen kannalta on pidettävä keskeisenä, että ohjaavat tahot ovat tunnistaneet sitä koskevan tarpeen ja ryhtyneet sitä koskeviin toimenpiteisiin.

Tutkimusaineisto ei osoita, että kohdeorganisaation olisi edellytetty toteuttavan valtiovarain controller –toiminnon antamaa suositusta valtion viraston ja laitoksen sekä rahaston sisäisestä valvonnasta ja riskienhallinnasta. Suosituksen voidaan katsoa olevan ohjaavan ministeriön näkemys sisäisen valvonnan ja riskienhallinnan asianmukaisesta järjestämisestä. Siten talousarviolain (423/1988, 24 b§) sisäisen valvonnan asianmukaista järjestämistä koskevan velvoitteen toteutumisen voitaisiin nähdä edellyttävän suosituksen toteuttamista, tai tämän olevan vähintään organisaatiolle kohdistettu odotus. Suosituksen käyttöä ei kuitenkaan ole esitetty edes tulosohjauksen yhteydessä, eikä sitä siten tässä yhteydessä lueta kohdeorganisaatiolle kohdistettuihin odotuksiin eikä velvoitteisiin.

Kohdeorganisaation erään vastuualueen suoritteiden laadulle osoitetut tulostavoitteet (asiakirjat B.2.8; B.2.9) eivät viittaa suoraan riskienhallintaan, mutta riskienhallinnalla voidaan tukea laadukasta toimintaa ja tulostavoitteiden saavuttamista. Oman pohdintansa arvoinen asia on se, voiko tulostavoitteiden asettamisen itsessään katsoa edellyttävän organisaatiolta toimenpiteitä, joiden avulla tavoitteiden saavuttaminen pyritään varmistamaan.

Kohdeorganisaation voi katsoa huolehtineen keskeisistä eri turvallisuuden osa-alueisiin liittyvistä säädösvelvoitteistaan laatimillaan suunnitelmilla ja niissä esitetyillä toimenpiteillä. Työsuojelun toimintaohjelmalla (asiakirja A.4.5) vastataan työturvallisuuslain (738/2002) ja lain työsuojelun valvonnasta ja työpaikan työsuojeluyhteistoiminnasta (44/2006) keskeisiin velvoitteisiin. Työsuojelupäällikkö, työsuojeluvaltuutettu ja työsuojelutoimikunta on nimetty lain työsuojelun valvonnasta ja työpaikan työsuojeluyhteistoiminnasta (44/2006, 28 §, 29 §, 30 §) mukaisesti (asiakirja A.4.5).

Pelastuslain (379/2011) edellyttämä pelastussuunnitelma on laadittu säädöksen sisältöisenä (asiakirja A.4.2). Empiirisen aineiston sisältämä pelastussuunnitelma käsitteli kuitenkin ainoastaan yhtä kohdeorganisaation toimipisteistä. Myös valmiuslain (1552/2011) tarkoittama valmiussuunnitelma on laadittu (asiakirja A.4.6). Tietoturvallisuuspolitiikan (asiakirja A.4.7) käsittämällä kokonaisuudella ja asiakirjojen suojelusuunnitelmalla vastataan osaan lain yksityisyyden suojasta työelämässä (759/2004) sekä lain viranomaisten toiminnan julkisuudesta (621/1999) tarkoituksesta.

Organisaation arvion (asiakirjat A.2.1; A.2.2; A.2.3) mukaan valtion talousarviosta annetun lain (423/1988) ja asetuksen (1243/1992) edellyttämästä sisäisen valvonnan asianmukaisuudesta on huolehdittu. Talousarviosäädökset edellyttävät huolehtimaan asianmukaisuudesta myös toiminnassa, josta virasto vastaa. Tutkimusaineistossa ei kuitenkaan ole viittauksia tässä tarkoitettuun toimintaan. Sisäisen valvonnan sekä siihen sisältyvän riskienhallinnan asianmukaisuutta ja riittävyyttä sekä näihin liittyviä kehittämistarpeita on arvioitu ja niistä on raportoitu asetuksen valtion talousarviosta (1243/1992, 63 §, 65 §) edellyttämästi (asiakirjat V.1.1;

V.1.2; V.1.3; V.1.4). Vastuu sisäisestä valvonnasta on osoitettu talousarviolain mukaisesti kohdeorganisaatio johdolle (asiakirja V.1.3).

Säädösvelvoitteiden täyttymistä tarkasteltaessa tulee kuitenkin huomata, ettei tähän liittyvä tutkimuksen yhteydessä tehty katsaus ole tyhjentävä. Säädösten täyttymisen arvioiminen edellyttäisi sekä säädösten ja niiden perustelutekstien että kohdeorganisaatioissa toteutettujen menettelyjen tarkempaa tarkastelua.

7.3 Riskienhallinnan nykytila kokonaisvaltaisen riskienhallinnan näkökulmasta

Kokonaisvaltainen riskienhallinta on organisaation kaikille osa-alueille ja tasoille ulottuva prosessi, jolla tavoitellaan kohtuullista varmuutta organisaation tavoitteiden saavuttamisesta. Prosessilla tunnistetaan organisaatioon kohdistuvia potentiaalisia tapahtumia ja pidetään riskit riskinottohalukkuuden rajoissa. Riskienhallinta tarkoittaa strategian ja riskinottohalukkuuden yhdenmukaistamista, tehokkaampaa riskeihin vastaamista, toiminnallisten yllätysten ja tappioiden vähentämistä, monitahoisten ja koko organisaatiota koskevien riskien tunnistamista ja hallintaa, tilaisuuksiin tarttumista sekä tehokkaampaa pääoman käyttöä. (Committee of Sponsoring Organizations of the Treadway Commission 2004, 1-2.) Kokonaisvaltaisen riskienhallinnan keskeisiä ilmenemismuotoja ovat riskienhallinnan ulottaminen organisaation toiminnan kaikille osa-alueille ja tasoille sekä riskienhallinnan sitominen päivittäiseen toimintaan, johtamiseen ja toiminnan suunnitteluun (Committee of Sponsoring Organizations of the Treadway Commission 2004; Ilmonen ym. 2013; Mäkinen 2007).

Valtiovarain controller –toiminto on todennut (Valtiovarain controller –toiminto 2005, 12) myös valtionhallinnon organisaatiossa riskienhallinnan olevan kokonaisvaltainen näkökulma organisaation toimintaan, joka toteutuu tehokkaimmillaan ollessaan täysin integroituna toimintayksikön tavanomaisiin toimintoihin. Myös valtiovarain controller –toiminto tähdentää riskienhallinnan olevan erillisprosessin sijaan osa organisaation tavanomaista johtamista ja muita prosesseja, jolloin riskien tunnistaminen, arviointi ja ratkaisut niiden hallitsemiseksi toteutetaan kulloinkin käsillä olevan päätöksenteon yhteydessä. Riskienhallinta tulisi kytkeä erottamattomaksi ja saumattomaksi osaksi tulosohjausta, johtamista ja toimintayksikön perustoimintoja.

Osa tutkimuksen empiirisestä aineistosta käsittelee valtiovarain controller –toiminnon antaman suosituksen ja siten kokonaisvaltaisen riskienhallinnan mallin toteutumista kohdeorganisaatiossa. Riskienhallinnan tilaa on kohdeorganisaatiossa arvioitu kokonaisvaltaisuuden näkökulmasta vuosittain organisaation johdolle tehdyn kyselyn tulosten perusteella. Kokonaisvaltaisen riskienhallinnan osa-alueet toteutuvat organisaation johdon arvion mukaan (liite 5) toimintaa ja tavoitteita uhkaavien sekä toiminnan laillisuuteen, tuloksellisuuteen ja rapor-

tointiin liittyvien riskien tunnistamista, arviointia ja hallintaa lukuun ottamatta kiitettävästi. Johdon antamia arvioita on kuvattu vuotuisten kyselyjen tulosten yhteenvedossa (asiakirja V.2.2), jonka mukaan kehitystä on tapahtunut erityisesti seurannan osalta (liite 5). Myös muilla osa-alueilla on kohdeorganisaation toimintavuosien aikana tapahtunut kehitystä.

Muusta tutkimusaineistosta voidaan tehdä joitakin päätelmiä siitä, ilmenevätkö tutkimustulokset kokonaisvaltaista lähestymistapaa riskienhallintaan. Riskienhallinnan ulottamisesta kohdeorganisaation toiminnan kaikille osa-alueille ja tasoille on yksittäisiä viittauksia. Tietoturvanäkökohdat tulee kohdeorganisaatiossa ottaa huomioon kaikessa toiminnassa ja tietoturvasopimukset laaditaan myös ulkopuolisten palveluntuottajien ja yhteistyökumppanien kanssa (asiakirja A.4.7). Työturvallisuudesta tulee huolehtia myös työskenneltäessä toimipaikkojen ulkopuolella ja turvallisuutta sekä terveellisyyttä koskevat toimenpiteet otetaan huomioon organisaation kaikkien osien toiminnassa (asiakirja A.4.5). Pelastussuunnitelman mukaisessa riskikartoituksessa huomioidaan puolestaan omasta toiminnasta aiheutuvien riskitekijöiden lisäksi viraston ulkoiset riskitekijät sekä eri tarkastelunäkökulmia (asiakirja A.4.2).

Tutkimusaineistossa ei ole viittauksia riskienhallintatoimenpiteiden sitomisesta kohdeorganisaation perusprosesseihin ja siten päivittäiseen toimintaan. Tämän toteutumista tukevat vastuut on kuitenkin osoitettu - vastuualueiden johtajat vastaavat vastuualueidensa toiminnan tuloksellisuudesta ja tulostavoitteiden saavuttamisesta (asiakirja A.3.1). Riskienhallintaan kuuluvaksi luettavat vastuut heijastavat myös riskienhallinnan ulottamista toiminnan kaikille tasoille, sillä kaikilla turvallisuuden osa-alueilla vastuita on osoitettu sekä organisaation johdolle että yksittäisille työntekijöille. Kohdeorganisaation johto on myös arvioinut henkilöstön tuntevan viraston yhteiset talous-, henkilöstö-, tietoturva- ynnä muut hallinnollisia menettelyjä koskevat toimintatavat ja ohjeistukset hyvin (liite 5). Tästä näkökulmasta puutteeksi voidaan katsoa se, ettei kohdeorganisaation työjärjestyksissä ole käsitelty riskienhallintaan luettavia asioita joitakin poikkeuksia lukuun ottamatta (asiakirjat A.3.1; A.3.2; A.3.3; A.3.4; A.3.5) sekä se, ettei toimintaa ja tavoitteita uhkaavien sekä toiminnan laillisuuteen, tuloksellisuuteen ja raportointiin liittyvien riskien osalta vastuita tutkimusaineiston valossa ole osoitettu valtionhallinnon organisaatioille suositellusti (Valtiovarain controller –toiminto 2005, 14-15) jokaiselle henkilöstöön kuuluvalle.

Kohdeorganisaation johto on myös arvioinut riskienhallintamenettelyjen olevan kohtuullisesti kytkettyjä osaksi suunnittelu- ja ohjausprosesseja, vaikka varsinaisissa menettelyissä onkin johdon arvion mukaan merkittäviä puutteita (liite 5). Kohdeorganisaation toiminnan vuosikellossa ei kuitenkaan ole riskienhallintaan liittyviä mainintoja (asiakirja A.5.1). Nykyisissä riskienhallintaan kuuluvissa menettelyissä on tätä tukevia toimintatapoja, sillä eri turvallisuuden osa-alueilla toteutettavat riskien arvioinnit, seurannat ja raportoinnit tapahtuvat vuosittain.

Riskienhallintapolitiikan puuttuessa on vaikeaa arvioida, onko kohdeorganisaatiossa toteutuva riskienhallinta organisaation toimintaa ja tavoitteita suojaava järjestelmällinen kokonaisuus. Analysoiduissa dokumenteissa on kuitenkin yksittäisiä viittauksia siihen, että eri turvallisuuden osa-alueilla toteutettavan riskienhallinnan tarkoituksena on myös organisaation tavoitteiden suojaaminen. Pelastussuunnitelman tavoitteena on myös organisaation toiminnan jatkuvuus ja suunnitelmassa on tuotu esille tämän kannalta kriittiset suojattavat kohteet (asiakirja A.4.2). Myös tietoturvatyöllä ja asiakirjojen suojelulla suojataan organisaation tavoitteita ja sen kannalta keskeisiä kohteita (asiakirja A.4.7; A.4.1). Kohdeorganisaation johto on sisäisen valvonnan ja riskienhallinnan vahvistuslausumien laadinnan yhteydessä myös nähnyt tietoturvallisuuden, toimitilaturvallisuuden ja työturvallisuuden osana organisaation riskienhallintaa (asiakirja V.2.2).

Viitteitä on myös siitä, ettei eri riskienhallinnan menettelyjen muodostama kokonaisuus ole järjestelmällinen ja koko henkilöstön tiedostama kokonaisuus. Tutkimusaineiston asiakirjoissa ei ole viittauksia toisiinsa, eikä esimerkiksi eri turvallisuuden osa-alueiden suunnitelmissa asemoida niiden mukaisia toimenpiteitä organisaation riskienhallinnan kokonaisuuteen. Sisäisen valvonnan ja riskienhallinnan vahvistuslausuman laatimiseksi tehtyyn kyselyyn annetuissa sanallisissa vastauksissa on osa vastaajista arvioinut riskienhallinnan olevan heikolla tasolla riskienhallinnan periaatteiden puuttumisen vuoksi (asiakirja V.1.3), vaikka organisaatiossa toteutetaankin merkittäviä riskienhallintatoimenpiteitä turvallisuuden osa-alueiden yhteydessä.

Kokonaisvaltaisen riskienhallinnan näkökulmasta keskeinen ja yksiselitteinen puute on riskienhallinnan kokonaisuuden määrittelyn puuttuminen, mikä väistämättä vaikuttaa kaikkiin organisaatiossa toteutettaviin riskienhallintatoimenpiteisiin ja järjestelmällisen kokonaisuuden muodostamiseen. Kokonaisvaltaisen riskienhallinnan käsitteeseen nähden selvä puute on myös se, ettei riskinottohalukkuutta ole määritelty (liite 5). Riskejä ei tällöin voi pitää riskinottohalukkuuden rajoissa, eikä organisaation strategiaa voi yhdenmukaistaa riskinottohalukkuuden kanssa. Kokonaisvaltaisen riskienhallinnan järjestämiselle ja kehittämiselle voidaan kuitenkin katsoa olevan kohdeorganisaatiossa vahva perusta, mikäli sisäinen toimintaympäristö, toiminnan tavoitteiden selkeys, tiedonkulku, seuranta ja kontrollit ovat kohdeorganisaation johdon arvion mukaisesti (liite 5) hyvässä kunnossa.

7.4 Riskienhallinnan nykyiset menettelyt ja vaatimukset

Valtiovarain controller –toiminnon (2005, 20-22, 25) mukaan valtion virastossa ja laitoksessa riskienhallintaa kehitettäessä tulee pyrkiä selkeisiin ja yksinkertaisiin menettelyihin, huomioida olemassa olevat toiminnan rakenteet sekä välttää erillisprosesseja ja ylimääräistä dokumentointia. Ilmonen ym. (2013, 18-19) puolestaan toteavat organisaation riskienhallinnan

järjestämisen lähtökohdaksi sille osoitetut ulkoiset ja sisäiset vaatimukset. Ulkoiset vaatimukset ovat vaatimuksia tai suosituksia riskienhallinnan toteuttamisesta, ja niiden lähteitä ovat siten esimerkiksi lait ja säädökset, toimialan standardit ja ohjeet sekä asiakasvaatimukset. Sisäiset vaatimukset ovat asioita, joista on sovittu organisaation visiossa, arvoissa ja strategioissa, tai joita riskienhallinnasta on jo kirjattu esimerkiksi organisaation politiikoissa tai toimintaohjeissa. Valtion virastossa ja laitoksessa riskienhallinnan puitteet muodostuvat myös muun muassa hallintosäännöksillä ja työjärjestyksillä tehdyistä organisaatioratkaisuista sekä muusta töiden järjestämisestä, jonka lisäksi sisäistä toimintaympäristöä muodostavat sekä viraston johdon että virastoa ohjaavien elimien riskinottoon ja valvontaan liittyvät asenteet ja toimenpiteet (Valtiovarain controller –toiminto 2005, 25).

Sisäisiä vaatimuksia muodostuu kohdeorganisaatiossa useissa asiakirjoissa, mutta erityisesti eri turvallisuuden osa-alueiden yhteydessä toteutettavista toimenpiteistä. Työturvallisuudesta ja työhyvinvoinnista huolehditaan niihin liittyvissä suunnitelmissa (asiakirjat A.4.3; A.4.4; A.4.5) linjatuin toimenpitein. Tietoturvallisuuden kokonaisuus on määritelty tietoturvapolitiikassa, ja siitä huolehditaan omana kokonaisuutenaan (asiakirja A.4.7). Erikseen on suunniteltu toimenpiteitä asiakirjojen suojelemiseksi (asiakirja A.4.1). Organisaation toimitiloihin liittyvistä turvallisuuskysymyksistä huolehditaan pelastussuunnitelman mukaisin menettelyin (asiakirja A.4.2). Valmiussuunnitelmassa on linjattu sekä organisaation toimintaa yhteiskunnan häiriötilanteissa ja poikkeusoloissa että toimintaedellytysten turvaamista (asiakirja A.4.6). Turvallisuuden osa-alueilla toteuttavien menettelyillä on osin päällekkäisiä tavoitteita siten, että erityisesti henkilöstön turvallisuus ja toiminnan tavoitteiden suojaaminen korostuvat.

Turvallisuuden osa-alueista huolehtimiseksi tarvittavia vastuita on osoitettu lukuisia, ja muodostettu on toteuttamista tukevia työryhmiä (asiakirjat A.3.2; A.4.2; A.4.5; A.4.6; A.4.7). Vastuita on osoitettu organisaation kaikille portaille ja vastuualueille. Myös vastuut sisäisen valvonnan ja riskienhallinnan järjestämisestä sekä tulostavoitteiden saavuttamisesta on osoitettu (asiakirjat V.1.3; A.3.1). Toiminnan ohjaamisen ja johtamisen menettelyt on kuvattu, ja työjärjestykset on laadittu (asiakirjat A.3.1; A.3.2; A.3.3; A.3.4; A.3.5). Organisaatiossa on sekä määrityksiä että menettelyjä kaikkiin riskienhallintaprosessin vaiheisiin ja useisiin riskiluokkiin liittyen, vaikka kokonaisuudessa onkin ilmeisiä puutteita. Kohdeorganisaatiolla on visio, arvot ja strategia sekä ydinprosessit (asiakirja A.1.1; kuvio 2). Viraston johdon ja virastoa ohjaavan keskeisen ministeriön riskienhallintaan liittyviä asenteita voi tutkimusaineiston valossa pitää myönteisinä ja toimenpiteitä riskienhallinnan kehittämiseksi on suunniteltu. Tutkimusaineistossa kohdeorganisaation riskinottoon liittyviä asenteista heijastelee organisaation arvoista johdettu lausuma strategiassa, jonka mukaan henkilöstön työhyvinvoinnista huolehditaan ja työympäristö pidetään terveellisenä ja turvallisena (asiakirja A.1.1).

