HAAGA-HELIA
ammattikorkeakoulu

Eduskunnan kanslian tietohallinnon riskienhallinnan kehittäminen

Antti Laulajainen

Opinnäytetyö
Liiketalouden ylempi
ammattikorkeakoulututkinto
Tietojärjestelmäosaamisen
koulutusohjelma
2015

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

12.5.2015

Tekijä(t)
Laulajainen Antti

Koulutusohjelma
Tietojärjestelmäosaamisen koulutusohjelma

Opinnäytetyön otsikko
Eduskunnan kanslian tietohallinnon riskienhallinnan kehittäminen

Sivu- ja liitesivumäärä
161 + 74

Eduskunnan kanslian tietohallintotoimisto tuottaa eduskunnan toiminnan kannalta keskeiset tietojärjestelmät, joiden toimivuus on oltava korkealla tasolla eduskunnalle asetettujen tehtävien saavuttamisen mahdollistamiseksi. Riskienhallinta on tämän varmistamisessa tärkeässä roolissa. Riskienhallinnalla voidaan ennakoida epävarmuudet, jotka voisivat estää organisaation toiminnan

Tutkimuksen tavoitteena oli kehittää tietohallintotoimistolle soveltuva mallia riskienhallintaan. Lisäksi selvitettiin, minkälaisia tarpeita toimistolla oli riskienhallinnalle ja miten sen toiminnassa voitaisiin tunnistaa, analysoi ja priorisoi riskejä.

Tutkimus toteutettiin toimiston sisäisenä kehitysprojektina. Opinnäytetyönä tehtävässä kehittämistehtävässä käytettiin konstruktiivista tutkimusmenetelmää ja haastatteluja sekä dokumenttianalyysia. Tutkimuksessa luotiin teoriatausta, kartoitettiin tarpeet riskienhallinnalle, analysoitiin nykytila ja näiden pohjalta kehitettiin riskienhallinnan malli.

Tutkimuksen teoriataustassa käytännönlähteinä käytettiin COSO riskienhallintamallia, ISO-standardia sekä VAHTI-ohjeistusta. Lisäksi haastateltiin muiden organisaatioiden riskienhallinnan ammattilaisia. Näitä tietoja täydennettiin kirjallisuuskatsauksella ja aiemmilla tutkimuksilla. Tietohallintotoimiston tarpeet riskienhallinnalle kartoitettiin haastattelemalla toimiston johtoryhmä. Riskienhallinnan nykytila arvioitiin dokumenttianalyysilla.

Konstruktiona kehitettiin tietohallintotoimistolle soveltuva riskienhallinnan malli. Malli koostuu yleisistä riskienhallinnan periaatteista, riskienhallinnan toteutuksen kuvaavasta puitekuvauksesta sekä riskienhallinnan käsikirjasta, jossa on kuvattu riskienhallinnan käytännön työskentely. Lisäksi kehitettiin näitä tukevia työkaluja.

Mallin toimivuus testattiin dokumenttien hyväksynnällä, käsittelemällä aikaisemmin tunnistettuja riskejä uudelleen sekä tekemällä kokonaan uusi riskienarviointi. Testausten perusteella voitiin todeta luodun mallin olevan toimiva, vaikka sen pitkäaikaista käyttöä ei voitu testata.

Tutkimuksen johtopäätöksenä on, että jos organisaatiolla on olemassa kevyt malli riskienhallintaan, luomalla sitä tukemaan määrämuotoinen kokonaisvaltaisempi hallintamalli, voidaan riskienhallinnan tehokkuutta huomattavasti parantaa. Jatkokehityksenä mallia tulisi soveltaa toimiston toimintaan ja mahdollisti myös laajemmalti eduskunnan kansliassa.

Asiasanat
Riskienhallinta, tietoturva, laatujohtaminen

HAAGA-HELIA
ammattikorkeakoulu

Abstract

12.5.2015

Author
Laulajainen Antti

Degree Programme
Master's Degree Programme in Information Systems Management

The title of the thesis
Risk management development at the IT-office of The Parliament of Finland

Number of report pages and attachment pages
161 + 74

The IT-office of the Parliament produces the information processing systems which are central from the point of view of the operation of the Parliament. The functionality of these systems must be a high level to make reaching of the tasks set for the Parliament possible. Risk management has an important role in the securing of this. Risk management can be used to anticipate the uncertainties which could undermine the operation of the organisation.

The objective of the study was to develop a suitable model for risk management for the IT-office. Furthermore the needs for risk management that there were at the office were recognised. Also it was clarified how the office could identify, analyse and prioritise its risks.

The study was carried out as an internal development project. In the developing task, which was done as a dissertation, a constructive research method and interviews and document analysis were used. In the study, a theory background was created, the needs for risk management were identified, a present state was surveyed, and, based on these, the model of risk management was developed.

In the theory background, constructive sources were COSO -risk management model, ISO-standard and VAHTI-guidelines. Furthermore, professionals in risk management at other organisations were interviewed. This information was supplemented by source literature that included studies. The needs of the IT-Office in risk management were surveyed by interviewing the management team of the office. The present state of risk management was estimated with a document analysis.

The risk management model which is suitable for the IT-office was developed by using constructive research approach. The model consists of the general principles of risk management, from the settings description which covers the implementation of risk management and from the manual in risk management in which the risk management practices have been described. Furthermore, supporting tools for the implementation were developed.

The functionality of the model was tested with the approval of documents by dealing again with risks that had been identified earlier and by a making totally new risk evaluation. On the basis of the testing one can state that the created model was operating even though it was not possible to test its long time use.

The conclusion of the study is that if at the organisation a light model existed of managing risks has, the effectiveness of risk management can be increased by creating a more comprehensive management model to support it. For further studies, the model should be adapted to the operation of the IT-office as a further development and possibly implemented on a larger scale in the office of the Parliament.

Key words
Risk management, information security, quality management

Sisällys

Kuviot

Taulukot

1 Johdanto

Riskienhallinnan merkitystä ei nykyisin juurikaan kyseenalaisteta organisaatioiden toiminnan osana. Erityisesti yksityissektorin toimijat tekevät aktiivista riskienhallintaa osana liiketoimintansa hallintaa ja toiminnan turvaamiseen tähtäävää yritysturvallisuutta. Myös julkisen sektorin organisaatiot tekevät riskienhallintaa toimintansa osana. Määritelmänä riskienhallinta on epävarmuustekijöiden hallintaa. Epävarmuustekijät ovat ulkoisten ja sisäisten tekijöiden vaikutuksia, jotka vaikeuttavat tai estävät organisaatioita saavuttamasta sille asetettuja tavoitteitaan.

1.1 Riskienhallinta yksityisellä ja julkisella sektorilla

Epävarmuustekijöiden vaikutuksia tavoitteisiin kuvataan riskeinä. Jokainen organisaatio kohtaa toiminnassaan riskejä. Organisaatioiden johdon on päätettävä kuinka paljon riskejä ja siten epävarmuustekijöitä se voi hyväksyä asetettujen tavoitteiden saavuttamiseksi. Johdon työkaluna epävarmuustekijöiden hyväksyttävissä rajoissa pitämiselle on riskienhallinta. Riskienhallinta on siis määrämuotoista toimintaa organisaation riskien tunnistamiseksi, analysoimiseksi, riskien merkityksen ymmärtämiseksi toimintaan nähden sekä niiden valvomiseksi. (Marchetti 2012, 2; SFS-ISO 2011, 6; VTT 2007.)

Häiriöiden ja muiden epävarmuustekijöiden hallitsemiseksi edellytetään toimenpiteitä. Yksityinen sektori tekee oman liiketoimintansa riskien hallitsemiseksi riskienhallintaa taloudellisesta näkökulmasta sekä osana yritysturvallisuutta. Yritysturvallisuuden mitoittamisen ja määrittämisen keskeinen edellytys on uhkien tunnistaminen ja arviointi. Riskien todennäköisyyksiä ja muutoksia on jatkuvasti seurattava ja tarkistettava (Elinkeinoelämän keskusliitto 2014.)

Julkisen sektorin riskienhallinta on myös vahvasti ollut osa taloushallintoa ja tarkastustoimintaa. Holmbergin (2013) mukaan tavoitteet julkishallinnon riskienhallinnalle voidaan tiivistää seuraavasti:

- Edistää tuloksellisuutta pitämällä toiminnan riskit hallinnassa.
- yhtenäistää organisaation käsitystä toimintaa uhkaavista riskityypeistä ja niiden merkityksestä.
- Pienentää tuloksiin kohdistuvia uhkia.
- Yhtenäistää ja selkiyttää toimintatapoja ja prosesseja.
- Lisää luottamusta hallintoon.
- Riskienhallinta sisältää myös ajallisen ulottuvuuden ja pakottaa arvioimaan toiminnan vaikutusta tulevina kausina ja tuleviin sukupolviin.

Tietohallinnon riskienhallinnan merkitys on korostunut liiketoiminnan muuttuessa riippuvaisuudesta tietojärjestelmistä ja tietoverkoista. Myös yhteiskunnan julkisten palvelujen

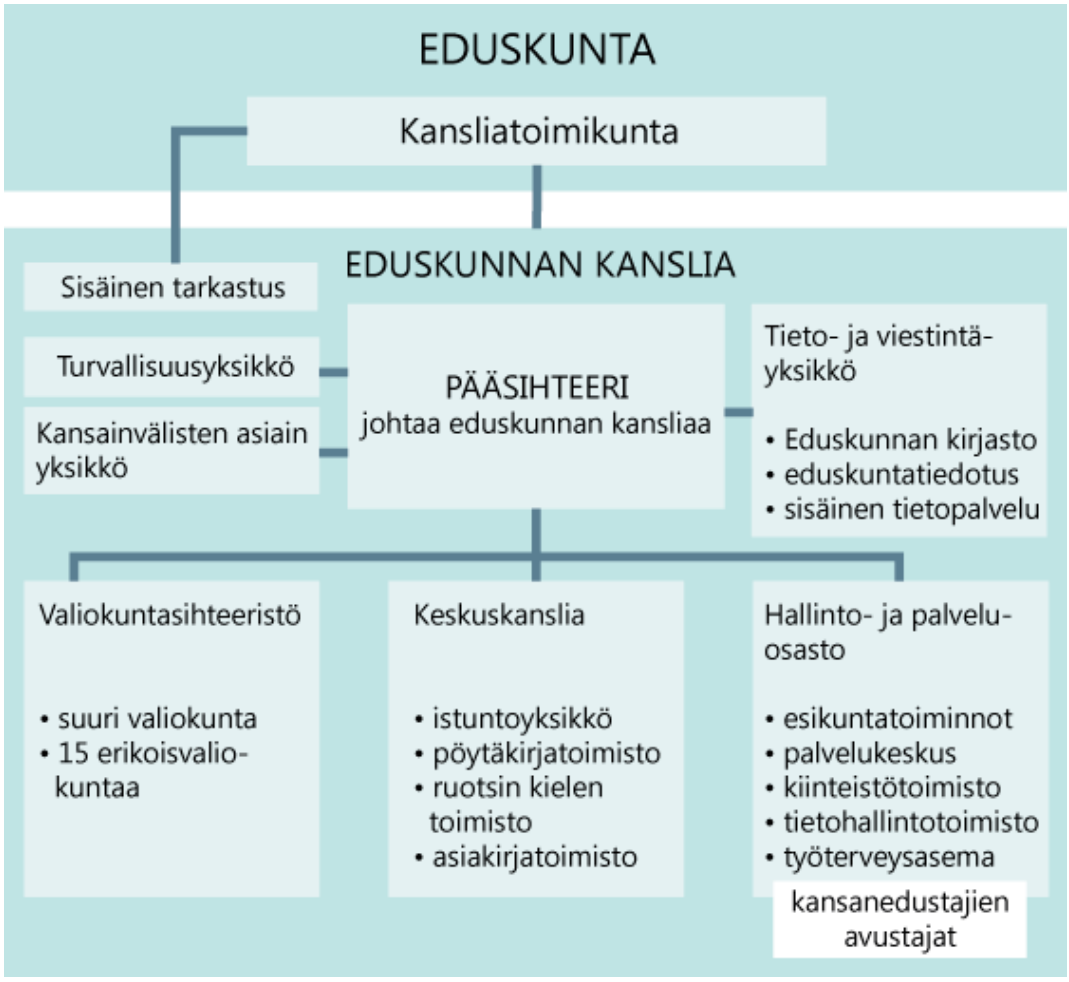
sähköisen asioinnin kehittyminen on tehnyt niiden tuottamisen riippuvaiseksi verkoista ja järjestelmistä. Molemmilla sektoreilla organisaatioiden sisäinen toiminta on myös täysin näiden varassa. Voidaankin todeta, että Suomi on tietoyhteiskuntana riippuvainen järjestelmien ja verkkojen toiminnasta ja näin ollen erittäin haavoittuvainen näihin kohdistuvista häiriöistä (Turvallisuus- ja puolustusasiain komitean sihteeristö 2013, 1).

Julkishallinnon osalta on riskienhallintaa korostettu sekä säädetty viime vuosina yhä voimakkaammin osaksi organisaatioiden johtamista sekä tietoturvallisuuden hallintaa. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681 5 § määrittelee yleiseksi tietoturvallisuusvelvollisuudeksi viranomaisen toimintaa liittyvien riskien kartoittamisen. Suomen kyberturvallisuusstrategian osana on ministeriöille määritelty kyberturvallisuustehtäviä. Ministeriöiden ja hallinnonalojen tulee analysoida riskinsä ja haavoittuvuutensa. Kokonaisriskienhallinta edellyttää myös yhteiskunnan toiminnan kannalta kriittisten tietojärjestelmien priorisointia, säännöllistä auditointia ja itsearviointia riskienarvioinnilla ja kolmansien suorittamana. (Turvallisuuskomitea 2014.)

Vaikka edelliset velvoitteet eivät suoraan velvoita tai ohjaa eduskunnan toimintaa, ei niitä voida jättää huomioimatta eduskunnan johtamisessa ja palvelujen tuottamisessa. Eduskunnan asema on keskeinen yhteiskunnassa ja sen tehokas toiminta on riippuvaista tietojärjestelmien ja verkkojen toiminnasta. Tätä varten on eduskunnan tietohallintotoimiston riskienhallinta oltava kattavaa ja tehokasta, jotta se voisi vastuualueellaan huolehtia palveluiden turvallisuudesta, jatkuvuudesta ja saatavuudesta.

1.2 Kohdeorganisaation esittely

Eduskunta säätää Suomessa kaikki lait ja päättää valtion talousarviosta, eduskunta myös valvoo maan hallituksen toimia sekä valitsee pääministerin. Lisäksi eduskunta hyväksyy tärkeimmät Suomea sitovat kansainväliset sopimukset ja vaikuttaa Euroopan unionin asioihin. Eduskunnan hallintoa johtaa kansanedustajista koostuva kansliatoimikunta. Kansliatoimikunta nimittää eduskunnan korkeimmat virkamiehet sekä ratkaisee eduskunnan hallintoa ja taloudenpitoa koskevat merkittävät asiat. (Eduskunta 2015a; Eduskunta 2015b) Eduskunnan hallinnon organisaatio on kuvattu seuraavassa kuviossa (kuvio 1).



Kuvio 1 Eduskunnan hallinnon organisaatiorakenne (Eduskunta 2015b)

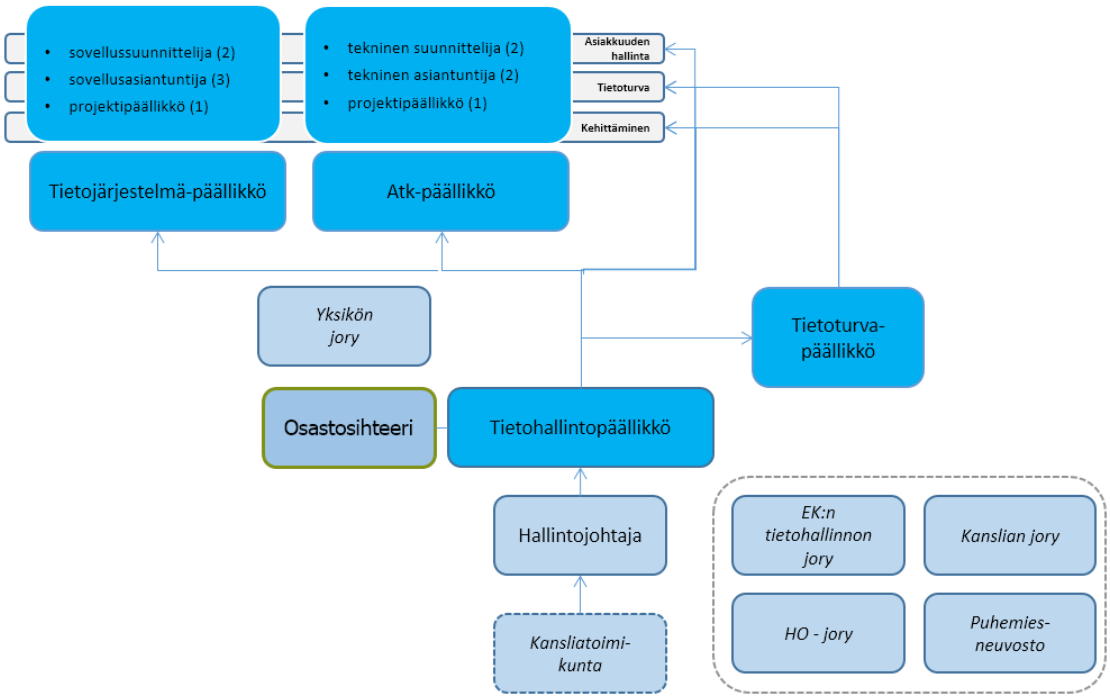
Eduskunnan kanslian tehtävänä on luoda eduskunnalle edellytykset hoitaa sille valtioelimenä kuuluvat tehtävät. Eduskunnan virkamiehet huolehtivat siitä, että eduskunnan toimielimillä ja kansanedustajilla on edellytykset hoitaa perustuslaissa ja eduskunnan työjärjestyksessä tarkoitetut tehtävät. Pääsihteerin johtamassa eduskunnan kansliaan kuusi toimintayksikköä huolehtivat lainsäädäntö- ja valiokuntatyöhön, kansainvälisiin asioihin, tieto- ja viestintäpalveluihin, hallintoon sekä turvallisuuteen liittyvistä tehtävistä. (Eduskunta 2015b.) Eduskunnan kanslian tietohallintotoimisto toimii osana hallinto- ja palveluosastoa.

Eduskunnan kanslian ohjesäännön 320/1987 13 a §:n mukaan tietohallintotoimisto vastaa tietotekniikan tai tietojärjestelmien hankkimisesta, käytöstä, huollosta, kehittämisestä, kehittämisen koordinoinnista ja näihin liittyvästä tietoturvasta. Eduskunnan tietohallinnon vision (2013) mukaan tietohallinto järjestää ja tuottaa asiakkailleen eduskunnan toiminnan edellyttämät tieto- ja viestintätekniikan palvelut laadukkaasti, tehokkaasti ja taloudellisesti. Toiminnassaan tietohallinto toteuttaa eduskunnan kanslian strategisia päämääriä. Tämä näkyy erityisesti tietoteknisen infrastruktuurin ja palvelujen toimintavarmuuden kehittämisessä. Palveluja kehitetään innovatiivisesti valituilla alueilla kehityksen kärjessä. Tietohal-

lintolinjauksen tavoite on suunnata eduskunnassa kehittämisen rajallisia resursseja siten, että tietohallinto omalta osaltaan mahdollistaa eduskunnan kanslian palvelujen tuottamisen ja toiminnan kehittäminen.

Tietohallintotoimistoa johtaa tietohallintopäällikkö. Hänen sijaisenaan toimii ATK-päällikkö, joka myös vastaa perustietotekniikan palveluista ja toimii esimiehenä perustietotekniikkatiimille. Tietojärjestelmäpäällikkö vastaa sovelluspalveluista ja toimii esimiehenä sovelluspalvelutiimille. Tietoturvapäällikkö vastaa hallinnollisesta tietoturvasta ja sen kehittämisestä. Teknisen tietoturvan vastuut ovat palveluita tuottavissa tiimeissä. Päälliköt muodostavat toimiston johtoryhmän.

Tietohallintopäällikkö raportoi toiminnastaan hallintojohtajalle, joka johtaa koko hallinto- ja palveluosastoa. Tämän lisäksi ohjaavana toimielimenä toimii tietohallinnon johtoryhmä. Eduskunnan tietohallinnon johtoryhmän muodostavat kanslian yksijöiden johtajat sekä kansanedustaja että avustajien edustajat. Seuraavassa kuviossa (kuvio 2) on esitetty tietohallintotoimiston organisaatiorakenne ja sen toimintaan vaikuttavat johtamisfoorumit.



Kuvio 2 Tietohallintotoimiston organisaatiorakenne ja johtamisfoorumit (Eduskunta 2013)

Tietohallintotoimisto palvelujen tuotantomalli on ulkoistettu malli. Tietohallintotoimisto hankkii tietoliikennepalvelut, palvelinten käyttöpalvelut, työasemapalvelut ja sovelluspalvelut yhteistyökumppaneilta. Oma henkilöstö vastaa palveluiden ohjauksesta ja kehittämisestä. Loppukäyttäjätuki on myös oman henkilöstön tuottamaa, mutta tietohallintotoimisto

ei vastaa tuen ohjauksesta. Tukiorganisaatio toimii osana hallinto- ja palveluosaston palvelukeskusta, joka vastaa loppukäyttäjätuesta.

1.3 Motivaatio kehittämiselle, tavoitteet ja rajaukset

Eduskunnan kansliassa käynnistettiin 2014 keskitetty riskienhallinnan kehittäminen. Alkuvaiheessa kanslian eri yksiköt arvioivat omia operatiivisia riskejään, joista saatiin tuloksena kanslian toiminnan yhteiset riskit. Tietohallintotoimisto teki oman riskianalyysinsä, jonka yhtenä riskienhallintatoimenpiteenä on kehittää tietoturvanhallintaa määrämuotoisemmaksi. Riskienhallinta on keskeinen toiminto tietoturvanhallinnalle ja sen kehittäminen asetettiin tavoitteeksi tietohallintotoimistolle. Lisäksi eduskunnan ylin johto, kansliatoimikunta, on määritellyt riskienhallinnan kehittämisen yhdeksi vuoden 2015 kehityskohteiksi koko eduskunnassa. Tietohallintotoimisto tuottaa myös kaikille muille yksiköille ja osastoille keskeisiä palveluita, joiden toiminnasta yksiköiden toiminta on riippuvaista. Erityistä huomiota vaativat eduskunnan ydintoimintoon, lainsäädäntöön liittyvät palvelut ja niiden riskienhallinta ja jatkuvuus. Riskienhallinnan kehittämisen motivaatioksi muodostui siten oman toiminnan kehittämistarpeet, eduskunnan muun toiminnan turvaaminen sekä organisaation johdon tahtotila.

Tietohallintotoimiston riskienhallinnan kehittämisen tavoitteena oli kehittää määrämuotoinen riskienhallinnan malli, joka sisältää riskienhallinnan viitekehyksen ja prosessin sekä kehittää edelleen riskianalyysiin liittyviä työkaluja ja dokumentaatiota. Kehitetyn mallin avulla tietohallintotoimiston riskienhallinta kattavuus laajenee ja sitä ohjataan sekä kehitetään suunnitellusti. Riskienhallinnan seurattavuus ja raportointi paranevat, jolloin se palvelee entistä paremmin toimiston johtamista. Malli auttaa toimistoa tuottamaan vastuualueellaan olevat palvelut entistä turvallisemmin ja huolehtia niiden saatavuudesta kattavasti

Kehittäminen pohjautui vahvasti riskienhallinnan teoriataustaan. Lisäksi huomioituun tietohallinnon omat tarpeet ja riskienhallinnan käytössä oleva menetelmä, joka keskittyi operatiivisten riskien analyysiin kerran vuodessa toiminnan ja talouden suunnittelun yhteydessä. Riskienhallintaa haluttiin kehittää laajemmaksi ja huomioimaan tietohallintoimiston toiminta ja siinä esiintyvät erot muihin yksikköihin ja toimistoihin.

Kehittämiskohde rajattiin tietohallintotoimiston riskienhallinnan kehittämiseen. Tietohallintotoimiston tuottamat palvelut tukevat eduskunnan muuta toimintaa, joten sen palveluiden toiminta on jatkuvuuden kannalta ratkaisevassa roolissa. Tietohallintotoimiston on tämän riippuvuuden vuoksi kiinnitettävä erityistä huomiota palveluiden ja oman organisaationsa riskienhallintaan. Toimiston palveluiden tuotantomalli on myös erilainen muihin yksiköiden nähden vahvan ulkoistuksen käytön vuoksi. Toimiston erityispiirteiden vuoksi kehitystyö

rajattiin koskemaan vain tietohallintotoimistoa. Kehitettyä mallia voidaan soveltaa eduskunnan muissa yksiköissä tarvittaessa.

Kehittämiskohteen rajauksena oli myös organisaation riskienhallinnan nykytila. Riskienhallinnan kypsyystaso tietohallintotoimistossa ei ollut erityisen korkealla, etenkin jos sitä mitataan määritellyillä prosesseilla. Riskienhallintaa tehtiin osana jokapäiväistä palvelutuotantoa, mutta sille ei oltu määritelty määrämuotoista menetelmää tai kuvattu prosessia ja siihen liittyviä työkaluja. Kehittämistyössä otettiin huomioon myös nykyinen toimintatapa ja työkalu. Kehitetty malli ei lähtötason vuoksi mene kovin syvälliseksi. Malli kehitettiin pääosin teoriataustan ja toimiston johtoryhmän haastatteluiden perusteella ensimmäiseksi versioksi riskienhallinnan viitekehyksestä, prosessista ja tähän liittyvistä työkaluista ja dokumenteista. Näiden kehitystyö jatkuu käyttöönoton ja jatkuvan toiminnan yhteydessä.

1.4 Kehittämistehtävä ja menetelmä

Tutkimuksen avulla pyrittiin kehittämään eduskunnan tietohallintotoimistolle malli riskienhallintaan, joka huomioi toimiston tarpeet ja antaa viitekehyksen säännönmukaiselle riskienhallinnan toteutukselle. Kehittämistehtävän keskeisenä kysymyksenä oli seuraava kysymys:

- Millaisella mallilla eduskunnan tietohallintotoimiston tulisi hallita sen toimintaan liittyviä riskejä?

Kehittämistehtävän alikysymyksenä käytettiin seuraavia kysymyksiä:

- Mitä riskienhallinnan tarpeita eduskunnan tietohallintotoimistolla on?
- Miten eduskunnan tietohallintotoimisto tunnistaa, analysoi ja priorisoi riskejään?

Kehittämistehtävä voitiin luokitella tutkimukselliseksi kehittämistyöksi. Tutkimuksellisella kehitystyöllä pyritään ratkaisemaan käytännön ongelmia ja sen lähtökohtana voi olla organisaation kehitystarve (Ojasalo, Moilanen & Ritalahti 2014, 19). Riskienhallinnan nykyinen toimintamalli ei ollut riittävän kattava toimiston tarpeisiin tai sille asetettuihin tavoitteisiin nähden. Riskienhallinnalle oli tarve kehittää määrämuotoinen malli eduskunnan toiminnan varmistamiseksi.

Kehitystyön lähestymistapana oli konstruktiivinen tutkimus. Konstruktiivisessa tutkimuksessa tavoitteena on käytännön ongelman ratkaisu luomalla konstruktio eli jokin konkreettinen tuotos. Konstruktiivinen tutkimuksen avulla tuotettava muutos on sidottu aikaisempaan teoriaan. Konstruktiivisessa tutkimuksessa kehitetyn ratkaisun toteuttaminen ja käytännön toimivuuden ja hyödyllisyyden arviointi ovat keskeinen osa tutkimusta. (Ojasalo

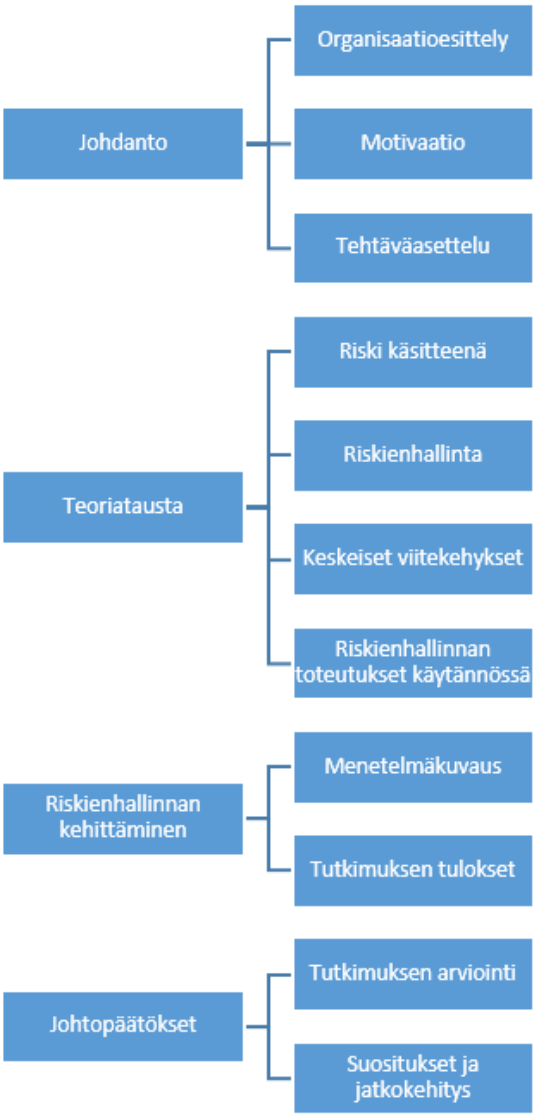
ym. 2014, 37-38.) Konstruktiona muodostettiin riskienhallinnan viitekehys ja siihen liittyvä toimintamalli.