Strategisella ohjauksella tai tulosohjauksella ei kohdeorganisaatiolle ole osoitettu sellaisia riskienhallinnan järjestämiseen liittyviä ulkoisia vaatimuksia, joita ei olisi jo toteutettu. Riskienhallintaan liittyviksi katsotuista säädösvelvoitteista muodostuneet ulkoiset vaatimukset on huomioitu turvallisuuden osa-alueilla toteutettavin menettelyin ja rakentein. Ulkoisia vaatimuksia muodostuu myös sisäisen valvonnan ja riskienhallinnan suosituksesta (Valtiovarain controller –toiminto, 2005). Opinnäytetyössä ei tehdyistä rajauksista johtuen selvitetty kohdeorganisaation riskienhallinnalle sopimuksista tai muista sidosryhmävaatimuksista mahdollisesti juontuvia ulkoisia vaatimuksia. Myös yhteiskunnan asenteet ja arvostukset voivat vaikuttaa riskienhallintaan kohdistuviin vaatimuksiin (Ilmonen 2013, 19), mutta tähän liittyvää tarkastelua ei myöskään tehty.

7.5 Yhteenveto riskienhallinnan nykytilasta

Johtopäätösten yhteenvetona voidaan todeta, että riskienhallinta on kohdeorganisaatiossa tunnistettu käsitteenä, tarpeena ja kehittämiskohteena. Organisaation kirjalliset lausumat ovat riskienhallinnalle ja turvallisuudesta huolehtimiselle myönteisiä. Kohdeorganisaatiolle on strategisella ohjauksella ja tulosohjauksella kohdistettu riskienhallintaan liittyviä odotuksia hyvin vähän, ja organisaatio on täyttänyt odotukset. Myös riskienhallintaan liittyviin säädösvelvoitteisiin on vastattu. Riskienhallinnan kokonaisuutta ja siihen liittyviä periaatteita esimerkiksi riskienhallintapolitiikan muodossa ei ole kuitenkaan määritelty (asiakirja V.2.1). Riskienhallintaa toteutetaan kohdeorganisaatiossa lähinnä eri turvallisuuden osa-alueilla tehtyjen toimenpiteiden kautta - tietoturvallisuudesta, työturvallisuudesta, toimitilaturvallisuudesta ja poikkeusolojen toimintaedellytyksistä on huolehdittu omina kokonaisuuksinaan, samoin on huolehdittu asiakirjojen suojelusta sekä onnettomuusvahinkojen ehkäisystä näitä koskevin suunnitelmin ja toimenpitein.

Kohdeorganisaatiossa toteutetuilla toimenpiteillä pyritään vastaamaan erityisesti tietoon, henkilöstöön ja toimitiloihin kohdistuviin riskeihin. Sekä toteutetuissa riskienhallintamenettelyissä että organisaation lausumissa painottuvat tiedon ja henkisten voimavarojen suojaaminen, mitkä ovat valtion virastojen ja laitosten keskeisiä toimintaedellytyksiä (Valtiovarain controller –toiminto 2005, 11). Turvallisuuden osa-alueilla tehdyin toimenpitein on nähty suojattavan myös organisaation toiminnan tavoitteita. Kohdeorganisaation johdon arvion mukaan organisaatiossa toteutetaan myös joitakin riskienhallinnan elementtejä liittyen toiminnan laillisuuteen, tuloksellisuuteen ja raportointiin liittyviin riskeihin (liite 5). Tutkimusaineisto ei kuitenkaan viittaa siihen, että osana tuloksellisuutta olisi tuotu esille avautuvien toimintamadollisuuksien ja riskienhallinnan yhteyttä. Kokonaisuutena toteutetut toimenpiteet vastaavat suurelta osin valtion organisaation riskienhallinnan tarkoitukseen ja keskeisiin riskeihin, mutta menettelyissä on puutteita.

Kokonaisvaltaista riskienhallintaa ja riskienhallintaprosessia tarkastellen merkittävimmät puutteet liittyvät riskienhallinnan kokonaisuuden määrittelyyn, riskienhallintamenettelyihin ja riskienhallinnan kehittämiseen. Kattavimmin riskienhallinnan järjestelyt toteutuvat vastuiden ja organisoinnin sekä seurannan, arvioinnin ja raportoinnin osalta. Yksittäisinä kehittämiskohteina voidaan nostaa esille riskien dokumentointi ja riskinottohalukkuuden määrittely sekä riskienhallintamenettelyjen tuotos-panos –suhteen arviointi (liite 5). Toisaalta tutkimusaineisto jättää avoimeksi useita riskienhallintatoimenpiteisiin liittyviä kysymyksiä, joista keskeisimpänä epäselväksi jää organisaation vastuualueilla toteutettavat riskienhallinnan menettelyt sekä sisäisen valvonnan menettelyt. Kehittämistarpeita on mahdollisesti myös riskienhallinnan integroimisessa organisaation perusprosesseihin ja ulottamisessa kaikille toiminnan osa-alueille.

Tutkimusaineisto ei myöskään viittaa siihen, että kohdeorganisaatiossa toteutetut toimenpiteet riskien hallitsemiseksi muodostaisivat yhtenäisen järjestelmällisen kokonaisuuden. Organisaation nykyiset menettelyt kuitenkin enemmän mahdollistavat kuin estävät riskienhallinnan kokonaisvaltaisen lähestymistavan. Lähtökohdat kohdeorganisaation riskienhallinnan kehittämiseksi kokonaisvaltaiseksi ovat hyvät, sillä usealla osa-alueella riskienhallinasta jo huolehditaan, organisaation johto näkee kehittämisen tarpeelliseksi (asiakirjat V.1.4) ja riskienhallinnan tilaa arvioidaan säännöllisesti (asiakirjat V.1.1; V.1.2; V.1.3). Riskienhallinnan järjestämiselle on vahva perusta myös siksi, että valtion virastoille ja laitoksille annettu suositus sisäisen valvonnan ja riskienhallinnan järjestämisestä toteutuu valta-osin hyvin – kohdeorganisaation sisäinen toimintaympäristö, toiminnan tavoitteiden selkeys, tiedonkulku, seuranta ja kontrollit ovat organisaation johdon arvion mukaan kunnossa (liite 5).

Riskienhallinnan kokonaisuuden nykytilan puutteet, ristiriidat ja epäselvyydet kumpuavat opinnäytetyön tekijän näkemyksen mukaan siitä, ettei kokonaisvaltaisen riskienhallinnan edellyttämiä määrittelyjä ole tehty esimerkiksi politiikassa, periaatteissa tai tulosohjauksen yhteydessä. Tämä heijastelee väistämättä kaikkiin riskienhallinnan osa-alueisiin. Riskienhallinnan kokonaisuus, tarkoitus ja menettelytavat määrittelemällä on mahdollista muodostaa organisaation normaaliin toimintaan sisältyvä prosessi, jolla toiminnan eri osa-alueilla tunnistetaan, arvioidaan ja hallitaan määritellyin periaattein ja menettelyin organisaation tavoitteita, toimintaa, tietoa, henkilöstöä, omaisuutta ja muita suojattavia arvoja uhkaavat riskit. Kohdeorganisaation riskienhallinnan määrittelemistä ja järjestämistä tukeva ohje on esitetty omana liitteenään (liite 6). Suosituksia kohdeorganisaation riskienhallinnan kehittämisessä etenemiseksi on esitetty toimenpidesuosituksina seuraavassa luvussa.

7.6 Toimenpidesuositukset

Ottaen huomioon suunnitelmat aluehallintovirastojen riskienhallinnan valtakunnallisesta kehittämisestä voidaan toimenpidesuosituksia lähestyä myös asioina, joihin kohdeorganisaatio voi kiinnittää huomiota valtakunnallisiin kehittämistoimenpiteisiin osallistuessa.

1. Toteuttaakseen valtion virastoille ja laitoksille annettua suositusta sisäisestä valvonnasta ja riskienhallinasta (Valtiovarain controller –toiminto, 2005) sekä yhtenäistääkseen viraston nykyisen riskienhallinnan menettelyjä, on suositeltavaa päättää kokonaisvaltaisen riskienhallinnan lähestymistavan omaksumisesta viraston toiminnassa. Päätöksen seurauksena tulisi muodostaa käsitys riskienhallinnan kokonaisuudesta viraston kontekstissa ja määritellä riskienhallinnan tarkoitus, tavoitteet, vastuut, menetelmät, seuranta, raportointi, dokumentointi, aikataulutus ja keskeinen käsitteistö (Ilmonen ym. 2013, 54-57; Juvonen ym. 2005, 38). Määrittelyn tulokset voidaan kirjata esimerkiksi periaatteet ja toimintatavat käsittävän riskienhallintapolitiikan muotoon.

   Riskienhallinnan kehittymiselle tulisi samassa yhteydessä asettaa pitkän aikavälin tavoitteita (Ilmonen ym. 2013; Valtiovarain controller –toiminto 2005, 21). Ensivaiheessa tulisi varmistua strategisia ja toiminnallisia tavoitteita uhkaavien riskien tunnistamisesta, arvioinnista ja hallintamenettelyistä päättämisestä, sitoa riskienhallinta osaksi viraston ja vastuualueiden toiminnan ohjaamista, suunnittelua ja johtamista sekä jäsentää turvallisuuden osa-alueilla tehtävien toimenpiteiden ja sisäisen valvonnan yhteys kokonaisuuteen. Riskienhallinnan kehittämisellä tulisi pyrkiä tilanteeseen, jossa riskienhallinnasta muodostuu organisaation normaaliin toimintaan sisältyvä prosessi, jolla toiminnan eri osa-alueilla tunnistetaan, arvioidaan ja hallitaan määritellyin periaattein ja menettelyin organisaation suojattavia arvoja uhkaavat riskit (Juvonen ym. 2005, 145; Mäkinen 2007, 106; Valtiovarain controller -toiminto 2005, 12). Nykyisin eri turvallisuuden osa-alueilla toteutetut menettelyt tulisi tässä yhteydessä ottaa tarkasteluun.

   Periaatteita ja menettelyjä muodostaessa viraston tulisi toimia vuorovaikutuksessa ohjaavien tahojen ja erityisesti yleishallinnollisesta ohjauksesta vastaavan valtiovarainministeriön kanssa. Esitettyjen aluehallintovirastojen valtakunnallisten kehittämistoimenpiteiden yhteydessä todettua aluehallintovirastojen yhteistä riskienhallintapolitiikkaa (asiakirja B.1.3) voidaan pitää tarkoituksenmukaisena ratkaisuna.

2. Aluehallintovirastojen riskienhallintaa kehitettäessä tulisi pyrkiä aluehallintovirastojen kesken yhteneviin menettelyihin. Tämä siksi, että esillä olevat aluehallinnon uu-

distukset (Valtiovarainministeriö 2014a, 2-3; Valtiovarainministeriö 2014b, 22) tulevat mahdollisesti yhdistämään virastoja tai osia niiden toiminnoista, kuten hallintopalvelujen osalta jo ollaan tekemässä (Aluehallintovirastojen hallinnollisten tehtävien…2014). Keskenään erilaiset menettelyt yhdistyvissä virastoissa edellyttäisivät toimeenpantujen menettelyjen uudistamista, mikä vähentäisi toiminnan tuloksellisuutta tarpeettomana resurssin käyttämisenä.

Riskienhallinnan menettelyt on suositeltavaa sovittaa mahdollisimman pitkälle yhteen myös ELY-keskuksissa toteutettavan riskienhallinnan (Työ- ja elinkeinoministeriö 2011) kanssa, kuten tietoturvallisuuden osalta jo on (asiakirja A.4.7). Tämä siksi, että aluehallinnon uudistaminen saattaa jollain aikavälillä käsittää myös näiden aluehallintoviranomaisten toimintojen yhdistämistä (Valtiovarainministeriö 2014a, 2-3). Myös ELY-keskuksissa toteutettavat menettelyt pohjautuvat COSO-ERM -malliin ja edelleen valtiovarain controller –toiminnon suositukseen (Työ- ja elinkeinoministeriö 2011).

3. Riskienhallinnan periaatteiden muodostamista ja järjestämistä koskevissa ehdotuksissa (liite 6) esitetään kokonaisvaltaisen riskienhallinnan koordinaattorin nimeämistä kohdeorganisaatioon. Aluehallintovirastojen sisäisen valvonnan ja riskienhallinnan yhteensovittamista voitaisiin tukea virastojen riskienhallinnan koordinaattoreiden yhdyshenkilöverkostolla. Verkoston työskentelyyn tulisi osallistua myös valtiovarainministeriön edustaja ja riskienhallinnan organisoinnista ja vastuista riippuen virastojen sisäisen tarkastuksen henkilöitä. Pyrittäessä ELY-keskusten kanssa yhteneviin menettelyihin olisi mahdollista harkita verkoston yhdistämistä ELY-keskusten välillä toimivaan (Työ- ja elinkeinoministeriö 2011, 13) sisäisen valvonnan yhdyshenkilöverkostoon.

   Verkosto palvelisi riskienhallinnan kehittymistä virastoissa hyvien käytäntöjen ja tietouden välittymisen kautta. Verkoston kautta riskienhallinnan koordinaattoreiden kouluttaminen ja osaamisen ylläpitäminen voitaisiin toteuttaa kootusti. Lisäksi toiminta pitäisi yllä yhteneviä menettelytapoja ja siten riskienhallintaan liittyvää vertailtavuutta sekä tukisi viraston ja ohjaavan ministeriön välistä vuoropuhelua sisäisen valvonnan ja riskienhallinnan kysymyksissä.

   Aluehallintovirastojen hallinnollisten palvelujen kokoamista suunnittelevan hankkeen (Aluehallintovirastojen hallinnollisten tehtävien…2014) eteneminen hallintopalvelujen vastuuyksiköiden lakkauttamiseen tulisi vaikuttamaan edellä esitettyyn menettelyyn. Jos perustettavalle aluehallintovirastojen hallinto- ja kehittämispalvelut –vastuualueelle nimettäisiin aluehallintovirastojen yhteinen riskienhallinnan koordinaattori, voisi tämä toimia esitetyn yhteistoimintaverkoston puheenjohtajana. Vi-

rastokohtaisen riskienhallinnan koordinoinnin toteuttaminen edellyttäisi opinnäytetyön tekijän näkemyksen mukaan kuitenkin sitä, että tehtävää suorittava henkilö työskentelisi kunkin viraston yhteydessä. Tästä näkökulmasta hankkeen riskinä on se, että virastoon jäävän johdon tuki –toiminnon henkilöresurssi ei olisi riittävän suuri huolehtimaan kaikista sille suunnitelluista tehtävästään.

7.7 Työn arviointi

Opinnäytetyön tavoitteena oli tutkimuksen keinoin selvittää kohdeorganisaation riskienhallinnan nykytila siihen liittyvine rakenteineen ja menettelyineen. Tarkoituksena oli tukea kohdeorganisaation riskienhallinnan kehittymistä esittämällä sitä tukevia toimenpiteitä, laatimalla kohdeorganisaatiolle riskienhallinnan periaatteiden muodostamista tukeva ohje sekä tarjoamalla jäsennetty katsaus riskienhallintaan siihen liittyvän tiedon ja osaamiseen lisäämiseksi organisaatiossa. Nykytilan arvioimiseksi ja ohjeen antamiseksi tuli myös selvittää kohdeorganisaation riskienhallinnalle kohdistetut odotukset. Edelleen tarkoituksena oli lisätä opinnäytetyön tekijän asiantuntijuutta riskienhallinnan saralla.

Tavoitteita opinnäytetyölle asetetaan myös ylemmän ammattikorkeakoulututkinnon opinnäyteyöohjeistossa. Ohjeen mukaan opinnäytetyö on muun muassa aihealueen aikaisempaan teoreettiseen tietoon perustuva kehittämistehtävä, jolla tavoitellaan työelämäkentästä nousseen ongelman tai haasteen ratkaisemista. Työ käsittää sekä tutkimuksellisuuden että kehittämistoiminnan, ja sitä voisi luonnehtia tutkimukselliseksi kehittämishankkeeksi. Valtioneuvoston asetuksen (423/2005, 7 a §) mukaan opinnäytetyön tavoitteena on kehittää ja osoittaa valmiutta itsenäiseen vaativaan asiantuntijatyöhön sekä kykyä soveltaa tutkimustietoa soveltamiseen ja valittujen menetelmien käyttämiseen työelämän ongelmien erittelemiseksi ja ratkaisemiseksi. (Ylemmän ammattikorkeakoulututkinnon opinnäytetyöohje 2008, 4.)

7.7.1 Tavoitteiden saavuttaminen ja tulosten luotettavuus

Kirkin ja Millerin (1986, 41-42) mukaan laadullisen tutkimuksen luotettavuutta voidaan arvioida kolmesta näkökulmasta. Voidaan arvioida käytetyn menetelmän luotettavuutta, jolloin tarkastellaan metodin luotettavuutta ja johdonmukaisuutta kyseisissä olosuhteissa. Toiseksi voidaan tarkastella havaintojen ja mittausten pysyvyyttä ja arvioida siten ajallista luotettavuutta. Lisäksi voidaan arvioida samaan aikaan eri välineillä saatujen tulosten johdonmukaisuutta. (ks. Saaranen-Kauppinen & Puusniekka 2006c.) On myös olemassa erilaisia näkemyksiä siitä, voidaanko luotettavuuden käsitettä käyttää laadullisen tutkimuksen yhteydessä. Yksimielisyyttä on kuitenkin siitä, että luotettavuutta voidaan parantaa esimerkiksi pyrkimällä tekemään perusteltuja ja auki kirjoitettuja kategorisointeja tekstien analysoimisen yhteydessä. (Saaranen-Kauppinen & Puusniekka 2006c.)

Empiirisen aineiston analysoinnissa käytetty analyysirunko oli muodostettu kootun riskienhallinnan teoreettisen viitekehyksen pohjalta ja se muodostui keskeisistä riskienhallinnan järjestämisen ja toteuttamisen elementeistä. Tuloksia tarkasteltiin teorian valossa huomioiden myös valtion virastossa toteutettavalle riskienhallinnalle suositellut seikat. Analyysin perusrakennetta ja sen yhteydessä huomioituja riskienhallinnan sisältötekijöitä sekä edelleen tulosten ja niiden pohjalta tehtyjen johtopäätösten tarkastelunäkökulmaa voi siten pitää perusteltuina.