Kehitystyön aineiston keräämisen menetelminä käytettiin haastatteluja ja dokumenttianalyysia. Haastattelut toteutettiin teemahaastatteluina, mahdollisimman kattavan tarvekartoituksen saamiseksi ilman liiallisia rajoituksia. Teemahaastattelussa ei täysin tunneta tutkimuksen kohdetta etukäteen eikä haluta ohjata vastaajia liikaa (Ojasalo ym. 2014, 41). Haastatteluilla kerättiin tietohallintotoimiston tarpeet sekä kartoitettiin muiden organisaatioiden riskienhallintamalleja. Myös dokumenttianalyysia hyödynnettiin nykytilan arvioinnissa. Dokumenttianalyysia käytetään yleensä yhdistettynä muihin tiedonkeruumenetelmiin tuomaan lisänäkökulmaa kehittävään asiaan (Ojasalo ym. 2014, 43).

Kehitystyössä luotiin uusi toimintamalli riskienhallinnalle teoriataustan nykytilan analyysin ja tarpeiden kartoittamisen pohjalta. Hallintamalli on määritelty kolmitasoiseksi malliksi. Periaatetasolla määritellään toimiston tahtotila riskienhallinnalle, puitetasolla kuvataan riskienhallinnan prosessi ja sen puitteet ja alimmalla tasolla kuvataan käytännön riskienarviointiprosessi. Riskienhallinnan keskeisiä ohjaavia dokumentteja ovat riskienhallinnan periaatteet ja riskienhallinnan puitekuvaus. Nämä hyväksytettiin toimiston johtoryhmällä. Riskienarvioinnin menetelmäkuvaukseksi luotiin riskienhallinnan käsikirja, joka sisälsi riskienhallinnan vuosisuunnitelman, riskienhallinnan välineet ja koulutusmateriaalin. Lisäksi luotiin riskienhallintasalkku riskien seurantaan. Nämä tuotokset hyväksytettiin toimiston johtoryhmällä ja testattiin tekemällä riskienarviointi yhdestä palvelusta ja käsittelemällä aiemmin arvioidut riskianalyysimenetelmillä. Tulokset näistä vietiin riskienhallintasalkkuun ja seurantaan vuosisuunnitelman mukaisesti tietohallintotoimiston johtoryhmään. Lopuksi arvioitiin näiden toiminta ja hyödyllisyys. Tutkimuksen tulokset on raportoitu tässä opinnäytetyöraportissa.

1.5 Raportin rakenne

Opinnäytetyöraportti on jaettu neljään lukuun. Luvut ovat johdanto, riskienhallinnan teoriatausta, tietohallinnon riskienhallinnan kehittäminen ja johtopäätökset. Rakenne on tarkemmin kuvattu seuraavassa kuviossa (kuvio 3) ja sitä seuraavissa kappaleissa.



Kuvio 3 Opinnäytetyöraportin rakenne

Johdanto-osan organisaatio-osiossa esitellään kohdeorganisaatio eduskunnan kanslia ja eduskunnan kanslian tietohallintotoimisto. Motivaatiossa-osio kuvaa taustatekijät ja ongelman, jota kehitystyössä ryhdyttiin ratkaisemaan, tavoitetila ratkaisulle sekä tämän rajat. Tehtäväasettelu-osio kuvaa mitkä ovat keskeiset ratkaistavat ongelmat ja lyhyesti millä menetelmillä niitä ratkaistiin.

Teoriatausta-osan riski käsitteenä-osiossa kuvataan yleisesti riskin käsitteenä ja sen merkitystä sekä toteutumisen seurauksia. Lisäksi esitellään riskien luokitusmalli. Riskienhallinta-osio kuvaa riskienhallinnan tavoitteet, riskienhallintaprosessin, riskien arvioinnin, riskienhallintakeinot, riskien raportoinnin, riskienhallinnan kehittämisen, riskienhallinnan käyttöönoton ja riskienhallinnan tason arvioinnin sekä standardien ja parhaiden käytäntöjen roolin riskienhallinnassa. Keskeiset viitekehykset-osiossa käsitellään COSO Enterprise

Risk Management –malli, ISO 31000 –standardi ja VAHTI –ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Riskienhallinnan toteutukset käytännössä –osiossa esitellään neljän organisaation riskienhallinnan toteutus ja niiden perusteella johtopäätökset tarpeista riskienhallinnalle.

Riskienhallinnan kehittäminen –osassa kuvataan menetelmäkuvaus-osiossa tutkimusmenetelmä ja sen toteuttamisprosessi. Tutkimuksen tulokset –osiossa esitetään tutkimuksen avulla luotu konstruktio ja sen testauksen tulokset.

Johtopäätökset-osassa tutkimuksen arviointi –osiossa arvioidaan tutkimuksen tuloksia ja hyödyllisyyttä. Suositukset ja jatkokehitys –osiossa annetaan arvion perusteella suosituksia tulosten käyttöönotolle ja pohditaan jatkokehitysmahdollisuuksia.

1.6 Keskeiset käsitteet

Raportin keskeiset käsitteet on esitelty seuraavassa taulukossa (taulukko 1)

Taulukko 1 Raportin keskeiset riskienhallinnan käsitteet (SFS-ISO 2011b; Suominen 2003; Ilmonen, Kallio, Koskinen & Rajamäki 2013)

Käsite	**Kuvaus 1 (SFS-ISO 2011)**	**Kuvaus 2 (Suominen 2003)**	**Kuvaus 3 (Ilmonen ym. 2013)**
Riski	Epävarmuuden vaikutus tavoitteisiin	Epävarmuutta, uhkaa ja vaaraa kuvaava teoreettinen termi	Määrätyn vaarallisen tapahtuman esiintymistaajuuden, tai –todennäköisyyden, ja seurauksen yhdistelmä
Riskien arviointi	Kokonaisprosessi, joka kattaa riskien tunnistamisen, riskianalyysin ja riskien merkityksen arvioinnin.	Prosessi joka kattaa riskien tunnistaminen, todennäköisyyksien ja vakavuudenarvioinnin, hallintamenetelmien kehittämisen ja valinnan, riskienhallinnan päätöksenteon ja toteutettujen ratkaisujen arviointi	Riskianalyysiin ja riskin merkityksen arvioinnin kokonaisprosessi
Riskianalyysi	Prosessi, jolla pyritään ymmärtämään riskin luonne ja määrittelemään riskitaso	Riskikohteiden, todennäköisyyksien ja riskin seurausten arviointiin käytetty työtapa	Saatavissa olevan tiedon järjestelmällistä käyttämistä vaarojen tunnistamiseksi sekä ihmisiin tai väestöön, omaisuuteen tai ympäristöön kohdistuvan riskin suuruuden arvioimiseksi

Riskienhallinta	Koordinoitu toiminta, jolla organisaatiota johdetaan ja ohjataan riskien osalta	Prosessi, jonka avulla yritystä uhkaavia vaaroja voidaan torjua ja niistä aiheutuvia menetyksiä minimoida	Johtamisperiaatteiden, menettelytapojen ja käytäntöjen järjestelmällistä hyväksikäyttämistä riskien analysoimiseksi, merkityksen arvioimiseksi ja valvomiseksi
Riskienhallintakeino	Riskiä muuttava toimenpide	Toimintatavat joilla riskienhallintaa käytännössä toteutetaan	Toimenpiteet joilla saatetaan riski hyväksyttävälle tasolle
Riskienhallintapolitiikka	Organisaation julkilausumat riskienhallintaan liittyvät periaatteet ja tavoitteet	Perustrategia riskienhallintaan	Kokoaa yhteen riskienhallintaperiaatteet ja muut asiaan liittyvät periaatteet yhdeksi kokonaisuudeksi
Riskienhallintaprosessi	Riskihallintaperiaatteiden, -menettelyjen ja –käytäntöjen järjestelmällinen soveltaminen.	Vaiheittain etenevä prosessi	Systemaattinen tapa, jolla riskejä arvioidaan, hallitaan ja raportoidaan
Riskisalkku	Tunnistettuja riskejä koskevan tiedon tallenteet	Erilaiset riskit mahdollisimman kattavasti hahmottava riskiluettelo	Yrityksen merkittävimpien riskien muodostama kokonaisuus
Seuraus	Tavoitteisiin vaikuttavan tapahtuman tulos		
Tapahtuma	Tiettyjen olosuhteiden esiintyminen tai muuttuminen		Tilanne, joka aiheuttaa tai voisi aiheuttaa loukkaantumisen tai vahingon ihmisille, laitokselle, laitteistolle, ympäristölle tai kolmannelle osapuolelle
Todennäköisyys	Jonkin tapahtuman toteutumismahdollisuus		
Uhka			Tiettyyn turvattavaan kohteeseen kohdistuvan vahingon tai häiriön mahdollisuus

2 Riskienhallinnan teoriatausta

Tässä luvussa kuvataan riskienhallinnan viitekehystä, joka toimii perustana kehittämistehtävälle. Teoriatausta muodostuu riskienhallinnan keskeisten tutkimusten, kirjallisuuden sekä suositusten ja standardien pohjalta. Lisäksi esitellään tulokset muiden organisaatioiden riskienhallinnan malleista haastattelutulosten muodossa. Teoriataustan, tarvekartoituksen ja nykytila-analyysin pohjalta kehitetään kehittämistehtävässä eduskunnan kanslian tietohallintoimistolle soveltuva riskienhallinnan viitekehys.

2.1 Johdanto riskienhallintaan ja käytettävään materiaaliin

Jokaisen organisaation ja yksilön voidaan todeta tekevän riskienhallintaa osana normaalia toimintaa. Riskienhallinta on yksilötasolla riippuvaista yksilön tietämyksestä ja mahdollisesti ohjeistuksesta, joita heille on annettu. Arkipäivän tilanteissa suojatien käyttäminen tai liikennevalojen noudattaminen on esimerkki riskienhallinnasta. Organisaatioissa riskienhallinta on usein kytketty organisaation tavoitteiden ja velvoitteiden täyttämiseen liittyvään toimintaan.

Riskienhallintaa on käsitelty useassa teoriataustan materiaalissa yritysten näkökulmasta. Kohdeorganisaatio on kuitenkin osa julkishallintoa, jolloin yritysten liiketoimintaan kohdistuvaa riskienhallintaa on sovellettava organisaation toiminta huomioiden. Julkishallinnonkin organisaatioiden toimintaan kohdistuu myös useita epävarmuustekijöitä. Täyttääkseen julkishallinnolle asetetut velvoitteet, on epävarmuustekijöitä pystyttävä hallinnoimaan. Tästä johtuen riskienhallinnan teoriat pätevät suurelta osin julkishallinnon toimintaan samalla tavalla kuten yritystenkin toimintaan. Erityisesti tukitoiminnot kuten tietohallinto, ovat tavoitteiltaan hyvin samankaltaisia julkishallinnossa kuin yrityksissä. Tästä syystä onkin syytä välttää luomasta julkishallinnolle kokonaan erillistä riskienhallintamallia kuin muussa samankaltaisessa toiminnassa.

Luku koostuu yleisesti riskienhallinnan teoriasta ja keskeisistä sovellettavista riskienhallinnan viitekehyksistä. Nämä ovat COSO Enteprise Risk Managemengt – Integrated Framework, SFS-ISO 31000 Riskienhallinta. Periaatteet ja ohjeet sekä VAHTI Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. COSO antaa viitekehyksen kokonaisvaltaiselle riskienhallinnalle, joita voi soveltaa organisaation toimintaan, SFS-ISO 31000 standardi määrittelee viitekehyksen tarkemmalla lähelle käytännön tasolla sovellettavaksi organisaatioon ja VAHTI antaa ohjeita julkishallinnossa tehtävään riskienhallintaan. Luvussa myös esitellään tulokset riskienhallinnan ammattilaisille tehdyistä haastatteluista riskienhallinnan toteutuksista erilaisissa organisaatioissa. Haastatteluilla haluttiin saada näkökulma käytännön riskienhallinnan toteutuksiin. Kirjallisuuden ja haastattelui-

den pohjalta muodostettiin synteesi, jota käytettiin hyväksi kehittämistehtävän konstruktion luonnissa.

2.2 Riski käsitteenä

Termiä riski käytetään kuvaamaan erilaisia asioita. Synonyymeina voidaan käyttää vahingonvaara ja vahingonuhka. Riski käsitteenä voidaan ymmärtää ihmisen ja yrityksen vapaudesta valita eri vaihtoehtojen välillä sekä uskalluksesta tehdä päätöksiä ja ryhtyä tekoihin. Arkikielessä riski sanaa käytetään kuvaamaan sitä vaaraa ja epätietoisuutta, joka liittyy onnettomuuden mahdollisuuteen. Vakuutusmielessä kyse on tapahtumista, jotka voivat kohdata ihmisten tai yritysten joukkoa sekä niitä arvoja ja pääomia, joita tuo joukko omistaa. (Kuusela & Ollikainen 2005, 16-17.)

Riski merkitsee niitä vaaratekijöitä, joille ihmiset ovat alttiina tietyllä hetkellä. Riski on vahingon mahdollisuus. Lähes kaikki riskit ovat ihmisten aiheuttamia ja siksi niihin voidaan vaikuttaa ja niiltä voidaan suojautua. Taloudellisessa toiminnassa joudutaan tekemään päätöksiä, joiden seurauksia ei päätöshetkellä tunneta. Päätökseen liittyy aina joko riskiä tai epävarmuutta. Riski voi liiketoiminnassa olla myös mahdollisuus, yritystoiminta edellyttää järkevää riskien ottamista. (Kahra, Kuusela & Kanto 2005, 72; SRHY 22015; Suominen 2003, 9.)

Riskin sanotaan olevan olemassa kun negatiivinen lopputulos on ennalta arvaamaton ja odottamaton. Päätöksentekijät eivät myöskään usein tiedosta tai havaitse omien päätösten haitallisia vaikutuksia. Vaikka päätöksentekijä tiedostaa negatiivisien tapahtumien mahdollisuuden, hän ei voi olla varma milloin ja minkä suuruisena tapahtuma toteutuu. Riskin toteutumisen suuruus on myös epävarmuutta aiheuttava tekijä. Epävarmuus ulottuu täydellisestä tietämättömyydestä laskennallisiin todennäköisyyksiin. Todennäköisyydet voivat perustua muutamaan kokemusperäiseen tapaukseen tai laajaan tietopohjaan. Riskin luonteeseen kuuluu se, ettemme voi tarkasti olla perillä ei-toivottujen tapahtumien sattumisesta. Yrityksen johto ei siten voi etukäteen tietää ei toivotuista tapahtumista. Historiatiedon perusteella voidaan laskea riskien todennäköisyyksiä. Riskille voidaan antaa matemaattinen määrittely: Riski = todennäköisyys x riskin laajuus tai vakavuus. (Kuusela & Ollikainen 2005, 30.; Suominen 2003, 10.)

2.2.1 Riskit ja seuraukset

Riskien toteutumisesta johtuvat menetykset voivat olla minkä tahansa arvon menetyksiä (Kuusela & Ollikainen 2005, 17). Kuusela ja Ollikainen (2005, 17) määrittelevät menettäviksi arvoiksi

- rahallisen arvon
- ympäristöarvon
- terveydellisen arvon
- yhteiskunnallisen arvon.

Teoreettisessa ajattelussa riski yhdistetään tulokseltaan erilaisten, onnistuneiden ja epäonnistuneiden, tapahtumien vaihteluksi. Riskiin liittyy poikkeuksetta tapahtumien todennäköisyyksien arviointia. Onnistuneita tapahtumia voidaan kutsua toivotuiksi ja epäonnistuneita ei-toivotuiksi. Riskiä määriteltäessä onkin tarkasteltava epätoivotun seuraamuksen haitallisuutta ja todennäköisyyttä. Riski toteutuu yleensä vaaralle altistumisen seurauksena ja sen hyväksyttävyys riippuu monista tekijöistä. Riskikokemukseen vaikuttavien tekijöiden tunnuspiirteitä ovat esimerkiksi riskin hallittavuus ja rajoitettavuus sekä henkilön arviointikyky, henkilökohtaiset ominaisuudet ja vapaaehtoisuus. Tarkastelunäkökulma, tilanne tai muut tekijät, kuten maantieteellinen sijainti, vaikuttavat riskikäsitteen ymmärtämiseen. Riskit ovat kontekstisidonnaisia ja henkilöiden riskiarviot muuttuvat ajan ja paikan suhteen. (Kuusela & Ollikainen 2005, 17-18; Suominen 2003, 9.)

Riskiin liittyy tappion mahdollisuus ja menettämisen uhka. Olennainen riskiin liittyvä piirre on epävarmuus. Emme varmuudella tiedä tulevia tapahtumia, vaikka tunnemme tapahtumien todennäköisyyksiä. Riskit ovat luonnostaan muuttuvia ja riippuvaisistaan toisistaan. Riskin olemukseen liittyy aina myös, että tapahtumien hajonta vaihtelee ja riskien toteutuminen on yksilöllistä. Ennalta-arvaamattomien tapahtumien seuraukset tai itse tapahtumat vaikuttavat yleensä organisaatioiden tapauksessa useisiin sen osiin. Tapahtumien poikkeamista odotetusta tuloksesta tai tapahtumasta voidaan arvioida todennäköisyyksien avulla. Usein riski koetaan henkilön subjektiiviseksi näkemykseksi lopputuloksesta. Näin riskiarviot vaihtelevat henkilöiden välillä. Riski konkretisoituu ihmisen ajattelun ja päätöksenteon kautta. Toiminnan myönteisiä ja kielteisiä seurausvaikutuksia pohditaan arvioinnissa olevien ja toteuttamiskelpoisten vaihtoehtojen joukosta. (Kuusela & Ollikainen 2005, 28-29; Marchetti 2012, 2.)

2.2.2 Riskien luokittelu

Riskejä on sekä dynaamisia että staattisia. Dynaamiset riskit muuttuvat suhdanteiden ja olosuhteiden mukaan. Näitä kutsustaan myös spekuloitaviksi riskeiksi, koska toimija voi itse vaikuttaa niihin, eikä niitä yleensä voi siirtää muiden kannettavaksi. Dynaamisista riskeistä voi seurata yhtä hyvin voittoa kuin tappiota. Staattista eli vakuutusriskeistä ei voi seurata voittoa, vain pelkästään menetyksiä. Nämä ovat yrityksen tai yksilön tahdosta riippumattomia. Tietty määrä vahingollisia tapahtumia sattuu, vaikka kuinka tiedostamme riskien olemassaolon. Termeinä voidaan käyttää myös vahinkoriski tai vakuuttamiskelpoi-

nen riski staattisille riskeille ja dynaamisille riskeille taas liiketaloudellinen riski. (Kuusela & Ollikainen 2005, 33-34; Suominen 2003, 12 .)

Jaon dynaamisiin ja staattisiin riskien lisäksi Kuusela ja Ollikaisen (2005, 29) mukaan riskejä voidaan myös luokitella

- voittaminen ja menettämisen riskeihin
- toimintapuitteiden muutosriskeihin esimerkiksi lainmuutoksen seurauksena
- riskit, jotka voivat aiheuttaa tuhoa tai vahinkoa.
- rikoksen kohteeksi joutumisen riskeihin
- vahingosta vastuuseen joutumisen riskeihin
- tulojen hankkimiskyvyn menettämisen riskeihin.

Riskejä jaetaan myös erilaisiin kategorioihin tai luokkiin, tyypillisesti jakoperusteena on käytetty riskin toteutumisen mahdollisia seurausvaikutuksia. Monet riskeistä kuuluvat useampaan riskiluokkaan. Riskien luokittelu helpottaa riskien tunnistamista ja hallintaa. Liikeriskien kategorisointi on hankalaa ja osin keinotekoistakin. Vahinkoriskien osalta jaottelu on yksinkertaisempi ja selkeämpi, sillä ne ovat luonteeltaan hitaasti muuttuvia. (SRHY 2015; Suominen 2003, 12-14.)

Suomen riskienhallintayhdistyksen SRHY (2015) mukaan riskit voidaan jakaa

- strategisiin riskeihin
- operatiivisiin riskeihin
- taloudellisiin riskeihin
- vahinkoriskeihin.

Strategiset riskit voivat lyhyellä tai pitkällä aikavälillä vaikuttaa strategisten tavoitteiden toteutumiseen tai jopa organisaation olemassaoloon. Operatiiviset riskit ovat seuraus tapahtumasta, joka aiheutuu riittämättömistä tai toimimattomista sisäisistä prosesseista, järjestelmistä tai ihmisistä. Taloudelliset riskit ovat epävarmuuksia, jotka liittyvät organisaation vakavaraisuuteen, pääomien riittävyyteen ja rahaprosessien toimivuuteen. Vahinkoriskit tarkoittavat uhkaa tapahtumasta, joka toteutuessaan aiheuttaa negatiivisia seurauksia. (SRHY 2015.)

Suomisen (2003, 14-19) sekä Kuusela ja Ollikainen (2005, 34) mukaan vahinkoriskit voidaan luokitella

- henkilöriskeihin
- omaisuusriskeihin ja esineriskeihin
- vastuuriskeihin
- keskeytysriskeihin
- verkosto – ja riippuvaisuusriskeihin
- teknologia- ja laaturiskeihin
- kuljetusriskeihin
- tietoriskeihin
- yhteiskunnallisiin riskeihin.

Henkilöriski voi olla liike- tai vahinkoriski joka kohdistuu erityisesti yrityksen avainhenkilöihin. Omaisuusriski on riski, joka toteutuessaan aiheuttaa vahinkoa yrityksen aineellisille tuotannon tekijöille. Vastuuriski merkitsee toteutuessaan yritykselle korvausvelvollisuutta tai tulojen menetystä. Keskeytysriski toteutuu kun yrityksen toiminta keskeytyy tapahtuman toteutumisesta johtuen. Verkosto- ja riippuvaisuusriski toteutuu, jos toisten sitoutuminen jää toteutumatta. Teknologia- ja laaturiski ilmenee tuotannon laadun ongelmina. Kuljetusriskit toteutuvat, jos tavarat eivät saavu ehjinä, oikeamääräisinä, sovittuna aikana ja oikeaan paikkaan. Tietoriskeihin liittyvät usein tietoturvallisuutta vaarantavat tekijät. Yhteiskunnalliset riskit liittyvät yhteiskunnan epävarmuustekijöihin, kuten työvoiman saatavuuteen tai lainsäädännön muutoksiin. (Kuusela & Ollikainen 2005, 34; Suominen 2003, 14-19.)

Verkostossa toimivan yrityksen on syytä huomioida verkoston aiheuttamia riskejä. Virolaisen ja Hallikkaan (2005, 222) mukaan verkoston aiheuttamat riskit voidaan luokitella

- erikoistuneisiin investointeihin liittyviin riippuvuusriskeihin
- osaamisen menetykseen ja suojaamiseen liittyviin riskeihin
- toimittajan kyvykkyyteen liittyviin riskeihin
- ajoitukseen liittyviin riskeihin.

Erikoistuneisiin investointeihin riippuvat riski liittyy investointeihin, joille ei välttämättä ole käyttöä yhteissuhteen ulkopuolella Tällöin organisaatiot tulevat toisistaan riippuviksi. Osaamisen menetykseen ja suojaamiseen liittyvä riski johtuu tiedonvaihtamisen tarpeista. Riittävä ja oikea-aikainen tieto verkoston eri osapuolille on tärkeää kilpailukyvyn saavuttamiseksi ja säilyttämiseksi. Tiedonkulkua on hallittava yli organisaation rajojen tahoihin, johon ei ole toimivaltaa. Varsinkin luottamuksellisen ja strategisen tiedon vaihtaminen on riski verkostossa. Tieto voi päätyä väärille osapuolille. Myös puutteet tiedonkulussa, tiedon saatavuudessa ja sen laadussa aiheuttavat verkoston yrityksille kustannuksia. Kyvykkyyteen liittyvä riski on yhteistyökumppanin valintaa liittyvä riski siitä, että valitaan väärä tai kyvytön kumppani. Ajoitukseen liittyvät riskit liittyvät eripituisiin suunnitteluhorisontteihin ja erilaisiin odotuksiin investointien takaisinmaksuajoista. (Virolainen & Hallikas 2005, 222.)

Scherfin (2012, 106) mukaan julkisen sektorin osalta on syytä myös kiinnittää huomiota maineriskeihin. Julkisen sektorin organisaation toiminnan luotettavuus ja kansalaisten luottamus toimintaan perustuvat ensisijaisesti hyvään maineeseen.

2.3 Riskienhallinta

Kaikkeen toimintaan kuuluu osana epävarmuus, niin ihmisten, kuin yritysten toimintaan. Epävarmuus on tietämättömyyttä tulevista tapahtumista, jotka voivat kielteisiä tai myönteisiä. Päivittäiseen päätöksentekoon liittyy aina riskejä, jotka voivat vaarantaa toiminnan jatkuvuutta ja estää niille asetettujen tulosten saavuttamista. Yrityksille riskin ottaminen on kuitenkin välttämätöntä menestyäkseen. Riskienhallinta on työtä yrityksen toiminnan jatkuvuuden ja henkilöstön hyvinvoinnin turvaamiseksi. Yritykset ja ihmiset pyrkivät etukäteissuunnittelulla parantamaan turvallisuuttaan ja tulevaisuudenhallintaa. Riskien tarkastelussa on otettava huomioon monia näkökohtia, kuten riskien suuruudet, hyväksyttävyys ja mihin ne kohdistuvat. Etukäteissuunnittelun eli riskienhallinnan peruslähtökohtana voidaan pitää tavoitetta pitää tilanne ennallaan. Hyvä riskienhallinta onkin ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä. Riskienhallinta on loppujen lopuksi nimenomaan ajattelutapa, joka auttaa organisaation strategian luomista ja maastouttamista hahmottamalla toiminnan pelikentän mahdollisuudet, sudenkuopat ja sivurajat. (Arnell 2011, 45; Kuusela & Ollikainen 2005, 15-16; SRH 2015.)

2.3.1 Riskienhallinnan tavoitteet

Riskienhallinta on tasapainoilua riskin ja hyödyn välillä. Hyvin suunniteltu riskienhallinnan toteutustapa rohkaisee ja mahdollistaa organisaatioiden ottaa hallittuja riskejä. Riskienhallinta toteutetaan arvioimalla laskennallisia tekijöitä ja tietoa sekä huomioidaan organisaation kokemus ja arviointikyky päätöksenteossa. Organisaatioiden riskienottokykyyn vaikuttaa siten sen koko henkilöstö. Hyvin määritelty ja toimiva riskienhallinta on käytännössä valintojen hallintaa, joka on jatkuvaa toimintaa. Jokaisessa valinnassa tulisi arvioida siihen liittyvät riskit ja miten ne vaikuttavat organisaation toimintaan. Riskienhallinta voidaan nähdä prosessina, jonka kautta tunnistetaan ja arvioidaan riskejä, sekä valitaan ja toteutetaan toimenpiteitä, jotka vähentävät niiden seurauksia. Organisaatioiden on päätettävä mitkä riskit se hyväksyy ja mitkä vaativat toimenpiteitä, joiden tavoitteena on yleensä riskin pienentäminen. (Kuusela & Ollikainen 2005, 35; Marchetti 2012, 1-2.)

Riskienhallinnan tavoite on tukea päätöksentekoa yrityksessä siten, että yrityksen johto voisi tehdä merkittävät liiketoimintapäätökset tietoisena siitä, mikä on yrityksen riskikuva ja miten tehtävä päätös vaikuttaa tähän. Tavoitteen saavuttaminen edellyttää yrityksen riskikuvan säännöllistä päivittämistä, päätöksen riittävää analysointia ja sitä, että yrityksellä on jonkinlainen ymmärrys riskinkantokyvystään. Normaali arkinen riskienhallinta perustuu terveen järjen käytön lisäksi yksinkertaisiin, hyväksi havaittuihin ratkaisuihin. Moderni riskienhallinta on systemaattinen kokonaisvaltainen, tilastolliseen tietoon pohjautuva prosessi. (Ilmonen ym. 2013, 10; Suominen 2003, 28.)

2.3.2 Riskienhallinta prosessina

Riskienhallinnan prosessiin liittyy useita vaiheita riskin tunnistamisesta aina riskienhallintaohjelman toteuttamiseen. Riskienhallintaa voidaan tarkastella joko suppeana tai laajennettuna ajattelu- ja toimintatapana. Tarkastelunäkökulma riippuu siitä, millaiset riskit otetaan riskienhallintaan mukaan. Suppea määrittely kattaa vahinkoriskipohjaisen riskienhallinnan. Laajemman määrittelyn mukaan riskienhallinta ulottuu yrityksen kaikkien riskien suojaamiseen. Riskienhallinta ymmärretään yleisimmin yrityksen toiminnan ja tuloksen suojaamisena ei-toivotuilta tapahtumilta ja niiden seurannaisvaikutuksilta. Riski ja riskienhallinta laajasti ymmärrettynä kattavat myös mahdollisuudet liiketoimintaan ja niiden tunnistamisen, arvioinnin ja hallinnan. Riskilajeista selvästi eniten liiketoimintamahdollisuuksia on strategisten riskien alueella. Vahinkoriskeissä niitä ei ole koskaan ja operatiivisissa riskeissä hyvin harvoin. Riskilajeista riippumatta yritys tarvitsee riskienhallinnan kokonaisvaltaista suojaa. (Ilmonen ym. 2013, 15; Suominen 2003, 27.)

Riskienhallinta on hahmotettava jatkuvaksi monimuotoiseksi prosessiksi, jonka kehitystä johdon tulee kaikin tavoin vaalia. Riskienhallintaa ei voida hoitaa yksittäisenä kertaprojektina. Saadakseen riskienhallinnasta selvää hyötyä, asioita on seurattava ja arvioitava monta kertaa vuoden aikana. Riskienhallinta toimii parhaiten silloin, kun siitä muodostuu organisaation toimintaan kytkeytyvä ajattelu- ja työskentelytapa. Aito riskienhallinta etenee suunnitelman mukaisena, vaiheittaisena toimintaprosessina. Riskien hallinnasta ei voi puhua ilman riskien arvioinnin esilletuomista. Määrämuotoisen riskien arvioinnin ja riskienhallinnan käyttöönotto on kriittistä organisaation riskienhallinnan kehittämisen kannalta. (Marchetti 2012, 2; Suominen 2003, 30-31.)