Kohdeorganisaation riskienhallinnalle kohdistetut odotukset kyettiin tehdyn rajauksen mukaisesti selvittämään siltä osin, kuin niitä on käsitelty strategisen ohjauksen ja tulosohjauksen asiakirjoissa sekä teoreettisen viitekehyksen muodostamisen yhteydessä esille nousseissa säädöksissä. On mahdollista, että asiakokonaisuutta on käsitelty asiakirjojen taustalla olevissa kohdeorganisaation ja ohjaavien tahojen välisissä neuvotteluissa, kohdeorganisaation ja muiden sidosryhmien välisissä mahdollisissa sopimuksissa tai muissa kuin esiin nousseissa säädöksissä. Riskienhallinnan järjestämiseen liittyvien säädösten perustelutekstejä ei käyty läpi, mikä korostaa säädösten osoittamiin velvoitteisiin liittyvää tulkinnanvaraisuutta. Tulokset eivät tukeneet oletusta siitä, että kohdeorganisaatiolta on ohjauksen yhteydessä odotettu tuloksellisuutta varmentavia toimenpiteitä.

Opinnäytetyön tuloksena saatiin selville kohdeorganisaation riskienhallinnan nykyiset menettelyt ja rakenteet pääpiirteissään. Tehdystä menetelmällisestä valinnasta johtuen näihin liittyvät tulokset jäivät kuitenkin paikoin kaipaamaan yksityiskohtiin liittyvää tarkennusta. Esimerkiksi riskien arvioimiseksi käytettävät menettelyt tai kaikkien menettelyiden aikataulutus eivät tulleet asiakirjoista ilmi. Keskeinen tarkennettava asia on se, toteutuvatko riskienhallintatoimenpiteet organisaation vastuualueilla ja yksiköissä ja millaisin menettelyin. On mahdollista, että tarkasteltavaa asiakokonaisuutta on käsitelty muissakin kuin käytettävissä olleissa asiakirjoissa, esimerkiksi asiakokonaisuuteen liittyvien työryhmien sisäisissä ohjeissa tai muistioissa tai organisaation vastuualueiden sisäisessä toiminnassa. Edelleen on mahdollista, että nyt tarkasteltuja asiakirjoja on myöhemmin päivitetty. Toisaalta tulee huomata, ettei ole varmuutta siitä kuvaavatko tarkasteltujen dokumenttien tiedot todellisuutta (Tuomi & Sarajärvi 2009, 107). Käytettäessä vain yhtä menetelmää ei tulosten johdonmukaisuutta voi arvioida.

Poimittaessa tietoja dokumenteista tulee huomata, ettei näitä dokumentteja ole tehty tutkimusta varten, vaan niiden tarkoituksena on ollut esimerkiksi tiedon välittäminen (Järvinen ja Järvinen 2004, 156). Tämän opinnäytetyön empiirisen aineiston osalta on huomioitava, että valtaosaa analysoiduista dokumenteista ei ollut laadittu kuvaamaan riskienhallinnan tai siihen lukeutuvien asioiden toteuttamista. Poikkeuksen tekivät jotkin turvallisuuden osa-alueisiin liittyvät suunnitelmat sekä erityisesti sisäisen valvonnan ja riskienhallinnan vahvistuslausuma

ja sen laatimiseksi organisaation johdolle tehdyn kyselyn vastaukset. Valmiin kyselyaineiston osalta tulee huomata, ettei vastaajilla välttämättä ole kaikilta osin tarvittavaa asiantuntijuutta riskienhallinnan tilan arvioimiseen. Kyselyaineiston keskeinen puute on se, ettei voida varmuudella tietää ovatko vastaajat tarkoittaneet riskienhallintamenettelyjä arvioidessaan ainoastaan vastuualueilla ja viraston johdossa tehtyjä toimenpiteitä, vai onko vastauksissa huomioitu myös turvallisuuden osa-alueilla tapahtuva riskienhallinta. Vastaajakohtaiset erot ovat kuitenkin erityisesti riskienhallinnan toteuttamista koskevan osa-alueen osalta pieniä.

Riskienhallinnan nykytilaan liittyvien tulosten luotettavuuden arvioinnissa voidaan myös pohtia sitä, olivatko dokumenttianalyysissä käytetyt hakusanat oikeita ja oikein muotoiltuja. Tällä ei kuitenkaan voi katsoa olevan merkittävää vaikutusta tuloksiin, sillä käytännössä valtaosa asiakirjoista luettiin läpi kokonaisuudessaan. Tarkasteltujen asiakirjojen valossa tulokset tukivat oletusta siitä, että riskienhallintaa toteutetaan lähinnä yksittäisten turvallisuuden osa-alueiden kautta. Laajan asiakokonaisuuden, menetelmän valinnan sekä empiirisen aineiston luonteen ja laajuuden vuoksi riskienhallinnan nykytilaan liittyvien johtopäätösten tekeminen ja esittäminen yksiselitteisessä muodossa oli haasteellista.

Kohdeorganisaation riskienhallinnan kehittämisen tukemiseen liittyvät tavoitteet saavutettiin. Tavoitteen saavuttamiseksi tarkoituksena oli tutkimustuloksiin perustuen esittää toimenpide-ehdotuksia riskienhallinnan kehittämiseksi, antaa riskienhallinnan periaatteiden muodostamista ja riskienhallinnan järjestämistä tukeva ohje sekä tarjota jäsennetty katsaus riskienhallintaan. Toimenpide-ehdotukset ovat yleisluonteisia, mutta liittyvät keskeiseen kehittämiskohteeseen. Toimenpide-ehdotuksissa myös huomioidaan odotettavissa olevat muutokset organisaatiorakenteessa ja pyritään sen kautta osaltaan vastaamaan valtion organisaatioille kohdistettuihin tuloksellisuuden velvoitteisiin. Sama koskee riskienhallinnan periaatteiden muodostamiseksi annettua ohjetta. Ohjeessa on puolestaan huomioitu paitsi riskienhallinnan periaatteiden yleinen teoria, myös riskienhallinnan toteuttaminen eräissä muissa valtion virastoissa. Tämän katsottiin olevan varautumista mahdollisiin tuleviin valtiokonsernin yhteisiin menettelyihin.

Opinnäytetyön yhteydessä muodostetun riskienhallinnan teoreettisen kehyksen on tarkoitus tarjota kohdeorganisaatiolle jäsennetty katsaus riskienhallinnan tarkoitukseen ja toteuttamiseen. Teoriaosuudessa näitä käsitellään otsikkotasolla jäsennetysti, mutta paikoin tarpeettoman pitkästi ja paikoin suppeasti. Teoriaosuus on tekstiltään opinnäytetyön tekijän arvion mukaan opinnäytetyön rikkonaisin osuus. Asiasisällöltään tämä osuus kuitenkin palvelee asetettua tavoitetta. Teoreettisen viitekehyksen muodostamisen yhteydessä täyttyi myös tavoite opinnäytetyön tekijän asiantuntijuuden lisäämisestä riskienhallinnan saralla.

Opinnäytetyö oli opinnäytetyöohjeiston mukaisesti aihealueen aikaisempaan teoreettiseen tietoon perustuva kehittämistehtävä, jolla tavoitellaan työelämäkentästä nousseen ongelman tai haasteen ratkaisemista. Työn tavoitteet perustuivat kohdeorganisaatiossa ja sitä ohjaavassa ministeriössä todettuun tarpeeseen, jonka ratkaisemista johtopäätökset, toimenpide-ehdotukset ja laadittu ohje tukevat. Tutkimusongelman ratkaiseminen nojautui aihealueen teoreettiseen tietoon riskienhallinnan nykytilan arvioimisen ja johtopäätösten esittämisen sekä annetussa ohjeessa esitettyjen ratkaisujen myötä. Työ käsittää tutkimuksellisuuden ratkaistessaan ongelman tutkimuksen keinoin, ja kehittämistoiminnan tuottaessaan kohdeorganisaatiolle tutkielmaan perustuvan ohjeen.

7.7.2 Lähestymistavan ja menetelmien valinta

Tutkimus rajattiin menetelmällisesti dokumenttianalyysiin ja empiirinen aineisto kohdeorganisaation tuottamiin valmiisiin aineistoihin sekä organisaation toiminnan ohjauksen asiakirjoihin. Tutkimusaineistojen keräämisessä tulisi lähtökohtaisesti pyrkiä ekonomiseen ja tarkoituksenmukaiseen menetelmään (Hirsjärvi ym. 1998, 185). Vaikka Hirsjärven ym. (1998, 202) mukaan haastattelun haittoina on sen edellyttämä työmäärä, olisi riskienhallinnan nykytilaa selvitettäessä haastattelu todennäköisesti ollut dokumenttianalyysiä taloudellisempi menetelmä. Toisaalta käytettävissä oli jo riskienhallinnan tilaa kartoittanut valmis valtiovarain controller –toiminnon suosituksen mukainen kyselyaineisto. Kyselyaineiston puuttuessa olisi voitu päätyä selvittämään riskienhallinnan nykytilaa vastaavalla kyselyllä tai suositukseen perustuvalla haastattelulla. Empiirinen aineisto olisi tällöin rajoittunut näin kerättyyn aineistoon nyt käytössä olleiden lukuisten dokumenttien sijaa.

Hirsjärvi ym. (1998, 201-202) pitävät haastattelun merkittävänä etuna muihin tiedonkeruumenetelmiin nähden myös sen joustavuutta sekä sitä, että vastaajat on mahdollista tavoittaa tarvittaessa myöhemminkin. Dokumenttianalyysiä tutkija pitää tässä tapauksessa kuitenkin haastattelua tarkoituksenmukaisempana menetelmänä; tuloksia kootessa jäi vahva oletus siitä, että asiakirjat paljastivat kohdeorganisaation riskienhallinnan tilasta asioita, joita haastatteluissa ei olisi tullut esille sekä siitä, että haastateltavien vastaukset olisivat väistämättä olleet asiakirjojen sisältö yleisluontoisempia. Laajan aihealueen ja jakautuneiden riskienhallinnan vastuiden vuoksi haastattelu ei välttämättä olisi paljastanut kaikkia riskienhallinnan nykyisiä menettelyjä sekä erityisesti vastuita ja muuta organisointia eikä näihin liittyviä mahdollisia päällekkäisyyksiä.

Laadullisessa tutkimuksessa tulisi tutkimusmenetelmien ja aineistonkeruun mukautua tutkimusprosessin edetessä, kun tutkijan tietoisuus kehittyy ja aineistosta nousee tutkimuksen kannalta kriittisiä ja lisää aineistoa kaipaavia kohtia (Aaltola & Valli (toim.) 2010, 76-78). Tässä opinnäytetyössä tehty menetelmällinen rajaus oli kohdeorganisaation riskienhallinnan

nykytilan arvioimisen kannalta haitallinen, sillä useat kohdeorganisaation riskienhallinnan nykytilaan liittyvät tulokset jäivät lopulta kaipaamaan tarkennuksia. Saatuja tuloksia huomattavasti tarkempi kuva tarkasteltavasta ilmiöstä olisi saatu käyttämällä valmiiden aineistojen rinnalla haastatteluaineistoa, joka olisi kerätty dokumenttianalyysin tulosten valmistuttua. Kohdeorganisaation riskienhallinnan nykyisten rakenteiden ja muiden sisäisten vaatimusten tunnistamiseen valittu menetelmä ja käytetty aineisto kuitenkin olivat riittäviä.

Riskienhallinnan periaatteiden määrittelemistä ja riskienhallinnan järjestämistä tukevan ohjeen tarkentamiseksi kohdeorganisaation johdon haastatteleminenkaan ei olisi tarjonnut kaikkea tarvittavaa tietoa, vaan aineiston kerääminen olisi riskienhallinnalle kohdistettujen ulkoisten vaatimusten osalta tullut ulottaa laajasti organisaatiota ohjaaviin tahoihin ja muihin sidosryhmiin. Tätä ei aikataulullisista syistä pidetty mahdollisena. Kohdeorganisaatiolle itselleen jää siten riskienhallinnan periaatteita muodostaessaan tehtäväksi joitakin selvityksiä, linjauksia ja päätöksiä sekä itsenäisesti että vuorovaikutuksessa organisaatiota ohjaavien tahojen kanssa.

7.7.3 Teoreettinen anti ja mahdollisia jatkotutkimusten aiheita

Opinnäytetyön antina voidaan pitää sen tuotoksena annettua ohjetta riskinhallinnan periaatteiden muodostamiseksi ja riskienhallinnan järjestämiseksi kohdeorganisaatiossa. Ohje liikkuu paikoin yleisellä ja paikoin kohdeorganisaation erityispiirteiden tasolla, mutta nivoo yhteen riskienhallinnan teoriaa sekä valtionhallinnon virastolta odotettuja ominaisuuksia ja valtionhallinnon virastoissa jo toteutettuja ratkaisuja. Ohjetta voi siten pitää hyödynnettävänä myös muissa aluehallintovirastoissa riskienhallinnan periaatteita muodostettaessa.

Uutena tietona tutkimus tarjosi kuvauksen yhden viraston riskienhallinnan nykytilasta sekä riskienhallintaan liittyvistä strategisen ohjauksen ja tulosohjauksen kautta kohdistetuista odotuksista. Riskienhallinnan nykytilaan liittyvät tulokset kuvaavat ainoastaan yhden itsenäisen viraston tilannetta, eikä niiden pohjalta voida tehdä muihin virastoihin vietyjä yleistyksiä. Strategisen ohjauksen osalta tulokset osoittivat, että toiminnan tuloksellisuutta ja henkisistä voimavaroista huolehtimista sen tekijänä korostetaan, mutta konkreettisia riskienhallinnan menettelyjä tai esimerkiksi häiriötöntä toimintaa varmistavia toimenpiteitä ei ole edellytetty. Virastojen yleishallinnollisesta ohjauksesta vastaava valtiovarainministeriö on kuitenkin tunnistanut tarpeen aluehallintovirastojen riskienhallinnan kehittämiselle ja asettanut siihen liittyviä yleisiä tulostavoitteita, vaikkakin niiden toteuttamista on lykätty. Ohjausasiakirjojen sisältö ei sulje pois sitä, etteikö aihepiiriä olisi käsitelty näihin liittyvien neuvottelujen yhteydessä.

Tulosohjauksen osalta tutkimustulokset osoittivat, ettei kohdeorganisaatioita ohjaavien tahojen asettamissa tulostavoitteissa riskienhallinnan esiintymisessä ole merkittäviä sopijaosapuolikohtaisia eroja. Kaikkien aluehallintovirastojen tulosohjaukseen liittyen voidaan puolestaan tehdä oletuksia. Voidaan olettaa, etteivät tulosohjauksella annetut tavoitteet eroa merkittävästi toisistaan myöskään eri aluehallintovirastojen kesken etenkään viraston toiminnan tukemiseen ja johtamiseen luettavan riskienhallinnan toteuttamisen ja kehittämisen osalta. Oletusta voi perustella sillä, että aluehallintovirastoille tulostavoitteita asettavat tahot ovat samoja ja ohjausta koordinoi yksi ministeriö apunaan tätä tarkoitusta varten asetettu työryhmä. Yhtä vahvaa oletusta ei voitaisi tehdä, jos kohdeorganisaationa olisi ollut jokin niistä aluehallintovirastoista, joissa ei ole edustettuna kaikkia aluehallintovirastojen vastuualueita. Tällöin tarkastelun ulkopuolelle olisi jäänyt joidenkin ohjaavien ministeriöiden tulosohjausasiakirjoja.

Esitetty oletus itsessään tarjoaa yhden jatkotutkimuksen mahdollisuuden. Opinnäytetyön yhteydessä tehtyjen rajausten vuoksi aiheita tutkimukselle tai kehittämistoiminnalle on löydettävissä lukuisia muitakin. Tutkimustuloksissa liikuttiin menetelmävalinnan vuoksi yleisellä tasolla, mikä mahdollistaa kohdeorganisaation riskienhallinnan tilan tarkemman selvittämisen. Kutakin sisäiseen valvontaan ja riskienhallintaan liittyvää osa-aluetta voidaan tarkastella tarkemmin. Samoin voitaisiin tutkia riskienhallinnan tilaa muissa aluehallintovirastoissa tai ELY-keskuksissa, joissa toimenpiteet riskienhallinnan kehittämiseksi on jo aloitettu.

Riskienhallinnan periaatteiden määrittämistä ohjaavia ulkoisia vaatimuksia voitaisiin selvittää sekä toiminnallisten sidosryhmien että erityisesti keskushallinnon näkökulmasta. Tähän liittyvä arvokas kehittämiskohde voisi olla riskien arvioimisen periaatteiden sekä riskinottokyvyn ja –halun määritteleminen aluehallintovirastolle. Tutkia voitaisiin myös yksittäisen viraston riskienhallinnan yhteensovittamista valtiokonsernin riskienhallinnan kanssa. Opinnäytetyöprosessin aikana heräsi tutkimus- ja kehittämisajatuksia myös valtiovarain controller –toiminnon antamaan suositukseen liittyen. Sisäisen valvonnan ja riskienhallinnan yhteyden kuvaaminen nykyistä selkeämmin auttaisi virastojen arjessa näiden asioiden kanssa toimivia henkilöitä. Lisäksi suositusta ja sen sisältämää arviointikehikkoa olisi mahdollista kehittää siten, että se huomioisi eri turvallisuuden osa-alueilla toteutettavat organisaation riskejä hallitsevat toimenpiteet.

Lähteet

Aaltola, J. & Valli, R. (Toim.). 2010. Ikkunoita tutkimusmetodeihin II. Jyväskylä: PS-kustannus.

Aluehallinto. 2014. Valtiovarainministeriö. Viitattu 23.3.2014. https://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/02_hallintorakenteen_kehittaminen/01_aluehallinto/index.jsp

Aluehallintovirastojen hallinnollisten tehtävien kokoamisprojekti (HALKO). 2014. Aluehallintovirastojen hallinnollisten tehtävien kokoaminen, väliraportti. Valtiovarainministeriön julkaisuja 18/2014. Helsinki: Valtiovarainministeriö.

Aluehallintovirastojen ja elinkeino-, liikenne- ja ympäristökeskusten ohjausjärjestelmän kehittämistyöryhmä. 2014. Aluehallintovirastojen ja elinkeino-, liikenne- ja ympäristökeskusten ohjausjärjestelmän kehittämistyöryhmän raportti. Valtiovarainministeriön julkaisuja 12/2014. Helsinki: Valtiovarainministeriö.

Aluehallintovirastojen tulosohjaustyöryhmä. 2011. Aluehallintovirastojen strategia-asiakirja 2012-2015, Valtiovarainministeriön julkaisuja 33a/2011. Helsinki: Valtiovarainministeriö.

Aluehallintovirastot. 2014. Aluehallintovirasto. Viitattu 23.3.2014. http://www.avi.fi/web/avi/aluehallintovirastot#.Uy6-G6zA7M8

Anttila, P. 1998. Tutkimisen taito ja tiedonhankinta. www.metodix.com. Viitattu 12.9.2014. http://www.metodix.com/fi/sisallys/01_menetelmat/01_tutkimusprosessi/02_tutkimisen_taito_ja_tiedon_hankinta/10_tutkimuksen_luotettavuus/10_2_2laadullisen_tutkimuksen_validiteetti

Arnell, J. 2010. Viestintäviraston kokonaisvaltaisen riskienhallinnan kehittäminen. Laurea-ammattikorkeakoulu. Turvallisuusosaamisen koulutusohjelma. YAMK opinnäytetyö.

Asetus valtion talousarviosta 1243/1992

Berg, K-E. 1996. Yrityksen riskienhallinta. Jyväskylä: Suomen vakuutusalan koulutus ja kustannus Oy.

Committee of Sponsoring Organizations of the Treadway Commission. 2004. Enterprise Risk Management Framework – Integrated Framework. Executive Summary. Tulostettu 2.6.2014. http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf

Etelä-Suomen aluehallintoviraston strateginen tulossopimus 2012-2015 – Päivitys vuosille 2013-2015. 2013. Viitattu 13.10.2014. https://www.avi.fi/documents/10191/37918/ESAVI_2013_2015_paivitys/6ab3186e-e5d3-45dd-948b-01cd46ada43d

Herrainsilta, J. 2006. Riskienhallinta valtionhallinnossa ja riskienhallintamenetelmän käyttöönotto. Tampereen yliopisto. Oikeustieteiden laitos. Tampere: Pro gradu –tutkielma.

Hirsjärvi, S., Remes, P. & Sajavaara. P. 1998. Tutki ja kirjoita. Helsinki: Kirjayhtymä Oy

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. 2013. Johda riskejä – käytännön opas yrityksen riskienhallintaan. Jyväskylä: Bookwell Oy.

Itä-Suomen aluehallintoviraston strateginen tulossopimus 2012-2015 – Päivitys vuosille 2013-2015. 2013. Viitattu 13.10.2014.

https://www.avi.fi/documents/10191/135258/ISAVI_Strateginen+tulossopimus+2012-2015+Paivitetty+2013-2015.pdf/899d2d2c-3106-44cb-9faa-2f14d3d09ccc

Juvonen, M., Korhonen, H., Ojala, V. M., Salonen, T. & Vuori, H. 2005. Yrityksen riskienhallinta. Helsinki: Suomen vakuutusalan koulutus ja kustannus Oy.

Järvinen, P. & Järvinen, A. 2004. Tutkimustyön metodeista. Tampere: Tampereen Yliopistopaino Oy.

Kerko, P. 2001. Turvallisuusjohtaminen. Jyväskylä: PS-kustannus.

Laki aluehallintovirastoista 896/2009

Laki työsuojelun valvonnasta ja työpaikan työsuojeluyhteistoiminnasta 44/2006

Laki valtion talousarviosta 423/1988

Laki viranomaisten toiminnan julkisuudesta 621/1999

Lain yksityisyyden suojasta työelämässä 759/2004

Lapin aluehallintoviraston strateginen tulossopimus 2012-2015 – Päivitys vuosille 2013-2015. 2013. Viitattu 13.10.2014.
https://www.avi.fi/documents/10191/149539/Lapin+aluehallintoviraston+strateginen+tulossopimus+2012-2015%2C%20p%C3%A4ivitys+vuosille+2013-2015/7c5513fa-d243-49e8-8dd4-61e152931c88

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Turvallisuusjohtamisen portfolio. Helsinki: Talentum.

Liikennevirasto. 2012. Liikenneviraston riskienhallinnan menettelytapaohje. Liikenneviraston ohjeita 7/2012. Helsinki: Liikennevirasto.

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo oy.

Lounais-Suomen aluehallintoviraston strateginen tulossopimus 2012-2015 – Päivitys vuosille 2013-2015. 2013. Viitattu 13.10.2014.
https://www.avi.fi/documents/10191/408260/LSAVIn+strateginen+tulossopimus+2012-2015_p%C3%A4iv2013-15.pdf/b910b6ae-4c88-4abb-997d-953020406bb8

Länsi- ja Sisä-Suomen aluehallintoviraston strateginen tulossopimus 2012-2015 – Päivitys vuosille 2013-2015. 2013. Viitattu 13.10.2014.
https://www.avi.fi/documents/10191/57272/LSSAVI_Strateginen_tulossopimus_2013-2015.pdf/591c7c1a-e563-42f1-a076-07d6f302c511

Mäkinen, K. 2007. Organisaation strateginen kokonaisturvallisuus. Helsinki: Edita Prima.

Ojasalo, K., Moilanen, T., Ritalahti, J. 2009. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. Helsinki: WSOYpro.

Organisaatio. 2014a. Aluehallintovirasto. Viitattu 24.3.2014.
https://www.avi.fi/web/avi/organisaatio?p_p_id=122_INSTANCE_aluevalinta&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_r_p_564233524_resetCur=true&p_r_p_564233524_categoryId=#.U5syE6zA7M8

Parmes, R. (toim.). 2007. Varautumisen käsikirja. Helsinki: Tietosanoma Oy.

Pelastuslaki 379/2011

Pohjois-Suomen aluehallintoviraston strateginen tulossopimus 2012-2015 – Päivitys vuosille 2013-2015. 2013. Viitattu 13.10.2014. https://www.avi.fi/documents/10191/1408139/Pohjois-Suomen+aluehallintoviraston+strateginen+tulossopimus+2012-2015+%28p%C3%A4ivitys+2013-2015%29/723c17a6-a6c6-43d1-81ec-170e4d58ae4f

Puolustusministeriö. Kansallinen turvallisuusauditointikriteeristö – versio II. 2011. Helsinki: Puolustusministeriö.

Reiman, T. & Oedewald, P. 2008. Turvallisuuskriittiset organisaatiot – Onnettomuudet, kulttuuri ja johtaminen. Helsinki: Edita Publishing Oy

Riskienhallinnalla tuetaan viraston tavoitteiden saavuttamista ja varmistetaan toiminnan jatkuvuus. 2013. Viestintävirasto. Viitattu 31.8.2013. https://www.viestintavirasto.fi/viestintavirasto/virastonesittelyjatehtavat/riskienhallinta.html

Riskienhallinnan organisointi. 2013. Rautaruukki Oyj. Viitattu 31.8.2013. http://www.ruukki.fi/Sijoittajat/Corporate-Governance/Risk-management/Riskienhallinnan-organisointi/

Riskienhallinta. 2014. Valtiokonttori. Viitattu 27.4.2014. http://www.valtiokonttori.fi/fi-FI/Virastoille_ja_laitoksille/Henkilostohallintoa_ja_johtamista_tukevat_palvelut/Kaikutyoelamapalvelut/Tyosuojelu/Riskienhallinta

Rusanen, S. 2009. Yhteisen turvallisuuden hallinta. Laurea-ammattikorkeakoulu. Turvallisuusosaamisen koulutusohjelma. YAMK opinnäytetyö.

Saaranen-Kauppinen, A. & Puusniekka, A. 2006a. KvaliMOTV - Menetelmäopetuksen tietovaranto. 7.3.2 Sisällönanalyysi. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 24.6.2014. http://www.fsd.uta.fi/menetelmaopetus/kvali/L7_3_2.html.

Saaranen-Kauppinen, A. & Puusniekka, A. 2006b. KvaliMOTV - Menetelmäopetuksen tietovaranto. 7.3.3 Kvantifiointi. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 24.6.2014. http://www.fsd.uta.fi/menetelmaopetus/kvali/L7_3_3.html

Saaranen-Kauppinen, A. & Puusniekka, A. 2006c. KvaliMOTV - Menetelmäopetuksen tietovaranto. 3.3.2 Reliabiliteetti. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 27.8.2014. http://www.fsd.uta.fi/menetelmaopetus/kvali/L3_3_2.html

Saaranen-Kauppinen, A. & Puusniekka, A. 2006d. KvaliMOTV - Menetelmäopetuksen tietovaranto. 5.5 Tapaustutkimus. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 7.9.2014. http://www.fsd.uta.fi/menetelmaopetus/kvali/L5_5.html

Saaranen-Kauppinen, A. & Puusniekka, A. 2006e. KvaliMOTV - Menetelmäopetuksen tietovaranto. 7.2 Aineiston käsitteleminen ja alkutoimenpiteet. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 12.9.2014. http://www.fsd.uta.fi/menetelmaopetus/kvali/L7_2.html

Saaranen-Kauppinen, A. & Puusniekka, A. 2006f. KvaliMOTV - Menetelmäopetuksen tietovaranto. 7.2.2 Koodaus. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 12.9.2014. http://www.fsd.uta.fi/menetelmaopetus/kvali/L7_2_2.html

Salminen, S. (toim.). 2005. Tulosohjauksen käsikirja. Valtiovarainministeriön julkaisuja 2/2005. Helsinki: valtiovarainministeriö.

Sisäinen valvonta ja riskienhallinta. 2013. Valtiovarainministeriö. Viitattu 28.5.2013. http://www.vm.fi/vm/fi/09_valtiontalous/045_tuloksellisuus/03_sisainen_valvonta_ja_riskienhall/index.jsp.

Sisäisen valvonnan ja riskienhallinnan neuvottelukunta. 2014. Valtiovarainministeriö. Viitattu 7.4.2014.
http://www.vm.fi/vm/fi/09_valtiontalous/045_tuloksellisuus/03_sisainen_valvonta_ja_riskienhall/01_neuvottelukunta/index.jsp

Sosiaali- ja terveysministeriö. 2011. Riskienhallinta- ja turvallisuussuunnittelu – Opas sosiaali- ja terveydenhuollon johdolle ja turvallisuusasiantuntijoille. Julkaisuja 20011:15. Helsinki: Sosiaali- ja terveysministeriö.

Suominen, A. 2003. Riskienhallinta. Helsinki: WSOY.

Toimialueet. 2014. Aluehallintovirasto. Viitattu 24.3.2014.
http://www.avi.fi/web/avi/toiminta-alue?p_p_id=122_INSTANCE_aluevalinta&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_r_p_564233524_resetCur=true&p_r_p_564233524_categoryId=#.VBHHIEzyWUk

Tolonen, S. M. 2013. Sisäisen valvonnan ja riskienhallinnan organisointi valtion organisaatiossa – Case ELY-keskus. Lappeenrannan teknillinen yliopisto. Kauppatieteiden tiedekunta. Kandidaatintutkielma.

Tulosohjaus. 2014. Valtiovarainministeriö. Viitattu 14.6.2014.
http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/01_hallintopolitiikka/01_ohjausjarjestelmat/index.jsp

Tuomi, J. & Sarajärvi, S. 2009. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Kustannusosakeyhtiö Tammi.

Tuominen, K. & Moisio, J. 2008. Toimintajärjestelmän kehittäminen: laatu, terveys, turvallisuus ja ympäristö. Benchmarking.

Työ- ja elinkeinoministeriö. 2011. ELY-keskusten sisäisen valvonnan ja riskienhallinnan toimintaperiaatteet; TEM päätös toimintaperiaatteiden vahvistamisesta. TEM/2799/00.04.01/2010. Helsinki: Työ- ja elinkeinoministeriö.

Työterveyshuoltolaki 1383/2001

Työturvallisuuslaki 738/2002

Valmiuslaki 1552/2011

Valtion hallintojärjestelmä. 2014. Valtiokonttori. Viitattu 27.4.2014.
http://www.suomi.fi/suomifi/suomi/valtio_ja_kunnat/valtion_hallintojarjestelma/index.htm

Valtion raportointipalvelu Netra. 2013. Valtiokonttori. Viitattu 20.10.2013.
http://www.netra.fi/cognos8/cgi-bin/cognosisapi.dll?b_action=xts.run&m=portal/cc.xts&gohome=;h_CAM_action=logonAs&CAMUsername=guestuser&CAMPassword=guestuser

Valtioneuvoston asetus aluehallintovirastoista 906/2009

Valtioneuvoston asetus kemiallisista tekijöistä työssä 715/2001

Valtiovarain controller –toiminto. 2005. Valtion viraston ja laitoksen sekä rahaston sisäinen valvonta ja riskienhallinta. Valtiovarainministeriö.

Valtiovarain controller –toiminto. 2013. Valtiovarainministeriö. Viitattu 28.5.2013.
http://www.vm.fi/vm/fi/02_ministerio/02_organisaatio_ja_tehtavat/13_controller/index.jsp

Valtiovarain controller -toiminto ja sisäisen tarkastuksen jaosto. 2009. Valtion viraston ja laitoksen sekä rahaston sisäinen valvonta ja riskienhallinta – Suppea sisäisen valvonnan ja riskienhallinnan arviointikehikko. Valtiovarainministeriö.

Valtiovarainministeriö. 2004a. Sisäisen valvonnan ja riskienhallinnan neuvottelukunnan pöytäkirja 30.11.2004. Helsinki: Valtiovarainministeriö.

Valtiovarainministeriö. 2004b. Sisäisen valvonnan ja riskienhallinnan neuvottelukunnan pöytäkirja 15.12.2004. Helsinki: Valtiovarainministeriö.

Valtiovarainministeriö. 2008a. Sisäisen valvonnan ja riskienhallinnan neuvottelukunnan pöytäkirja 16.6.2008. Helsinki: Valtiovarainministeriö.

Valtiovarainministeriö. 2008b. Sisäisen valvonnan ja riskienhallinnan neuvottelukunnan pöytäkirja 1.12.2008. Helsinki: Valtiovarainministeriö.

Valtiovarainministeriö. 2009a. Sisäisen valvonnan ja riskienhallinnan neuvottelukunnan pöytäkirja 6.4.2009. Helsinki: Valtiovarainministeriö.

Valtiovarainministeriö. 2009b. Sisäisen valvonnan ja riskienhallinnan neuvottelukunnan pöytäkirja 28.10.2009. Helsinki: Valtiovarainministeriö.

Valtiovarainministeriö. 2010. Sisäisen valvonnan ja riskienhallinnan neuvottelukunnan pöytäkirja 9.12.2010. Helsinki: Valtiovarainministeriö.

Valtiovarainministeriö. 2011. Sisäisen valvonnan ja riskienhallinnan neuvottelukunnan tehtävät ja tulevaisuus. Sisäisen valvonnan ja riskienhallinnan neuvottelukunnan pöytäkirja VM127:00/2007 12.4.2011. Helsinki: Valtiovarainministeriö.

Valtiovarainministeriö. 2013. Aluehallintovirastojen ohjausryhmän ja aluehallintovirastojen tulosohjausryhmän asettamispäätös 19.12.2013. Helsinki: Valtiovarainministeriö.

Valtiovarainministeriö. 2014a. Keskus- ja aluehallinnon virastoselvitys –hankkeen asettamispäätös 11.4.2014. VM040:00/2014. Helsinki: Valtiovarainministeriö.

Valtiovarainministeriö. 2014b. Keskus- ja aluehallinnon virastoselvitys –hankkeen yleisesittely. Viitattu 20.8.2014.
https://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/VIRSUn_yleisesittely_05_2014.pdf

Ylemmän ammattikorkeakoulututkinnon opinnäytetyöohje. 2008. Laurea-ammattikorkeakoulu.

Yritysturvallisuus. 2014. Elinkeinoelämän keskusliitto. Viitattu 5.6.2014. http://ek.fi/mita-teemme/tyoelama/yritysturvallisuus

JULKAISEMATTOMAT LÄHTEET

Helkiö, M. Valtiovarain controller-toiminnon erityisasiantuntijan kanssa käyty puhelinkeskustelu 24.3.2014. Valtiovarainministeriö. Helsinki.

Suoninen, J. Palvelupäällikön kanssa käyty puhelinkeskustelu 24.3.2014. Valtiokonttori. Helsinki.

Takkinen, E. Riskienhallintapäällikön kanssa käyty puhelinkeskustelu 24.3.2014. Valtiokonttori. Helsinki.

Kuviot

Taulukot

Liitteet

Liite 1. Riskienhallinnan käsitteistöä

Käsite	Määritelmä	Lähde
Riskienhallinta	Riskienhallinta on ”yrityksen kokonaisvaltaista toimintaa vaarojen ja uhkien tunnistamiseksi ja niiden aiheuttamien haittojen ja vahinkojen estämiseksi, minimoimiseksi ja valvomiseksi.”	Reiman & Oedewald 2008, 433
	”Riskienhallinnan tehtävänä on varmistaa osaltaan yrityksen toiminnan jatkuvuus yrityksen arvoja noudattaen. Riskienhallinnan tavoitteena on tukea strategiassa asetettujen tavoitteiden saavuttamista valvomalla, että yrityksen ottamat riskit ovat oikeassa suhteessa yrityksen riskinkantokykyyn ja valittuun riskinottohaluun.”	Ilmonen ym. 2013, 20
	”Riskienhallinta on systemaattista ja tavoitteellista toimintaa, jolla tuetaan organisaation johtamista ja kehittymistä. Usein sanaa riski käytetään uhka-sanan synonyyminä, mutta pohjimmiltaan riski voi olla yhtä hyvin positiivinen asia, mahdollisuus saada hyötyä jollain toimenpiteellä. Riskienhallinnan tarkoituksena on löytää organisaation kilpailukykyyn ja tuloksellisuuteen ja henkilöstön hyvinvointiin vaikuttavat tekijät. Riskianalyysin perusteella saadaan selville ne tasapainotetut toimet, joilla tulevaisuuden uhkia ja mahdollisuuksia hallitaan. Riskienhallintaan sisältyvät toimintakulttuuri, prosessit ja rakenteet, jotka edesauttavat mahdollisuuksien toteutumista ja joiden avulla hallitaan haitallisia tapahtumia. Riskienhallinta on parhaimmillaan työyhteisön yhteistoimintaa, jolla näkökulmat saadaan esille monipuolisesti.”	Riskienhallinta 2014
	”Riskienhallinta on sellaisten riskejä koskevien päätösten tekemistä ja toimeenpanoa, jotka perustuvat riskien arvioimiseen ja laskemiseen”. ”Riskienhallinnan ensisijainen tavoite on katastrofien välttäminen ja siten liiketoiminnan jatkuvuuden varmistaminen kaikissa olosuhteissa. … Toinen tavoite on riskikustannusten optimointi ja liiketoimintamahdollisuuksien hyödyntäminen”. Riskienhallinnalla suojataan yrityksen toimintaa ja tulosta käyttämällä systemaattisesti yrityksen fyysisiä, taloudellisia ja henkisiä voimavaroja estämään vahingon sattuminen tai minimoimaan sen seurausvaikutukset yritykselle.	Juvonen ym. 2005, 18, 20-21
	Riskienhallinta on "toimintatapa, prosessit ja rakenteet, joilla tunnistetaan, arvioidaan ja hallitaan tavoitteita uhkaavia riskejä."	Valtiovarain controller -toiminto 2005, 38
Riski	"Tapahtuma tai tekijä, jolla on kielteinen vaikutus tavoitteiden saavuttamiselle."	Valtiovarain controller -toiminto 2005, 38
	”Riski on todennäköisyyslaskelma sille, että jotakin ei-haluttua tai odottamatonta tapahtuu tai että jonkin halutun tai toivotun asian tapahtuminen estyy.”	Limnéll ym. 2014, 243
Organisaatioturvallisuus	”Organisaatioturvallisuus koostuu kaikista niistä toimenpiteitä, joiden avulla organisaation turvallisuusriskejä hallitaan. Organisaatioturvallisuutta yleisemmin on käytetty käsitettä yritysturvallisuus.” ”Organisaatioturvallisuus ei ole itsenäinen kokonaisuus, vaan se tarkoittaa niiden toimenpiteiden kokonaisuutta, joiden tavoitteena on häiriöttömän toiminnan varmistaminen.” ”Organisaatioturvallisuustoiminnot jakaantuvat suojattavien kohteiden määrittelyyn, riskien arviointiin, riskien hallinta- ja turvallisuustoimenpiteiden suunnitteluun ja toteutukseen sekä jatkuvaan arviointiin ja parantamiseen.”	Leppänen 2006, 59