Ilmonen ym. (2013, 85) määrittelevät riskienhallintaprosessin viisivaiheiseksi prosessiksi, jonka vaiheet ovat

- tavoitteiden määrittely ja kohdentaminen
- riskientunnistaminen ja arviointi
- riskienhallintatoimenpiteet
- riskiraportointi ja seuranta
- riskienhallinnan arviointi ja jatkuva parantaminen.

Riskienhallintaprosessi on kuvattu yksinkertaistettuna seuraavassa kuviossa (kuvio 4).

Kuvio 4 Riskienhallintaprosessi Ilmonen ym. mukaillen (Ilmonen ym. 2013, 86)

2.3.3 Riskien arviointi

Riskit pitää saada laajuutensa ja seurausvaikutustensa suhteen tärkeysjärjestykseen. Tähän riittää käytännössä melko karkea arvio. Seuraukset voidaan esimerkiksi luokitella vähäisiksi, kohtalaisiksi, suuriksi tai katastrofaalisiksi. Riskin seurauksiin liitetään mielikuvia, jotka eivät ole yhteismitallisia. Myöskään laajuusrajat eivät ole yksiselitteisiä, suuri menestyvä yritys kestää paljon suuremman vahingon kuin voimavaroiltaan vähäisempi, yleensä pieni yritys. Laajuuden arvioinnissa voidaan käyttää myös euromääräistä arviointia. Arviointien kohdalla voidaan myös tehdä yliarviointia. Jos riskistä puhutaan ja kirjoitetaan paljon, kuten riskien haitallisista vaikutuksista, aiheuttaa se riskin toteutumisen yliarviointia. (Kuusela & Ollikainen 2005, 30; Suominen 2003, 11)

Yleinen riskianalyysi ja vahinkoriskien arviointi

Riskejä arvioidaan riskianalyysin avulla. Kun riskienhallinta etenee suunnitellusti järjestyksessä, voidaan puhua riskianalyysistä. (Suominen 2003, 35.) Suomisen (2003, 35) mukaan riskianalyysin tehtävänä on selvittää

- riskikohteet
- riskien todennäköisyys
- riskien vakavuus
- riskeistä aiheutuvat seurausvaikutukset.

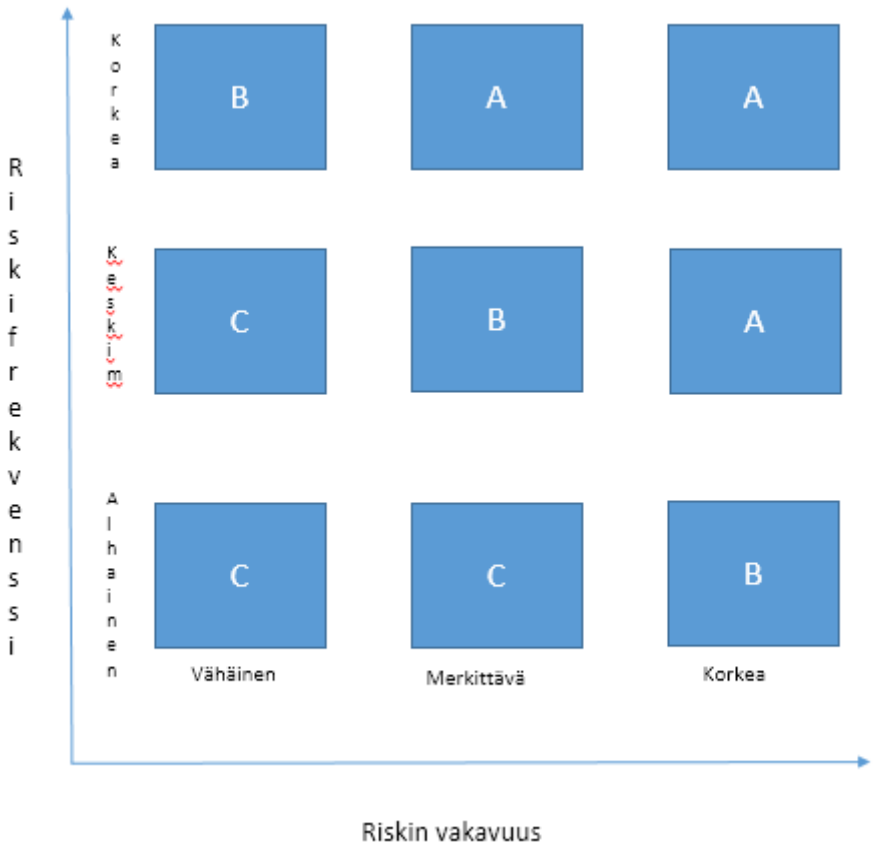
Riskianalyysin avulla pyritään selvittämään tapahtumien todennäköisyys ja sen seuraukset. Riskianalyysin avulla riskikohteet käydään läpi systemaattisesti tiettyjä logiikan sään-

töjä noudattaen. Toimivan riskianalyysin edellytyksenä on riskikohteiden tunnistaminen. Käytännössä tämä tarkoittaa sitä, että yritys pystyy erilaisin menetelmin havaitsemaan erilaisia vaaratilanteita. Tunnistamistyön helpottamiseen tarvitaan monipuolisia välineitä, joiden avulla päätöksentekijä voi arvioida onko riski mahdollinen. Välineiden avulla saadaan esille myös piileviä riskejä joiden olemassaolosta ja sattumismahdollisuuksista ei oltu tietoisia. Riskien tunnistamisen jälkeen päästään arvioimaan niiden laajuutta ja seurausvaikutuksia. Arvioinnissa voidaan käyttää apuna todennäköisyyksien ja laajuuden jakamista neljään luokkaan karkeiden arvioiden perusteella. Todennäköisyydelle pitää antaa selkeät erot, kuten vuosisata, vuosikymmen, vuosi ja kuukausi. Yrityksen koosta riippuu hyvin pitkälle, minkälainen asteikko vahingon laajuudelle annetaan. Iso, tuottava yritys kykenee ottamaan kannettavakseen jopa miljoonien eurojen vahingot. Pienelle yritykselle jo 5 00 euron suuruinen vahinko voi olla kohtalokas. (Suominen 2003 20; Suominen 2003, 35; Suominen 2003, 40; Suominen 2003, 43; Suominen 2003, 45.) Jaon perusteella voidaan muodostaa taulukko (taulukko 2) esittämään laajuutta ja todennäköisyyttä.

Taulukko 2 Riskin laajuuden ja todennäköisyyden arviointi (Suominen 2003, 21)

Riskin laajuus	**Todennäköisyys**
1 = vähäinen riski, < 500 €	1 = erittäinen harvinainen, 1 kerta /200 v
2 = kohtalainen riski, > 2 000 €	2 = melko harvinainen, 1 kerta / 10 v
3 = suuri riski, > 20 000 €	3 = suuri, 1 kerta / 1 vuosi
4 = katastrofiriski, > 200 000 €	4 = yleinen, useita kertoja vuoden aikana

Riskin arviointiin liittyy monenlaisia tekijöitä, joita ei voida perustella suoralla logiikalla ilman psykologista näkökulmaa. Arviointiin vaikuttavat useat näennäisesti epärelevantit seikat, esimerkiksi ongelman muotoilu tai panoksen suuruus. Ihmisten on myös vaikea arvioida hyvin pieniä tai hyvin suuria todennäköisyyksiä. Yleensä pienet todennäköisyydet yliarvioidaan ja suuret aliarvioidaan. Yritysten on myös hankalaa arvioida riskien todennäköisyyden ja seurausvaikutusten vakavuutta. Arvioinnissa voidaan käyttää apuna Sticlesin ja Firthin kehittämää ruudukkoa, jossa riskit sijoitetaan niiden todennäköisyyden ja vakavuuden perusteella kuvaajaan. (Kahra ym. 2005, 78; Suominen 2003, 25.) Ruudukko on esitetty seuraavassa kuviossa (kuvio 5).



Kuvio 5 Riskin suuruuden määrittelyruudukko (Suominen 2003, 25)

Näin saadaan muodostettua kuva mihin riskeihin yrityksen tulisi keskittyä. Kuvion perusteella ne riskit jotka sijoittuvat A-tyyppiin, muodostavat keskeisen tehtäväkentän yrityksen riskienhallinnalle. Kaikissa yrityksissä esiintyy A-, B- ja C-tyyppisiä riskejä. A-tyyppisille on tehtävä välittömiä toimenpiteitä ja B-tyypin riskien hallitsemiseksi on tehtävä suunnitelmia. C-tyypin riskit voidaan ottaa omalle vastuulle. Ruudukkoa voidaankin käyttää riskienhallinnan peruslähtökohtana. (Suominen 2003, 25-26.)

Edellisten arvioiden tuloksena saadaan riskitulo, suure, joka osaltaan kuvaa vahinkojen suuruusluokkaeroja ja parantaa erilaisten riskien välistä vertailtavuutta. Riskitulo auttaa määrittelemään tavanomaisten riskien välisiä eroja, mutta katastrofiriskien kohdalla tuloajattelu ei toimi. Tulo on laskennallinen suure, jonka merkitystä ei pidä päätöksenteossa korostaa. Onkin kyseenalaista katastrofaalisten riskien arvioinnissa voidaanko niitä arvioida samalla kertolaskuun perustuvalla asteikolla. Niiden aikajänne ulottuu yli ihmisten tai yrityksen iän. (Suominen 2003, 45-46.)

Riskianalyysin yhteydessä on myös huomioitava riskin merkittävyys. Tietyt riskit ovat seurauksiltaan vähäisempiä kuin toiset, jolloin niiden merkittävyyttä on tarkisteltava erikseen. Riskituloajattelua voidaan laajentaa niin, että siinä huomioidaan laajuusarvioinnissa use-

ampia tekijöitä, esimerkiksi henkilö- ja omaisuusvahingon suuruus sekä vahingon yhteiskunnallinen suuruus. Toimintamallilla saadaan laajennettua arviointitarkkuutta eikä kokonaisriskiarvio ole enää omaisuuspainotteinen. Laajennetussa arvioinnissa riskikohteille luodaan vastaava asteikko kuin yleinen asteikko riskin laajuudelle, mutta se huomioi arvioitavan riskiluokan tapahtumat. Henkilövahingoissa esimerkiksi 1= mitätön henkilövahinko johon ei liity pysyviä vammoja ja 5 = katastrofivahinko johon liittyy useita kuolemantapauksia. Tämän perusteella tarkennetun kokonaisvaikutuksen kaavaksi voidaan edellä mukaan otettujen esimerkkivahinkojen perusteella esittää kaava: Riski = todennäköisyys x (henkilövahinkoarvio + omaisuusvahinkoarvio + riskin yhteiskunnalliset vaikutukset). Riskien arvioinnissa on huomioitava, että taloudellisten tappioiden ohella riskiarvioon vaikuttavat myös tunnepohjaiset tekijät, joiden arviointiin on lähes mahdotonta kehittää yleispäteviä mittaussuureita. Tästä esimerkkinä vahingon arviointi, joka aiheutuisi Ateneumin tulipalosta johtuvasta kansallisten taideaarteiden menetyksinä. (Suominen 2003, 46-47; Suominen 2003, 49-50.)

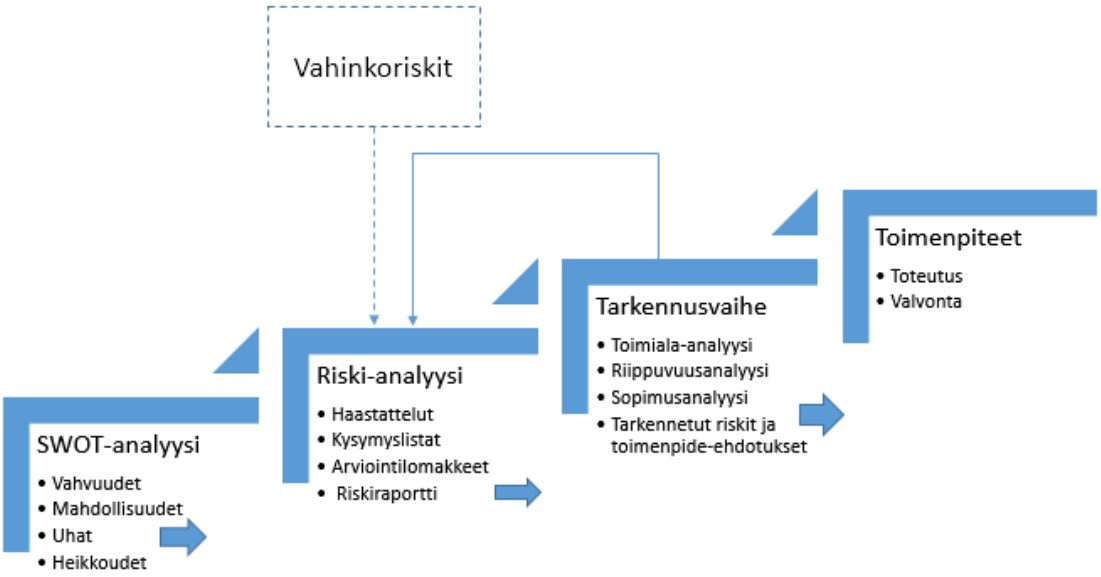
Liikeriskien huomioiminen riskien arvioinnissa

Liikeriskien arviointi eroaa vahinkoriskeistä. Liikeriskeihin liittyy vieras, tuntematon elementti. Vahinkoriskien arvioinnissa voidaan käyttää apuna vahinkotilastoja tai muita vastaavia tilastoja. Liikeriskien osalta vastaavia tilastoja ei ole käytettävissä. Liikeriskien toteutuminen havaitaan esimerkiksi yritysten tiedotteista ja talouselämän lehdistä. Liikeriskien toteutuminen tarkoittaa sitä, että yritystoiminta tuottaa tavoitellun voiton sijasta tappioita. (Suominen 2003, 51-52.)

Liikeriskejä on mahdollista arvioida käymällä läpi kattavasti yrityksen keskeiset toiminnot sekä liiketoimintaympäristö ja siihen liittyvät tekijät. Liikeriskien arviointi voi olla laajuudeltaan, syvällisyydeltään ja toimintatavoiltaan hyvin vaihtelevaa yrityksen toimialan ja koon mukaan. Käytännössä on usein tarpeen soveltaa rinnan erilaisia, toisiaan täydentäviä arviointimenetelmiä. Liiketoimintariskien hallinnassa, kuten muussakin riskienhallinnassa, riskienhallinta ei saa olla liian vahvasti yhden menetelmän tai toimintatavan varassa. (Suominen 2003, 53-54.)

Liikeriskien arviointi ja analyysi toteutetaan eri pohjalta kuin vahinkoriskien analyysi. Liikeriskejä arvioidessaan päätöksentekijä joutuu puntaroimaan tehtyjen päätösten yhteyksiä odotettavissa oleviin tuottoihin ja kustannuksiin. Liikeriskien todennäköisyyttä ei kyetä arvioimaan samalla tavalla kuin vahinkoriskien todennäköisyyttä ja seurausvaikutuksia. Riskit on kuitenkin syytä arvioida tavalla tai toisella. Riskianalyysin avulla yritys voi kerätä organisaatiossa hajallaan olevan tiedon kokonaisuudeksi ja tehdä laadukkaampia ratkaisuja. Analyysi on mielekästä kohdentaa yrityksen kannalta keskeisiin kysymyksiin. (Suo-

minen 2003, 54-55.) Liikeriskien arviointi ja analyysiprosessista on johdettu Suomista (2003, 55-76) mukaillen seuraava kuvio (kuvio 6).



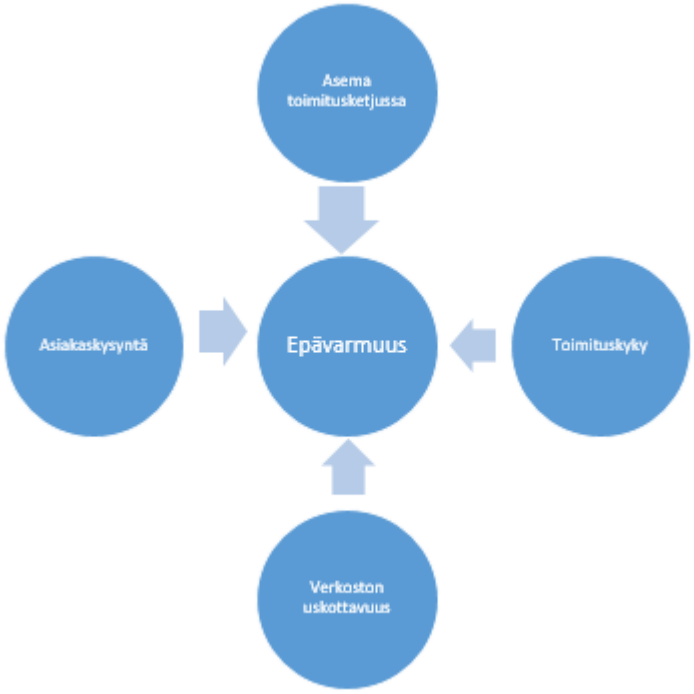
Kuvio 6 Mukaelma liikeriskien arviointiprosessista (Suominen 2003, 55-76)

Esimerkiksi liikeriskienanalyysi voidaan suorittaa vaiheittain siten, että ensiksi laaditaan yleisluontoinen yrityksen vahvuuksia, heikkouksia sekä uhkia ja mahdollisuuksia ilmentävä perusselvitys nelikenttänä eli SWOT-analyysi. Analyysia jatketaan ottamalla edellisessä vaiheessa havaitut heikkoudet ja tiedostetut uhat tarkemman erittelyn kohteiksi riski-analyysiin. Tässä vaiheessa erilaisia riskejä on syytä tarkastella rinnan ja samanaikaisesti. Tämä on mielekästä, koska yrityksen johto tarkastelee riskejä kokonaisuutena, eikä tee teoreettista jakoa liike- ja vahinkoriskien välille. Analyysissa käydään läpi kaikki yrityksen toimintaa ja toiminnan tuloksellisuutta uhkaavat riskitekijät. Nelikentässä tehtyjä havaintoja voidaan tarkentaa kysymyslistojen ja arviointilomakkeiden avulla. Näiden avulla arvioidaan olennaiset riskit ja niiden toteutumismahdollisuudet sekä varmistetaan vastausten yhdenmukaisuus (Suominen 2003, 55-57; Suominen 2003, 59.)

SWOT-analyysin ja tarkistuslistojen pohjalta voidaan laatia riskiraportti. Raportissa ei puututa yksityiskohtaisella tasolla yrityksen eri toimintoihin. Raportti esittää johdon keskeisinä pitämiä riskejä ja tuo esille joukon suosituksia ja toimenpide-ehdotuksia. Raportin tavoitteena on liiketoiminnan perusteiden turvaaminen ja yrityksen menestysmahdollisuuksien kirjaaminen. Analyysin jatkamiseen tarkentamisvaiheella tarvitaan yksityiskohtaisia kysymyssarjoja ja muita analyyseja. Jotta riskianalyysi olisi mahdollisimman kattava, toistetaan sitä kaikissa yrityksen toiminnoissa. Tuloksena saadaan joukko riskienhallinnan perustaksi soveltuvia raportteja, suosituksia ja toimenpiteitä. Tämän jälkeen voidaan edetä tarkastelemaan toimenpiteitä ja suosituksia. (Suominen 2003, 64; Suominen 2003, 76.)

Verkostoitumisen erityispiirteet riskien arviointiin

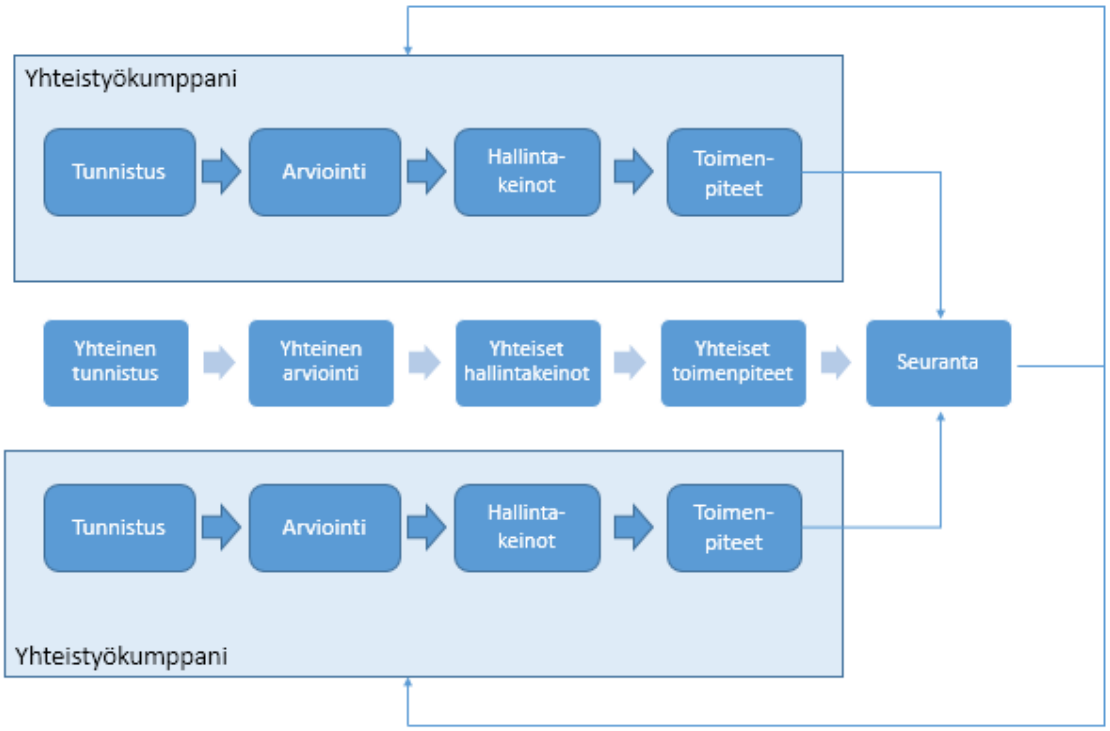
Verkostoitumisella on moninaisia vaikutuksia yrityksen riskikenttään. Yritykset toimivat useissa verkostoissa ja yhtä yhteistä verkoston riskiä ei ole. Verkostossa yritykset tulevat riippuvaisiksi toisistaan ja toistensa riskeistä. Verkostossa tapahtuu riskin jakamista ja siirtoa osapuolelta toiselle. Verkosto monimutkaistuu, koska varsinaisen toimitusverkoston lisäksi siihen linkittyy erilaisia tietoon ja tiedonkäsittelyyn liittyviä yrityksiä. Lisääntynyt riippuvuus eri systeemeistä ja toimijoista sekä verkoston rakenteen kompleksisuus vaikeuttaa riskin tunnistamista ja niihin varautumista. Haittavaikutusten arviointi on hankalaa, koska yhden verkoston jäsenen riskin toteutumisen heijastusvaikutukset voivat ulottua pitkälle-kin. Riskiin liittyy olennaisesti ei-toivottujen tapahtuman epävarmuus. Verkostoyrityksen riskien taustalla on useita tekijöitä kuten kysyntä loppuasiakkaalta, verkoston asema sekä uskottavuus, yrityksen asema toimitusketjussa tai verkostossa ja tuotteen toimituskyky. (Virolainen & Hallikas 2005, 227-228.) Verkoston epävarmuuslähteet on esitetty seuraavassa kuviossa (Kuvio 7).



Kuvio 7 Verkoston epävarmuuslähteet (Virolainen &Hallikas 2005, 229.)

Vastaavat tekijät esiintyvät myös ei-verkottuneessa ympäristössä. Verkostoituminen ei poista näitä epävarmuuksia, mutta se voi muuttaa niiden seurauksia, Verkostoituminen vaikuttaa riskien jakautumiseen eri yrityksille, vähentää joitakin riskejä ja taas lisää toisia. Verkostoitumisen vaikutus riippuu yrityksen asemasta, tilanteesta, toimintaympäristöstä ja toimintatavoista. (Virolainen & Hallikas 2005, 229.)

Verkostoriskejä tarkasteltaessa on otettava huomioon, että yritykset ovat verkostossa riippuvaisia toisistaan ja voivat vähentää riskejä yhteistyöllä. Riskienhallintaprosessin riskianalyysit voivat olla osittain yhteisiä. (Virolainen & Hallikas 2005, 230.) Seuraavassa kuviossa (kuvio 8) on esitetty malli riskienhallinnasta verkostossa.



Kuvio 8 Verkoston riskienhallintamalli (Hallikas ym. 2001; Virolainen & Hallikas 2005, 231)

Verkostojen rakenteen monimutkaisuus saattaa vaikeuttaa riskien tunnistamista. Verkoston ja yksittäisten yritysten on voitava suojautua tunnistettujen riskitekijöiden vaikutukselta ja valita kuhunkin tilanteeseen sopivia riskienhallintakeinoja. Jokaisen yrityksen ja verkoston tulisi räätälöidä riskien arviointimalli omiin tarkoituksiinsa sopivaksi. Verkostoyhteistyössä riskien arviointi voidaan tehdä luotettavimmin, jos se tehdään yhteisten riskien osalta yhdessä. (Virolainen & Hallikas 2005, 231-232.)

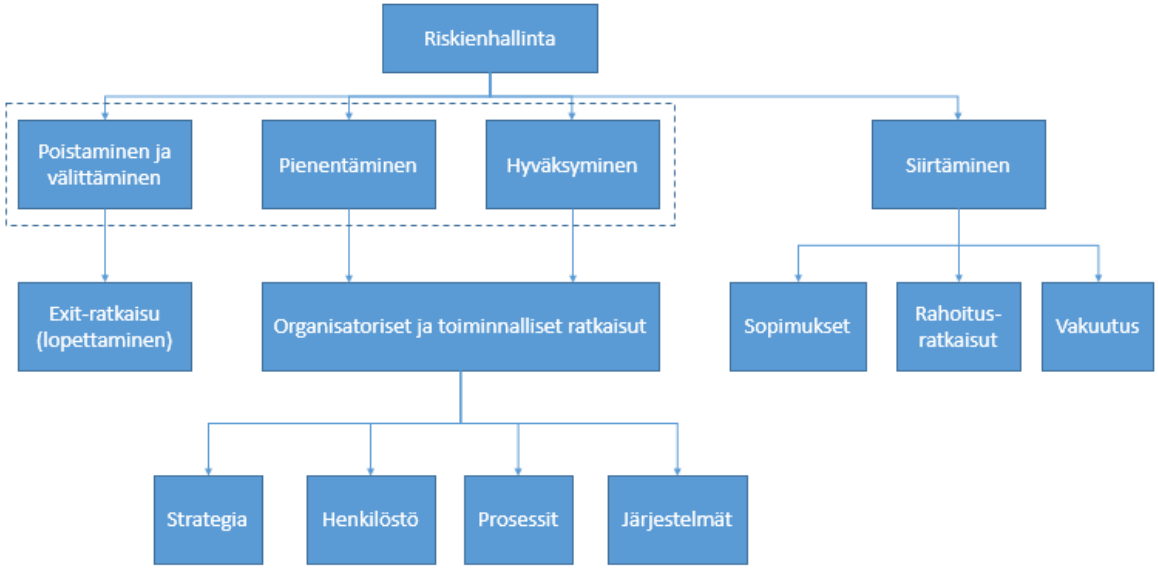
2.3.4 Riskienhallintakeinot

Riskienhallintaprosessin tarkoitus on lisätä ymmärrystä riskeistä, jotta voidaan tehdä toimenpiteitä ja päätöksiä riskien hallitsemiseksi. Toimiva riskienhallinta edellyttää yritykseltä sekä pitkäaikaista sitoutumista että valmiutta ryhtyä riskienhallintaa edistäviin toimenpiteisiin. Yritys joutuu riskienhallintakeinoja tehdessään pohtimaan, millaisen suojan riskienhallintatoimet antavat ja mitä ne maksavat. Riskit pyritään tunnistamaan ja arvioimaan riskianalyysin avulla. Vain tunnistettuja ja arvioituja riskejä vastaan voidaan kehittää riskienhallintatoimenpiteitä. Analysoidut riskit on pystyttävä mukauttamaan yrityksen nor-

maaliin toimintaan. Yrityksen on myös kyettävä kantamaan riskeistä aiheutuvat taloudelliset seuraukset. Hyvältä riskienhallinnalta vaaditaan ennen kaikkea riskienhallintakeinojen tehokasta soveltamista sekä riskien rahoittamiseen liittyvien kysymysten hallitsemista. (Suominen 2003, 97-98; Ilmonen ym. 2013, 116.)

Hallintakeinojen jaottelu

Riskienhallintatoimet voidaan karkeasti jakaa omiin riskienhallintatoimenpiteisiin ja riskin siirtämiseen. Lähtökohtaisesti riskejä täytyy pyrkiä hallitsemaan omilla riskienhallintakeinoilla. Mikäli nämä eivät riitä, niin osa riskeistä voidaan siirtää vakuutusyhtiöille, rahoituslaitoksille tai muille sopimuskumppaneille. (Ilmonen ym. 2013, 116.) Ilmonen ym. (2013, 116) esittävät seuraavan kuvion (kuvio 9) mukaisen jakauman hallintakeinoille.



Kuvio 9 Riskienhallintakeinoja (Ilmonen ym. 2013, 116)

Suomisen (2003, 98) mukaan tavanomaisina keinoina hallita riskejä ovat

- riskin välttäminen
- riskin pienentäminen
- riskin jakaminen
- riskin siirtäminen
- riskin ottaminen.

Virolaisen ja Hallikkaan (2005, 232-233) mukaan verkoston riskeihin varautumiskeinoina toimivat

- yleiset hyvät toimintatavat
- tyypillisten verkostoriskien välttäminen
- riskien systemaattinen tarkastelu verkostoyhteistyössä.