Turvallisuusjohtaminen	”Turvallisuusjohtaminen on kokonaisvaltaista toimintaa organisaation turvallisuuden hallitsemiseksi. Sillä tarkoitetaan kaikkia niitä yritysjohdon ja työnjohdon toimenpiteitä, joilla pyritään yrityksen turvallisuustason kehittämiseen. Turvallisuusjohtamisessa yhdistyvät menetelmien, toimintatapojen ja ihmisten johtaminen. Turvallisuusjohtaminen käsittää sekä ennakoivan että korjaavan toiminnan työympäristön jatkuvaksi parantamiseksi.”	Reiman & Oedewald 2008, 435
Yritysturvallisuus	”Yritysturvallisuudella tarkoitetaan yrityksen kaikkien turvallisuusasioiden yhtenäistä tulostavoitteita tukevaa kokonaishallintaa. Sillä pyritään takaamaan yrityksen lailliset toimintaedellytykset, tuotannon ja toiminnan häiriöttömyys sekä suojaamaan yrityksen henkilöstöä, omaisuutta, tietoa ja ympäristöä onnettomuuksilta, vahingoilta ja rikolliselta toiminnalta.”	Kerko 2001, 21
Kokonaisturvallisuus	”Kokonaisturvallisuudessa on kysymys siitä, että johto ja organisaatio tietävät mitä tehdään, ja päätöstä tehtäessä toimitaan tietoisena uhkista ja riskeistä. Kokonaisturvallisuuden tarkoituksena ei ole välttää uhkia ja riskejä, vaan hallita ne sekä niiden mahdolliset seuraamukset ja seurannaisvaikutukset.” ”Kokonaisturvallisuuden tavoitteena on liiketoiminnan jatkuvuuden varmistaminen kaikissa tilanteissa ja olosuhteissa.”	Mäkinen 2007, 155
Jatkuvuuden hallinta	Jatkuvuuden hallinta on prosessi, jolla organisaatio muun muassa tunnistaa toimintaan kohdistuvat uhat ja niiden vaikutukset sekä luo toimintamallin organisaation toimintakyvyn hallinnalle. Jatkuvuuden hallinta on organisaation ylimmän johdon hyväksymää strategista ja taktista toimintaa, jonka avulla varaudutaan hallitsemaan toimintaa häiritsevät tilanteet ja jatkamaan toimintaa ennalta määritellyllä hyväksyttävällä tasolla.	Ilmonen ym. 2013, 194
Jatkuvuussuunnittelu	Jatkuvuussuunnittelun avulla pyritään häiriöiden minimoimiseen ja mahdollisimman nopeaan normaalioloihin palautumiseen tilanteissa, joissa toimintaa uhkaava riski on realisoitunut ja aiheuttanut häiriötilanteen	Leppänen 2006, 325-326
	Jatkuvuussuunnittelulla organisaatio varautuu liiketoiminnan keskeytyksiin niin, että se pystyy erilaisissa toimintaa kohtaavissa häiriötilanteissa jatkamaan toimintaansa ja rajoittamaan tappioita.	Ilmonen ym. 2013, 194
Varautuminen	Varautuminen tarkoittaa toimenpiteitä, joilla hallinto, elinkeinoelämä tai jopa yksittäinen henkilö pyrkii varmistamaan tehtäviensä mahdollisimman häiriöttömän hoidon kaikissa oloissa. Tähän sisältyvää suunnittelua kutsutaan valmiussuunnitteluksi. Valmiussuunnittelu tähtää organisaation toiminnan turvaamiseen, toimintavalmiuden kohottamiseen varautumiseen ja turvallisuuteen liittyvien uhkien minimoimisen. Näin määriteltynä varautumiseen sisältyy moni riskienhallintaan liittyvä asia, kuten yritysturvallisuus ja tietoturvallisuus.	Parmes (toim.) 2007, 31
Valtionhallinto	Valtionhallinto on osa Suomen hallintorakennetta, joka muodostuu eduskunnasta, tasavallan presidentistä, valtioneuvostosta, riippumattomista tuomioistuimista, valtionhallinnosta ja muusta julkisesta hallinnosta. Muu julkinen hallinto koostuu kunnallishallinnosta, kirkollishallinnosta ja välillisestä julkisesta hallinnosta. Kansaneläkelaitos, Suomen Pankki ja Työterveyslaitos ovat esimerkkejä välillisestä julkisesta hallinnosta. Valtionhallintoon kuuluu Suomessa valtion keskushallintoa, aluehallintoa ja paikallishallintoa. Aluehallintovirastot ovat osa valtion aluehallintoa, jonka avulla ministeriöt huolehtivat velvoitteistaan alue- ja paikallistasolla.	Valtion hallintojärjestelmä 2014

Liite 2. Sisäisen valvonnan ja riskienhallinnan suppea arviointikehikko

VALTION VIRASTON JA LAITOKSEN SISÄISEN VALVONNAN JA RISKIENHALLINNAN ARVIOINTI
Suppea sisäisen valvonnan ja riskienhallinnan arviointikehikko
Valtiovarain controller toiminto ja sisäisen tarkastuksen jaosto; 2.4.2009

Arviointivuosi:

e Ei sovellettavissa
1 Heikosti
2 Kohtuullisesti
3 Melko hyvin
4 Hyvin ja järjestelmällisesti

ARVIOINTIALUE	KYSYMYKSIÄ	ARVIO (1-4)	HUOMIOT / PERUSTELU
Sisäinen toimintaympäristö ja toimintarakenteet			
Toimintakulttuuri	Onko virastolla yhteiset pelisäännöt ja arvot ja toimitaanko niiden mukaisesti?		
	Onko virastolla yhtenäiset talous-, henkilöstö-, tietoturva- ym hallinnollisia menettelyjä koskevat toimintatavat ja ohjeistukset ja onko ne tunteeko henkilöstö ne riittävästi?		
	Onko virastossa määritelty riskinottohalukkuus riskinottokyvyn puitteissa?		
	Puututaanko virastossa johdonmukaisesti sääntöjen vastaiseen toimintaan?		
	Arvostetaanko virastossa kehittämiskohteiden tai puutteiden esiin tuomista?		
	Onko viraston toimintakulttuuri työolobarometrin perusteella terve ja oikeudenmukainen?		
Organisaatiorakenne	Onko viraston organisaatiorakenne selkeä ja toimiva?		
	Onko viraston toiminta (ml. hankehallinto) vastuutettu yksiköille kattavasti ja selkeästi esim. työjärjestyksessä?		
	Onko henkilöiden tehtävänkuvat dokumentoitu selkeästi?		
Resurssit	Onko virastolla riittävä toiminnan rahoitus (budjettirahoitus, tulorahoitus, muu rahoitus)?		
	Onko virastolla tehtävien edellyttämä määrä henkilöstöä ja/tai ulkoistettuja palveluita käytössään?		
	Onko virastolla käytössään tehtävien edellyttämä osaaminen?		
	Onko virastolla tehtävien edellyttämät toimitilat, laitteet ja tietojärjestelmät?		
Yleisarvio viraston toimintakulttuurista			
Tavoitteiden asettaminen			
Päämäärä ja tehtävä	Onko virastolla selkeä perustehtävä ja tehtävää tukevat strategiset tavoitteet?		
	Onko viraston strategiset tavoitteet viestitetty riittävästi eri yksiköille?		
Toiminnan suunnittelu	Suunnitellaanko viraston toimintaa koordinoidusti eri organisaatiotasoilla?		
	Asetetaanko toiminnalle ja hankkeille suunnitteluprosessissa konkreettisia tavoitteita?		
	Arvioidaanko suunnittelussa tehtävien, tavoitteiden ja resurssien yhteensopivuutta ja realistisuutta?		
	Onko tavoitteet priorisoitu, aikataulutettu ja vastuutettu?		
	Onko tavoitteet viestitetty virasto henkilöstölle?		
	Käytetäänkö suunnitelmia toiminnan toteutuksessa?		
Yleisarvio toiminnan suunnittelusta ja tavoitteiden asettamisesta			
Riskien tunnistaminen, arviointi ja hallinta			
Riskienhallintamenettelyt	Onko virastossa menettelyt, joilla eri organisaatiotasoilla ja hankkeissa järjestelmällisesti tunnistetaan toimintaa ja tavoitteita uhkavia riskejä?		
	Onko riskienhallintamenettelyt kytketty osaksi suunnittelu- ja ohjausprosesseja?		
Riskien tunnistaminen	Kattaako riskien tunnistaminen toiminnan laillisuuteen, tuloksellisuuteen ja raportointiin liittyvät riskit?		
	Dokumentoidaanko tunnistetut riskit?		
Riskien arviointi	Arvioidaanko tunnistettujen riskien merkitys (esiintymistodennäköisyys ja vaikutukset)?		
	Perustuuko riskien arviointi viraston yhteisiin arviointikriteereihin?		
	Raportoidaanko olennaisista riskeistä viraston johdolle?		
	Luokitellaanko arvioituja riskejä niiden luonteen ja merkityksen mukaisiin ryhmiin?		
Riskeihin vastaaminen	Priorisoidaanko tunnistettuja riskejä niiden merkityksen mukaan?		
	Määritelläänkö olennaisille riskeille hallintamenettelyt ja -vastuut?		
	Arvioidaanko hallintamenettelyiden kustannukset suhteessä hyötyyn?		
	Hyväksyykö viraston johto hallintamenettelyiden periaatteet (esim. riskienhallintapolitiikassa tai osana suunnitteluprosessia)?		
	Onko olennaiset riskienhallintamenettelyt dokumentoitu riskienhallintapolittikkaan tai vastaavaan?		
Yleisarvio riskienhallinnasta			

ARVIOINTIALUE	KYSYMYKSIÄ	ARVIO (1-4)	HUOMIOT / PERUSTELU
Kontrollit (valvontatoimenpiteet)			
Toimintaprosessien kontrollien suunnittelu	Onko keskeiset toimintaprosessit ja hankehallinnon menettelyt kuvattu ja dokumentoitu?		
	Sisältyykö toimintaprosessien ja hankehallinnon kuvauksiin myös olennaiset kontrollit?		
Tukiprosessien kontrollien suunnittelu	Onko tavaroiden ja palveluiden hankintaprosessit kattavasti ja selkeästi määritelty?		
	Onko taloussääntö ajan tasalla?		
	Onko laskujen käsittelyprosessi ja tehtävien eriyttäminen määritelty?		
	Onko maksullisen toiminnan laskutusprosessi ja tehtävien eriyttäminen ja saatavien valvonta määritelty?		
	Onko käyttöomaisuuskirjanpito ja inventointimenettely kattavaa ja luotettavaa?		
	Onko valtuuskirjanpidon prosessi selkeä ja luotettava?		
	Onko palkkahallinnon prosessi selkeä ja luotettava?		
	Onko siirtomenojen prosessi selkeä ja luotettava?		
	Onko sopimushallintamenettelyt dokumentoitu ja seurataanko sopimusten noudattamista?		
	Rekisteröidäänkö ja valvotaanko viraston mahdollisia saatavia?		
Kontrollien koordinointi	Onko organisaatiorajat/yksikkörajat ylittävien prosessien kontrollit määritelty keskitetysti tai yhteisesti (esim. työjärjestyksessä, taloussäännössä)?		
Kontrollien toimivuuden varmistaminen?	Ylläpidetäänkö toimintaan liittyvää poikkeamaseurantaa?		
	Arvioidaanko toimintaprosessien ja hankehallinnon toimivuutta säännöllisesti?		
	Arvioidaanko olennaisten kontrollien tarpeellisuutta säännöllisesti?		
	Dokumentoidaanko hankintoihin, sopimuksiin ja menoihin liittyvät tapahtumat riittävästi?		
Toiminnan seuranta	Arvioiko johto säännöllisesti toiminnan tuloksellisuutta?		
	Seurataanko määrärahojen käyttöä jatkuvasti tai säännöllisesti?		
	Seurataanko valtuuksien käyttöä jatkuvasti tai säännöllisesti?		
	Tuotetaanko toiminnan kustannuksista suoritekohtaista tietoa?		
	Annetaanko viraston tilinpäätöksessä ja toimintakertomuksessa riittävät tiedot ja tase-erittelyt?		
Yleisarvio kontrollien toteutumisesta			

Tiedonkulku ja informaation käytettävyys			
Johdon laskentatoimi	Saako johto järjestelmällisesti ja oikea-aikaisesti tietoa viraston tuotosten kustannuksista?		
	Tuottaako virasto oikeaa tietoa maksullisen ja yhteisrahoitteisen toiminnan kokonaiskustannuksista?		
	Hankkiiko virasto tarvittavat tiedot toimintaympäristön muutoksista?		
	Saako johto tarvittavat tiedot toiminnan laadusta (läpimenoajat, virheet, poikkeamat, asiakastyytyväisyys)?		
	Saako johto tiedon työajan kohdentumisesta eri suoritteille?		
Sisäinen tiedonkulku	Onko johdon laskentatoimen, kustannuslaskennan ja toimintaympäristön tiedot viraston eri toimijoiden käytettävissä oikea-aikaisesti? Saavatko yksiköt riittävästi tietoa suunnitelmista, niiden muutoksista ja niihin vaikuttavista tekijöistä?		
	Onko virastolla toimivat tiedonkulkua ja vuorovaikutusta tukevat menettelyt?		
	Saavatko yksiköt riittävästi tietoa suunnitelmista, niiden muutoksista ja suunnitelmiin vaikuttavista tekijöistä?		
	Onko poikkeustilanteiden viestinnälle nopeat ja kattavat menettelyt?		
Ulkoinen tiedonkulku	Onko virastolla järjestelmälliset tavat raportoida ja tiedottaa toiminnastaan ja riskeistään ohjaavalle taholle (esim. ministeriölle)?		
	Onko virastolla järjestelmälliset tavat raportoida ja tiedottaa toiminnastaan suurelle yleisölle ja erityisille kohderyhmille?		
	Onko virastolla toimivat menettelyt tiedonvaihtoon sidosryhmien kanssa?		
	Onko virastolla suunnitelmat ulkoisen viestinnän toteuttamisesta poikkeustilanteissa?		
Yleisarvio viraston tiedonkulusta			
Seuranta			
Jatkuva seuranta	Saako johto säännölliset tiedot poikkeamaseurannasta?		
	Hyödynnetäänkö yksiköissä poikkeamaseurannan tietoja?		
	Arvioidaanko prosessien ja hankehallinnon toimivuutta säännöllisesti prosessi- ja muiden indikaattorien avulla?		
Sisäinen arviointi	Arvioiko virasto itse sisäisen valvonnan ja riskienhallinnan toimivuutta säännöllisesti?		
	Ovatko arviointien tulokset olleet hyviä aiemmin?		
Ulkoinen arviointi	Käsitelläänkö ulkoisten arviointien tulokset säännöllisesti?		
Yleisarvio seurannasta			

YLEISARVIO VIRASTON/LAITOKSEN SISÄISEN VALVONNAN JA RISKIENHALLINNAN TOMIVUUDESTA:

Liite 3. Tutkimuksen empiirinen aineisto

Asiakirjaluokka		Asiakirja	
V. Vahvistuslausumat ja niihin liittyvä kyselyaineisto	V.1 Vahvistuslausumat	V.1.1	Sisäisen valvonnan ja riskienhallinnan vahvistuslausuma vuodelta 2013
		V.1.2	Sisäisen valvonnan ja riskienhallinnan vahvistuslausuma vuodelta 2012
		V.1.3	Sisäisen valvonnan ja riskienhallinnan vahvistuslausuma vuodelta 2011
		V.1.4	Sisäisen valvonnan ja riskienhallinnan vahvistuslausuma vuodelta 2010
	V.2 Kyselytulokset	V.2.1	Kyselytulokset vuodelta 2013
		V.2.2	Kyselytulosten yhteenveto vuosilta 2011-2013
A. Muut kohdeorganisaation riskienhallinnan nykytilaa kuvaavat dokumentit	A.1 Strategiat	A.1.1	Aluehallintoviraston strategia
	A.2 Toiminnan ja tuloksellisuuden raportit	A.2.1	Aluehallintoviraston tuloksellisuusraportti vuodelta 2013
		A.2.2	Aluehallintoviraston tuloksellisuusraportti vuodelta 2012
		A.2.3	Aluehallintoviraston toimintakertomus vuodelta 2011
		A.2.4	Aluehallintoviraston toimintakertomus vuodelta 2010
	A.3 Työjärjestykset	A.3.1	Aluehallintoviraston työjärjestys
		A.3.2	Aluehallintoviraston hallintopalvelujen vastuuyksikön työjärjestys
		A.3.3	Aluehallintoviraston pelastustoimen ja varautumisen vastuualueen työjärjestys
		A.3.4	Aluehallintoviraston peruspalvelut, oikeusturva ja luvat-vastuualueen työjärjestys
		A.3.5	Aluehallintoviraston ympäristölupavastuualueen työjärjestys
	A.4 Turvallisuuden osa-alueisiin liittyvät asiakirjat	A.4.1	Aluehallintoviraston asiakirjojen suojelusuunnitelma
		A.4.2	Aluehallintoviraston päätoimipaikan kiinteistöjen pelastussuunnitelma
		A.4.3	Aluehallintoviraston työhyvinvointisuunnitelma 2012-2013
		A.4.4	Aluehallintoviraston työhyvinvointisuunnitelma 2011
		A.4.5	Aluehallintoviraston työsuojelun toimintaohjelma 2011-2012
		A.4.6	Aluehallintoviraston valmiussuunnitelma
		A.4.7	Aluehallintovirastojen tietoturvapolitiikka
	A.5 Muut asiakirjat	A.5.1	Aluehallintoviraston toiminnan vuosikello 2013
B. Kohdeorganisaation riskienhallinnan järjestämiseen liittyviä odotuksia kuvaavat dokumentit	B.1 Strateginen ohjaus	B.1.1	Aluehallintovirastojen strategia-asiakirja vuosille 2012-2015
		B.1.2	Aluehallintovirastojen strategia-asiakirja vuosille 2010-2011
		B.1.3	Aluehallintoviraston strateginen tulossopimus 2012-2015
		B.1.4	Aluehallintoviraston strateginen tulossopimus 2012-2015 Päivitys vuosille 2013-2015
		B.1.5	Aluehallintoviraston strateginen tulossopimus 2010-2011
		B.1.6	Aluehallintoviraston strategista tulossopimusta 2010-2011 täydentävä asiakirja
	B.2 Tulosohjaus	B.2.1	Sosiaali- ja terveysministeriön ja aluehallintoviraston peruspalvelut, oikeusturva ja luvat-vastuualueen välinen toiminnallinen tulossopimus 2011
		B.2.2	Sosiaali- ja terveysministeriön ja aluehallintoviraston työsuojelun vastuualueen välinen tulossopimus 2012-2015, tulostavoiteet 2013
		B.2.3	Sosiaali- ja terveysministeriön ja aluehallintoviraston työsuojelun vastuualueen välinen tulossopimus 2012-2015
		B.2.4	Sosiaali- ja terveysministeriön ja aluehallintoviraston työsuojelun vastuualueen välinen tulossopimus 2010-2011
		B.2.5	EVIRAn ja aluehallintoviraston välinen tulossopimus 2012
		B.2.6	EVIRAn ja aluehallintoviraston välinen tulossopimus 2011
		B.2.7	EVIRAn ja aluehallintoviraston välinen tulossopimus 2010
		B.2.8	Kilpailuviraston ja aluehallintoviraston välinen toiminnallinen tulossopimus 2012
		B.2.9	Kilpailuviraston ja aluehallintoviraston välinen toiminnallinen tulossopimus 2011
		B.2.10	Kilpailuviraston ja aluehallintoviraston välinen toiminnallinen tulossopimus 2010
		B.2.11	Tukesin ja aluehallintoviraston välinen tulossopimus 2012
		B.2.12	Tukesin jaaluehallintoviraston välinen tulossopimus 2011
		B.2.13	Tukesin ja aluehallintoviraston välinen tulossopimus 2010
		B.2.14	Sisäasiainministeriön ja aluehallintoviraston välinen tulossopimus 2011
		B.2.15	Sisäasiainministeriön ja aluehallintoviraston välinen tulossopimus 2010

Liite 4. Analyysirunko

Pääkategoriat Sisältötekijöitä	Ilmeneminen dokumenteissa	Dokumentti	**Virasto (V) vastuualue (Va) Yksikkö (Yk) Sidosryhmä (S)**	Yhteenveto
Riskienhallinnan määrittely				
Määrittelyn kattavuus				
Määritysten sisältö				
Ulkoisten ja sisäisten vaatimusten huomioiminen				
Riskienhallintamenettelyt				
Riskien tunnistaminen				
Riskien arvioimien				
Riskien hallitseminen				
Perustuminen määrittelyyn				
Riskien ja riskienhallinnan seuraaminen ja raportointi				
Riskien seuraaminen				
Riskienhallinnan arviointi				
Riskien ja riskienhallinnan sisäisen ja ulkoinen raportointi				
Riskienhallinnan kehittäminen				
Kehittämistarpeiden tunnistaminen				
Kehittämistoimenpiteiden toteuttaminen				
Kehittämisen suunnitelmallisuus				
Vastuut ja organisointi				
Vastuut				
Muu organisointi				

Liite 5. Valmiin kyselyaineiston kuvioita

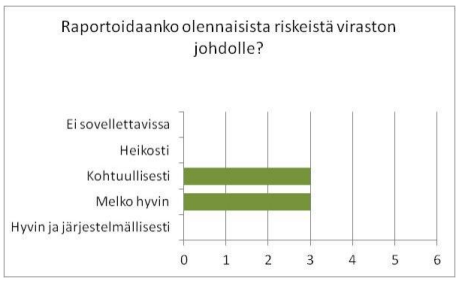
Kuviot 1-17 ovat sisäisen valvonnan ja riskienhallinnan vahvistuslausuman antamiseksi kohdeorganisaation johdolle vuonna 2013 tehdyn kyselyn niitä tuloksia, mihin tutkimustulosten yhteydessä on viitattu. Kaavioiden ala-akselilla kuvataan vastaajien määrää. (asiakirja V.2.1.) Kysely on toteutettu sisäisen valvonnan ja riskienhallinnan arvioinnin suppean arviointikehikon (liite 2) mukaisena (asiakirja A.2.1).

Kuvio 18 on kyselytulosten vuosien 2011-2013 yhteenveto. Kuvio käsittelee sisäisen valvonnan ja riskienhallinnan arvioinnin kokonaisuutta. Kuviossa uloin kehä kuvaa arvoa 4, jolloin asia toteutuu järjestelmällisesti ja sisin arvoa 1, jolloin asia toteutuu heikosti. (asiakirja V.2.2.) Kysely on toteutettu vuosittain samansisältöisenä (asiakirjat A.2.1; A.2.2).

Kuviot 1 ja 2. Toimintakulttuuri kohdeorganisaatiossa vastaajien mukaan (asiakirja V.2.1).

Kuviot 3 ja 4. Riskienhallintamenettelyjen toteutuminen kohdeorganisaatiossa vastaajien mukaan (asiakirja V.2.1).

Kuviot 5 ja 6. Riskien tunnistamisen toteutuminen kohdeorganisaatiossa vastaajien mukaan (asiakirja V.2.1).

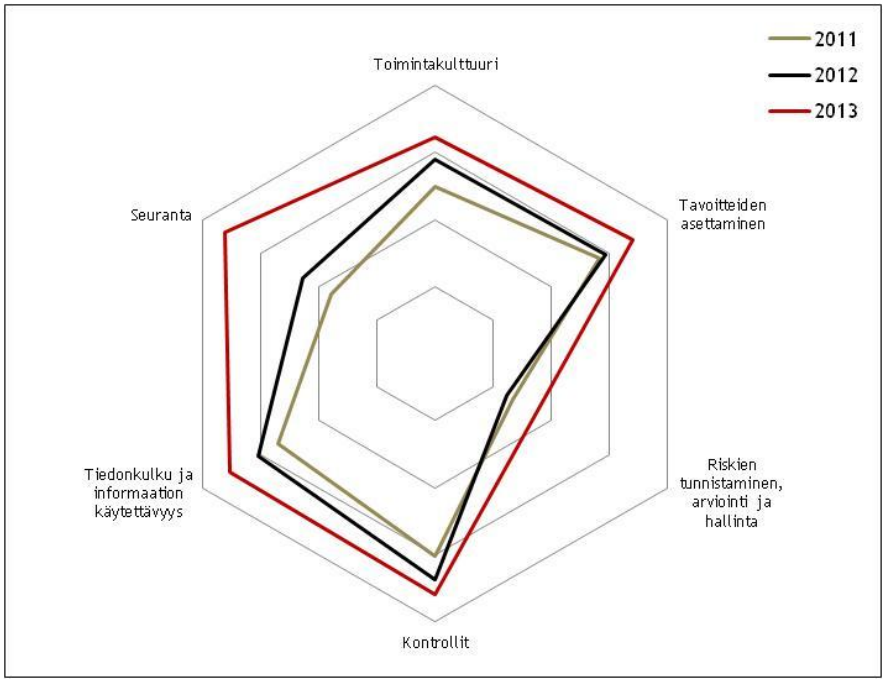


Kuviot 7-10. Riskien arvioinnin toteutuminen kohdeorganisaatiossa vastaajien mukaan (asiakirja V.2.1).

Kuviot 11-14. Riskeihin vastaamisen toteutuminen kohdeorganisaatiossa vastaajien mukaan (asiakirja V.2.1).

Kuviot 15-16. Jatkuvan seurannan toteutuminen kohdeorganisaatiossa vastaajien mukaan (asiakirja V.2.1).

Kuvio 17. Ulkoisen tiedonkulun toteutuminen kohdeorganisaatiossa vastaajien mukaan (asiakirja V.2.1).



Kuvio 18. Kohdeorganisaation sisäisen valvonnan ja riskienhallinnan arvioinnin tulokset osa-alueittain vuosina 2011-2013 (asiakirja V.2.2).

Liite 6. Ehdotuksia riskienhallinnan periaatteiden määrittelemiseksi ja riskienhallinnan järjestämiseksi kohdeorganisaatiossa

Ehdotuksissa on huomioitu kohdeorganisaation riskienhallintaan liittyvät nykyiset rakenteet ja menettelyt. Ehdotuksia laadittaessa on käytetty valtiovarain controller –toiminnon suositusta (Valtiovarain controller –toiminto 2005), Työ- ja elinkeinoministeriön päätöstä ELY-keskusten sisäisen valvonnan ja riskienhallinnan toimintaperiaatteista (Työ- ja elinkeinoministeriö 2011), kokonaisvaltaisen riskienhallinnan toteuttamista Viestintävirastossa (Arnell 2010), Liikennevirasto riskienhallinnan menettelytapaohjetta (Liikennevirasto 2012) sekä opinnäytetyön tekijän näkemyksiä siitä, mitä riskienhallinnan toteuttaminen voisi tarkoittaa kohdeorganisaation kontekstissa.

1. Riskienhallinnan tarkoitus ja tavoitteet

Kokonaisvaltaisen riskienhallinnan tarkoituksen ja tavoitteiden määrittelyssä toistuvat usein erityisesti organisaation tavoitteiden saavuttamiselle ja toiminnan jatkuvuudelle haitallisten riskien tunnistaminen ja hallitseminen sekä päätöksenteon tukeminen hallitun riskinoton ja tavoitteiden saavuttamista koskevan kohtuullisen varmuuden kautta. Valtion ja sen toimintayksikön riskienhallinta tarkoittaa valtiovarain controller –toiminnon mukaan yleisesti menettelyitä, joilla tunnistetaan, arvioidaan ja hallitaan tavoitteiden saavuttamista heikentäviä uhkia, niiden todennäköisyyksiä sekä avautuneiden toimintamahdollisuuksien menettämistä. Mahdollisuuksien menettämisellä tarkoitetaan tässä yhteydessä sitä, että menetetään tilaisuus tehokkaampaan ja tuloksellisempaan toimintaan. Riskienhallintaa toteutetaan usein myös organisaatioturvallisuuden osa-alueilla tehdyin toimenpitein.

Valtiovarain controller -toiminnon mukaan valtionhallinnon organisaatioissa riskit liittyvät erityisesti tuloksellisuuteen, lain ja talousarvion noudattamiseen, hyvän hallinnon periaatteiden ja arvojen toteutumiseen sekä valtion ja sen vastuulla olevien varojen ja omaisuuden turvaamiseen. Valtion virastojen ja laitosten keskeisiä toimintaedellytyksiä ja voimavaroja ovat henkiset voimavarat sekä informaatio ja tieto. Henkiset voimavarat liittyvät tässä yhteydessä henkilöstön määrään, osaamiseen, työmotivaatioon ja työhyvinvointiin. Keskeinen osa riskienhallintaa valtion virastossa ovat siten henkilöstöön ja osaamiseen sekä tiedon laatuun ja tietoturvallisuuteen liittyvä riskien hallinta.

Riskienhallinnan tarkoituksen ja sille asetettavien tavoitteiden määrittäminen edellyttää lisäksi käsitystä viraston sisäisestä toimintaympäristöstä, riskienhallinnalle asetettavista ulkoisista ja sisäisistä vaatimuksista sekä riskienhallinnan nykytilasta. *Ulkoisia vaatimuksia* muodostuu aluehallintoviraston tapauksessa lainsäädännön ja tulosohjauksen osoittamista vaatimuksista, ohjaavien tahojen antamista ohjeista sekä mahdollisista sidosryhmien asettamista

vaatimuksista. Tulosohjauksella on toistaiseksi annettu hyvin vähän suoraan riskienhallinnan järjestämiseen liittyväksi katsottavia vaatimuksia, mutta lainsäädännössä näitä osoitetaan useita: organisaation tulee esimerkiksi huolehtia sisäisen valvonnan asianmukaisuudesta sekä työntekijöiden terveydelle ja turvallisuudelle aiheutuvien haittojen tunnistamisesta sekä varmistaa tehtäviensä mahdollisimman hyvä hoitaminen myös poikkeusoloissa. Annettuina ohjeina on esimerkiksi valtiovarain controller –toiminnon suositus sisäisestä valvonnasta ja riskienhallinasta, mutta ohjeita voi olla annettuina myös aluehallintovirastossa edustettuina olevilla toimialoilla. Mahdollisista muiden sidosryhmien asettamista vaatimuksista tulee riskienhallintaa määriteltäessä varmistua.

Sisäiset vaatimukset ovat asioita, joista on sovittu viraston visiossa, arvoissa ja strategiassa, tai joita riskienhallinnasta on jo kirjattu esimerkiksi viraston toimintaohjeissa. Valtion virastossa ja laitoksessa riskienhallinnan puitteita muodostuu myös muun muassa hallintosäännöksillä ja työjärjestyksillä tehdyistä organisaatioratkaisuista sekä muusta töiden järjestämisestä. Viraston strategiassa on esimerkiksi todettu huolehdittavan henkilöstön työhyvinvoinnista ja toimittavan tietoturvallisuuden periaatteiden ja tavoitteiden mukaisesti. Aluehallintovirastojen tietoturvapolitiikka ja sisäisen valvonnan menettelyt ovat keskeiset tässä yhteydessä huomioitavat kokonaisuudet, ja menettelyjä määriteltäessä tulee huomioida näissä tehdyt linjaukset. Riskienhallintaan liittyviä asioita, esimerkiksi vastuita, on lisäksi jo käsitelty muun muassa työsuojelun toimintaohjelmassa, työjärjestyksissä ja pelastussuunnitelmassa. Sisäistä toimintaympäristöä muodostavat myös sekä viraston johdon että virastoa ohjaavien elimien riskinottoon ja valvontaan liittyvät asenteet.

Aluehallintoviraston riskienhallinnan tarkoitus voidaan määritellä esimerkiksi siten, että riskienhallinnalla tunnistetaan, arvioidaan ja hallitaan riskejä, jotka vaikuttavat haitallisesti

- viraston strategisten päämäärien ja tulostavoitteiden toteutumiseen,
- viraston keskeisten toimintojen laadukkaaseen toteutumiseen,
- viraston toiminnan jatkuvuuteen kaikissa oloissa,
- viraston henkilöstöön, tietoon ja omaisuuteen sekä
- lainsäädännön ja hyvän hallintotavan toteutumiseen.

Lisäksi riskienhallinnalla tarjotaan johdon käyttöön järjestelmälliset menettelyt riskien arvioimiseksi ja hallitsemiseksi. Menettelyjen avulla johdolla on käytössään tarpeellinen tieto tavoitteiden saavuttamista ja toimintaa uhkaavista riskeistä sekä niihin liittyvistä seurauksista, joita viraston toiminnalla on sidosryhmiin ja yhteiskuntaan. Menettelyt mahdollistavat hallitun riskinoton esimerkiksi tuloksellisempaa toimintaa tavoiteltaessa, ja tarjoavat johdolle riittävät tiedot toimintaan ja riskeihin liittyvää raportointia varten.

Tarkoituksen määrittelyssä on edellä huomioitu valtiovarain controller -toiminnon suosituksen ohella organisaation toiminnan luonteen kannalta keskeisten turvallisuuden osa-alueiden sitominen viraston riskienhallinnan kokonaisuuden yhteyteen. Riskienhallinnan tarkoitus laajenisi siten selvemmin sisäisen valvonnan yhteydestä organisaation kaikkeen toimintaan. Määrittelyn yhteydessä tarpeellinen nykyisten menettelyjen tarkastelu mahdollistaa myös jo kirjattujen asioiden muokkaamisen mahdollisen uuden kokonaisvaltaisen lähestymistavan mukaiseksi.

Koska kokonaisvaltaisessa riskienhallinnassa on kyse jatkuvasta kehittämisen prosessista, edellyttää tavoitteiden määrittäminen tietoa myös *riskienhallinnan nykytilasta*. Nykytilaa on kartoitettu vuosittain sisäisen valvonnan ja riskienhallinnan vahvistuslausuman antamisen yhteydessä. Riskienhallinnan määrittelyn yhteydessä voidaan tarkastella, onko riskienhallinnan nykytilaa tarpeen arvioida uudelleen suhteessa määriteltyyn riskienhallinnan kokonaisuuteen. Myös ulkopuolista auditointia voi käyttää. Nykytilaa tulee arvioida myös suhteessa tunnistettuihin ulkoisiin ja sisäisiin vaatimuksiin.

Keskeisenä riskienhallintatyölle asetettavana tavoitteena on suositeltavaa olla se, että riskienhallinta muodostuu jollain aikavälillä osaksi organisaation normaalia toimintaa ja ulottuu kaikille toiminnan osa-alueille ja tasoille. Ensimmäisenä tavoitteena voi olla vakiintunut menettely riskien tunnistamiseksi ja arvioimiseksi toiminnan suunnittelun ja johtamisen yhteydessä. Muina yksityiskohtaisina tavoitteina voivat olla esimerkiksi riskitietoisuuden ja riskienhallintaan liittyvän osaamisen lisääminen, selkeiden riskien tunnistamisen, arvioimisen ja hallinnan menettelyjen luominen, toiminnan häiriöherkkyyden vähentäminen tai vaikkapa riskiraportoinnin kehittyminen. On huomattava, että riskienhallinnan kehittyminen on monivuotinen prosessi, eikä sitä voi saattaa valmiiksi kerralla. Myös kehittämistä voi linjata jo riskienhallintaa määriteltäessä - kehittämiseen liittyvinä tavoitteina voidaan todeta tavoiteltuja kehitysvaiheita aikatauluineen.

2. Riskienhallinnan vastuut ja tehtävät

Riskienhallintaan liittyviä vastuita ja organisointia on käsitelty säädöksissä, aluehallintovirastojen tietoturvapolitiikassa ja organisaation jo laatimissa suunnitelmissa sekä työjärjestyksissä. Sisäiseen valvontaan ja riskienhallintaan liittyviä vastuita ja tehtäväjakoja on käsitelty myös valtiovarain controller –toiminnon antamassa suosituksessa ja edelleen viraston toimintakertomuksessa, jonka mukaan aluehallintoviraston sisäisen valvonnan ja riskienhallinnan järjestämistä johtavat ja sen asianmukaisuudesta ja riittävyydestä vastaavat ylijohtaja ja osaltaan vastuualueiden ja hallintopalvelujen vastuuyksikön johtajat. Riskienhallintaan liittyen säädökset edellyttävät työsuojelupäällikön ja –valtuutettujen nimeämistä.

Viraston johto tai yksittäinen vastuuhenkilö ei käytännössä voi toteuttaa kaikkia kokonaisvaltaisen riskienhallinnan edellyttämiä toimenpiteitä, joten tehtäviä tulee jakaa muulle organisaatiolle. Riskienhallinnan tehtävien organisointi vaikuttaa edelleen kaikkiin tuleviin riskienhallinnan vaiheisiin. Vastuiden jakaminen voidaan tehdään millä tahansa parhaaksi katsotulla tavalla viraston johdon vastuun delegointia lukuun ottamatta, mutta vastuita määriteltäessä tulee pyrkiä ulottamaan riskienhallinta koko organisaation tehtäväksi. Erillisen riskienhallintaprosessin järjestäminen ei myöskään ole tarkoituksenmukaista.