Riskienhallintatoimenpiteistä omina toimenpiteinä voidaan pitää riskien kontrollointia. Siirtämistä ja omalla vastuulla pitäminen ovat riskien rahoituskeinoja. Pääsääntönä toimenpiteiden suunnittelussa on ensisijaisesti riskien toimenpiteiden avulla pienentää riskin todennäköisyyttä ja seurausta. Vasta toissijaisesti siirretään jäljelle jäävä osuus riskistä kolmannelle osapuolelle. Yrityksen riskienhallinnan edellytyksenä on siten sekä kontrollointitoimien että rahoitustoimien toteuttaminen. (Ilmonen ym. 2013, 117; Suominen 2003, 98.)

Riskin välttäminen ja syvällisempänä keinona poistaminen, edellyttää sitä, että riskin aiheuttanut syy pystytään kokonaan eliminoimaan esimerkiksi luopumalla toiminnasta tai luopumalla tuotannossa riskialttiin materiaalin käytössä. Riskien poistaminen sopii lähinnä henkilöriskien ja erilaisten ympäristö- ja turvallisuusriskien osalta, joissa ainoa tavoite on nollatoleranssi. Välttäminen voidaan toteuttaa pidättäytymällä riskialttiista toimista kokonaan. (Ilmonen ym. 2013, 199; Suominen 2003, 101-102.)

Riskin pienentäminen tähtää vahinkotapahtuman todennäköisyyden tai seurausten pienentämiseen. Mahdollinen vahinko pyritään riskiä pienentämällä saamaan pienemmäksi tai se pyritään rajoittamaan ainoastaan osaan riskikohteesta. Riskin pienentäminen voidaan toteuttaa useilla erilaisilla tavoilla, kuten lisäämällä teknisiä suojelutoimenpiteitä, henkilöresursseja, koulutusta ja muita keinoja. Useimpien riskien osalta riskin pienentäminen on mahdollista. (Ilmonen ym. 2013, 119; Suominen 2003; 102.)

Riskien jakaminen on tunnetuin ja eniten sovellettu riskienhallintakeino. Riskiä jakamalla lisätään itsenäisten riskikohteiden määrää. Vahinkotapahtuman sattuessa on todennäköistä, että ainakin osa riskikohteista säilyy vahingoittuma. Esimerkiksi rakennuksen jako palo-osastoihin ja laivojen vesitiiviit osastot ovat riskin jakamista. Riskin jakaminen on keskeinen liikeriskien hallinnan menetelmä. Tällä pyritään purkamaan yksipuolisuustilanteita esimerkiksi jakamalla markkinat uudella tavalla, hankkimalla vaihtoehtoisia tavarantoimittajia, pienentämällä tietyn tuotteen hallitsevuutta tai kehittämällä vaihtoehtoisia toimintatapoja ja uusia kilpailukykyisiä tuotteita. (Suominen 2003, 102-104.)

Riskien hyväksyminen saattaa olla paras ratkaisu pienten ja epätodennäköisten tunnistettujen riskien osalta. Riskin ottaminen eli pitäminen tai hyväksyminen omalla vastuulla on mahdollista, jos yritys pitää mahdollisena riskin rahoittamista omasta kassasta. Rahoituksessa riskejä voidaan pitää omalla vastuulla ja maksaa seuraukset kassasta, joka toimii useasti sattuvien pienten vahinkojen riskien osalta. Toinen tapa on rahastointi, yritys varautuu vahinkojen aiheuttamiin taloudellisiin menetyksiin vuosittaisella tietyn summan rahastoinnilla. Vakuutusten ja sopimusten omavastuiden valinta on myös riskin hyväksymis-

tä. Organisatorisesti ratkaisuna hyväksyntätoimenpide saattaa rajoittua siihen, että sovitaan selkeästi kenellä on vastuu seurata ja raportoida pienistä tunnistetuista riskeistä. Pienten riskien osalta seurannassa tulee huomioida niiden mahdolliset riippuvuudet, kerrannaisvaikutukset ja kehittyminen. Myös yrityksen riskinkantokyvyn muutokset ja riskinottohalun muutokset saattavat muuttaa riskienhallintatoimenpiteitä pienten riskien osalta. (Ilmonen ym. 2013, 118-119; Suominen 2003 140.)

Riskin siirtäminen merkitsee riskialttiin toiminnan siirtymistä sopimuksen perusteella jollekin toiselle osapuolelle. Riskit voidaan siirtää sopimuksilla, rahoitusratkaisulla tai vakuutuksilla. Yleisin tapa on siirtää riski vakuutussopimuksella vakuutusyhtiölle. Sopimuksilla siirto voi tarkoittaa esimerkiksi toiminnan ulkoistamista. Yritys voi siirtää riskejä sisältävää omaisuutta tai riskipitoisia toimintojaan toisen yrityksen kannettavaksi sopimuksella. Rahoitusratkaisulla tarkoitetaan lähinnä erilaisten rahastoivien ratkaisujen ja johdannaisten käyttöä riskienhallintavälineinä. Riskien siirrossa, kuten vakuuttamisessa, riskien vastuut ja vastuu riskienhallinnasta eivät siirry. Vakuutukset harvoin korvaavat koko vahinkoa kaikkine seurannaisvaikutuksineen. Korvauksena on omavastuun jälkeinen taloudellinen vahinko, mutta yrityksen kustannuksiksi voi jäädä maineriskejä, viivästyksestä ja ylimääräisestä työstä aiheutuneita kuluja. (Ilmonen ym. 2013, 120; Suominen 2003, 114-115.)

Verkostoriskeissä yleiset hyvät toimintatavat tukevat riskienhallintaa. Yhtenä tärkeimmistä riskienhallinta keinoista on yrityksen verkkostrategian kehittäminen. Tällä liitetään yrityksen tavoitteet verkoston yhteisiin tavoitteisiin ja tulevaisuuden visioihin. Yrityksen tulee pystyä kehittämään omaa ydintoimintaansa ja resurssejaan suhteessa verkostostrategiaan, jolla on vaikutusta yrityksen asemaan verkostossa. Lisäksi yrityksen tulee analysoida keskeiset riippuvuudet ja niistä aiheutuvat mahdollisuudet ja riskit. Yleisesti avoimuus yhteystyöhön ja luottamus verkoston sisällä ovat tärkeitä elementtejä tiedon jakamisessa ja kommunikoinnissa. Toiminnan tasolla toimintaprosessien ja materiaali- ja informaatiovirtojen yhteinen kehittäminen ja hallinta on koettu tärkeäksi. Tämän lisäksi kilpailijoiden kanssa on pystyttävä tekemään yhteistyötä, jos ylemmän tason tavoitteiden saavuttaminen sitä edellyttää. Sopimuskäytäntöjä kehittämällä pyritään ottamaan huomioon ja määrittelemään riskin hinnoittelua ja tasapainottamista yhteistyössä. (Virolainen & Hallikas 2005, 232.)

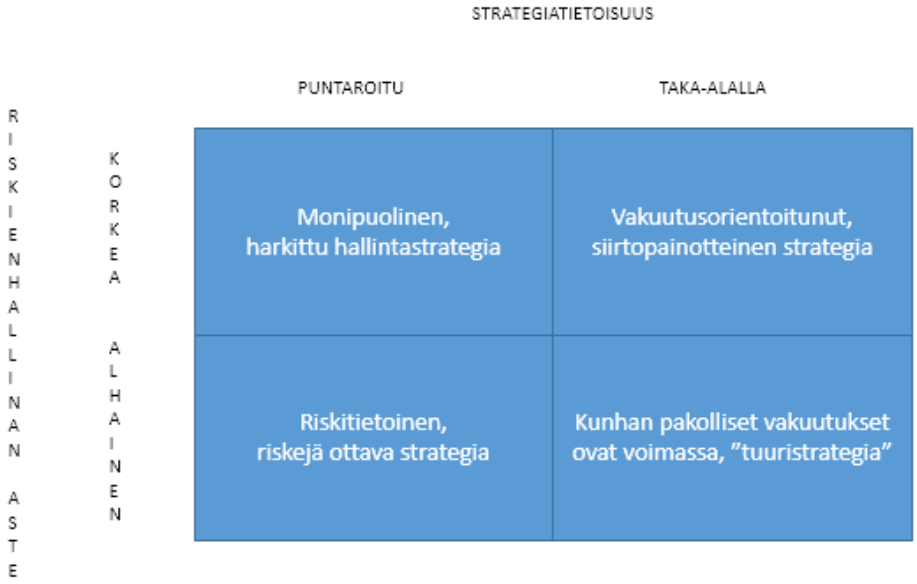
Tyypillisten verkostoriskien välttämistä voidaan tehdä kohdentamalle yleisille verkostoriskeille hallintakeinoja ja toimintatapoja, joilla riskejä voi alentaa tai muita vaikutuksia muuttaa. Yleisesti oleellista on pyrkiä välttämään liian suurta riippuvuutta yksittäisestä verkoston toimijasta. Riskin systemaattinen tarkastelu verkostoyhteistyössä edellyttää yrityksen oman riskitilanteen tunnistamista ja priorisointia. Tällöin voidaan keskittyä riskeihin, jotka

ovat omassa yrityksessä merkittäviä ja voidaan päästä tehokkaampiin, tarkemmin kohdistettuihin toimenpiteisiin. Analyysi antaa pohjan myös riskitilanteiden seurannalle ja helpottaa mahdollisten muutosten ennakointia ja niihin reagointia. Tämä antaa perustan myös yrityksen tärkeille päätöksentekotilanteille. Riskitietoisuuden jakaminen päähankkijan ja toimittajan välillä voi tukea riskien hallintaa. Toisaalta se voi myös johtaa yhteistyösuhteista ja tasapainosta riippuen toisen osapuolen hyväksikäyttöön. (Virolainen & Hallikas 2005, 232- 233.)

Hallintakeinojen valinta

Riskienhallintaprosessissa riskianalyysin jälkeen siirrytään vaiheeseen, jossa tehdään hallintakeinoja koskevat valintapäätökset. Päätöksenteossa tarvitaan myös ajallinen ulottuvuus. Riskienhallinta tähtää vahinkojen ennaltaehkäisyyn, joten yrityksen pitää varautua riskeihin tekemällä ratkaisuja tulevaisuuden varalle. Tärkeää on myös, miten toimitaan vahingon tapahduttua. Riskienhallintapäätökset voidaan siten jakaa loogisesti kolmeen tyyppiin: ennen vahinkotapahtumaa tehdyt päätökset, välittömästi vahingon yhteydessä tehtävät ratkaisut ja päätökset jotka tehdään vasta vahinkotapahtuman jälkeen. (Suominen 2003, 99-100.)

Erilaiset riskit vaativat erilaisia suojaustapoja. Onnistuneessa riskienhallintatyössä kyetään hyödyntämään laajalti riskienhallintakeinoja. Keinojen käyttötapa muodostaa yrityksen riskienhallintastrategian. Riskienhallintastrategia näkyy konkreettisesti siinä, miten tunnettuihin riskienhallintakeinoihin suhtaudutaan ja miten yritys suojautuu tunnistamiensa riskien varalta. Yrityksissä toteutetut riskienhallinta- ja vakuutusratkaisut ilmentävät yrityksen omaksumaa toimintalinjaa yritystä uhkaavien riskien suhteen. Käyttäytyminen näkyy riskistrategioina, riski joko pyritään hallitsemaan eri keinoja soveltamalla tai hallintapyrkimys jää tai se jätetään päätöksentekomielessä taustalle. (Suominen 2003, 159-160.) Strategisia vaihtoehtoja riskienhallintaan on kuvattu seuraavassa kuviossa (kuvio 10).

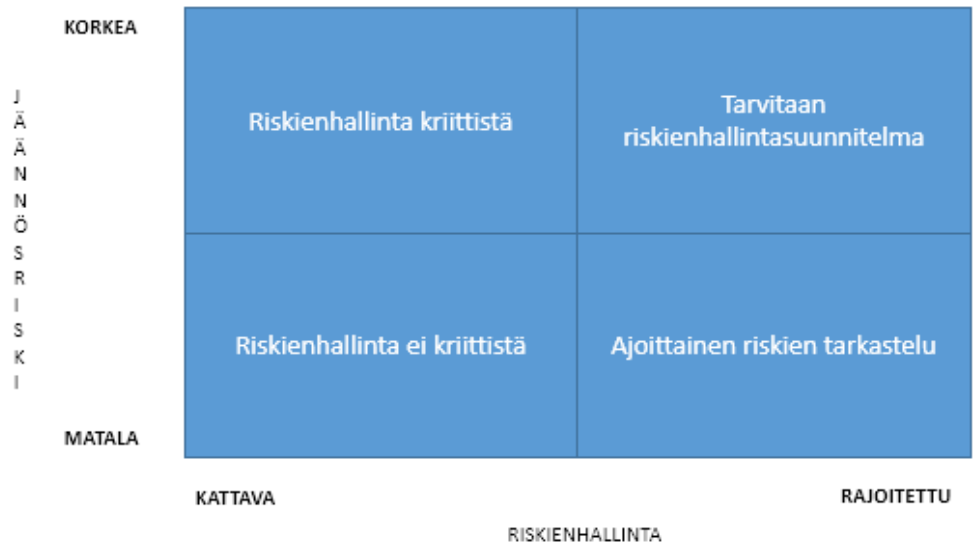


Kuvio 10 Riskienhallinnan perusstrategiat (Suominen, 1994)

Kun yritys arvioi ja valitsee riskienhallintatoimenpiteitä, on tärkeää, että asiaa tarkastellaan kokonaisvaltaisesti hyödyntäen kaikkea saatavilla olevaa tietoa. Tapahtuneista poikkeamista kerätty tieto ja vahinkojen listaaminen ja analysointi sekä niistä oppien kerääminen on esimerkki tiedoista joita voidaan hyödyntää. Näiden perusteella voidaan valita toimia, jotka pyrkivät estämään vahinkoja tapahtumasta tai että vahinkojen vaikutukset olisivat paremmin ennakoitavissa ja hallinnassa. Riskienhallintatoimenpiteiden valintaa ja kohdistamista helpottaa jos riskit on luokiteltu tarkoituksenmukaisella tavalla. Tämä voi tarkoittaa riskien jakoa riskiluokkiin, kuten luvussa 2.2.2 on esitetty. Riskejä voidaan myös jakaa suuruuden ja todennäköisyyksien avulla tärkeysjärjestykseen esimerkiksi kolmiportaisesti liikennevaloja mukailemalla tai useampaan luokkaan. Riskejä voidaan myös arvioida euroissa, joka mahdollistaa rahamääräisen tärkeysjärjestyksen luomisen. (Ilmonen ym. 2013; 118.)

Riskienhallintaan on yleensä käytettävissä niukasti varoja, joten on pohdittava tarkkaan miten varat on järkevä käyttää riskien suojaamiseen. Keskeinen kysymys on lisäksi se, millaisia riskejä yrityksen ei kannata suojata lainkaan. Riskin suojauksesta maksettava hinta voi olla liian korkea, suojausta ei ole saatavissa tai yrityksen taloudellinen tilanne voi olla niin vahva, että se voi kantaa osan riskeistä itse. Riskienhallintaa käytettävien varojen puntarointi on keskeinen ongelma, jonka jokainen yritys joutuu ratkaisemaan. Yrityksen kannalta on tärkeintä pystyä painamaan riskikustannukset mahdollisimman alhaisiksi. (Suominen 2003, 116.)

Ilmonen ym. (2013, 90) mukaan riskienhallinnassa tarvittavaa ja tarkoituksenmukaista resursointia ja toimenpiteitä eri riskiluokille voidaan arvioida seuraavan kuvion (kuvio 11) mukaisella riskimatriisilla.



Kuvio 11 Riskimatriisi resursoinnin ja toimenpiteiden arviointiin (Ilmonen ym. 2013, 91)

Julkisen sektorin organisaation tulisi kiinnittää erityistä huomiota maineriskien hallintaan. Niiden siirtäminen ei ole mahdollista eikä niitä voida kokonaan poistaa tai vakuuttaa. Maineriskien toteutuminen voi vaikuttaa jopa organisaation toiminnan jatkuvuuteen. Luottamus organisaation toimintaan on helppo menettää, mutta äärimmäisen työläs tai jopa mahdotonta palauttaa. (Scherf 2012, 108.)

2.3.5 Riskien raportointi

Riskien ja riskienhallinnan raportointi liittyy riskienhallinnan johtamiseen. Riskien raportointi on olennainen osa johdon raportointia. Raportointi kannattaa liittää osaksi johtamis- tai strategiaprosessia, jolloin johdon riskiraportointi tapahtuu määrävälein. Mitä tehokkaammin riskienhallinta on osana liiketoimintaa ja johtamista, sitä enemmän riskienhallinnan tietoja voidaan hyödyntää päätöksenteon tukena. (Ilmonen ym. 2013, 177.)

Raportoinnin taso ja sisältö

Raportointi voidaan jakaa ulkoiseen ja sisäiseen raportointiin. Ulkoisella riskienhallintaraportoinnilla tarkoitetaan julkista ja sidosryhmäraportointia. Sisäisellä riskienhallintaraportoinnilla tarkoitetaan kokonaisvaltaista riskienhallintaraportointia sekä muuta sisäistä ris-

kienhallintaraportointia, jotka yleensä sisältävä yrityksen kannalta hyvin luottamuksellista tietoa. Sisäiseen raportointiin voidaan laskea mukaan myös operatiivinen raportointi, jossa raportoidaan liiketoimintatason läheltä piti –tilanteita ja vahinkoja. (Ilmonen ym. 2013, 178.)

Riskiraporttien laajuus ja sisältö vaihtelee käyttötarkoituksen mukaan. Hallitustason riskiraportointi on usein kooste. Yrityksen johdon riskiraportointi on seikkaperäisempi ja siihen on usein liitetty merkittävimpien strategisten ja toimintaympäristöriskien seuranta. Yksikkötason raportointi on laajempi ja yksityiskohtaisempi raportti. Yksikkötason raportissa on painopiste yleensä riskienhallintatoimenpiteiden suunnittelussa, vastuuttamisessa ja toteutuksen seurannassa. Yksikkötasolla voidaan yksityiskohtaisesti arvioida riskienhallintatoimenpiteiden kustannus- ja hyötysuhdetta sekä tarvittavia resursseja ja aikatauluja. Operatiivisella tasolla voidaan parhaimmillaan riski- ja muiden raporttien perusteella seurata viikkopalavereissa omia riskejä, läheltä piti –tilanteita ja tapahtuneita vahinkoja, niistä saatuja oppeja ja ennaltaehkäiseviä toimia. (Ilmonen ym. 2013, 176.)

Johtamisen ja kontrollin kannalta on tärkeää, että johdon riskiraportit noudattavat säännönmukaista aikataulua ja rakennetta. Suurimmat riskit yrityksissä pysyvät usein samana, mutta niiden vaikutus ja näkymät saattavat muuttua ja sen mukaisesti myös hallintatoimenpiteet. Riskiraporttien pohjalta voidaan pyytää lisäselvityksiä esimerkiksi vastuullisilta henkilöiltä tai sopia tarkemmista muutoksista ja toimenpiteistä. Painopiste johdon riskiraportoinnissa on siirtynyt toimenpiteiden ja niiden vaikuttavuuden seurantaan ja tulevaisuuden arviointiin ennakoimalla mihin suuntaan riskit kehittyvät. (Ilmonen ym. 2013, 177.)

Leino ym. (2005, 141) ovat määritelleet sisäisen liiketoimintayksikön riskiraportin sisällöksi

- riskin kuvaus ja riskin lähde
- seuraus, jos ei reagoida
- taloudellinen vaikutus
- muut vaikutukset
- toteutumisen todennäköisyys.

Leino ym. (2005, 144-145) mukaan yhtiötasoisen avainriskien analyysiraportti sisältää

- riskin kuvaus
- riskin omistaja
- riskin syy, riskin lähteet
- todennäköisyys
- vaikutusaika
- bruttovaikutus
- nettovaikutus (kontrollien riittävyyden arviointi)
- liitännäisriskit
- todennäköisin kokonaisvaikutus
- pahin mahdollinen vaikutus
- suunnitellut kontrollit ja toimenpiteet

- riskienhallinnan kustannukset
- riskin suunta (kasvava, pienenevä)
- seurantavastuut ja aikataulut
- tarkistuspäivämäärä.

Riskiraportti ohjaa johtamista ja auttaa ylintä johtoa ja toimintayksiköiden johtoa tekemään päätöksiä koskien operatiivista ja riskienhallintatoimintaa ja resursseja. Hallituksen ja ylimmän johdon riskiraportti on yhteenveto kaikista riskiraporteista. Siinä keskitytään yrityksen kannalta kriittisiin riskeihin ja niiden muutosten ja riskienhallintatoimenpiteiden vaikutusten seurantaan. Operatiivisella tasolla on tärkeää keskittyä oman toiminnan riskeihin ja konkreettiseen riskienhallintatoimien analysointiin. (Ilmonen ym. 2013, 181.)

Riskisalkku raporttien lähteenä

Yrityksen tunnistamat, analysoimat ja toimenpiteiden suunnittelua varten priorisoimat keskeiset riskit kannattaa koota yrityksen riskisalkuksi. Siihen kannattaa ottaa merkittävimmät riskit suuruusjärjestyksessä. Priorisointi voidaan tehdä riskiluvun avulla. Tämä menetelmä on esitelty luvussa 2.3.3. Riskejä tulee ennen salkkuun viemistä analysoida, ettei sinne päädy samaa riskiä kahteen kertaan sekä tunnistaa riippuvuudet riskien välillä, jotta syy-seuraussuhteet tunnistetaan ja voidaan raportoida vain kerran. Riskisalkkuun on hyvä merkitä myös lyhyesti suhteet riskien välillä. (Ilmonen ym. 2013, 172.)

Riskisalkun sisältö riippuu riskienhallinnan fokuksesta. Jos fokuksessa on ollut tunnistaa riskit, joilla voi olla negatiivisia seurauksia strategisten tavoitteiden saavuttamisessa, tästä yleensä seuraa, että riskisalkku painottuu strategisiin riskeihin. Operatiiviset riskit ovat myös suuri joukko ja sen jälkeen taloudelliset. Vahinkoriskejä on tyypillisesti vähiten. Painotukset riippuvat jossain määrin myös yrityksen koosta, pienissä yrityksissä yksittäiset operatiiviset tai vahinkoriskit olla yrityksen merkittävimpiä riskejä. (Ilmonen ym. 2013, 173.)

Salkku mahdollistaa tarkastelun mitkä riskit vaikuttavat strategisten tavoitteiden saavuttamiseen. Tämä edellyttää riskien kiinnittämistä strategiseen tavoitteiseen. Riskien raportoinnin yhteydessä päivitetään tilannetta ja saadaan kuva mikä on strategisen tavoitteen suunnitellun vaikutuksen suhde sen esteenä tai hidasteena oleviin analysoituihin riskeihin. Salkun avulla voidaan muodostaa näkemys yrityksen riskeistä suhteessa riskinkantokykyyn. Riittävän kattava otanta keskeisistä riskeistä riskisalkussa ja sen vertailu asetettuun riskinkantokykyyn mahdollistaa riskitilanteen tarkastelun järkevällä tarkkuudella ja tasolla sekä samalla on mahdollista saada varmuus riskinkantokyvyn riittävyydestä. Salkkua voidaan myös hyödyntää riskiskenaarioiden tarkasteluun. Käymällä läpi skenaarioita ja vertaamalla niitä riskisalkun sisältöön, voidaan tarkastella skenaarioiden vaikutuksia. Näitä

voidaan taas puolestaan tarkastella yrityksen riskinkantokykyyn nähden. (Ilmonen ym. 2013, 173.)

2.3.6 Riskienhallinnan kehittäminen

Riskienhallinnan kehittäminen tulee nähdä mahdollisuutena vaikuttaa yrityksen kilpailukykyyn. Parhaassa tapauksessa riskienhallinnan kehittämisellä saadaan tuloksia ja läpinäkyvyyttä yrityksen strategisten tavoitteiden saavuttamisessa sekä päätöksenteon tuessa. Organisaation on kuitenkin huomioitava sen organisaatiokulttuuri ja kehitettävä tähän sopiva menetelmä riskienhallintaan. Asioita ei tule monimutkaistaa, vaan rohkaista keskusteluun ja alussa keskittyä riskienhallinnan hyötyihin. Työntekijöitä tulee ohjata keskustelemaan organisaation toiminnasta ja mikä siinä voi mennä pieleen ja siten vaikuttaa haitallisesti asetettujen tavoitteiden saavuttamiseen. (Marchetti 2012, 2; Leino, Steiner & Wahlroos 2005, 127-128.)

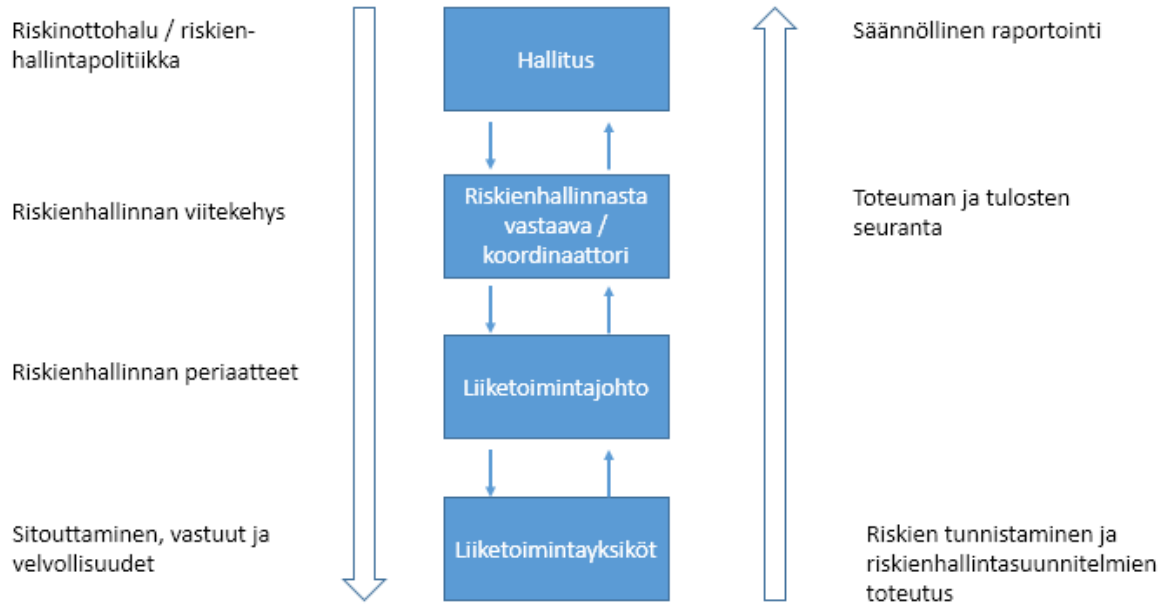
Kehittämisen tavoitteet

Riskienhallintaa kehitettäessä on syytä aluksi määritellä ja tarkentaa riskienhallinnan tavoitteet ja periaatteet. Tähän liittyvä ohjeistus voidaan tarkentaa kolmiportaisena: riskinhallintapolitiikka, riskienhallinnan periaatteet ja toimintapolitiikat. Riskienhallintapolitiikka on periaatedokumentti, joka kuvaa riskienhallinnan yleiset periaatteet ja tavoitteet sekä riskienhallintapolitiikan kattavuuden sekä mitä riskillä tarkoitetaan. Politiikka on yleensä pelkistetty muutaman sivun mittainen dokumentti. Riskienhallinnan periaatteet dokumentaatio kuvaa tarkemmin riskienhallinnan strategiat ja tavoitteet, riskienhallintaprosessin, merkittävimmät riskialueet, organisatoriset vastuut, mittarit ja miten johto varmistuu riskienhallinnan prosessien ja toimenpiteiden tehokkuudesta ja riittävyydestä. Toimintapolitiikat kuvaavat eri toiminta-alueiden riskienhallinnan toiminnan ja menetelmät. (Leino ym. 2005, 128-129.)

Organisaation tulisi pyrkiä rakentamaan sen toimintaan integroitu riskienhallinta. Tähän kuuluu kolme osaa: keskitetty riskienhallinnan raportointi ylimmälle johdolle, integroitu riskienhallinnan strategia, joka huomioi kaiken tyyppiset riskit organisaatiossa ja integroitu riskienhallinta liiketoimintaprosesseihin. Näiden tavoitteiden saavuttaminen ei ole helppoa. Menetelmä ja prosessit tavoitteiden saavuttamiseksi vaihtelee huomattavasti riippuen organisaation koosta, rakenteista ja organisaatiokulttuurista. Jokaisen organisaation on päätettävä sille parhaiten sopiva toteutus. Integroitu lähestyminen mahdollistaa riskienhallinnan muodostua ennakoivaksi hyödylliseksi työkaluksi johdolle, eikä tavanomaiseksi tapahtumiin reagoivaksi toiminnaksi. (Marchetti 2012, 3.)

Johdon rooli riskienhallinnan kehittämisessä

Vastuu riskienhallinnasta tulee olla tarpeeksi ylhäällä organisaatiossa. Riskienhallinta on pohjimmiltaan laadukasta johtamista ja sitä ei voi siten kehittää kattavasti ilman yrityksen ylimmän johdon sitoutumista ja jatkuvaa tukea sekä selkeää mandaattia tehtävälle työlle. Vastuuhenkilöllä pitäisi olla tarpeeksi asiantuntemusta ja valtaa viedä kehittämiseen liittyviä asioita eteenpäin organisaatiossa. Osa yrityksistä on nimennyt riskienhallintajohtajan, joka raportoi toimitusjohtajalle tai talousjohtajalle. Riskienhallinnan johtamisessa ja kehittämisessä johdon eri osapuolille on määritelty omat roolinsa. Hallitus määrittelee yrityksen riskinottohalun sekä vastaa riskienhallinnan tulosten ja toimenpiteiden seurannasta. Lisäksi hallitus vastaa riskienhallintaprosessien toimivuuden arvioinnista vuosittain. Riskienhallintajohtaja tai sen koordinoinnista vastaava johtaja vastaa riskienhallinnan viitekehyksen kehittämisestä ja käyttöönotosta. Riskienhallintajohto vastaa hallitukselle raportoinnista. Liiketoimintajohto vastaa riskienhallinnan strategiasta ja periaatteista sekä toteutumisen seurannasta hallituksen antamilla valtuuksilla. Liiketoimintayksikön johto vastaa toteuttamisen organisoinnista ja henkilöstön sitouttamisesta omalla alueellaan. Yksikön johto vastaa riskienhallintasuunnitelmien laatimisesta sekä riskien seurannasta. Lisäksi yksikön johto raportoi säännöllisesti oman liiketoimintayksikkönsä riskeistä. (Ilmonen ym. 2013, 37; Leino ym. 2005, 129-130.) Johdon rooli johtamisessa ja kehittämisessä on kuvattu seuraavassa kuviossa (kuvio 12).



Kuvio 12 Johdon rooli riskienhallinnassa (Leino ym. 2005, 131)

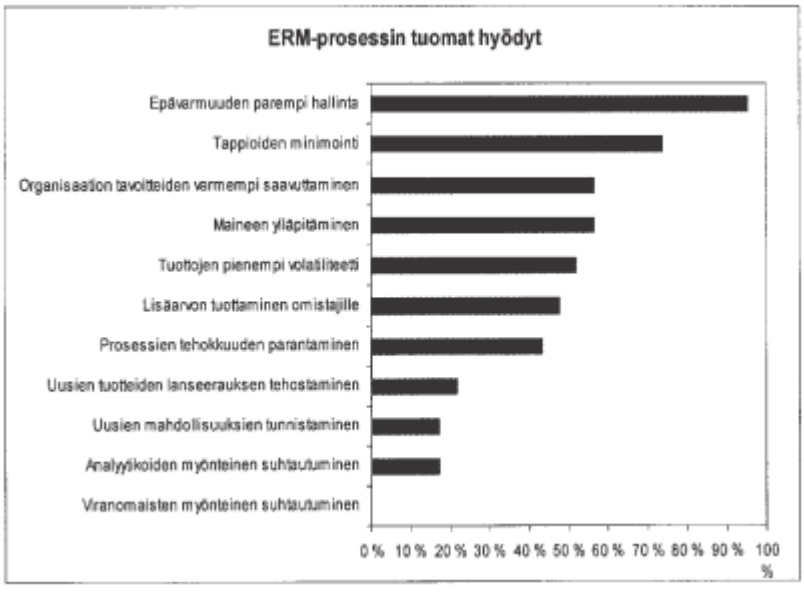
Sisäisen tarkastuksen, jos sellainen on käytettävissä, rooli riskienhallinnassa tulisi painottua riskienhallintaprosessin toimivuuden valvontaan. Sisäinen tarkastus voi esimerkiksi

arvioida, miten johto varmistuu riskienhallinnan osa-alueiden tehokkuudesta ja riittävyydestä. Myös tarkastusvaliokunnalla on rooli riskienhallinnassa, jos sellainen on perustettu. Tarkastusvaliokunnan tehtävänä on yhtiön riskiprofiilin läpikäynti ja varmistaminen, että taloudellista raportointia koskevat riskienhallintamenettelyt ovat olemassa. Säännellyillä toimialoilla on yleistä, että yhtiöt perustavat erityisiä riskienhallinnan koordinointiin ja valvontaan keskittyviä toimielimiä tai lisäävät riskienhallinta-asiat tarkastusvaliokunnan tehtäviin. Näissä tapauksissa tarkastusvaliokunnan tulee ymmärtää näiden toimielimine asema ja tehtävät ja varmistaa hallituksen kautta säännölliset yhteydet esimerkiksi riskivaliokuntaan. (Leino ym. 2005, 131; Leino ym. 2005, 133.)

Riskienhallinnan kehittämisen hyödyt

Riskienhallintaprosessin avulla yritykset pystyvät tehokkaammin tunnistamaan, minimoimaan ja hallitsemaan riskitekijöitä, jotka uhkaavat niiden toimintaa ja strategisia tavoitteita. Päätöksenteon laatua voidaan myös parantaa. (Leino ym. 2005, 132; PricewaterhouseCoopers 2004a)

Suomalaisten suuryritysten näkemys kokonaisvaltaisen riskienhallinnan prosessin tuomista eduista painottuu epävarmuuden parempaan hallintaan, tappioiden minimointiin, organisaation tavoitteiden saavuttamiseen sekä yritysten maineen ylläpitämiseen. Myös tuottojen pienempi volatiliteetti, lisäarvon tuottaminen omistajille ja prosessin tehostaminen katsotaan tärkeäksi. (Leino ym. 2005, 134.) Hyödyt on esitetty seuraavassa kuviossa (kuvio 13).



Kuvio 13 ERM-riskienhallinnan hyödyt (Leino ym. 2005, 134; PricewaterhouseCoopers Oy 2004b.)

Kun yritys pyrkii riskienhallinnan keinoin ymmärtämään sekä tulevia mahdollisuuksiaan että riskejään, erilaisten toimintakenttää ja markkinoihin liittyvien ilmiöiden ja trendien ymmärtäminen helpottuu huomattavasti. Yrityksen johto kykenee tällöin ottamaan tehokkaammin alan ja toimintaympäristön muutospaineet huomioon osana johtamista. Riskienhallinnan avulla yritys pyrkii ymmärtämään, miten se voisi parhaiten varmistaa strategisiin tavoitteisiin pääsyn estämällä uhat ja hyödyntämällä mahdollisuudet. (Ilmonen ym. 2013, 16.)

Riskienhallinta on käytettyjen resurssien, pääomien ja kustannusten optimoimista suhteessa tavoiteltaviin hyötyihin. Riskienhallinnan optimitason löytäminen onkin yksi riskienhallinnan keskeisimpiä tavoitteita. Kun yritys onnistuu tässä, sille syntyy kilpailuetu muihin kilpaileviin yrityksiin verrattuna, jotka joko panostavat liikaa tai liian vähän riskienhallintaan suhteessa omiin riskeihinsä. Integroimalla riskienhallinta kaikkiin johtamisprosesseihin helpottaa keskittymistä olennaiseen. Riskien ja liiketoimintamahdollisuuksien analysoinnin tarkoitus on auttaa löytämään positiiviset ja negatiiviset asiat, joihin panostaminen antaa parhaan mahdollisen lopputuloksen pienimmällä mahdollisella panostuksella suhteessa yrityksen tavoitteisiin. (Ilmonen ym. 2013, 16-17.)

Organisaation sisäistä yhteistyötä voidaan parantaa riskienhallinnan avulla. Riskienhallinnan työvaiheet ja erityisesti riskiraportointi tuovat läpinäkyvyyttä, auttavat osoittamaan organisaation rajapintoihin liittyviä ongelmia, analysoimaan ja arvioimaan niitä sekä kehittämään ratkaisuja. Riskienhallinta tuottaa myös systemaattisesti tietoa yrityksen kulloisesta tilasta sekä mahdollistaa yritystä löytämään uudenlaista synergiaa. Tehokas ja kokonaisvaltainen riskienhallinta on myyntiargumentti. Kun riskienhallinta on viety yrityksen perusprosesseihin tehokkaasti, tämä yleensä välittyy myös asiakkaille ja antaa yrityksestä hyvin hallitun vaikutelman. (Ilmonen ym. 2013, 17.)

Riskienhallintaprosessi yhtenäistää ja systematisoi organisaation turvallisuustoimintaa. Yhtenäiset toimintatavat ovat tärkeitä organisaation sisäisen turvallisuuskulttuurin kehittämisessä ja erityisesti viranomaisyhteistyön sujuvuuden kannalta. Riskienhallintaprosessin termistön yhteneväisyys ja toiminnan mitattavuus luovat hyvän perustan myös eduskunnan kanslian turvallisuustoiminnan tason mitattavuudelle ja kehittämiselle. (Scherf 2012, 106.)

Scherfin (2012, 110) mukaan eduskunnan kanslian riskienhallinnan kehittäminen höytyjä ovat:

- Toimintaprosessien tehostuminen ja toimintokohtaiset riskikuvat.

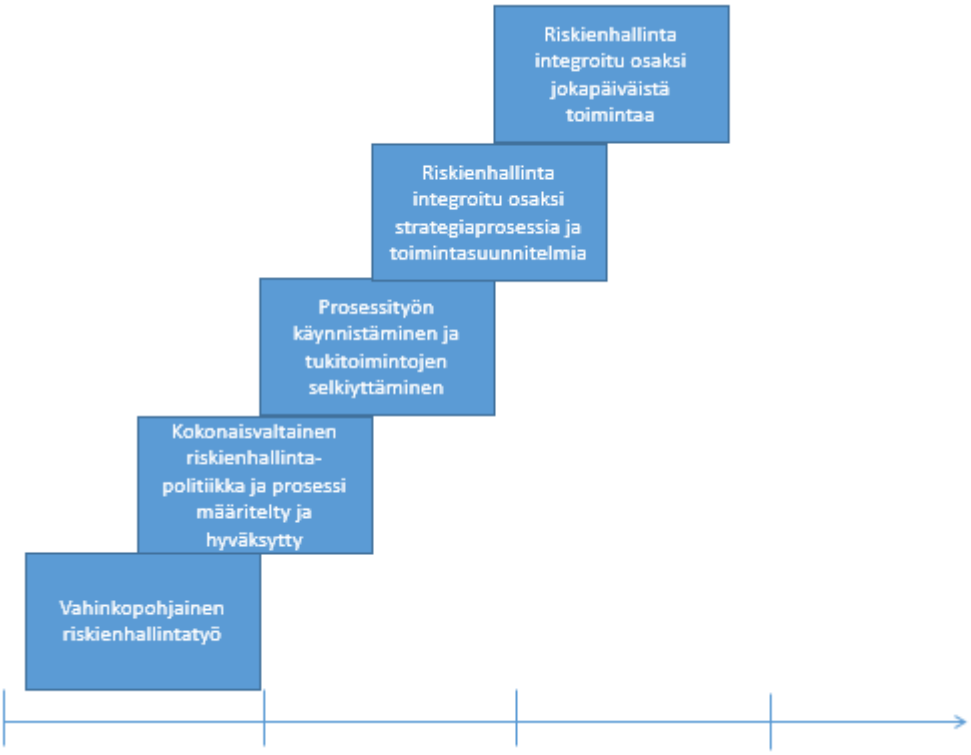
- Henkilöstön yleisen riskitietoisuuden nousu ja turvallisuuskulttuurin rakentuminen.
- Eduskunnan kanslian eri yksikköjen välisen yhteistoiminnan lisääntyminen, joka johtaa organisaatiokulttuurin vahvistumiseen.
- Johtamisen ja johtamisjärjestelmän kehittyminen hyvän hallintotavan kautta.
- Eduskunnan maineen suunnitelmallinen kokonaisvaltaisen hallinnan parantuminen.

2.3.7 Riskienhallinnan käyttöönotto

Riskienhallinnan pelisääntöjen ja tavoitetilan määritteleminen edellyttää riskienhallinnan kokonaiskuvan ja riittävän yhteisymmärryksen saavuttamista. Yrityksessä ymmärretään mitä riskienhallinta sille merkitsee sekä mistä tekijöistä ja osa-alueista se muodostuu. Käyttöönottoa suunniteltaessa avainkysymys on, kuinka riskienhallinnan prosessit ja toiminto rakennetaan ja järjestetään mahdollisimman tehokkaasti. Tehokas riskienhallinnan käyttöönotto vaatii aloitusprojektin, jonka keskeisenä henkilönä on riskienhallinnasta vastaava ylemmän johdon edustaja. Riskienhallinnan kehitysprojektin keskeisenä tehtävänä on selvittää, mitä tietoja riskeistä tarvitaan ja kuinka usein johdon eri tasot tätä tietoa tarvitsevat. Riskienhallintaprosessin käyttöönoton keskeisenä osana on sen sitominen yhtiön strategia- ja suunnitteluprosesseihin, liiketoiminnan päivittäiseen toteutukseen ja normaaleihin seuranta- ja raportointimenetelmiin. Lisäksi on tunnistettava linkit muihin prosesseihin, kuten sisäinen tarkastuksen ja taloushallinnon prosesseihin. (Ilmonen ym. 2013, 35; Leino ym. 2005, 135-136.) Oheiset elementit on kuvattu seuraavassa kuviossa (kuvio 14).

Kuvio 14 Riskienhallinnan käyttöönoton elementit (Leino ym. 2005, 136)

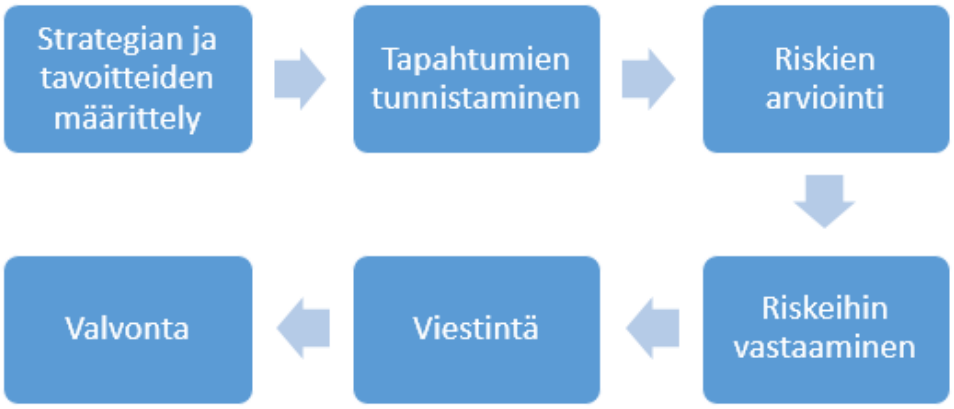
Riskienhallinnalle määriteltäessä konkreettisia tavoitteita ja aikatauluja, niin lähtökohtana on, että riskienhallinnan nykytila ja kypsyysaste ovat tiedossa. Kypsyysmallissa riskienhallinnan kehittäminen jaotellaan yleensä askelmiin, joilla kiivetään ylöspäin tavoitteena kypsempi ja järjestelmällisempi toiminta. Riskienhallinnan lopullisena tavoitteena on sen integroiminen osaksi liiketoimintaa. Riskienhallinnan ja riskianalyysin kehityskaaren alkuvaiheessa kannattaa keskittyä pelkästään riskeihin. Pitkään analyysejä tehneen yritysten on mahdollista arvioida riskien lisäksi myös mahdollisuuksia. Tämä vaatii riskienhallinnalta enemmän työtä sekä haasteellisempaa ylläpitoa. (Ilmonen ym. 2013, 86-87.) Riskienhallinnan kypsyysmalli on esitetty seuraavassa kuviossa (kuvio 15).



Kuvio 15 Riskienhallinnan kypsyysmalli (Ilmonen ym. 2013, 87)

On tärkeätä yrityksen omista lähtökohdista määritellä sellaiset riskienhallinnan osa-alueet, joita tullaan käyttämään ja jotka tuottavat lisäarvoa. Kehittämiseen liittyvät tekemiset täytyy jakaa, arvottaa ja priorisoida. Kehitys on suositeltavaa aloittaa rakentamalla kokonaisviitekehys, määrittää peruskäsitteet ja vastuualueet sekä asettaa mittarit ja tavoitteet riskienhallintatyölle. Riskienhallinnan käsitteellisestä luonteesta johtuen on tärkeätä määritellä keskeiset käsitteet ymmärrettävällä tasolla. Vastuut riskienhallinnan raportoinnista, korjaavista toimenpiteistä ja valvonnasta on myös hyvä määrittää mahdollisimman tarkasti jo kehityksen alkuvaiheessa. (Ilmonen ym. 2013, 35-36.)

Marchetti (2012, 36) on määritellyt riskienhallinnan käyttöönotolle kuuden askeleen käyttöönoton, joka perustuu COSO ERM kehikkoon. Seuraava kuvio (kuvio 16) havainnollistaa askeleet.



Kuvio 16 Riskienhallinnan käyttöönoton askeleet mukaillen Marchettin määrittelemiä askelia (Marchetti 2012, 36-46)

Ensimmäisessä askeleessa määritellään riskienhallinnan strategia ja tavoitteet. Ilman näitä ei kehitystä voida tehdä. Tavoitteissa määritellään operatiiviset tavoitteet, raportointitavoitteet ja vaatimuksenmukaisuuden tavoitteet riskienhallinnalle. Myös organisaation riskinottokyky määritellään tässä vaiheessa. Tapahtumien tunnistamissa kerätään tapahtumia jotka ovat joko mahdollisuuksia tai riskejä. Tapahtumien lähteinä voivat olla sisäiset ja ulkoiset tiedonlähteet. Kun tapahtumia on tunnistettu ja kerätty, arvioidaan niiden vaikutus organisaatiolle. Vaikutukseltaan merkittävät tapahtumat ovat riskejä, joita pitää arvioida. Tämä muodostaa pohjan riskien arvioinnille. Riskien arvioinnissa määritellään riskien vaikutus organisaatiolle ja organisaation haavoittuvuus jokaiselle riskille. Riskeihin vastaamisessa määritellään miten riskejä hallitaan eri toimenpiteillä. (Marchetti 2012, 36-41.)

Viestinnässä organisaatio määrittelee kuinka se viestii riskienhallinnasta tarvittaville kohderyhmille. Sisäisesti on oleellista välittää organisaation toimintamalli riskien suhteen, jotta kaikki sen toimijat ymmärtävät riskienhallinnan tavoitteet, riskien sietokyvyn, yhteisen kielen ja vastuut riskienhallinnasta. Ulkoisesti välitetään tarvittavaa tietoa sitä tarvitseville tahoille. Valvonnan tavoitteena on varmistaa riskienhallinnan toimivuus ja tehokkuus sekä arvioida sen tasoa. (Marchetti 2012, 45-46.)

Ilmonen ym. (2013, 38-41) ovat määritelleet riskienhallinnan kehittämiselle seuraavassa taulukossa (taulukko 3) esitetyt vaiheet ja teemat jotka tulisi huomioida kehittämisessä.

Taulukko 3 Riskienhallinnan kehityksen vaiheet ja teemat (Ilmonen ym. 2013, 38-41)

Kehitysvaihe tai teema	Kuvaus
Yhteisen kielen määrittely	Yrityksen riskienhallinnan kehittämisen edellytyksenä on keskeisten käsitteiden määrittely ja se, että kaikki käyttävät niitä samalla tavalla.
Toiminnan tavoitteet	Yrityksen pitää määritellä ne tavoitteet, joihin pyritään yrityksen omalla tavalla hallita riskejä. Näitä ovat riskienhallinnan laajuus ja milloin riskienhallintaa tehdään, esimerkiksi vain vuosisuunnittelussa tai kaikissa prosesseissa, projektinhallinnassa, hankkeissa tai muussa prosessissa.
Käytännön lähestymistapa	Riskienhallinnan menettelytapojen ja työkalujen tulee olla yksinkertaisia. Muutoin fokus siirtyy pois pääasiallisesta tekemisestä. Riskienhallina on tukiprosessi, ei pääprosessi.
Sisällytä johtamisen perusprosessiin	Riskienhallinta on yrityksen toimintaan liittyvien negatiivisten riskien ja positiivisten mahdollisuuksien hallitsemista. Nämä elementit ovat osa normaalia liiketoiminnan päätöksentekoa. Riskienhallinnan tulee kuulua samaan päätöksentekoon.
Määrittele selkeät vastuut ja roolit	Kaikilla yrityksessä pitäisi olla ideaalitilanteessa jokin kirjattu vastuu riskienhallintaan liittyen. Tarkkuutta tulee kiinnittää riskienhallinnan kehittämisen vastuissa. Kehityksestä vastaava henkilö ei voi vastata liiketoimintariskien kokonaisuuden hallinnasta, näistä vastuun voi kantaa vain liiketoiminta-johto, joka tekee päätökset näihin liittyvistä riskeistä.
Huolehdi resurssien riittävyydestä	Uusia toimintatapojen kehittämisessä ja käyttöönottamisessa tarvitaan riittävästi henkilöresursseja tavoitteiden saavuttamiseksi. Riskienhallintavastuita voidaan ja kannattaa jakaa useammalle henkilölle vaikka käytettävissä olisi päätoiminen henkilö riskienhallintaan. Työkaluina voidaan käyttää tavanomaisia toimistosovelluksia, mutta erityissovellukset työtä voidaan automatisoida enemmän. Huomioitava on myös se, että hallintakeinot aiheuttavat kustannuksia kuten laiteinvestointeja tai muita kustannuksia.
Muista kehittämisnäkökulma	Riskienhallinnan tulee katsoa eteenpäin tulevaisuuteen, eikä sen tavoitteena ole etsiä syyllisiä menneisiin epäonnistumisiin siitä huolimatta, että toteutuneet riskit pitää analysoida. Tämä näkökulma on toistettava kaikessa kehittämisessä ja kommunikoinnissa.
Kehittäminen vaatii aikaa	Riskienhallinnan kehittyminen on pitkäjänteistä tekemistä ja kiinteästi sidoksissa yri-

	tyksen johtamisen kypsyyteen. Aluksi kannattaa pyrkiä laittamaan perusasiat kuntoon. Jatkossa pitää muistaa, että riskien hallinta on hallintatoimien suunnittelua, kohdentamista ja päätöksentekoa, ei siis pelkkää riskien tunnistamista ja analysointia.

Eduskunnan kanslian riskienhallintatoiminnon käynnistäminen edellyttää riskienhallintaa ohjaavaa asiakirjaa tai asiakirjoja. Riskienhallinnan ohjausasiakirjat voidaan eriyttää pienemmille ryhmille sopivaksi laatimalla yksikkötasolle erilliset asiakirjat. Yksikkötason ohjausasiakirjoissa määritellään organisaatiotason tavoitteet osatavoitteiksi. Ohjaavien asiakirjojen lisäksi tulee valita riskienhallintaan soveltuvat työkalut. Kanslian kannalta on myös hyvä käynnistää kehitystä hallitusti pienemmissä kokonaisuuksissa. Tärkeintä on kuitenkin pyrkiä integroimaan riskienhallintaan organisaation strategiatyöhön ja olemassa oleviin johtamisjärjestelmiin. (Scherf 2012, 111-112.)

2.3.8 Riskienhallinnan tason arviointi

Riskienhallintakeinojen monipuolinen käyttö merkitsee yleensä hyvän ja kattavan riskisuojauksen olemassaoloa. Itsestäänselvyys tämä ei kuitenkaan ole, yritys voi panostaa vääränlaisten riskien suojaukseen, riskisuojauksessa saattaa olla tiedostamattomia päällekkäisyyksiä tai jotkin keskeisistä riskeistä on jätetty kokonaan ilman suojausta. Riskienhallintaprosessiin kaivataan automatiikkaa, jota soveltamalla pahimmat karikot voidaan välttää. Riskienhallinnan tason arviointia varten on kehitetty käytännön tarpeista syntyneitä menetelmiä ja mittauksia. (Suominen 2003, 111-112.)

Riskiasioiden benchmarkkaus eli onko tarkasteltava yritys suojautunut paremmin, huonommin tai alalla keskimäärin vallitsevan käytännön mukaisesti, on kiinnostavaa tietoa kehityksen kannalta. Benchmarking eli esikuva-analyysiksi, vertailuanalyysiksi tai valioanalyysiksi kutsutaan työmenetelmää, jossa yritys määrittelee jonkin toimintansa kehityskohteet, identifioi ja analysoi parhaimmat käytännöt alallaan ja muualla yritysmaailmassa sekä soveltaa niitä omaan toimintaansa. Riskienhallinnassa on joitakin keskeisiä elementtejä joita ilman riskienhallintaa on vaikea saada toimimaan optimaalisesti. Näiden elementtien toteutustapaa eri yritysten välillä kannattaa vertailla, mikäli tähän on tilaisuus. Keskeisiä elementtejä vertailemalla voi välttää ongelmakohtia ja löytää omaan yritykseen toimivia malleja. (Ilmonen ym. 2013, 187-188; Suominen 2003, 12.) Ilmonen ym. (2013, 187) mukaan esimerkkejä vertailtavista riskienhallintaelementeistä ovat

- riskienhallintaprosessin sisällyttäminen strategia tai vuosisuunnitteluprosessiin
- käytettävät työkalut

- riskien vaikutusten arviointitavat ja –asteikot
- raportoinnin järjestäminen
- riskinkatokyvyn laskentamallit ja niiden merkitys riskisalkun johtamisessa
- riskienhallinnan resursointi.

Bencmarkingin kautta löydetyt referenssit ovat myös hyvä argumentoinnin tuli riskienhallintavastaavalle perusteltaessa ylimmälle johdolle miksi riskienhallinta kannattaisi organisoida tietyllä tavalla. Menestyvä yrityksen toimiessa tietyllä tavalla voi siinä olla jotain mitä kannattaa omassa yrityksessä kokeilla. Yrityksen toimintaan liittyvä verkosto tarjoaa mahdollisuuden tehdä vertailuja, toimintaa on avattava toisille, jotta muut voisivat arvioida toiminnan laadukkuutta ja sen aiheuttamia riskejä omalle toiminnalle. Sopimuksissa varattu auditointioikeus antaa tilaisuuden tutustua kohteeseen ja löytää asioita joita voi tuoda omaan yritykseen. Myös yrittäjä- ja toimialajärjestöjen kautta voi löytää vertailukohteita. Näissä voi ehdottaa riskienhallinta hyvien käytäntöjen käsittelyä ja koulutuksia. Myös kaupallisten seminaarien ja koulutustilaisuuksien kautta voi tutustua yritysten case-esimerkkeihin ja verkostoitua muiden toimijoiden kanssa. Kun riskienhallinta on kehittynyttä, voi vertailua tehdä erilaisiin riskienhallinnan kypsyysmalleihin esimerkiksi itsearvioinnin kautta. (Ilmonen ym. 2013, 188-189.)

2.3.9 Standardit ja parhaat käytännöt riskienhallinnan tukena

Riskienhallinta voidaan järjestää noudattaen yleisesti hyväksyttyjä riskienhallintastandardeja. Standardien tarkoitus on kattaa mahdollisimman laajasti riskienhallinnan eri osa-alueet. Standardit ovat ohjeellisia ja niitä voi hyödyntää soveltuvin osin. Suurin hyöty on siinä, että ne luovat yhteisen riskienhallintasanaston ja metodin. Tämä mahdollistaa jatkuvuuden ja toistettavuuden riskienhallinnan toteuttamistavalle. (Ilmonen ym. 2013, 27.)

Ilmonen ym. (2013, 27) mukaan useimmat riskienhallintastandardit ja metodit noudattavat samaa perusrunko, joka on seuraava:

- Määritä riskienhallintatavoitteet.
- Tunnista riskit (uhat ja mahdollisuudet).
- Arvioi riskit määrän ja todennäköisyyden suhteen.
- Suunnittele ja toteuta riskienhallintatoimenpiteet.
- Varmista tehokas raportointi ja kommunikointi.
- Arvioi säännöllisesti riskienhallinnan taso ja onnistuminen.

Riskienhallinnan prosessista ja terminologiasta on laadittu paljon suosituksia, Ilmonen ym. (2013,27) mukaan tunnetuimmat standardit ovat

- US COSO ERM-kehikko
- AS/NZS 4360:2004
- ISO/DIS 3100
- ISO/IEC 27005:2008
- BS25999

- ISO/IEC 1799:2005.

COSO esitteli vuonna 2004 kokonaisvaltaisen riskienhallinnan kehikon Enteprise Risk Management. Sitä on sovellettu laajasti erityisesti isoissa organisaatioissa. Kokonaisvaltaisessa riskienhallinnassa on laajasti tukeuduttu COSO ERM -viitekehykseen. Riskienhallintamalli koostuu kahdeksasta toisiinsa liittyvästä osa-alueesta jotka ovat kiinteä osa johtamisjärjestelmää. COSO ERM –viitekehyksen mukaan riskienhallinta ei ole vain tapahtumaketju, jossa yksi osa-alue vaikuttaa ainoastaan seuraavaan, vaan monisuuntainen jatkuva prosessi, jossa kaikki osa-alueet vaikuttavat toisiinsa. (Ilmonen ym. 2013, 28.)

ISO/DIS 31000 –standardia on valmisteltu pitkään , ja sen tavoitteena on ollut kerätä yleisesti hyväksytyt riskienhallintatermit ja käytännöt yhteen dokumenttiin. Standardi on ensimmäinen kansainvälinen standardi, joka on sovellettavissa kaikenlaisiin yrityksiin. Standardissa kootaan yhteen kokonaisvaltaisen riskienhallinnan yleisesti hyväksytty sanasto, viitekehys ja toimintatapa. Standardissa on yksitoista riskienhallintaa määrittävää periaatetta. Riskienhallinnan toimet on yksinkertaistettu neljään osaan: suunnittele, toteuta, seuraa ja paranna. Standardi on saanut erittäin positiivisia arvioita. (Ilmonen ym. 2013, 29.)

Valtiovarainministeriö on antanut tietoturvaohjeen riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnosta. Ohjeen on laatinut valtiovarainministeriön asettaman ja johtaman Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä VAHTI. Valtionhallinnon organisaatioissa riskien hallintaa ja arviointi tulee hoitaa suunnitelmallisesti ja laaja-alaisesti siten, että eri toimintojen näkökulmat ja turvaamistarpeet tulevat katetuiksi. Riskien hallinnan ja arvioinnin tulee sisältää myös varautuminen vakaviin häiriötilanteisiin ja valmiuslaissa määriteltyihin poikkeusoloihin. Ohjeessa on esitetty välineitä ja keinoja joiden avulla riskejä voidaan arvioida. Ohjeessa kuvataan myös lainsäädännön riskienhallintaa koskevia velvoitteita, riskien arvioinnin merkitystä ja organisointia, toimenpiteiden määrittelyä ja jatkokehitystä. Erityisen tärkeätä on tunnistaa merkittävimmät ja kiireellisimpiä toimenpiteitä vaativat riskit. (VAHTI 2003, 3.)