Riskienhallintaan liittyvä organisointi on suositeltavaa toteuttaa siten, että riskien tunnistaminen, arviointi ja hallitseminen painottuvat viraston vastuualueille, sillä viraston toiminta tapahtuu keskeisiltä osiltaan siellä. Tällöin:

- Viraston johto vastaa riskienhallintapolitiikan laatimisesta ja sen vaatimista linjavedoista, resursoinnista ja organisaation sitouttamisesta, strategian toteutumiseen liittyvien riskien tunnistamisesta, arvioimisesta ja hallinnasta, ulkopuolelle tehtävästä raportoinnista sekä kokonaisuuden yhteensovittamisesta ja seurannasta.

- Hallintopalvelujen vastuuyksikkö vastaa tavoitteidensa saavuttamiseen ja keskeisiin toimintoihinsa liittyvien riskien tunnistamisesta, arvioimisesta, hallitsemisesta ja seurannasta sekä viraston johdolle raportoinnista ja yksikön riskirekisterin ylläpitämisestä. Yksikkö myös arvioi viraston riskienhallintaa sekä pitää yllä viraston kokoavaa riskirekisteriä. On suositeltavaa, että yksikkö toimisi johdon tukena kokonaisvaltaisen riskienhallinnan koordinoijana ja asiantuntijana, ja tähän tehtävään nimettäisiin henkilö.

- Vastuualueet vastaavat tulostavoitteidensa saavuttamiseen sekä keskeisiin toimintoihinsa ja ydinprosesseihinsa liittyvien riskien tunnistamisesta, arvioimisesta, hallitsemisesta ja seurannasta sekä viraston johdolle raportoinnista ja vastuualueen riskirekisterin ylläpitämisestä. Vastuualueet huomioivat tässä yhteydessä viraston yhteiset ohjeet esimerkiksi lainsäädäntöön ja hyvään hallintotapaan sekä eri turvallisuuden osa-alueisiin liittyen. Suurilla vastuualueilla riskienhallinnan toteuttamista voi joltain osin harkita toteutettavaksi myös yksiköittäin. Vastuualueet myös tunnistavat viraston strategisten riskien liittymiseen vastuualueen toimintaan.

- Jokaisen henkilökuntaan kuuluvan velvollisuutena on tiedostaa sisäisen valvonnan ja riskienhallinnan merkitys omien tavoitteiden ja työtehtävien näkökulmasta. Työntekijän velvollisuutena on riskien havainnointi, sovittujen toimintatapojen noudattaminen ja raportointi.

On myös mahdollista määritellä ne viraston toiminnan osa-alueet, joiden osalta riskienhallinta voidaan hoitaa keskitetysti joko virastossa tai valtakunnallisesti. Tällöin esimerkiksi eri turvallisuuden osa-alueisiin liittyvien riskien tunnistaminen, arviointi ja hallintatoimenpiteistä päättäminen voidaan toteuttaa erillisin turvallisuuden osa-alueisiin keskittynein työryhmin, joita virastossa on jo nimetty esimerkiksi tietoturvallisuuden osalta. Ryhmien toiminnan kautta voidaan huolehtia turvallisuuteen liittyvien säädösvelvoitteiden toteuttaminen ja samalla tiettyjen viraston keskeisten toimintaedellytysten suojaaminen. Tiettyjen riskityyppien osalta riskien tunnistamista, arviointia tai hallintaa voi olla mahdollista toteuttaa valtakunnallisesti.

Ryhmät voitaisiin toteuttaa esimerkiksi siten, että tietoturvallisuusryhmässä käsiteltäisiin tietoon liittyviä riskejä, työ- ja toimitilaturvallisuusryhmässä näihin liittyviä riskejä, ja varautumisen ja valmiussuunnittelun ryhmässä jatkuvuussuunnitteluun ja poikkeusoloihin varautumiseen liittyviä asioita. Ryhmät pitäisivät yllä aihealuettaan koskevaa riskirekisteriä sekä tarvittavia viraston yhteisiä erillissuunnitelmia, raportoisivat viraston johdolle sekä ohjeistaisivat työnsä pohjalta vastuualueita ja koko virastoa.

Eri turvallisuuden osa-alueiden toteuttaminen erillisinä toimintoinaan edellyttää tiedonkulun ja koordinoinnin varmistamista sekä päällekkäisten toimenpiteiden ehkäisemistä. Siten riskienhallintakoordinaattori osallistuisi ryhmien työskentelyyn, ja ryhmiin nimettäisiin edustaja kaikilta vastuualueilta. Yksittäisiin turvallisuuden osa-alueisiin liittyvät vastuutehtävät voitaisiin tällöin osoittaa esimerkiksi viraston tietoturvallisuudesta vastaavalle henkilölle, työ- ja toimitilaturvallisuudesta vastaavalle henkilölle sekä varautumisen ja valmiussuunnittelun vastuuhenkilölle.

Edellä mainitut osa-alueet ovat osin päällekkäisiä ja yhteydessä toisiinsa, eikä niitä siten ole tarkoituksenmukaista toteuttaa toisistaan irrallisina ilman riskienhallinnan koordinointia. Sisäisen valvonnan ja eri turvallisuuden osa-alueiden sekä niitä koskevien suunnitelmien rooli ja osuus kokonaisuudessa on pyrittävä muodostamaan selkeäksi ja ymmärrettäväksi. Tässä yhteydessä on tarpeen keskustella ja määritellä riskienhallintaan liittyvien eri osa-alueiden väliset suhteet ja yhteys viraston toimintaan. Huomioitavia asioita ovat esimerkiksi se, että sisäisen valvonnan ja riskienhallinnan tarkoituksella ja toteuttamisella on välitön yhteys, tietojärjestelmien ja toimitilojen häiriöttömyydellä sekä henkilöstöllä on välitön yhteys vastuualueiden mahdollisuuksiin suoriutua tehtävistään, viraston päivittäisen toiminnan varmistamisella on yhteys häiriötilanteiden ja poikkeusolojen toimintaedellytyksiin, ja että asiakirjojen suojelusuunnitelma on luonnollinen osa tietoturvallisuutta.

Viraston riskienhallinnan kokonaisuuden koordinointia tukemaan voitaisiin hallintopalvelujen vastuuyksikön avuksi tarvittaessa perustaa viraston riskienhallintaryhmä. Ryhmää johtaisi riskienhallinnan koordinaattori, ja siihen nimettäisiin edustaja jokaiselta vastuualueelta ja eri

turvallisuuden osa-alueista huolehtivista työryhmistä. Ryhmä toteuttaisi riskienhallinnan kokonaisuuden yhteensovittamisen ja viraston kattavan riskienhallintaraportin kokoamisen. Ryhmän eduksi voidaan katsoa erityisesti yhdenmukaisen toiminnan edistyminen sekä riskien yhteisvaikutusten ja keskinäisriippuvuuksien tunnistaminen. Ryhmällä myös ehkäistäisiin riskienhallinnan koordinaattoriin liittyvää avainhenkilöriskiä ja riskienhallinnan eriytymistä omaksi toiminnokseen.

Aluehallintovirastolla on riskienhallinnan toteuttamista tukevia organisoinnin yhteydessä huomioitavia etuja jo toteutettujen turvallisuuteen liittyvien toimenpiteiden lisäksi; viraston työsuojelun vastuualueella on työturvallisuuteen ja turvallisuusjohtamiseen liittyvää ja pelastustoimen ja varautumisen vastuualueella onnettomuusvahinkojen ehkäisyyn sekä häiriötilanteisiin ja poikkeusoloihin liittyvää asiantuntemusta. Organisointiin liittyvänä haasteena on puolestaan se, että virastolla on toimintaa usealla paikkakunnalla ja useissa toimipisteessä.

Vastuita ja organisointia määriteltäessä on tarpeen huomioida myös palveluntuottajat, yhteistyökumppanit ja verkostot, erilliset projektit tai hankkeet sekä mahdolliset muut toiminnot ja tehtävät, joista virasto vastaa. Verkostojen ja projektien tai hankkeiden osalta voidaan noudattaa menettelyä, jossa nämä huomioivat riskienhallinnan osana toimintaansa ja pitävät viraston johdon tietoisena toimintaan liittyvistä riskeistä sekä sisällyttävät riskienhallinnan valmistelemiinsa dokumentteihin. Yhteistyökumppaneiden ja palvelutuottajien kanssa toimittaessa viraston tulee huomioida riskienhallinnan menettelyt esimerkiksi sopimuksin tai yhteisen riskienhallintaa koskevan suunnitelman avulla. Palveluntuottajien osalta tulee tarkastella sitä, millaisia riskienhallinnan menettelyitä virasto palveluntuottajilta edellyttää.

Aluehallintovirastojen hallinnollisten palvelujen kokoamista suunnittelevan hankkeen seurauksena tullaan hallintopalvelujen vastuuyksiöt mahdollisesti lakkauttamaan. Edellä esitettyjen vastuiden ja tehtävien näkökulmasta tulisi muutoksen yhteydessä varmistua siitä, että viraston kokonaisvaltaisen riskienhallinnan koordinointi olisi edelleen toteuttavissa viraston yhteydessä työskentelevän henkilön toimesta.

3. Riskienhallintamenettelyt

Riskienhallintaa tulee lähtökohtaisesti soveltaa kaiken päätöksenteon yhteydessä, mutta erityisesti strategisia päämääriä ja toiminnallisia tulostavoitetta asetettaessa sekä normaalissa viraston toiminnan ohjauksessa. Riskienhallintamenettelyjen osalta on tarpeen määritellä riskienhallintaprosessiin, riskien tunnistamiseen ja arviointiin sekä riskienhallintatoimenpiteisiin liittyviä tekijöitä. Menettelyt on tarkoituksenmukaista kuvata erillisessä menettelytapaohjeessa tai muussa riskienhallinnan toteuttamista tarkentavassa yhteydessä, ja niiden tavoit-

teeksi on suositeltavaa asettaa selkeys, käytännönläheisyys ja tarpeettoman dokumentoinnin välttäminen.

Riskienhallintaprosessin tulee olla systemaattinen ja jatkuva kehä. Sen tulee muodostua

- tarkasteltavan suojattavan kohteen rajauksesta. Kohde voi olla esimerkiksi yksittäinen strateginen päämäärä tai tulostavoite,
- kohdetta uhkaavan riskin tunnistamisesta,
- riskin arvioimisesta,
- hallintamenettelyn valinnasta,
- seurannasta ja
- raportoinnista.

Riskien tunnistamisen tarkoituksena on tunnistaa uhkaako jokin tarkasteltavaa kohdetta, kuten henkilöstön terveyttä, perustehtävän toteuttamista tai tulostavoitteen saavuttamista. Kohdeorganisaatiolla on tässä yhteydessä etuna se, että sisäisen valvonnan arvioinnin mukaan viraston perustehtävä, strategiset tavoitteet sekä toimintojen ja hankkeiden konkreettiset tulostavoitteet ovat selkeitä.

Riskejä ovat kaikki sellaiset epävarmuustekijät, jotka vaikuttavat haitallisesti tavoitteiden saavuttamiseen, keskeisiin toimintoihin tai muihin viraston määrittelemiin tarkastelun kohteena oleviin suojattaviin arvoihin. Riskien tunnistamisen ja myöhemmin riskirekisterien muodostamisen tueksi voidaan tarvittaessa päättää virastossa käytettävästä riskiluokittelusta ja edelleen laatia riskiluokkakohtaisista uhkaluetteloita tai tarkistuslistoja. Perinteisesti riskit luokitellaan strategisiin, operatiivisin, taloudellisiin ja vahinkoriskeihin tai esimerkiksi tiedollisiin riskeihin, mutta luokittelu voidaan tehdä millä tahansa tarkoituksenmukaiseksi katsotulla tavalla. Luokittelun pohjana voidaan esimerkiksi käyttää riskienhallinnalle määriteltyä tarkoitusta. On kuitenkin syytä muistaa, että eri riskiluokat ovat hyvin läheistä sukua keskenään ja monesti saman asian eri ilmenemismuotoja.

Tunnistaminen ja siihen kytkeytyvä riskien arvioiminen voidaan tehdä riskienhallinnan organisointiin ja tarkasteltavaan asiaan perustuen viraston johdossa, vastuualueella, turvallisuuden osa-alueista huolehtivissa ryhmissä tai muussa tarkoituksenmukaisessa yhteydessä. Organisoinnista riippumatta tunnistaminen ja arviointi tulisi tehdä ryhmätyönä, ja etenkin ensivaiheessa riskienhallinnan koordinaattorin on suositeltavaa osallistua työskentelyyn. Riskien tunnistaminen voidaan tehdä esimerkiksi siten, että:

- Viraston johto pyrkii tunnistamaan strategisten päämäärien toteutumista uhkaavia riskejä. Myös viraston toiminnan leikkaavia ydinprosesseja voidaan käsitellä. Tunnis-

tamista helpottamaan voidaan luoda uhkaluetteloita tai tarkistuslistoja, jotka strategian osalta voidaan jakaa esimerkiksi toimintaympäristöön, talouteen, henkilöstön määrään ja osaamisen sekä muihin toimintaedellytyksiin liittyviin tekijöihin. Tässä yhteydessä keskeistä on ulkoisen ja sisäisen toimintaympäristön muutostekijöiden tunnistaminen. Tulevaisuusskenaarioiden käyttäminen tukee tunnistamista.

- Viraston vastuualueet ja hallintopalvelujen vastuuyksikkö pyrkivät tunnistamaan omien tavoitteidensa toteutumista sekä keskeisiä toimintojaan ja ydinprosessejaan uhkaavia riskejä. Myös tulostavoitteiden ja keskeisten toimintojen osalta uhkia voidaan tunnistaa toimintaympäristöä, taloutta, henkilöstöä ja muita toimintaedellytyksiä tarkastellen. Riskejä tunnistettaessa kiinnitetään huomiota lainsäädännön ja hyvän hallintotavan toteutumiseen sekä viraston keskeisten strategisten riskien liittymiseen vastuualueen toimintaan. Suurilla vastuualueilla riskien tunnistamista esimerkiksi tulostavoitteiden osalta voi harkita toteutettavaksi myös yksiköittäin.

- Viraston henkilöstön turvallisuuteen, tietoon, toimitiloihin ja muuhun omaisuuteen sekä varautumistarpeeseen ja –menettelyihin liittyviä riskejä tunnistetaan näistä huolehtivissa työryhmissä viraston tarkoituksenmukaiseksi katsomalla organisoinnilla. Näidenkin osa-alueiden suhteen voidaan käyttää eri turvallisuuden osa-alueisiin liittyviä uhkaluetteloita tai tarkistuslistoja.

Viraston sisäinen keskinäinen kommunikaatio ja riskienhallinnan koordinointi on tässäkin yhteydessä tärkeää erityisesti riskien yhteisvaikutusten ja keskinäisriippuvuuksien tunnistamisen vuoksi. Riskienhallintaa koordinoiva ryhmä voi toimia tarvittavan kommunikaation välineenä. Laajojen ja monimutkaisten kartoitusten sijaan on kuitenkin erityisesti alkuvaiheessa syytä keskittyä olennaisimpiin seikkoihin.

Jos riskien tunnistamisvaiheessa käsitelty uhka todetaan suojattavan kohteen suhteen aiheelliseksi, muodostuu riski, jonka merkittävyys tulee arvioida. Riskin merkittävyyden arvioinnilla kyetään erottamaan kohtalokkaat riskit, merkittävää vahinkoa aiheuttavat riskit sekä seurauksiltaan pienet mutta usein realisoituvat riskit.

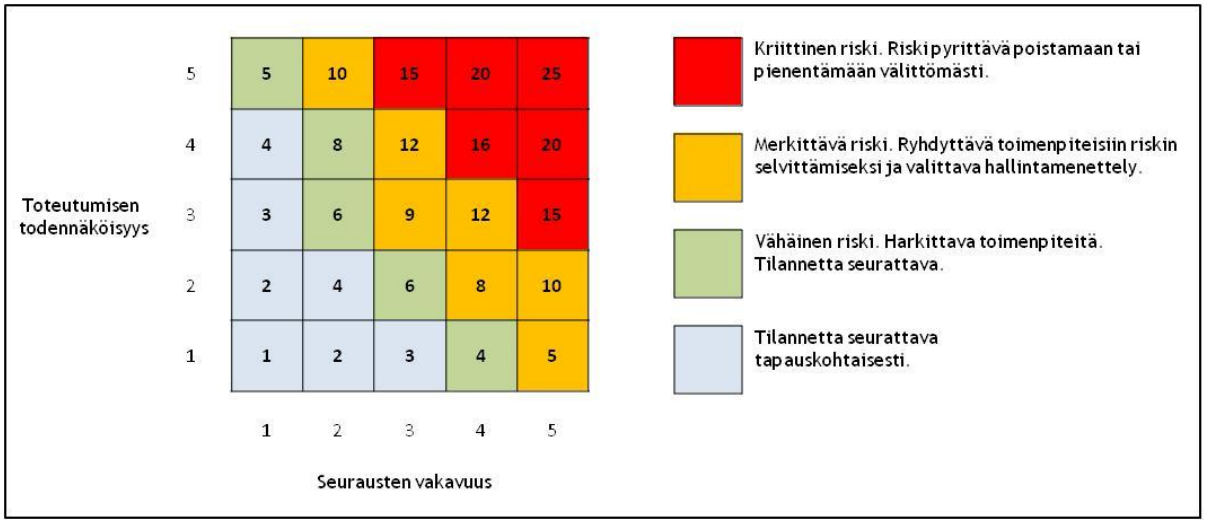
Riskin suuruus arvioidaan tavallisesti sen toteutumisen todennäköisyyden ja mahdollisten seurausten tulona (riskin suuruus = todennäköisyys x seuraukset). Vaihtoehtoisesti riskin seurausten vakavuutta voidaan korostaa, jolloin (riskin suuruus = todennäköisyys x vakavuus^2). Sekä todennäköisyyttä että seurauksia voidaan kuvata lukuarvolla 1-5, jolloin:

Lukuarvo	*Todennäköisyys*	*Seuraus*
1	Hyvin epätodennäköinen	Merkityksetön
2	Epätodennäköinen	Vähäinen
3	Lievästi todennäköinen	Kohtalainen
4	Melko todennäköinen	Merkittävä
5	Hyvin todennäköinen	Sietämätön

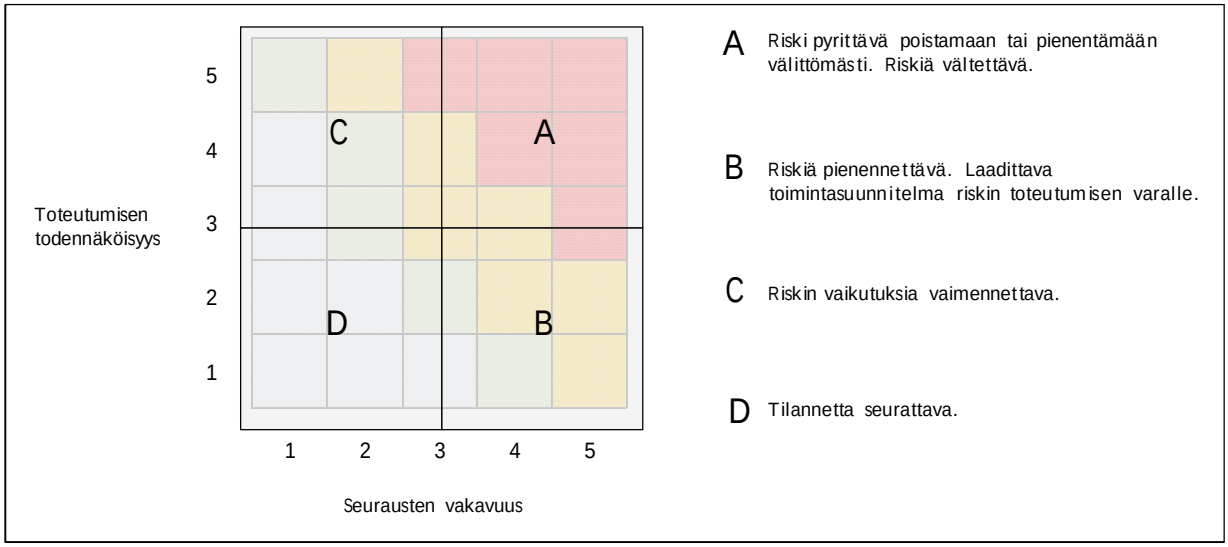
Toteutumisen todennäköisyyden arvioinnissa voidaan käyttää historiatietoa tai asiantuntija-arvioita. Lukuarvoille voidaan antaa esimerkiksi toteutumisen todennäköisyyden raja-arvoja tietyllä tarkastelujaksolla. Seurausten vakavuuden raja-arvojen asettaminen on vaikeampaa, mutta paikoin on mahdollista käyttää euromääräistä arviointia. Myös sanallisia arvioita voidaan käyttää, kunhan riskit kyetään asettamaan vakavuuden suhteen johonkin järjestykseen.