2.4 COSO Enterprise Risk Management

COSO Enterprise Risk Management, ERM, määrittelee organisaation laajuisen riskienhallinnan viitekehyksen. Organisaation kokonaisvaltainen riskienhallinta on prosessi, johon vaikuttaa koko henkilöstö ja jota toteutetaan strategian suunnittelussa sekä siten koko organisaation toiminnassa. Kokonaisvaltainen riskienhallinta on suunniteltu tunnistamaan mahdollisia tapahtumia, joilla voilla vaikutusta organisaation toimintaan ja auttaa hallitsemaan tapahtumista aiheutuvia riskejä hyväksyttävällä tasolle. Näin riskienhallinta antaa

kohtalaisen varmuuden siitä, että organisaation asetetut tavoitteet ovat saavutettavissa. (COSO 2004a, 4.)

Viitekehyksen tavoitteena on muodostaa yhtenäinen näkemys riskienhallinnasta koko organisaation laajuisesti ja mahdollistaa organisaation tavoitteiden saavuttamisen riippumatta siitä onko kyseessä kaupallinen tai ei-kaupallinen toiminta. Organisaation toiminnan lopputuloksille on määritelty siten joku arvo, jolla on merkitystä organisaation sidosryhmille. Tätä lopputulosten arvoa kokonaisvaltainen riskienhallinta pyrkii auttamaan luomaan ja säilyttämään tukemalla organisaation päätöksentekoa. (COSO 2004a, 13-14.)

2.4.1 Organisaation tavoitteet ja ERM osa-alueet

COSO ERM viitekehys jaottelee organisaation tavoitteet neljään eri kategoriaan, joihin liittyviä riskejä se pyrkii hallitsemaan (taulukko 4).

Taulukko 4 COSO ERM Organisaation tavoitekategoriat (COSO 2004a, 5)

Kategoria	Tavoitteiden kuvaus
Strategiset tavoitteet	Korkean tason tavoitteet, organisaation toiminta-ajatukseen liittyvät tavoitteet
Toiminnan tavoitteet	Resurssien tehokas käyttö
Raportointi	Raportoinnin luotettavuus
Vaatimuksenmukaisuus	Lakien ja muun säätelyn vaatimukset

Kategorioiden avulla organisaation tavoitteisiin voidaan keskittyä eri näkökulmista. Vaikka tavoitteet ovat usein päällekkäisiä, voivat ne olla kuitenkin eri henkilöiden vastuulla. Kategorioiden avulla voidaan kuitenkin erotella mitä eri tavoitteilta odotetaan ja mitä riskejä niihin liittyy. (COSO 2004a, 5.)

COSO ERM koostuu kahdeksasta toisiinsa liittyvästä osa-alueesta. Osa-alueet on johdettu organisaation toimintatavoista ja integroitu osaksi prosesseja (taulukko 4).

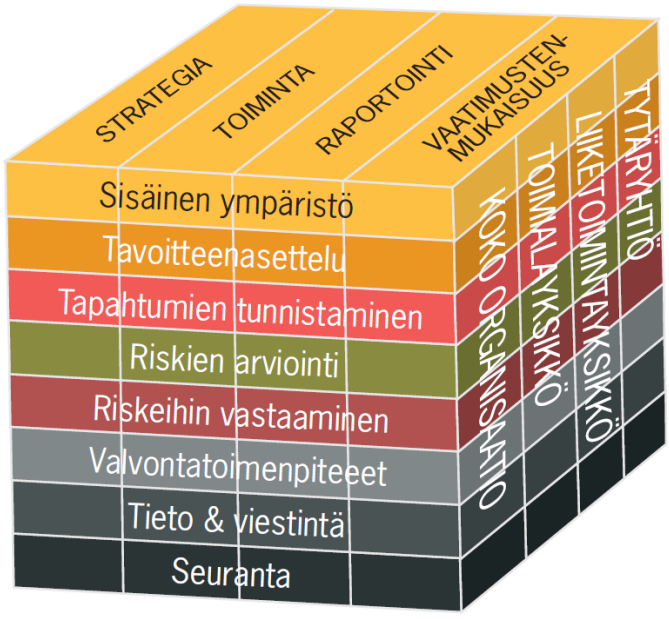
Taulukko 5 COSO ERM osa-alueet (COSO 2004a, 5-6)

Osa-alue	Kuvaus
Sisäinen ympäristö	Organisaation toimintaympäristö joka määrittelee kuinka riskejä tarkastellaan ja kuinka hyväksyttävissä ne ovat suhteessa toimintaan.
Tavoitteenasettelu	Riskienhallinnan toimintaedellytys on toiminnalle asetetut tavoitteet. ERM viitekehyksen on huolehdittava, että tavoitteet on asetettu
Tapahtumien tunnistaminen	Organisaation on kyettävä tunnistamaan sisäiset ja ulkoiset tapahtumat jotka vaikuttavat sille asetettujen tavoitteiden saavut-

	tamiseen. Lisäksi organisaation on kyettävä erottamaan toisistaan riskit ja mahdollisuudet
Riskien arviointi	Riskit arvioidaan huomioimalla niiden todennäköisyydet ja vaikutukset sekä päätetään tämän perusteella hallintatoimenpiteet. Riskit analysoidaan kokonaisuudessaan ja jäännösriskien osalta.
Riskeihin vastaaminen	Organisaation johto valitsee riskeihin vastaamisen toimenpiteet perustuen organisaation riskinottokykyyn.
Valvontatoimenpiteet	Käytännöt ja toimenpiteet joiden avulla varmistetaan riskien vastaamisen onnistumisen.
Tieto & viestintä	Tarpeellinen tieto tunnistetaan ja viestitään siinä muodossa ja ajassa, joka mahdollistaa henkilöstön suorittaa tehtävänsä.
Seuranta	ERM:n toimintaa seurataan kokonaisuutena ja muutoksia tehdään tarvittaessa.

ERM ei ole pelkästään sarja prosesseja, jossa yksi osa-alue vaikuttaa vain seuraavaan. Se on monisuuntainen, iteratiivinen prosessi, jossa melkein mikä tahansa osa-alue voi ja vaikuttaa toisiinsa. (COSO 2004a, 6.)

Organisaation tavoitteiden ja riskienhallinnan osa-alueiden välillä on suora yhteys. Yhteys on kuvattu kolmiulotteisena kuutiona (kuvio 17). Organisaation tavoitteet ovat kuvattu sarakkeina ja riskienhallinnan osa-alueet riveinä. Sivustalla on kuvattu organisaatiorakenne. Kuvaustapa mahdollistaa ERM kokonaisuuden kuvauksen tai keskittymisen yhteen tavoitealueeseen tai ERM osa-alueeseen. (COSO 2004a, 6-7.)



Kuvio 17 COSO ERM osa-alueiden suhde tavoitteisiin (COSO 2004a, 7)

ERM järjestelmän tehokkuutta ja kattavuutta voidaan arvioida sen osa-alueiden toimivuutta arvioimalla. Lähtökohtana on, että kaikkien osa-alueiden täytyy olla toiminnassa, jotta organisaation riskit tulisivat kokonaisvaltaisesti hallituksi. ERM riskienhallintamalli on tehokas kun kaikki osa-alueet ovat toiminnassa muodossa tai toisessa. (COSO 2004a, 7.)

COSO ERM osa-alueet muodostavat riskienhallinnan viitekehyksen, joita kokonaisvaltaisen riskienhallinnan tulee sisältää. Seuraavissa aliluvuissa kuvataan eri osa-alueet.

2.4.2 COSO ERM Sisäinen ympäristö

Sisäinen ympäristö muodostaa perustan kaikille muille riskienhallinnan osa-alueille. Se vaikuttaa miten strategiat ja tavoitteet muodostetaan, liiketoiminnan muodostavat toiminnot on määritelty sekä miten riskit tunnistetaan, analysoidaan ja hallitaan. Sillä on myös vaikutusta miten valvontatoimenpiteet suunnitellaan ja toteutetaan, riskienhallinnan tiedonkulku ja viestintä järjestetään sekä miten seurantatoimenpiteet toteutetaan. Sisäisen ympäristön osa-alueeseen vaikuttaa organisaation historia ja organisaatiokulttuuri kuten arvot, organisaation pätevyys sekä johtamistapa. Keskeisesti sisäiseen ympäristöön vaikuttaa ylin johto ja sen toimintatapa. (COSO 2004a, 27.) Sisäinen ympäristön vaikutus onkin merkittävä riskienhallinnan kannalta sekä organisaatioiden toiminnalle. Tehoton sisäinen ympäristö voi merkittävästi vaikuttaa organisaatioiden tavoitteiden saavuttamisen tavoittamiseen. Pahimmillaan vaikutukset voivat taloudellisia tappiota, maineen menetys tai liiketoiminnan epäonnistuminen. (COSO 2004a, 34.) Sisäisen ympäristön osa-alueen keskeiset tekijät on kuvattu alla olevassa kuviossa (kuvio 18 ja 19).

Kuvio 18 COSO ERM sisäisen ympäristön rakenne (COSO 2004b, 2)

Kuvio 19 COSO ERM sisäisen ympäristön rakenne (COSO 2004b, 2)

Riskienhallinnan filosofia on organisaation yhteinen näkemys ja asenne kuinka organisaatio huomioi riskit sen kaikessa toiminnassa. Riskienhallinnan filosofia kuvastaa organisaation muuta toimintaa ja se vaikuttaa kuinka riskienhallinta toteutetaan. Ilman yhtenäistä riskienhallintafilosofiaa voivat eri organisaatioyksikköjen riskienhallinnan erot muodostaa ongelmia organisaatiolle ja estää tavoitteiden saavuttamista. (COSO 2004a, 27-28.)

Riskinottokyky kuvaa laajalla tasolla riskiä joita organisaatio on halukas hyväksymään toiminnassaan. Riskinottokyky heijastaa riskienhallintafilosofiaa ja se puolestaan vaikuttaa organisaatiokulttuuriin ja toimintatapoihin. Organisaation ylin johto on kriittinen osa ERM sisäisen ympäristön osa-aluetta ja vaikuttaa merkittävästi sen tekijöihin. Ylimmän johdon itsenäinen asema hallinnosta, kokemus ja maine, organisaation toiminnan tarkastelu ja siihen osallistumisen laajuus sekä ylimmän johdon toimien tarkoituksenmukaisuus kaikki vaikuttavat sisäiseen ympäristöön. (COSO 2004a, 28-29.)

Organisaation arvot vaikuttavat riskienhallintaan, kuten koko organisaation toimintaan. ERM riskienhallinta on riippuvaista ihmisten toiminnasta ja ihmisten toimintaa taas vaikuttavat heidän arvonsa. Organisaatiot pyrkivät vaikuttamaan työntekijöiden arvoihin julkaisemalla viralliset linjaukset kirjallisessa muodossa. Nämä kuvaavat tahtotilaa joka ylin johto haluavat organisaatiossa toteutuvan. Organisaation pätevyys kuvastaa tietoja ja taitoja, joita tarvitaan tehtävien suorittamiseen. Organisaation johto päättää kuinka hyvin tehtävä tulee suorittaa suhteessa strategiaan ja asetettuihin tavoitteisiin. Tehtävien haluttu

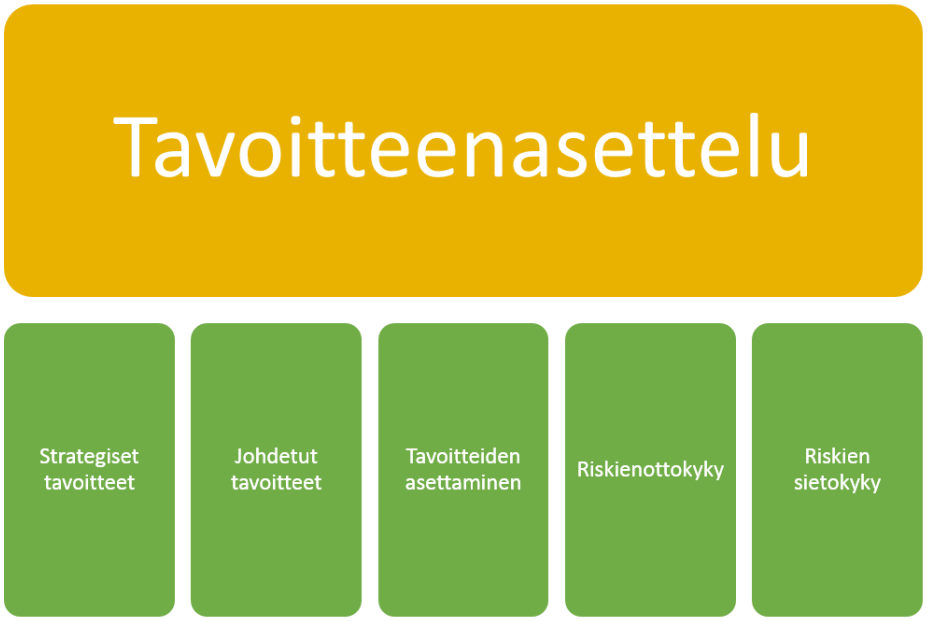
suoritustaso taas määrittelee henkilöstölle asetetut vaatimukset. (COSO 2004a, 28-29; COSO 2004a, 31.)

Organisaatiorakenteet luovat tavat joilla suunnitellaan, toteutetaan, hallitaan ja valvotaan organisaation toimintoja. Riskienhallinnan toimivuuden kannalta organisaatiorakenteet tulee olla määriteltynä, jotta sen olisi mahdollista saavuttaa sille asetetut tavoitteet. Johtamisrakenteilla organisaatiot määrittelevät kuinka paljon yksilöille ja ryhmille annetaan valtuuksia ja rohkaistaan päätöksentekoon sekä määritellään missä päätöksenteon rajat kulkevat. ERM sisäisen ympäristön osa-alueeseen vaikuttaa paljon se kuinka hyvin henkilöt ymmärtävät oman vastuunsa päätöksistään. (COSO 2004a, 32-33.)

Henkilöstöhallinnan käytännöt määrittelevät vahvasti miten organisaation henkilöstö pystyy käsittelemään työssä esiintyviä haasteita ja riskejä. Henkilöstön kouluttaminen on erityisen tärkeää muuttuvassa toimintaympäristössä ja sen tulisi olla jatkuvaa toimintaa. (COSO 2004a, 33-34.)

2.4.3 COSO ERM Tavoitteenasettelu

Tavoitteenasettelu on edellytys tapahtumien tunnistamiselle, riskien arvioinnille ja riskeihin vastaamiselle. Tavoitteet on asetettava ennen kuin organisaation johto voi arvioida ja hallita niihin kohdistuvia riskejä. (COSO 2004a, 35.) Tavoitteenasettelun osa-alueen rakenne on kuvattu alla olevassa kuviossa (kuvio 20).



Kuvio 20 COSO ERM tavoitteenasettelun rakenne (COSO 2004b, 2)

Organisaation toiminta-ajatus määrittelee laveasti mitä toiminnalla tavoitellaan. Tämän perusteella ylin johto muodostaa strategiset tavoitteet, strategian sekä siihen liittyvät toiminnot, vaatimukset ja raportoinnin tavoitteet organisaatiolle. Strategiset tavoitteet ovat korkean tason tavoitteita, jotka noudattavat ja tukevat toiminta-ajatusta. Johdetut tavoitteet tuovat tavoitteet strategiatasolta toimintotasolle. Ne johdetaan organisaation strategisista tavoitteista yksityiskohtaisiksi tavoitteiksi organisaatioiden eri toiminnoille. Yhdessä strategisten tavoitteiden kanssa ne antavat mahdollisuuden organisaatioille tunnistaa kriittiset menestystekijät. Johdetut tavoitteet voidaan jakaa karkeasti kolmeen kategoriaan: operatiiviset tavoitteet, raportointitavoitteet ja vaatimuksenmukaisuuden tavoitteet. (COSO 2004a, 35-36.)

Määrämuotoinen tavoitteiden asettamisesta huolehtiva prosessi on kriittinen tekijä riskienhallinnassa. Riskienhallinta ei määrää mitä tavoitteita asetetaan, mutta se tukee niiden asettamisen prosessia. Tehokas riskienhallinta antaa suhteellisen varmuuden siitä, että organisaation raportointitavoitteet ja vaatimuksenmukaisuuden tavoitteet saavutetaan. Strategisten ja operatiivisten tavoitteiden saavuttamisessa suhteen riskienhallinta voi antaa suhteellisen varmuuden siitä, että johto ja ylin johto ovat tietoisia riittävän ajoissa miten asetetut tavoitteet ovat mahdollista saavuttaa. Riskienhallinnan tulee myös kaikissa tavoitteiden asettamisessa varmistaa, että valitut tavoitteet ovat organisaation riskienottokyvyn rajoissa. (COSO 2004a, 39.)

Riskinottokyky, jonka johto luo ylimmän johdon ohjauksessa, toimii ohjenuorana organisaation strategian luonnissa. Riskinottokyky ja strategia liittyvät toisiinsa. Eri strategiat joilla organisaatiot voivat saavuttaa tavoitteensa, sisältävät erilaisia riskejä. Riskienhallinnan avulla johto voi valita strategian, joka on riskinottokyvyn mukaista. Koska riskienottokyky ohjaa strategian muodostamista, näkyy tämä organisaation resurssien käytössä. Johto ohjaa resurssit strategian perusteella tarvittaviin toimintoihin ja siten mahdollistaa toiminnan pysymisen riskinottokyvykkyyden rajoissa. Riskien sietokyky määrittelee kuinka paljon vaihtelua tavoitteiden saavuttamisessa hyväksytään. Riskien sietokykyä määritellessään johto harkitsee johdettujen tavoitteiden tärkeyttä ja asettaa sen riskinottokyvyn sisälle. Sietokyvyn rajoissa pysyvä toiminta antaa lisävarmuutta, että organisaatio ei ylitä riskienottokykyä ja siten sillä on mahdollisuus saavuttaa tavoitteensa. (COSO 2004a, 40.)

2.4.4 COSO ERM Tapahtumien tunnistaminen

Tapahtumien tunnistamisessa johto tunnistaa mahdollisia tapahtumia, jotka toteutuessaan vaikuttavat organisaatioon. Johto päättää ovatko tapahtumat mahdollisuuksia tai vaikuttavatko ne negatiivisesti organisaation tavoitteiden saavuttamiseen. Negatiiviset tapahtumat kuvaavat riskejä, jotka vaativat arviointia ja vastaamista. Mahdollisuudet huomioidaan

strategian ja tavoitteiden asettamisen prosesseissa. Tapahtumien tunnistamisessa huomioidaan sisäisiä ja ulkoisia tekijöitä koko organisaation toiminnassa. (COSO 2004a, 41.) Tapahtumien tunnistamisen osa-alueen rakenne on kuvattu alla olevassa kuviossa (kuvio 21).

Kuvio 21 COSO ERM tapahtumien tunnistamisen rakenne (COSO 2004b, 2)

Tapahtumia tunnistaessaan johto tietää, että epävarmuuksia on olemassa, mutta ei sitä toteutuko tapahtuma, tai milloin se tapahtuu ja mitä tarkkoja vaikutuksia sillä on toteutuessaan. Arvioidessaan mahdollisia tapahtumia, voi johto tunnistaa sekä mahdollisuudet että haittavaikutukset. Tapahtumat vaihtelevat itsestään selvistä epätodennäköisiin ja vaikutuksiltaan merkityksettömistä hyvin merkityksellisiin. Tapahtumien tunnistaminen tulisikin tehdä ilman todennäköisyyksien ja vaikutusten arvioimista, jotta mitään tapahtumaa ei ylenkatsottaisi. (COSO 2004a, 41.)

Tapahtumiin vaikuttavia tekijöitä on lukemattomia määriä. Osana riskienhallintaa johdon tulee tunnistaa ulkoiset ja sisäiset tekijät, jotka tapahtumiin vaikuttavat. Lisäksi johdon tulee tunnistaa mitä tapahtumia näistä tekijöistä voi syntyä. Ulkoisia tekijöitä ja näistä kehittyviä tapahtumia on esitetty seuraavassa taulukossa (taulukko 6). (COSO 2004a, 41.)

Taulukko 6 Ulkoiset tekijät ja tapahtumat (COSO 2004a, 42)

Ulkoinen tekijä	Tapahtumia
Talous	Hintojen muutokset, pääoman saanti, uudet kilpailijat
Luonto	Tulva, tulipalo, maanjäristys
Politiikka	Muuttuvat lait ja säädökset
Sosiaalinen	Muuttuvat väestörakenteet, sosiaaliset tavat, perherakenteet, työn ja vapaa-ajan prioriteetit
Teknologia	Sähköinen kaupankäynti, tiedon saannin lisääntyminen, infrastruktuurin kustannusten pienentyminen ja sähköisten palvelujen lisääntynyt kysyntä.

Sisäisiä tekijöitä ja näistä kehittyviä tapahtumia on esitetty alla olevassa taulukossa (taulukko 7).

Taulukko 7 Sisäiset tekijät ja tapahtumat (COSO 2004a, 42)

Sisäinen tekijä	Tapahtumia
Infrastruktuuri	Lisääntynyt pääoman käyttö ennaltaehkäisevään ylläpitoon ja call center tukeen, laitteiden alhaalla oloajan vähentäminen ja asiakastyytyväisyyden parantaminen.
Henkilöstö	Työpaikkaonnettomuudet, väärinkäytökset, työehtosopimusten vanhentuminen joka vaikeuttaa työvoiman saantia, rahaliset ja mainetappiot sekä tuotantokatkokset.
Prosessit	Prosessien muokkaus ilman muutoshallintaan, prosessien suorittamisen virheet ja asiakastoimitusten väärä ulkoistaminen joka voi johtaa markkinaosuuksien menetyksiin, tehottomuuteen ja asiakastyytymättömyyteen
Teknologia	Resurssien käytön lisääntyminen vaihteluiden hallinnassa, tietomurtoja ja järjestelmien alhaalla olon kasvaminen, joka johtaa varaston pienemiseen, väärinkäytöksiin sekä liiketoiminnan pysähtymiseen.

Organisaation tapahtumien tunnistamisen menetelmät voivat koostua useasta tekniikasta ja tätä tukevista työkaluista. Tapahtumien tunnistamisen tekniikat tarkastelevat historiaa sekä tulevaa. Historiaa tarkastellaan menneiden tapahtumien ja trendien kautta. Tulevaa tarkastelevat tekniikat huomioivat muuttuvia kulutustottumuksia, uusia markkinaolosuhteita ja kilpailijoiden toimia. (COSO 2004a, 43.) Tapahtumien tunnistamiseen käytettäviä tekniikoita on esitetty alla olevassa taulukossa (taulukko 8).

Taulukko 8 Tapahtumien tunnistamisen tekniikoita (COSO 2004a, 44-45)

Tapahtumien tunnistamisen tekniikka	Kuvaus
Tapahtumaluettelo	Yksityiskohtainen listaus mahdollisista tapahtumista jotka koskevat organisaatiota ja sen toimialaa.
Sisäiset analyysit	Organisaation toiminnan analyysi, esimerkiksi osana liiketoiminnan suunnittelua.
Raja-arvojen asettaminen	Raja-arvojen määrittämien, jotka informoivat johtoa niiden ylittyessä tapahtumista ja niiden vaatimista toimenpiteistä
Johdetut työpajat tai haastattelut	Tietojen kerääminen organisaation henkilöstöltä ja näiden tulosten analysointi
Prosessianalyysit	Analysoidaan prosessien toimivuutta ja tunnistetaan tätä kautta mahdollisia tapahtumia.
Tapahtumiin johtavien merkkien tunnistaminen	Tarkkailemalla merkkejä, jotka ovat aikaisemmin johtaneet tapahtumiin, voivat auttaa tunnistamaan mahdollisia tulevia tapahtumia.
Tapahtuma-arkistot	Arkistot vanhoista tapahtumista joista on aiheutunut organisaatiolle menetyksiä auttavat huomaamaan trendejä tai juurisyitä, jotka aiheuttavat tapahtumia.

Tapahtumien havaitseminen tekniikat vaihtelevat organisaatioittain. Tapahtumien tunnistamisen tulee toimia vakaalla pohjalla, koska se muodostaa perustan riskien arvioinnille ja riskeihin vastaamiselle. (COSO 2004a, 45.)

Useimmiten tapahtumat eivät esiinny eristyksissä. Yksi tapahtuma voi käynnistää toisen ja tapahtumat voivat esiintyä rinnakkain. Analysoimalla tapahtumien riippuvuuksia voidaan riskienhallinnan keinoja kohdistaa sinne missä ne tehoavat parhaiten. Riippuvuuksien tunnistamisessa voidaan hyödyntää tapahtumien jakamista eri kategorioihin. Jakamalla tapahtumat esimerkiksi horisontaalisesti koko organisaation laajuisesti ja vertikaalisesti eri toimintayksiköiden välillä, auttaa hahmottamaan tapahtumien suhdetta toisiinsa. Samankaltaisten tapahtumien kerääminen yhteen auttaa havaitsemaan mahdollisuudet ja uhat sekä auttaa tunnistamaan onko tapahtumien havaitseminen riittävän kattavaa. (COSO 2004a, 45-46.)

Tapahtumilla on niiden toteutuessaan negatiivinen vaikutus tai positiivinen vaikutus. Negatiiviset vaikutukset ovat riskejä, joihin tarvitaan organisaation johdon tekemään analyysiä ja toimenpiteitä. Positiiviset vaikutukset ovat mahdollisuuksia tai riskien vastatapahtumia riskien negatiivisille vaikutuksille. Mahdollisuuksia tuottavat tapahtumat ohjataan johdon strategian tai tavoitteiden asettamisen prosesseihin. Riskejä tuottavat tapahtumat käsitellään johdon tekemässä riskien arvioinnissa ja riskeihin vastaamisen toimenpiteissä. (COSO 2004a, 47.)

2.4.5 COSO ERM Riskien arviointi

Sisäiset ja ulkoiset tekijät vaikuttavat siihen mitkä tapahtumat realisoituvat ja mitkä niiden vaikutukset ovat organisaation tavoitteisiin. Vaikka tietyt tekijät ovat vakioita organisaatioiden toimialalla, ovat tapahtumien vaikutukset yksilöllisiä johtuen erilaisista tavoitteista ja päätöksenteon valinnoista. Riskien arvioinnissa johto tarkastelee mahdollisia tapahtumia, jotka ovat merkityksellisiä organisaatiolle. Tarkastelussa huomioidaan organisaation toiminta ja sen riskiprofiili kuten organisaation koko, toiminnan monimutkaisuus ja sitä koskeva sääntely. Tapahtumien tarkastelussa huomioidaan odotetut ja odottamattomat tapahtumat. Päähuomio kohdistuu odottamattomiin tapahtumiin, joille tehdään riskien arviointi. Myös odotetut tapahtumat, joilla voi olla merkittävää vaikutusta organisaatioon, otetaan mukaan riskien arviointiin. Riskien arviointi on COSO ERM viitekehyksessä jatkuva ja toistuva vuorovaikutteinen toimenpiteiden sarja, jota tehdään koko organisaatiossa. (COSO 2004a, 49.) Riskien arvioinnin osa-alueen rakenne on kuvattu alla olevassa kuviossa (kuvio 22).

Kuvio 22 COSO ERM riskien arvioinnin rakenne (COSO 2004b, 2)

Johto tarkastelee sekä luontaisia ja jäännösriskejä. Luontainen riski on se riski joka kohdistuu organisaation ilman mitään toimenpiteitä vaikuttaakseen sen todennäköisyyteen tai vaikutuksiin. Jäännösriksi on se riski joka jää jäljelle riskiin vastaamisen toimenpiteiden

jälkeen. Jäännösriskiä tarkastellaan sen jälkeen kun vastaamisen toimenpiteet on kehitetty. (COSO 2004a, 49.)

Mahdollisten tapahtumia arvioidaan kahdesta näkökulmasta, todennäköisyys ja vaikutus. Todennäköisyys kuvaa kuinka todennäköisesti tapahtuma tulee toteutumaan ja vaikutus mitä tapahtuma toteutuessaan voi aiheuttaa. Todennäköisyyksien ja vaikutusten määrittäminen voidaan tehdä kvalitatiivisilla tai kvantitatiivisillä menetelmillä. Kvalitatiivisesti arvioitaessa käytetään termejä korkea, keskimääräinen ja matala. Kvantitatiivisesti arvioinnissa käytetään prosentteja, kuinka monta kertaa tapahtuma toistuu tai muu numeerinen arvo. Kumpaa tahansa menetelmää käyttämällä, tärkeintä on kuitenkin, että se tapahtuu järkevästi ja huolellisesti. Todennäköisyyksien ja vaikutusten määrittämisestä tulisi käyttää samaa aikaperspektiiviä kuin siihen liittyvässä strategiassa ja tavoitteissa. Yleensä näitten aikaväli on lyhyt, mutta pitkän aikavälin strategia ja tavoitteet tulee myös huomioida riskien arvioinnissa. Arvioinnin laatua voidaan myös parantaa käyttämällä samoja mittareita kuin tavoitteiden saavuttamisen mittaamisessa. (COSO 2004a, 50.)

Todennäköisyyksien ja vaikutusten määrittelyssä käytetään usein apuna aikaisemmin toteutuneita tapahtumia. Tämä antaa objektiivisemman näkökulman tarkasteluun. Sisäisesti tuotettu tieto, joka perustuu organisaation omiin kokemuksiin antaa usein parempia tuloksia määrittelyssä kuin ulkoisesti tuotettu tieto. Ulkoisesti tuotettu tieto on kuitenkin hyödyllistä esimerkiksi toimimaan tarkistuspisteenä tai parantamaan määrittelyssä tehtävää arviointia. Organisaation riskien arvioinnissa käyttämät arviointitekniikat ovat yhdistelmä kvalitatiivisia ja kvantitatiivisia tekniikoita. (COSO 2004a, 51-52.)

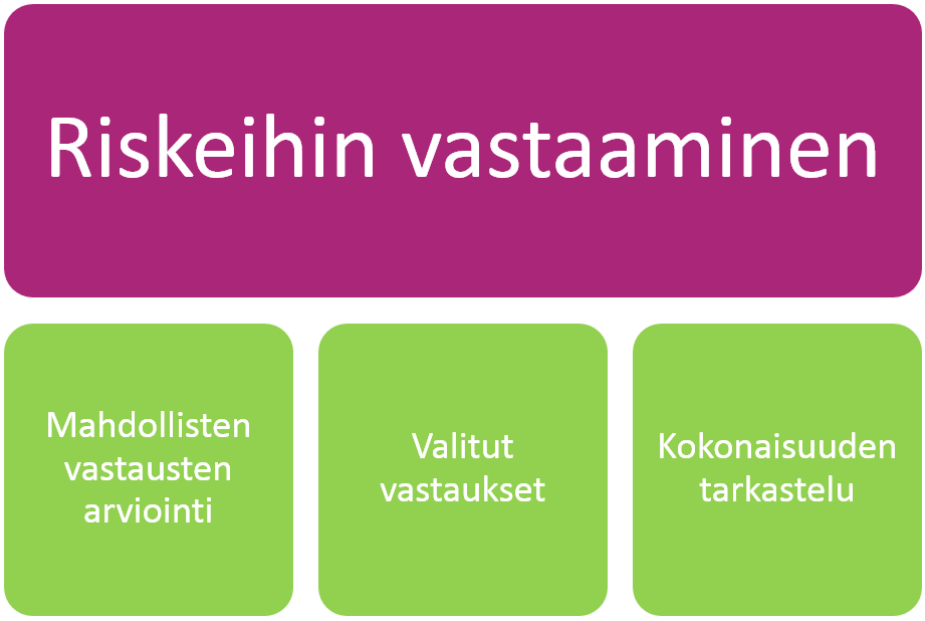
Organisaation ei ole pakollista käyttää samoja teknikoita eri yksiköissä. Käytettävän tekniikan valinnassa tulisi huomioida yksikön tarve tulosten tarkkuudelle ja yksikön toimintakuluttuuri. Organisaation laajuisen yhteenvedon tekemisessä on huomioitava käytetyt tekniikat. Kvantitatiivinen yhteenveto edellyttää, että kaikkien riskiarviointien tulokset on esitetty kvantitatiivisesti. Käytettäessä yhdistelmätekniikoita, johto tekee yhteenvedon kvalitatiivisesti ja esittää tulokset kvalitatiivisessa muodossa. Muodostamalla yhteiset todennäköisyys- ja vaikutustermistöt sekä riskikategoriat koko organisaatiossa, helpottaa eri tekniikoiden tuottamien tulosten yhdistämistä. (COSO 2004a, 53.)

Tapahtumat joilla ei ole yhteyttä toisiinsa voidaan arvioida erikseen. Tapahtumat joilla on yhteyttä toisiinsa, tai tapahtumat joilla on yhteisvaikutuksia ja ne aiheuttavat merkittävästi erilaisia todennäköisyyksiä ja vaikutuksia kuin yksittäiset tapahtumat, arvioidaan yhdessä. Jos riskit vaikuttavat useampaan organisaatioyksikköön, ne voidaan yhdistää saman tapahtumakategoriaan. Tällöin niitä voidaan ensin arvioida yksiköittäin ja sen jälkeen koko

organisaation kannalta. Lisäksi on syytä huomioida, että tehokas ERM riskienhallinta edellyttää, että riskien arviointi kattaa sekä luontaiset riskit että riskeihin vastaamisen toimenpiteiden jälkeen jäljelle jäävät jäännösriskit. (COSO 2004a, 54.)

2.4.6 COSO ERM Riskeihin vastaaminen

Johto päättelee miten se vastaa arvioituihin merkityksellisiin riskeihin. Toimenpiteiden valinnat riippuvat riskin todennäköisyydestä ja vaikutuksista sekä toimenpiteiden kustannuksista ja hyödyistä. Myös tapahtumien tuomat mahdollisuudet arvioidaan riskien ohella. Toimenpiteiden jälkeen jäännösriskin on oltava organisaation riskienottokyvyn mukainen. (COSO 2004a, 55.) Riskeihin vastaamisen osa-alueen rakenne on kuvattu alla olevassa kuviossa (kuvio 23).



Kuvio 23 COSO ERM riskeihin vastaamisen rakenne (COSO 2004b, 2)

Riskeihin vastaamisen toimenpiteet voidaan jakaa kategorioihin (COSO 2004a, 55). Kategoriat on esitelty alla olevassa taulukossa (taulukko 9).

Taulukko 9 COSO ERM riskeihin vastaamisen toimenpiteiden kategoriat (COSO 2004a, 55)

Kategoria	Selitys
Välttäminen	Lopetetaan tai ei käynnistetä organisaation toimintaa joka aiheuttaa riskin.
Pienentäminen	Tehdään toimenpiteitä, joilla pienennetään todennäköisyyttä tai vaikutusta tai molempia.
Jakaminen	Pienennetään riskin todennäköisyyttä tai vaikutusta siirtämällä tai muuten jakamalla

	osa riskistä.
Hyväksyntä	Ei tehdä toimenpiteitä riskin todennäköisyyden tai vaikutusten suhteen.

Mahdollisten vastausten arvioinnissa pyritään löytämään toimenpiteet joilla jäännösriskeille löydetään taso joka on organisaation riskien sietokyvyn mukainen. Usein jo yksittäiset toimenpiteet riittävät tai voidaan tarvita useiden toimenpiteiden yhdistelmiä. Joskus yksi toimenpide voi vaikuttaa useampaan riskiin, jolloin johto voi jättää ne riskit kokonaan käsittelemättä. (COSO 2004a, 56.)

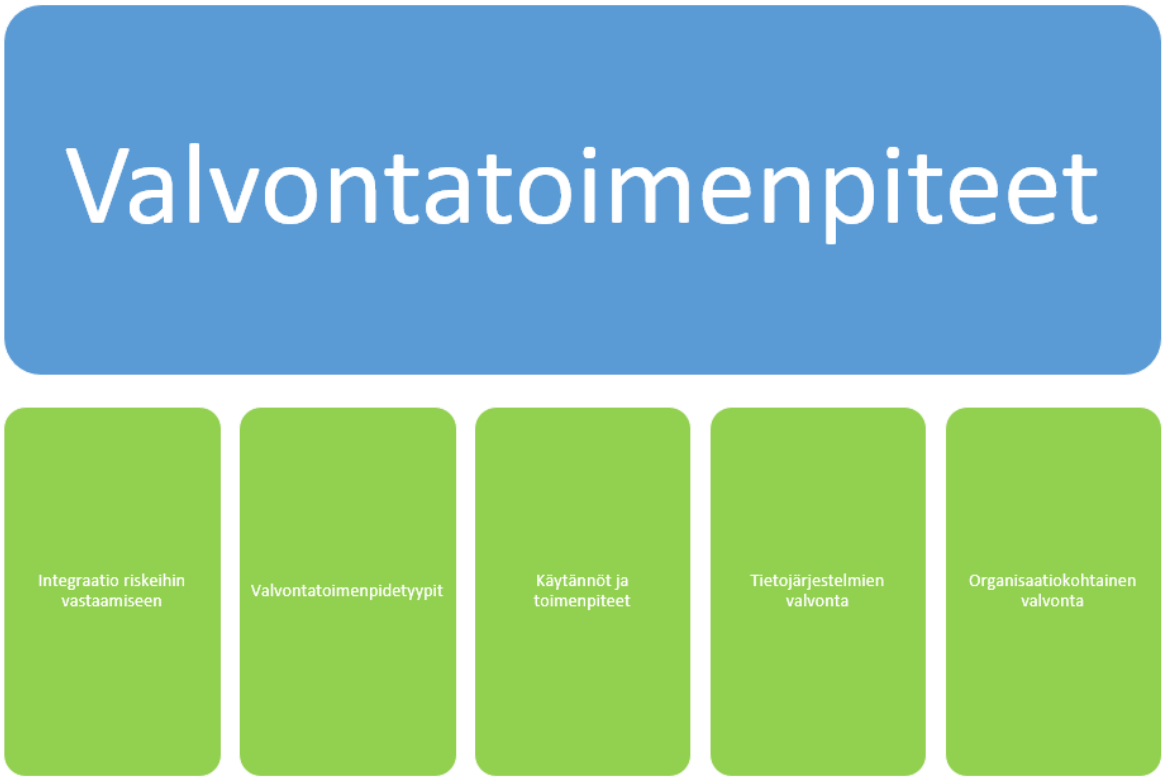
Toimenpiteitä arvioitaessa huomioidaan niiden vaikutukset usealta kannalta. Arvioinnissa huomioidaan vaikutukset riskien todennäköisyyksiin ja vaikutuksiin, kustannukset verrattuna hyötyihin sekä arvioidaan toimenpiteiden luomat mahdollisuudet organisaatiolle. Toimenpiteiden arvioinnissa huomioidaan niiden vaikutukset todennäköisyyksiin ja vaikutuksiin. Pelkästään toista pienentämällä voidaan päästä riskien sietokyvyn kannalta hyväksyttävälle tasolle. Toimenpiteitä arvioitaessa arvioidaan niiden vaikutuksia käyttäen samoja tai yhteneväisiä mittareita kuin johdettujen tavoitteiden mittaamisessa käytetään. Mahdollisuuksia voidaan myös tunnistaa arvioitaessa riskeihin vastaamisen toimenpiteitä. Tyypillisesti mahdollisuudet havaitaan, kun käytössä olevat toimenpiteet eivät ole enää tehokkaita ja niiden jalostaminen muuttaa vain marginaalisesti riskien todennäköisyyksiä ja vaikutuksia. (COSO 2004a, 57-58.)

Kun eri riskeihin vastaamisen toimenpiteiden vaikutukset on arvioitu, johto päättää miten se aikoo hallita riskejä. Riskit hallitaan valitsemalla riskeihin vastaamisen toimenpiteet, jotka muuttavat riskien todennäköisyydet ja vaikutukset riskien sietokyvyn sallimiin rajoihin. Toimenpiteet eivät välttämättä tuota mahdollisimman pientä jäännösriskiä. Jos jäännösriski ylittää riskien sietokyvyn, harkitsee johto valittuja toimenpiteitä uudelleen ja muuttaa niitä tarvittaessa. Joissakin tapauksissa myös riskien sietokykyä voidaan muuttaa. Tästä johtuen, riskien ja riskien sietokyvyn arviointi on toistuva prosessi. Riskeihin vastaamisen arviointi vaatii myös toimenpiteistä aiheutuvien riskien arviointia. Tämä voi käynnistää uudelleen arviointiprosessin, jossa arvioidaan toimenpiteistä aiheutuvat riskit ennen riskeihin vastaamisen toimenpiteiden valintaa. Tehtyään valinnan toimenpiteistä riskeihin vastaamiselle, johdon täytyy luoda toimenpideohjelma niiden käyttöönottamiselle. Kriittinen osa toimenpideohjelmaa on luoda valvontamekanismit, jotta riskeihin vastaaminen tehdään asianmukaisesti. Johdon on myös hyvä huomata, että jäännösriskit ovat aina olemassa, kaikkeen organisaation toimintaa liittyy aina epävarmuustekijöitä. (COSO 2004a, 58.)

ERM riskienhallinta edellyttää, että riskiä tarkastellaan organisaation näkökulmasta huomioiden kokonaisuus. Kokonaisnäkymä voidaan esittää monella tavalla. Näkymä voidaan muodostaa keskittymällä suuriin riskeihin, riskikategorioihin tai riskeihin jotka kohdistuvat koko organisaatioon. Kokonaisnäkymän avulla voidaan kohdistaa resursseja eri yksiköihin ja muuttaa strategiaa. Organisaation johto voi kokonaisnäkymän avulla tunnistaa onko organisaation toiminta riskienottokyvyn mukaista sekä mitä riskejä se toiminnassaan on valmis hyväksymään. Jos kokonaisnäkymästä selviää, että organisaation riskit ovat huomattavan alhaisempia kuin riskienottokyky sallisi, voi johto kannustaa ottamaan riskejä. Tavoitteena tällä on lisätä organisaation kasvua ja tuottoa. (COSO 2004a, 59-60.)

2.4.7 COSO ERM Valvontatoimenpiteet

Valvontatoimenpiteet ovat käytäntöjä ja toimenpiteitä, joilla henkilöstö huolehtii siitä, että johdon valitsemat riskeihin vastaamisen toimenpiteet tulevat tehdyiksi. Valvontatoimenpiteet voidaan kategorisoida sen perusteella mihin organisaation tavoitteeseen ne liittyvät: strategiset, operatiiviset, raportointi ja vaatimuksenmukaisuus. Vaikka jotkin valvontatoimenpiteet liittyvät vain yhteen tavoitekategoriaan, on niissä usein päällekkäisyyksiä. Riippuen olosuhteista, yksittäinen toimenpide voi auttaa saavuttamaan organisaation tavoitteita useammassa kategoriassa. (COSO 2004a, 61.) Valvontatoimenpiteiden osa-alueen rakenne on kuvattu alla olevassa kuviossa (kuvio 24).



Kuvio 24 COSO ERM valvontatoimenpiteet rakenne (COSO 2004b, 2)

Tarvittavat valvontatoimenpiteet tunnistetaan riskeihin vastaamisen toimenpiteiden valinnan jälkeen. Valittaessa valvontatoimenpiteitä johto tarkastelee kuinka toimenpiteet liittyvät toisiinsa. Joissakin tapauksissa yksittäinen valvontatoimenpide riittää kattamaan useita riskeihin vastaamisen toimenpiteitä, toisissa tapauksissa tarvitaan useita valvontatoimenpiteitä yhtä riskin vastaamisen toimenpidettä valvomaan. Joskus erillisiä valvontatoimenpiteitä ei tarvita, koska nykyiset ovat riittäviä. (COSO 2004a, 61-62.)

Valvontatoimenpiteitä valittaessa tulee huomioida näitten riittävyys ja sopivuus riskeihin vastaamisen toimenpiteisiin ja siihen liittyvään organisaation tavoitteiseen. Valvontatoimenpiteitä ei tehdä vain niiden itsensä takia tai vain sen vuoksi, että niin on oikein toimia. Valvontatoimenpiteet toimivat mekanismina, jolla hallitaan asetettujen tavoitteiden saavuttamista. Useita erityyppisiä valvontatoimenpiteitä on kehitetty kuten estävät, valvovat, manuaaliset, automatisoidut tai tietokoneistetut ja johtamistoimenpiteet. Valvontatoimenpiteet voidaan myös eritellä kontrollitavoitteiden perusteella kuten tietojenkäsittelyn eheyden ja tarkkuuden varmistavat kontrollit. Usein yhdistelmää eri valvontatoimenpiteistä käytetään riskien vastaamisen toimenpiteiden valvonnassa. (COSO 2004a, 62-63.)

Valvontatoimenpiteet yleensä koostuvat kahdesta osasta käytännöt ja toimenpiteet. Käytäntö tai politiikka kuvaa mitä pitäisi tehdä ja toimenpiteet miten käytäntö toteutetaan. Tietojärjestelmistä riippuvaisuus on luonut tarpeen valvoa keskeisiä järjestelmiä. Valvontatoimenpiteet tietojärjestelmien osalta voidaan jakaa kahteen ryhmään, yleiset toimenpiteet ja sovelluskohtaiset toimenpiteet. Yleisiä toimenpiteitä käytetään huolehtimaan jatkuvasta asianmukaisesta ylläpidosta joita voidaan kohdistaa lähes kaikkiin tietojärjestelmiin. Sovelluskohtaisia toimenpiteitä tehdään sovelluksen sisällä kontrolloimaan tietojenkäsittelyä. Yhdessä edelliset toimenpiteet ja tarvittavat manuaaliset toimenpiteet varmistavat tiedon eheyden, tarkkuuden ja luotettavuuden. (COSO 2004a, 64.)

Organisaatiokohtainen valvontatoiminta on riippuvaista sen tavoitteista ja toiminnasta. Tästä johtuen organisaatiokohtaisesti riskeihin vastaamisen toimenpiteet ja niihin liittyvät valvontatoimenpiteet eroavat toisistaan. Vaikka organisaatioilla olisi samat tavoitteet ja samankaltaiset tavoitteiden toteuttamistoimenpiteet, johtamistavat ja siten seuranta ovat yksilöiden tekemää ja siten yksilöllisiä. Lisäksi valvontatoimenpiteet riippuvat organisaation toimintaympäristöstä, koosta, organisaatiorakenteista, historiasta ja organisaatiokulttuurista. Hallintamalli vaikuttaa myös valvontatoimenpiteisiin, keskitetyllä toiminnalla on erilaiset valvontatoimenpiteet kuin hajautetulla mallilla. Muita vaikuttavia tekijöitä ovat organisaation sijainti ja globaalitoimintaympäristö, operatiivisen toiminnan kehittyneisyys sekä tiedonhallintaprosessit. (COSO 2004a, 66.)

2.4.8 COSO ERM Tieto & viestintä

Joka organisaatio tunnistaa ja kerää laajalti tietoa, joka liittyy ulkoisiin ja sisäisiin tapahtumiin sekä toimintaan, jolla on merkitystä organisaation johtamiselle. Tieto välitetään henkilöstölle sopivassa muodossa ja aikataulussa, joka mahdollistaa henkilöstön suorittaa riskien hallinnan ja muut velvollisuudet. (COSO 2004a, 67.) Tiedon ja viestinnän osa-alueen rakenne on esitetty alla olevassa kuviossa (kuvio 25).

Kuvio 25 COSO ERM Tieto & viestintä rakenne (COSO 2004b, 2)

Tietoa tarvitaan kaikissa organisaation osissa tunnistamaan, arvioimaan ja vastaamaan riskeihin sekä muuhun organisaation toimintaan tavoitteiden saavuttamiseksi. Tietoa on saataville niin paljon, että johdon haasteena on käsitellä se ja muodostaa siitä olennainen tieto, jonka pohjalta voi tehdä päätöksiä. Tätä varten on tiedon käsittelyn helpottamiseksi luotu tietojärjestelmäinfrastruktuureja. Usein nämä ovat tietokoneistettuja, mutta niissä on osana myös manuaalista tietojenkäsittelyä. Tietoa käsitellään näiden avulla sekä sisäisistä että ulkoisista lähteistä. Tietoa käsittelevät järjestelmät voivat olla virallisia tai epävirallisia. Keskustelut asiakkaiden, toimittajien, asetusten säätäjien ja organisaation henkilöstön kanssa tuottavat usein kriittistä informaatiota, jota tarvitaan riskien tai mahdollisuuksien tunnistamiseen. Myös seminaarit ja muut vastaavat tapahtumat voivat tuottaa tärkeätä tietoa organisaation käyttöön. Kerätyn tiedon tulee olla tarpeidenmukaista, erityisesti jos organisaatio kohtaa usein muutoksia. Järjestelmät auttavat tunnistamaan ja muodostamaan tarvittavat taloudelliset ja ei-taloudelliset tiedot. Järjestelmät myös raportoivat tiedot ajanmukaisesti ja sillä tavalla mikä on hyödyllistä organisaation toimintojen ohjaamiselle. (COSO 2004a, 67-68.)

Tietojärjestelmät ovat keskeisiä tehokkaalle riskien hallinnalle. Järjestelmien avulla voidaan antaa pääsy tietoon, joka on aiemmin ollut vain tietyn organisaation osan käytössä. Tieto on siten laajalti johdon käytössä päätöksenteon tukena. Riskien hallinnan tueksi voidaan käyttää historiallista ja nykyhetken tietoja. Historiallinen tieto mahdollistaa organisaation seurata tavoitteiden, suunnitelmien ja odotusten täyttymistä. Tieto antaa näkymän kuinka organisaatio toimii tietyissä olosuhteissa, joka mahdollistaa ennusteiden tekemisen. Historiallinen tieto voi antaa myös ennakkovaroituksen tapahtumista joihin johdon tarvitsee reagoida. Nykyhetken tieto antaa kuvan siitä kuinka organisaatio pysyy riskien sietokyvyn rajoissa. Tiedot antavat kuvan riskien tilasta eri organisaation toiminnoissa ja kuinka riskit vaihtelevat odotuksista. (COSO 2004a, 68-69.)

Tietojen merkitys toiminnalle on luonut tiedon laadulle vaatimuksia. Tietojen laadun varmistamiseksi organisaatioilla on omia laadunvalvontatoimia, jotka kattavat tiedon hankinnan, ylläpidon ja jakelun. Ilman laadunvarmistusta tietojärjestelmät eivät välttämättä tuota johdon ja henkilöstön tarvitsemia tietoja. (COSO 2004a, 70-71.) Seuraavassa taulukossa on esitetty tiedon laatuvaatimukset (taulukko 10).

Taulukko 10 COSO ERM tietojen laatuvaatimukset (COSO 2004a, 70)

Laatuvaatimus	**Kuvaus**
Sisältö on asiankuuluvaa	Yksityiskohtaisuus on oikealla tasolla
Tieto on oikea-aikaista	Tieto on saatavilla kun sitä tarvitaan
Tieto on ajankohtaista	Tieto on viimeisintä mitä on saatavilla
Tieto on tarkkaa	Tieto on oikeata ja luotettavaa
Tieto on saatavilla	Tieto on helposti niiden saatavilla, jotka sitä tarvitsevat

Viestintä on luontaisesti osa tietojärjestelmiä. Viestintää on kuitenkin tapahduttava tietojärjestelmien ulkopuolella kuten käsiteltäessä odotuksia, yksilöiden ja ryhmien vastuita ja muita organisaatiolle tärkeitä asioita. Johdon pitää tuottaa sisällöltään määrättyä ja kohdistettua viestintää, jolla määritellään henkilöstön odotettu käyttäytyminen ja vastuun. Tähän kuuluu selkeästi määritelty organisaation riskienhallinnan filosofia ja sen toteutus sekä selkeä vastuiden jako. Viestintä prosesseista ja toimenpiteistä tulisi olla yhdenmukaista ja vahvistaa haluttua kulttuuria. (COSO 2004a, 71.) COSO (2004a, 71) mukaan viestinnän tulisi tehokkaasti ilmaista

- riskienhallinnan tärkeyden ja merkityksen organisaatiolle
- organisaation tavoitteet
- organisaation riskinottokyvyn ja riskien sietokyvyn
- yhteinen riskisanasto
- henkilöstön roolit ja vastuut riskien hallinnassa ja riskien hallintaa tukevat välineet.

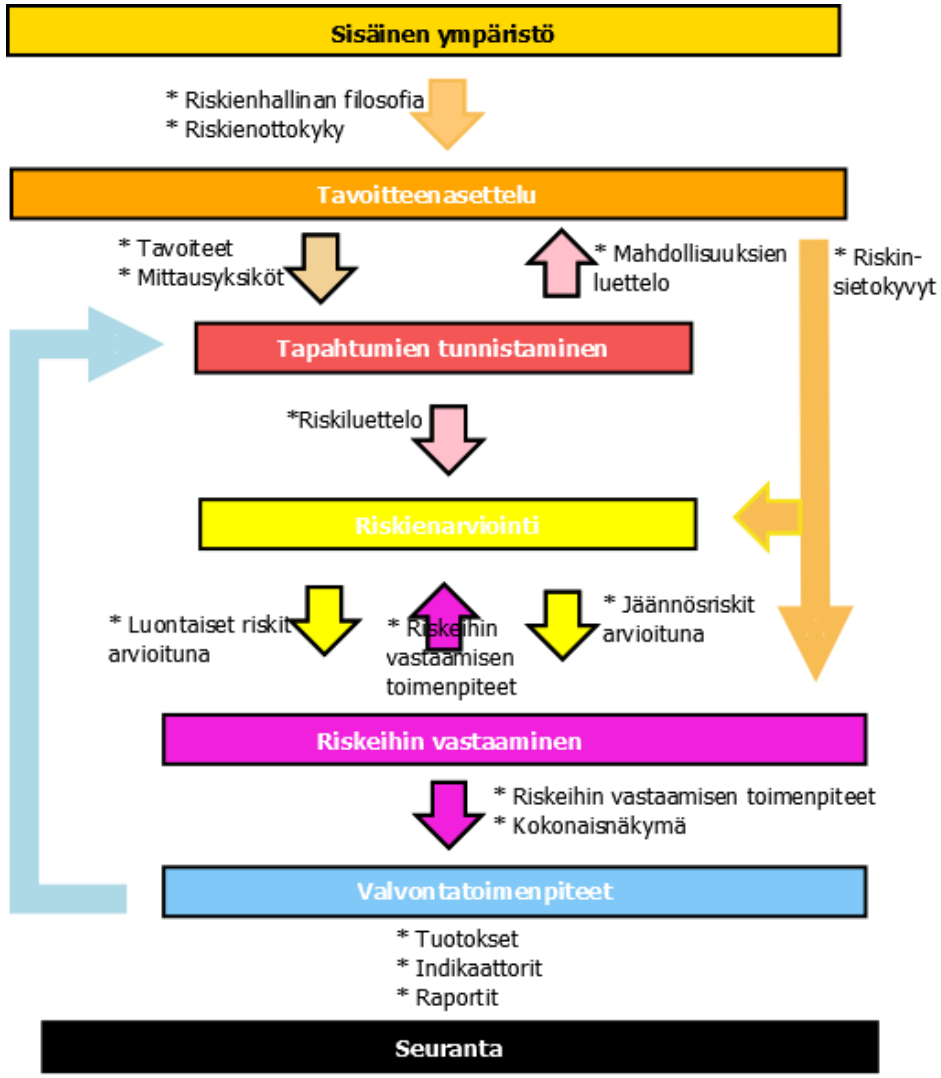
Koko henkilöstölle on tultava selvä viesti ylimmältä johdolta, että riskien hallinta on otettava vakavasti. Henkilöstön on myös tiedettävä miten omat työtehtävät vaikuttavat muiden

työhön. Tämä tieto on oleellista ongelmien tunnistamisessa tai määriteltäessä sen syyt ja korjaavat toimenpiteet. Henkilöstön on myös tiedettävä mikä on hyväksyttävää ja mikä ei ole hyväksyttävää käytöstä. (COSO 2004a, 72.)

Lähellä operatiivista toimintaa olevat työntekijät ovat usein ensimmäisiä jotka huomaavat mahdollisia toiminnan ongelmia. Viestintäkanavien pitäisi pystyä huolehtimaan, että viestit ongelmista saadaan organisaation sisällä kulkemaan helposti. Usein normaalit raportointikanavat ovat riittäviä, mutta voi olla tilanteita joita varteen on tarpeen luoda suoria yhteyksiä raportoida ongelmista ylemmälle johdolle tai muulle taholle, jolla on pääsy ylemmän johdon puheille. Nämä yhteydet ovat tehokkaan riskien hallinnan kannalta oleellisia. Nämä antavat henkilöstölle kanavan raportoida havainnoista suoraan johdolle ja luovat kuuntelemisen kulttuurin. Oleellista on myös kannustaa henkilöstöä raportoimaan havainnoistaan. Myös koulutuksella ja määritellyillä säännöillä vahvistetaan raportoinnin tärkeyttä. Tärkeimpiä sisäisen viestinnän kanavia on johdon ja ylimmän johdon välinen viestintä. Johdon on pidettävä ylin johto tietoisena organisaation suorituskyvystä, riskeistä, riskien hallinnan toiminnasta sekä muista tähdellisistä asioista. Mitä paremmin viestintä toimii, sitä tehokkaammin ylin johto voi tehdä oman tehtävänsä eli organisaation johtamisen valvonnan ja palautteen antamisen. Ylimmän johdon tulee myös kertoa johdolle mitä tietoja se tarvitsee toiminnassaan. (COSO 2004a, 72-73.)

Ulkoista viestintää varten tarvitaan suunniteltua viestintää. Avoimen viestinnän kautta esimerkiksi kuluttajat ja tuottajat voivat antaa palautetta organisaation toiminnasta kuten tuottein suunnittelusta ja laadusta. Avoin viestintä organisaation riskinottokyvystä ja riskien sietokyvystä on tärkeää erityisesti organisaatioille, jotka ovat osa toimitusketjua tai sähköistä kaupankäyntiä. Johto voi siten arvioida miten oma riskinottokyky ja riskien sietokyky sopii yhteistyökumppanien vastaaviin. Tällä varmistetaan, ettei organisaatio ota liikaa riskejä yhteistyökumppaneiden kautta. Viestintä sidosryhmien, säädöstentekijöiden, talousanalysoijien ja muiden ulkoisten tahojen kanssa antaa niille tärkeätä tietoa, jotta ne ymmärtäisivät mitä riskejä organisaatio kohtaa. Tämän viestinnän tulisi olla tarkoituksenmukaista, asiaankuuluvaa, ajankohtaista sekä täyttää lakien ja muun sääntelyn vaatimukset. Ulkoisten tahojen kanssa tehtävä viestintä vaikuttaa myös sisäisesti tehtävään viestintään antamalla viestin miten sitä tehdään. (COSO 2004a, 73.)

Organisaation tulevien ja organisaation sisäisten tietokulun lisäksi, tieto kulkee myös riskienhallinnan eri osa-alueiden välillä (COSO 2004b, 69). Tiedon kulku riskienhallinnan sisällä voidaan kuvata seuraavalla kuviolla (kuvio 26).



Kuvio 26 COSO ERM osa-alueiden väliset tietovirrat (COSO 2004b, 69)

2.4.9 COSO ERM Seuranta

Organisaation riskien hallinta muuttuu ajan myötä. Riskeihin vastaamisen toimenpiteet voivat muuttua epäolennaisiksi, valvontatoimenpiteet menettävät tehokkuutensa tai niitä ei tehdä tai organisaation tavoitteet voivat muuttua. Nämä voivat aiheutua useista syistä joiden yhteydessä johdon on pääteltävä onko riskien hallinta enää tehokasta nykymuodossaan. Toiminnan seurantaa voidaan tehdä kahdella tavalla joko jatkuvana toimintana tai erillisinä arviointeina. Yleensä käytetään yhdistelmää jatkuvasta arvioinnista ja erillisarvioinneista varmistamaan tehokkaan riskien hallinnan toimivuutta. (COSO 2004a, 75.) Seurannan osa-alueen rakenne on esitelty seuraavassa kuviossa (kuvio 27).