Riskin suuruutta arvioitaessa tulee uhkan ohella huomata myös virastossa toteutetut menettelyt, jotka jo suojaavat riskin toteutumiselta tai sen vaikutuksilta. Esimerkiksi tietoon, toimitiloihin ja työturvallisuuteen liittyviä riskejä on kohdeorganisaatiossa jo tunnistettu ja arvioitu, ja niihin liittyviä hallintamenettelyjä toteutettu.

Määrittelemällä riskin suuruus sen toteutumisen todennäköisyyden ja seurausten vakavuuden tulona voidaan riskin merkittävyys havainnollistaa esimerkiksi kuvan 1. kaltaisessa riskimatriisissa. Riskin merkitystä arvioitaessa voidaan myös korostaa todennäköisyyden ja vaikuttavuuden välistä suhdetta esimerkiksi kuten kuvassa 2. Kuvissa on esimerkkejä riskin suuruuteen perustuvasta riskienhallintatoimenpiteisiin ryhtymisestä.



Kuva 1. Riskin suuruuden määrittäminen sen toteutumisen todennäköisyyden ja seurausten vakavuuden tulona Liikenneviraston riskienhallinnan menettelytapaohjetta (Liikennevirasto 2012) mukaillen.



Kuva 2. Riskin merkityksen määrittäminen korostaen todennäköisyyden ja seurausten välistä suhdetta Viestintäviraston mallia (Arnell 2010) mukaillen.

Riskienhallintatoimenpiteitä ja riskinoton periaatteita voidaan lainsäädäntö ja ohjaavien ministeriöiden linjaukset huomioiden määritellä riskienhallintapolitiikassa tai vastaavassa asiakirjassa. Koska kaikkien riskien hallinta ei ole tarkoituksenmukaista, tulee riskienhallintatoimenpiteiden valinnan lähtökohtaisesti perustua lainsäädännön vaatimusten lisäksi kustannus- ja hyötyanalyysiin ohjaavien tahojen linjaukset huomioiden. Määriteltävänä on se, milloin riskienhallinnan keinoista syntyvät kustannukset ovat kohtuullisia verrattuna riskin toteutumisen aiheuttamaan menetykseen. Tässä yhteydessä on tarpeen määritellä riskinottohaluk-kuus ja siihen perustuvat kynnykset, jolloin riskin toteutumisen aikaan sama tila a) edellyttää toimenpiteisiin ryhtymistä, ja b) on sietämätön. Lisäksi on syytä huomioida vähäisiltä tuntuvien riskien mahdolliset yhteis- ja seurannaisvaikutukset.

Riskienhallinnan periaatteilla voidaan linjata myös riskienhallintaan liittyviä strategisia valintoja. Ottaen huomioon organisaation yhteyden valtiokonserniin ja julkisten palvelujen tuottamiseen ei ole perusteltua valita riskejä ottavaa tai muuta matalan riskienhallinnan strategiaa ilman, että asiasta vallitsee yhteisymmärrys ohjaavien tahojen kanssa. Organisaation toiminnan luonne ei myöskään mahdollista riskien siirtämiseen painottunutta strategiaa. Riskejä tulee siten hallita lähtökohtaisesti viraston omin toimenpitein, joista riskityypin ja sen suuruuden perusteella voidaan valita riskin poistamiseen, välttämiseen, pienentämiseen tai hyväksymiseen perustuvia toimenpiteitä. Hallintatoimenpiteen valintaa tukee riskin perussyyn tunnistaminen. Tarvittaessa tulee myös varautua riskin toteutumiseen.

Jokaiselle tunnistetulle riskille tulee osoittaa vastuuhenkilö, ja toimenpiteiden kohteeksi otetulle riskille lisäksi aikataulu. Vastuu sisältää tarvittavat hallintatoimenpiteet ja aikataulut, seurannan, valvonnan ja raportoinnin.

Riskien tunnistamisen ja arvioimisen yhteydessä tulee muodostaa esimerkiksi vastuualuekohtaista riskirekisteriä, jota voidaan edelleen täydentää hallintatoimenpiteitä valittaessa. Riskeistä merkittävimmät tulee edelleen koota viraston yhteiseen riskirekisteriin, jota ylläpitää viraston riskienhallinnan koordinaattori. Viraston yhteinen kokoava riskirekisteri voi sisältää esimerkiksi 10-15 merkittävintä riskiä, ja on tavallista, että se painottuu viraston strategian toteutumista ja tulostavoitteiden saavuttamista uhkaaviin riskeihin. Riskirekisterit voivat myöhemmin toimia seurannan ja sekä viraston johdolle että virastoa ohjaaville tahoille tehtävän riskiraportoinnin runkona. Rekisterin kaltaisen kokoavan menettelyn keskeinen merkitys on siinä, että se mahdollistaa viraston toimintaan liittyvän riskikokonaisuuden hallinnan.

Jos mahdollista, on tunnistetut ja arvioidut riskit syytä kuvata kiinnittämällä ne lisäksi viraston prosessien kuvauksiin. Sekä rekisteriin että mahdollisiin prosessikuvauksiin voidaan merkitä esimerkiksi:

- riskin nimi ja yleiskuvaus
- riskin luokittelu esimerkiksi henkilö- tai tietoriskeihin ja tarvittaessa tiettyyn vastuualueeseen
- riskin toteutumisen seuraukset
- riskin toteutumisen todennäköisyys jollakin tarkastelujaksolla
- riskin toteutumisen syyt
- päätetyt riskienhallintatoimenpiteet aikatauluineen ja vastuineen
- vaikutuksiin, todennäköisyyteen ja hallintatoimenpiteisiin perustuva riskin merkittävyys.

4. Seuranta ja raportointi

Riskienhallintaan liittyvällä seurannalla ja raportoinnilla seurataan tunnistettujen riskien ja niitä koskevien hallintatoimenpiteiden tilaa ja vaikuttavuutta sekä viraston riskienhallinnan tilaa. Seurannan avulla pidetään sekä viraston johto että virastoa ohjaavat tahot tietoisena keskeisistä viraston toimintaan liittyvistä riskeistä ja tuetaan siten päätöksentekoa. Seurannan avulla myös havaitaan riskienhallinnan kehittämistarpeita. Seurannan toteutuminen edellyttää sitä tukevaa raportointia.

Seuranta ja raportointi on suositeltavaa sitoa viraston ja sen vastuualueiden johtamisen ja suunnittelun menettelyihin. Vastuualueiden sisäisten menettelyjen mahdollista eroista riippumatta voidaan noudattaa esimerkiksi periaatetta, jossa:

- riskin vastuuhenkilö vastaa riskin ja sille kohdistetun riskinhallintatoimenpiteen toteutumisen seurannasta ja raportoi riskirekisterin haltijalle tarkoituksenmukaiseksi katsotuin väliajoin.

- Riskirekisterin haltija (esimerkiksi riskienhallinnan koordinaattori, vastuualue, tietoturvallisuuden vastuuhenkilö) seuraa rekisterinsä riskien ja niitä koskevien hallintatoimenpiteiden tilaa ja raportoi viraston johdolle muun säännöllisen raportoinnin yhteydessä. Vastuualueen tulee tuoda viraston johdon tietoon havaitsemansa uudet riskit tai tunnistettuja riskejä koskevat muutokset. Tieto on aina saatettava myös riskienhallinnan koordinaattorille viraston riskirekisterin ylläpitämiseksi.

- Johdolle tehtävän säännöllisen raportoinnin lisäksi voidaan toteuttaa erillinen riskienhallintaan keskittyvä johdon katselmointi esimerkiksi vuosittain. Katselmointia varten viraston riskienhallinnan koordinaattori kokoaa ylläpitämänsä viraston kokoavan riskirekisterin ja vastuualueiden raporttien pohjalta yhdessä riskienhallintaryhmän kanssa riskienhallinnan tilaa ja kehittämistarpeita koskevan raportin.

- Viraston johto raportoi keskeisistä riskeistä ja riskienhallinnan tilasta ohjaaville tahoille tulosohjausprosessin yhteydessä. Keskeisenä menetelmänä toimii toimintakertomus ja siihen liittyvä sisäisen valvonnan ja riskienhallinnan vahvistuslausuma, mutta menettelynä voi lisäksi olla erillinen ja tarkempi raportointi.

Seurannan ja raportoinnin menettelyistä riippumatta viraston riskienhallinnan koordinaattorin tulee olla riskien tilasta tietoinen, jotta viraston kokoavan riskirekisterin ylläpito on mahdollista. Myös havaitut riskienhallintaan liittyvät kehittämistarpeet tulee saattaa koordinaattorin tietoon. Seurantaa tukevina välineinä voidaan käyttää esimerkiksi asiakas- ja sidosryhmäpalautteita, jonka lisäksi on suositeltavaa varmistua poikkeamaraportoinnin käytännöistä.

Riskienhallinnan tilan arvioimiseksi tulee toteuttaa sisäistä arviointia. Sisäinen arviointi voidaan toteuttaa nykyisen menettelyn mukaisesti säännöllisesti sisäisen valvonnan ja riskienhallinnan tilaa tarkastelevana arviointina esimerkiksi tilinpäätöksen ja toimintakertomuksen yhteydessä valtiovarain controller –toiminnon antaman suosituksen avulla. On suositeltavaa, että arviointi tehtäisiin ainakin tietyin väliajoin suosituksen laajaa arviointikehikkoa käyttäen aluehallintoviraston riskienhallinnan tarkoituksen määrittely huomioiden. Sisäinen arviointi on lähtökohtaisesti sisäisen tarkastuksen tehtävä. Arvioinnin tulosten tulee heijastua riskienhallinnan toimintasuunnitelmaan tai muuhun vastaavaan kehittämistoimenpiteitä kokoavaan dokumenttiin.

5. Dokumentointi

Kokonaisvaltaisen riskienhallinnan keskeinen elementti on riskienhallintaa koskeva systemaattinen dokumentointi. Ylimitoitettua dokumentaatiota tulee kuitenkin pyrkiä välttämään. Dokumentoinnin menettelyt on siten tarkoituksenmukaista määritellä. Tässä yhteydessä tulee kiinnittää huomiota siihen, ettei asiakirjojen keskinäisissä suhteissa ole epäselvyyksiä, ja että viraston henkilöstö perehdytetään niihin ja niiden yhteyteen omiin työtehtäviin. Riskienhallintaan liittyvän dokumentoinnin runko voi muodostua esimerkiksi seuraavista asiakirjoista:

- Aluehallintovirastoille yhteiseksi laadittavat riskienhallinnan periaatteet tai riskienhallintapolitiikka. Jos aluehallintovirastoille ei laadita yhteistä linjaavaa asiakirjaa ja aluehallintovirasto muodostaa periaatteet itsenäisesti, tulisi ohjaavien tahojen linjausten kuitenkin välittyvä näihin.
- Aluehallintovirastojen tietoturvallisuuspolitiikka. Tietoturvallisuuspolitiikka siihen sisältyvine asiakirjoineen määrittää tietoturvallisuuteen liittyvien toimenpiteiden kokonaisuuden.
- Aluehallintovirastojen yhteinen tai virastokohtainen riskienhallinnan menettelytapaohje tai muu riskienhallinnan toteuttamista käytännössä tarkentava ohje. Ohjeet voivat olla myös esimerkiksi vastuualuekohtaisia, mutta niiden tulee noudattaa viraston riskienhallinnasta annettuja periaatteita.
- Aluehallintovirastokohtainen riskienhallinnan toimintasuunnitelma. Toimintasuunnitelma voi toimia riskienhallinnan vuosiohjelmana, jossa päätetään tarvittavista riskienhallintaa koskevista kehittämistoimenpiteistä. Ohjelma voi olla esimerkiksi kaksivuotinen, jolloin jälkimmäisen vuoden toimenpiteet tarkentuvat ensimmäisen vuoden tulosten pohjalta. Ohjaavien tahojen linjaukset välittyvät myös näihin.
- Sisäisen tarkastuksen ohjesääntö. Jo laadittu viraston ohjesääntö tarkastelee muun muassa sisäisen tarkastuksen asemaa, valtuuksia, tehtäviä ja niiden toteuttamista sekä raportointia. Riskienhallinasta tehdyt linjaukset ja ohjesääntö tulee sovittaa yhteen.
- Riskirekisterit. Viraston yhteinen keskeiset riskit kokoava riskirekisteri, vastuualuekohtainen riskirekisteri ja mahdolliset ydinprosesseja tai turvallisuuden osa-alueita koskevat riskirekisterit. Rekisterit voivat pitää sisällään riskikohtaiset hallintasuunnitelmat.
- Yksittäisiä turvallisuuden osa-alueita koskevat suunnitelmat, kuten työsuojelun toimintaohjelma, pelastussuunnitelma ja valmiussuunnitelma.

Kokonaisuuden hallitsemiseksi on suositeltavaa määritellä missä muissa asiakirjoissa riskienhallinta huomioidaan. Esimerkiksi:

- Riskienhallintaan liittyviä tavoitteita voidaan ottaa esille viraston strategiassa sekä strategisissa ja toiminnallisissa tulossopimuksissa. Keskeistä on kiinnittää huomiota tavoitteiden ja muun määrittelyn yhdenmukaisuuteen tilanteessa, jossa virastoa ohjaavat useat eri tahot.
- Riskienhallintaan liittyvien vastuiden tulee käydä ilmi myös viraston, vastuualueiden ja hallintopalvelujen vastuuyksikön työjärjestyksistä.
- Riskit voidaan esittää viraston prosessikuvauksissa.
- Riskeistä ja riskienhallinnan tilasta raportoidaan sisäisesti sisäisen raportoinnin asiakirjoin ja ulkoisesti esimerkiksi toimintakertomuksen yhteydessä.
- Riskienhallintaan liittyviä menettelyitä ja tavoitteita voidaan käsitellä verkostojen ja hanke- tai projektien suunnitelmissa ja muissa näihin liittyvissä asiakirjoissa sekä yhteistyökumppaneiden ja palvelutuottajien kanssa laadittavissa sopimuksissa.

6. Aikataulutus

Riskienhallinta tulee kytkeä osaksi viraston tavanomaista toimintaa ja siten toiminnan suunnitteluun sekä muuhun johtamiseen ja raportointiin. Lähtökohtaisesti riskit tunnistetaan ja arvioidaan sekä menettelyt niiden hallitsemiseksi valitaan aina kulloisenkin päätöksenteon yhteydessä, ja raportointi tapahtuu muun säännöllisen raportoinnin yhteydessä. Käytännössä tämä voi tarkoittaa esimerkiksi sitä, että:

- strategisten ja toiminnallisten tulossopimusten valmistelun yhteydessä viraston johdossa ja vastuualueilla tunnistetaan ja arvioidaan näihin sisältyvien tavoitteiden saavuttamiseen liittyvät riskit.
- Asetettuja tavoitteita koskevien riskien tunnistaminen, arviointi ja hallintatoimenpiteistä päättäminen tehdään tulossopimusten valmistuttua. Valittujen hallintamenettelyjen ja riskin tilaa arvioidaan puolivuotisraportoinnin yhteydessä.
- Jos viraston yhteisiä tai vastuualueiden ja hallintopalvelujen vastuuyksikön keskeisiä tehtäviä, ydinprosesseja tai muuta toimintaa jää tämän tarkastelun ulkopuolelle, voidaan niihin liittyvät riskit käsitellä omana projektinaan. Tulosten tulee kuitenkin välittyä asianomaisiin riskirekistereihin ja johdon tietoon. Mahdollisia uusia prosessikuvauksia laadittaessa voidaan toteuttaa niitä koskeva riskianalyysi.
- Yksittäisiä turvallisuuden osa-alueita koskevien riskien osalta voidaan tunnistaminen, arvioiminen ja hallintamenettelyistä päättäminen tehdä omina projekteinaan näitä koskevissa työryhmissä. Tulosten tulee välittyä asianomaisiin riskirekistereihin ja johdon tietoon.
- Hankkeiden ja muiden tulosohjauksen ulkopuolisten päätösten yhteydessä tunnistetaan ja arvioidaan niitä uhkaavat riskit ja päätetään hallintamenettelyistä. Tulosten tulee välittyä asianomaisiin riskirekistereihin ja johdon tietoon.

- Riskienhallintaan keskittyvä johdon katselmointi voidaan toteuttaa esimerkiksi puolivuotisraportoinnin yhteydessä.
- Riskienhallinnan tilaa arvioidaan toimintakertomuksen laadinnan yhteydessä.
- Tarvittava mahdollisesti vuosittainen koulutus voidaan järjestää ennen tulostavoitteisiin liittyvien riskien tunnistamista.

Kokonaisvaltaiseen riskienhallintaan liittyvät aikataulut on tarkoituksenmukaista esittää viraston toiminnan vuosikellossa.