Kuvio 27 COSO ERM seuranta osa-alueen rakenne (COSO 2004b, 2)

Usein organisaation normaalit seurantamekanismit toimivat riskien hallinnan seurantamekanismeina. Näissä yleensä seurataan vaihteluja, verrataan tietoja eri lähteistä sekä käsitellään odottamattomia tapahtumia. Toiminnasta vastaavat tahot seuraavat tietoja ja tekevät näistä johtopäätöksiä onko tarve huomioida poikkeamia sekä keskustella mahdollisten korjaavien toimenpiteiden käynnistämisestä. (COSO 2004a, 76.) Esimerkkejä jatkuvan toiminnan seurannan toimenpiteistä on esitelty seuraavassa taulukossa (taulukko 11).

Taulukko 11 COSO ERM jatkuva toiminnan seurannan esimerkkejä (COSO 2004a, 76-77)

Seurantatoimenpide	**Kuvaus**
Toimintaraporttien seuranta	Tunnistetaan raportoinnista epätarkkuuksia tai eroja odotettuihin tuloksiin.
Muutosten seuranta	Muutoksia organisaation taloudellisiin uhkiin suhteessa tehtyihin rahallisiin panostuksiin verrataan toisiinsa
Ulkoisen viestintä	Ulkoisen viestintä tukee/vahvistaa sisäistä viestintää toiminnan tasosta tai vihjaa ongelmista.
Säädösten valvojien kanssa käytävä viestintä	Säädösten valvojat antavat johdolle viestejä onko toiminta vaatimuksenmukaista vai ei, joka kertoo riskien hallinnan toimivuudesta.
Sisäinen tarkastus ja ulkoinen auditointi sekä konsultointi	Auditointien sekä konsultointien kautta saadaan tietoja riskien hallinnan toiminnasta. Auditoinnissa havaitaan yleensä heikkouksia ja konsultoinnissa saadaan parannusehdotuksia.
Koulutukset, suunnittelu- ja muut kokoukset	Palaute antaa merkkejä siitä onko riskien hallinta tehokasta ja kuinka tietoisia osallistujat ovat riskeistä.
Keskustelut henkilöstön kanssa	Riskien hallinnan toimivuutta arvioida osa-

	na normaaleja keskusteluja henkilöstön kanssa tuomalla esille toimintatapoja, kuinka riskejä tunnistetaan ja miten valvontatoimenpiteet toimivat.

Erillisarvioinnit ovat hyödyllisiä antamaan arvioita siitä kuinka riskien hallinta itsessään toimii. Niillä voidaan myös arvioida miten jatkuva toiminnan seurata toimii. Erillisarvioinnit vaihtelevat laajuudeltaan ja tiheydeltään. Ne riippuvat usein riskien merkityksestä organisaatiolle ja riskien vastaamisen toimenpiteiden tärkeydestä sekä niihin liittyviin hallintatoimenpiteistä. Korkean prioriteetin riskialueet ja niiden vastaamisen toimenpiteet arvioidaan yleensä useimmin. Kokonaisuudessaan riskien hallinnan arviointeja tehdään yleensä harvemmin. Tämä tehdään yleensä jos organisaatiossa tapahtuu merkittäviä muutoksia kuten strategian muutos, johdon muutos, hankinnat, hajautukset, muutokset taloudellisissa tilanteissa, muutokset operatiivisissa toiminnassa tai merkittävät muutokset tietojen käsittelyn prosesseissa. Jos kokonaisuutta arvioidaan, tulee sitä arvioida myös strategiatasolla toimenpiteiden ohella. Arvioinnin rajaus riippuu myös mitä tavoitteita arvioidaan, strategisia, operatiivisia, raportoinnin tai vaatimuksenmukaisuuden tavoitteita. (COSO 2004a, 77.)

Erillisarvioinneissa voidaan käyttää useita eri menetelmiä ja työkaluja, kuten tarkistuslistat, kyselyt ja prosessikaavioiden analyysit. Menetelmänä voidaan käyttää myös vertailuja organisaatioiden välillä. Vertailuissa täytyy aina muistaa erot organisaatioiden välillä niiden tavoitteissa ja toimintaympäristöissä. Riskien hallinnan dokumentaatiotasoissa on myös eroja riippuen organisaation koosta ja monimutkaisuudesta. Suurilla organisaatioilla on yleensä hyvin kattava dokumentaatio, joita pienissä organisaatioissa ei välttämättä ole. Riskien hallinnassa on useita epävirallisia toiminta joita ei ole dokumentoitu, kuitenkin nämä tehdään säännöllisesti ja tehokkaasti. Vaikka näitä ei ole dokumentoitu ei se tarkoita että toiminnot eivät olisi tehokkaita tai niitä ei voisi arvioida. Dokumentointi auttaa arvioinnin tekemistä sekä tehostaa sitä. Arvioinnin lopputuloksena on usein raportti itse arviointiprosessista joka liitetään osaksi riskien hallintadokumentaatiota. Erityisesti kun johto esittää ulkopuolisille arvion riskien hallinnan tehokkuudesta, on tätä varten syytä olla dokumentaatio tukemassa arviota. Dokumentaatio on erityisen hyödyllistä jos riskien hallinnan tehokkuutta kyseenalaistetaan. (COSO 2004a, 79.)

Puute on riskien hallinnan tila, johon tulee kiinnittää huomiota. Se voi olla havaittu, mahdollinen tai oikea puute riskien hallinnasta. Se voi olla myös mahdollisuus parantaa riskien hallintaa, joka lisää organisaation todennäköisyyttä saavuttaa tavoitteensa. Riskien hallinnan puutteiden raportointia varten voidaan hyödyntää useita tietolähteitä. Puutteita voidaan havaita jatkuva seurannassa, erillisarvioissa ja ulkoisten toimijoiden raportoimana.

Kaikki havainnot riskien hallinnan puutteista, jotka vaikuttavat organisaation kykyyn kehittää ja ottaa käyttöön strategiaa sekä asettaa ja saavuttaa tavoitteita tulisi raportoida vastuuhenkilöille. Asiat jotka viestitään eteenpäin, riippuvat yksilön valtuuksista käsitellä itse tilanteita ja esimiesten valvontatoimista. Arvioitaessa mitä viestitään eteenpäin, on tarpeellista myös arvioida ja raportoida havaitun puutteen syyt, kuten virheelliset toimintatavat. Myös havainnot joilla ei ole suurta vaikutusta kokonaisuuteen on syytä raportoida eteenpäin jos niillä on merkitystä toimintakulttuuriin ja siihen mikä on sallittua toimintaa ja mikä ei. (COSO 2004a, 79-80.)

Havainnot puutteista raportoidaan normaaleja viestintäkanavia pitkin lähimmille esimiehille. Organisaatiossa pitäisi olla myös kanavat raportoida sensitiivisistä havainnoista kuten laittomista tai sopimattomista toimista. Riskien hallinnan puutteet tulisikin aina raportoida vastuullisen henkilön esimiehille, jotta nämä voivat antaa tukea ja valvoa korjaavien toimien tekemistä. Jos havainnoista pitää raportoida organisaation ulkopuolelle, on tämä tapahduttava tarpeeksi päätösvaltaisen tason kautta, jotta se tapahtuisi asianmukaisesti. Riskien hallinnan toimivuuden kannalta on oleellista saada tietoa mahdollisista puutteista oikealle taholle. Tätä varten tuli muodostaa säännöstöt mitä tietoja tarvitaan milläkin tasolla tehokkaan päätöksenteon takaamiseksi. Mitä alemmaksi organisaatiorakenteessa mennään, sen yksityiskohtaisempia raportoitavien tietojen tulisi olla. Raportoinnin sisältö tulisikin olla määriteltynä organisaation johdosta käsin. (COSO 2004a, 81.)

2.4.10 COSO ERM roolit ja vastuut

Riskien hallintaan vaikuttavat useat tahot, joilla on tärkeitä vastuita riskien hallinnan kannalta. Riskienhallinnan vastuut ovat aina organisaation sisällä. Ulkopuoliset tahot, jotka osallistuvat suoraan tai epäsuorasti organisaation tavoitteiden saavuttamisen, eivät ole osa tai vastuullisia organisaation riskien hallinnasta. Organisaation koko henkilöstö vaikuttaa ja osallistuu riskien hallintaa omalla toiminnallaan. (COSO 2004a, 83.)

COSO (2004, 83-88) mukaan riskien hallinnan kannalta organisaation sisällä joilla on merkitys ja vastuita riskien hallinnassa

- ylimmällä johdolla
- johdolla
- riskienhallintajohtajalla
- talousjohdolla
- sisäisellä tarkastuksella
- muulla henkilöstöllä

COSO (2004a, 89-91) mukaan Ulkoisia tahoja jotka vaikuttavat riskien hallintaan ovat

- ulkopuoliset auditoijat
- lakien ja asetusten säätäjät ja valvojat

- tahot jotka ovat vuorovaikutuksessa organisaation kanssa
- ulkoistuskumppanit
- talousanalysoijat, media.

Ylin johto

COSO (2004a, 83-84) mukaan ylin johto osallistuu riskien hallintaan valvonnalla tai olemalla tietoinen seuraavista:

- Riskien hallinnan toteutuksen laajuus organisaatiossa.
- Tukemalla organisaation muun johdon näkemystä organisaation riskinottokyvystä.
- Katselmoimalla organisaation riskien kokonaisnäkymän ja arvioimalla niitä riskienottokykyä vasten.
- Ylimmälle johdolle tiedotetaan suurimmista riskeistä ja reagoiko johto asianmukaisilla toimenpiteillä.

Ylin johto on osa sisäisen ympäristön osa-aluetta ja sillä on oltava riskien hallinnan toimivuuden kannalta vaadittava osaaminen sekä kiinnostus siihen. (COSO 2004a, 84.)

Johto

Johto on suorassa vastuussa kaikesta organisaation toiminnasta, myös riskien hallinnasta. Vastuut riippuvat tehtävistä ja organisaatiotasosta ja ne voivat vaihdella huomattavasti riippuen organisaation toiminnasta. Organisaatioissa toimitusjohtaja, pääjohtaja tai vastaavassa roolissa toimiva henkilö on riskien hallinnan omistaja ja vastuussa siitä, että riskien hallinnan kaikki osa-alueet ovat toiminnassa. (COSO 2004a, 84.)

Riskienhallintajohtaja

Joissakin organisaatioissa on keskitetty riskien hallinnan johtaminen riskienhallintajohtajalle. Riskienhallintajohtaja toimii suoraan toimitus- tai pääjohtajan alaisuudessa ja hänellä on käytettävissä resursseja tehokkaan riskienhallinnan aikaansaamiseksi. Rooli voidaan antaa toiselle johtajalle muiden tehtävien lisäksi tai nimetä pelkästään tähän rooliin keskittyvä henkilö. Toimivan riskien hallinnan aikaansaamiseksi on riskienhallintajohtajan roolin vastuiden oltava selkeitä. Riskienhallintajohtaja tukee muita riskien hallinnassa, muun johdon vastuulla on oman alueensa riskien hallitseminen. (COSO 2004a, 86.)

Talousjohto

Talousjohdolla ja muulla henkilökunnalla on merkittävä rooli organisaation riskien hallinnalle. Tämän alueen toiminta on koko organisaation laajuista toiminnan suunnittelusta valvontaan. Talousjohto ja henkilökunta ovat keskeisessä roolissa estämässä ja havaitsemassa valheellista raportointia. Talousjohtaja osana organisaation ylintä johtoa omalta

osaltaan määrittelee organisaation eettisen toiminnan tapoja sekä vaikuttaa organisaation raportointikäytäntöihin. (COSO 2004a, 87-88.)

Sisäinen tarkastus

Sisäinen tarkastus arvioi riskien hallinnan tehokkuutta ja antaa parannusehdotuksia. Sisäisen tarkastukseen luotujen standardien mukaan sisäisen tarkastuksen tulisi keskittyä riskien hallintaan ja siihen liittyvien valvontatoimenpiteiden tarkastamiseen. Sisäiset tarkastajat avustavat johtoa ja ylintä johtoa tutkimalla, arvioimalla, raportoimalla ja suosittelemalla toimenpiteitä riskien hallinnan riittävyydestä ja sen tehostamisesta. (COSO 2004a, 88.)

Muu henkilöstö

Riskien hallinta on jollain asteella kaikkien vastuulla organisaatiossa. Riskien hallinnan tulisi olla suoraan tai epäsuorasti olla jokaisen työntekijän työnkuvaa. Riskienhallinta kuuluu kaikille ja roolit sekä vastuut tulisi olla tarkasti määritelty tehokkaasti viestitty (COSO 2004a, 88-89).

Ulkoiset tahot

Ulkoiset tahot voivat auttaa organisaation tavoitteiden saavuttamisessa. Ulkoiset tahot voivat myös antaa hyödyllistä tietoa riskien hallinnan käyttöön. Ulkoiset auditoijat antamat riippumattoman näkökulman organisaation toiminnasta. Lakien ja asetusten säätäjät ja valvojat vaikuttavat riskien hallintaa vaatimusten kautta tai tekemällä tarkastuksia organisaation toimintaan. Organisaation kanssa vuorovaikutuksessa olevat tahot kuten asiakkaat, toimittajat ja yhteistyökumppanit antavat informaatiota organisaation toiminnasta, jota voidaan hyödyntää riskien hallinnassa. Ulkoistuskumppanit tekevät organisaation puolesta toimenpiteitä, joita organisaatioiden tulee valvoa koska riskeihin liittyviä vastuita ei voi ulkoistaa. Talousanalysoijat ja media tekevät ulkopuolisen näkökulmasta arvioita organisaation toiminnasta. Tätä tietoa voidaan hyödyntää osana riskien hallintaa. (COSO 2004a, 89-91.)

2.4.11 COSO ERM rajoitukset

Riskien hallinnassa on huomioitava, ettei se anna täyttä varmuutta siitä, että organisaatio saavuttaa tavoitteensa (COSO 2004a, 93). COSO (2004a, 93) mukaan rajoituksissa on huomioita kolme rajoittavaa tekijää, jotka ovat seuraavat:

- Riskit liittyvät tuleviin tapahtumiin, jotka ovat luontaisesti epävarmoja.
- Riskien hallinta toimii eri tasoilla eri tavoitteiden mukaisesti. Strategisten ja operatiivisten tavoitteiden suhteen riskien hallinta auttaa varmistamaan, että organisaation johto on ajoissa tietoinen siitä, missä suhteessa organisaation tilanne on asetettuihin tavoitteisiin nähden. Riskien hallinta ei voi antaa edes kohtuullista varmuutta siitä, että asetetut tavoitteet saavutetaan.
- Riskien hallinta ei voi antaa täyttä varmuutta mihinkään tavoitekategoriaan.

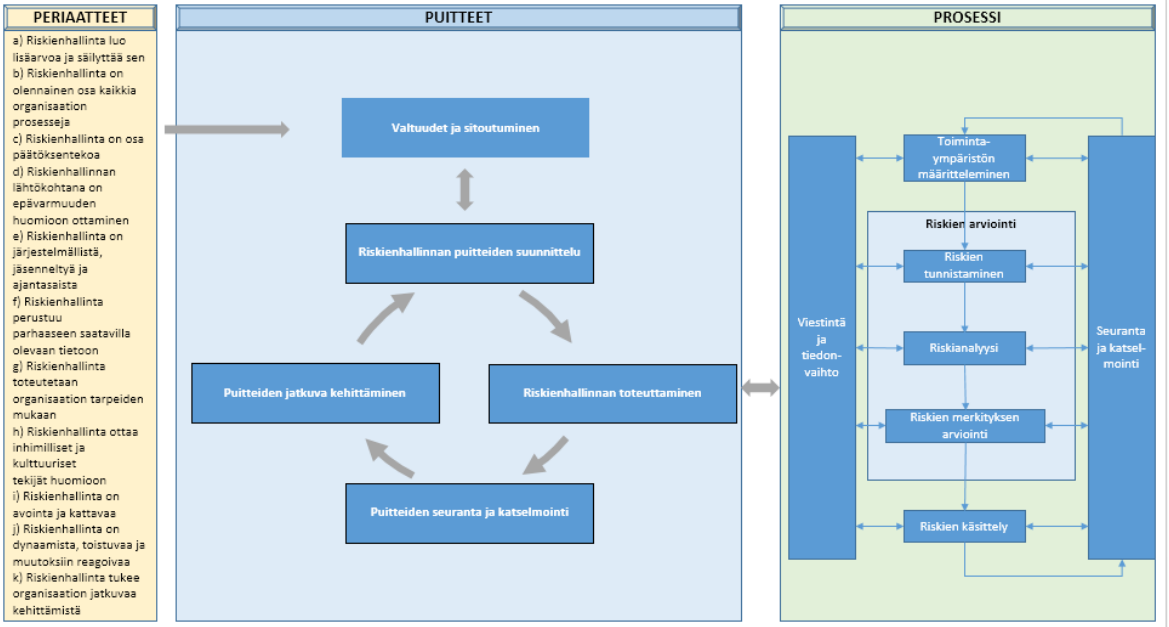
Ensimmäinen tekijä huomioi, että tulevaisuutta ei voida ennustaa varmasti. Toinen tekijä huomioi, että joitakin tapahtumia johto ei voi hallita. Kolmas tekijä huomioi, että prosessit eivät aina toimi kuten on aiottu. Kohtuullinen varmuus ei kuitenkaan tarkoita sitä, että riskien hallinta säännöllisesti epäonnistuu. Riskien hallinnan vaikutus pienentää riskejä, jotka estävät organisaatioiden tavoitteiden saavuttamista. Hyvin hallitut organisaatiot todennäköisemmin saavuttavat tavoitteensa säännöllisesti. Aina kuitenkin voi tapahtua tapahtumia joita ei voida kontrolloida kuten virheellinen toiminta. (COSO 2004a, 93-94.)

2.5 ISO 31000

ISO 31000 standardi määrittelee periaatteet, viitekehyksen ja prosessit riskien hallintaan. Standardi kuvaa yleisluonteisen toimintamallin, joka antaa periaatteet ja ohjeet erimuotoisten riskien hallitsemiseen järjestelmällisellä, avoimella ja uskottavalla tavalla. Jokaisella toimialalla tai riskienhallinnan soveltamiskohteella on omat tarpeensa riskienhallinnalle. Siksi standardin keskeisin piirre on toimintaympäristön määritteleminen riskienhallintaprosessin yleisiin lähtökohtiin. Toimintaympäristöön kuuluvat organisaation tavoitteet, sidosryhmät, riskikriteerit sekä ympäristö, jossa organisaatio toimii. (SFS-ISO 2011, 6.)

2.5.1 ISO 31000 koostumus ja soveltuvuus

Standardi kuvaa riskienhallinnan periaatteet, puitteet ja riskienhallinnan prosessin. Näiden välinen suhde on kuvattu seuraavassa kuviossa (kuvio 28).



Kuvio 28 ISO 31000 standardin osien suhde (SFS-ISO 2011, 10)

Riskienhallintaa voidaan soveltaa koko organisaatioon, sen eri alueisiin ja tasoihin. Sitä voidaan myös soveltaa yksittäisiin tehtäviin, projekteihin ja toimintoihin minä tahansa ajankohtana. (SFS-ISO 2011, 6.) Seuraavissa aliluvuissa on kuvattu ISO 31000 standardin osien sisältö.

2.5.2 ISO 31000 periaatteet

Riskienhallinnan vaikuttavuuden vuoksi organisaation on syytä noudattaa riskienhallinnan periaatteita kaikilla tasoilla (SFS-ISO 2011, 22). Periaatteet on kuvattu seuraavassa taulukossa (taulukko 12).

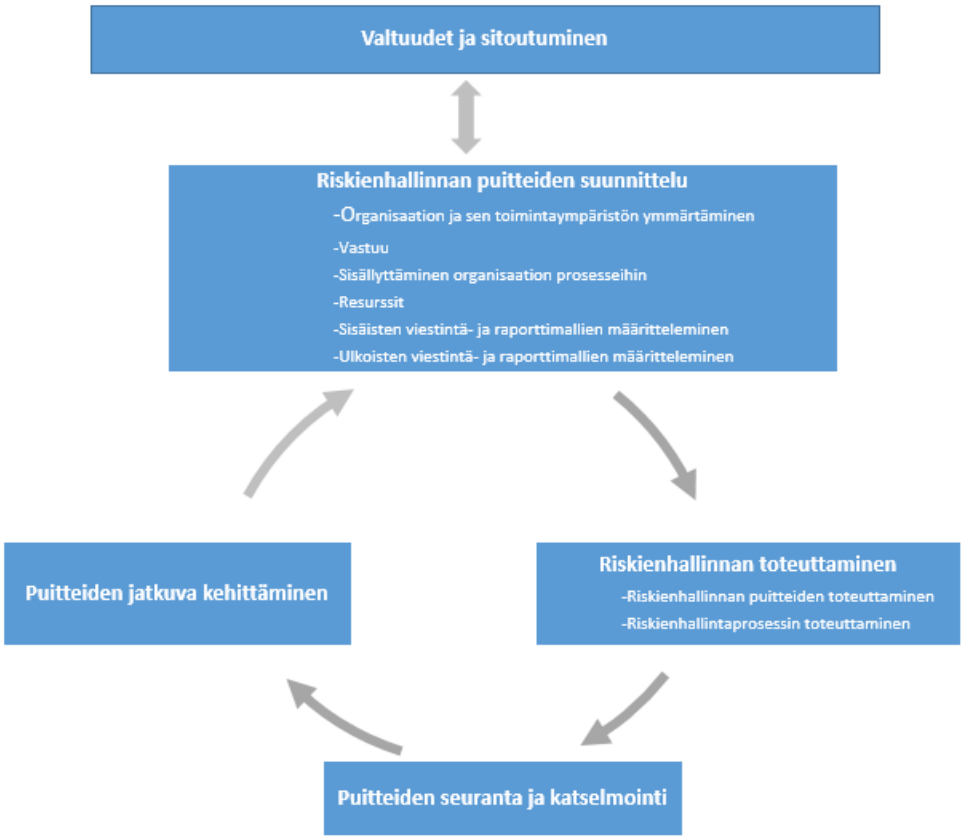
Taulukko 12 ISO 31000 riskienhallinnan periaatteet (SFS-ISO 2011, 22-24)

Riskienhallinnan periaate	Kuvaus
Riskienhallinta tuo lisäarvoa ja säilyttää sen.	Riskienhallinta auttaa tavoitteiden saavuttamista ja toiminnan tason kehittymistä
Riskienhallinta on olennainen osa kaikkia organisaation prosesseja.	Riskienhallinta ei ole organisaation toiminnoista ja prosesseista erillinen toiminto. Riskienhallinta on osa johdon vastuualuetta ja olennainen osa kaikkia organisaation prosesseja
Riskienhallinta on osa päätöksentekoa.	Riskienhallinta auttaa tekemään tietoisia valintoja, asettaa toimintoja tärkeysjärjestykseen ja erottamaan vaihtoehtoiset toimintatavat.
Riskienhallinnan lähtökohtana on epävarmuuden huomioon ottaminen.	Riskienhallinnan otetaan huomioon epävarmuus, sen luonne ja käsittelymahdollisuudet.
Riskienhallinta on järjestelmällistä, jäsennettyä ja ajantasaista.	Järjestelmällinen, ajantasainen ja jäsennetty toimintamalli lisää tehokkuutta ja tekee

	tuloksista yhdenmukaisia, luotettavampia ja helpommin vertailtavia.
Riskienhallinta perustuu parhaaseen saatavilla olevaan tietoon.	Riskienhallintaprosessin lähtötiedot perustuvat tietolähteisiin, kuten historiatiedot, kokemus, palaute ja havainnot. Päätöksentekijöiden on otettava selvää tietoihin liittyvistä rajoituksista ja toisistaan poikkeavat asiantuntijoiden näkemykset sekä otettava nämä huomioon.
Riskienhallinta toteutetaan organisaation tarpeiden mukaan.	Riskienhallinta on sovitettu yhteen organisaation ulkoisen ja sisäisen toimintaympäristön ja riskiprofiilin kanssa.
Riskienhallinta ottaa inhimilliset ja kulttuuriset tekijät huomioon.	Riskienhallinnalla tunnistetaan organisaation omien ja ulkopuolisten henkilöiden kyvyt, näkemykset ja aikomukset jotka voivat auttaa tai haitata organisaation tavoitteiden saavuttamista.
Riskienhallinta on avointa ja kattavaa.	Sidosryhmien ja organisaatioiden eri tasoilla olevien päätöksentekijöiden ottaminen oikealla tavalla ja oikeaan aikaan mukaan riskienhallintaa takaa, että se pysyy tarkoituksenmukaisena ja ajantasaisena.
Riskienhallinta on dynaamista, toistuvaa ja muutoksiin reagoivaa.	Riskienhallinnan avulla muutokset havaintaan ja niihin reagoidaan viipymättä. Ulkoisten ja sisäisten tapahtumien myötä toimintaympäristö ja tietämys muuttuvat, riskejä seurataan ja katselmoidaan, uusia riskejä ilmaantuu, osa riskeistä muuttuu ja osa katoaa.
Riskienhallinta tukee organisaation jatkuvaa kehittämistä.	Organisaation olisi kehitettävä ja toteutettava strategioita, joilla niiden riskienhallintaa kehitetään organisaation muun kehittämisen ohella.

2.5.3 ISO 31000 puitteet

Riskienhallinnan onnistuminen riippuu sen perustana olevien johtamisrakenteiden vaikuttavuudesta ja järjestelyistä, joilla riskienhallinta sisällytetään organisaation kaikkeen toimintaan. Puitteet auttavat hallitsemaan riskejä vaikuttavasti, kun riskienhallintaprosessia sovelletaan organisaation eri tasoilla ja toimintaympäristöissä. Puitteet varmistavat, että riskienhallintaprosessista saatu tieto riskistä raportoidaan oikealla tavalla ja sitä käytetään päätöksenteon ja vastuiden perustana kaikilla olennaisilla organisaation tasoilla. (SFS-ISO 2011, 26.) ISO 3100 puitteiden osat ja niiden suhde on kuvattu seuraavassa kuviossa (kuvio 29).



Kuvio 29 ISO 31000 puitteet (SFS-ISO 2011, 26)

Puitteiden tarkoitus ei ole määritellä johtamisjärjestelmän rakennetta, vaan auttaa organisaatiota sisällyttämään riskienhallinta sen yleiseen johtamisjärjestelmään. Organisaatio voi muuttaa puitteiden osia omia tarpeita vastaaviksi. (SFS-ISO 2011, 26.)

Valtuudet ja sitouttaminen

Riskienhallinnan käyttöönotto ja sen jatkuvan vaikuttamisen varmistaminen edellyttää johdon vahvaa ja jatkuvaa sitoutumista. Tarvitaan myös strategista ja perusteellista suunnittelua, jotta kaikki organisaation tasot saataisiin sitoutumaan riskienhallintaan.(SFS-ISO 2011, 26.) SFS-ISO (2011, 26-28) mukaan standardissa sitoutumisen varmistamiseksi johdon tulisi muun muassa tehdä seuraavaa:

- Määritettävä ja vahvistettava riskienhallintapolitiikka.
- Määritettävä riskienhallinnan suorituskykyindikaattorit, jotka ovat samansuuntaisia organisaation suorituskykyindikaattoreiden kanssa.
- Laadittava riskienhallinnan tavoitteet niin, että ne ovat samansuuntaisia organisaation tavoitteiden ja strategioiden kanssa.
- Nimettävä riskienhallinnasta organisaation eri tasoilla vastaavat tahot.
- Varmistettava, että riskienhallintaan varataan riittävät resurssit.
- Varmistettava, että riskienhallinnan puitteet pysyvät tarkoituksenmukaisina.

Riskienhallinnan puitteiden suunnittelu

Seuraavissa luvuissa on esitetty riskienhallinnan puitteiden kehittämiseen liittyvät tavoitteet. Lisäksi kappaleissa on kuvattu mahdolliset dokumentaatiot ja tehtävät.

Organisaation ja sen toimintaympäristön ymmärtäminen

Ennen riskienhallinnan puitteiden suunnittelua ja toteuttamista on tärkeää arvioida ja ymmärtää sekä organisaation ulkoinen että sisäinen toimintaympäristö. Nämä voivat vaikuttaa merkittävästi puitteiden suunnitteluun. (SFS-ISO 2011, 28.)

SFS-ISO (2011,28) mukaan standardissa ulkoisen toimintaympäristön arviointiin kuuluvat

- kansainvälinen, kansallinen, alueellinen tai paikallinen yhteiskuntaan, kulttuuriin, politiikkaan, lainsäädäntöön, viranomaismääräyksiin, rahoitukseen, teknologiaan, talouteen, luontoon tai kilpailukykyyn liittyvä toimintaympäristö
- keskeiset organisaation tavoitteisiin vaikuttavat tekijät ja kehityssuunnat
- suhteet ulkoisiin sidosryhmiin sekä näiden näkemykset ja arvot.

SFS-ISO (2011, 28) mukaan standardissa sisäisen toimintaympäristön arviointiin kuuluvat

- hallintotapa, organisaatiorakenne, roolit ja vastuut
- toimintaperiaatteet, tavoitteet ja niiden saavuttamiseen tarvittavat strategiat
- resurssit ja tietämykseen liittyvät voimavarat kuten pääoma, aika, henkilöt, prosessit, järjestelmät ja teknologia
- tietojärjestelmät, tiedonkulku ja päätöksentekoprosessit mukaan lukien muodolliset ja epämuodolliset
- suhteet sisäisiin sidosryhmiin sekä näiden näkemykset ja arvot
- organisaation kulttuuri
- organisaation käyttöön ottamat standardit, ohjeet ja mallit
- sopimussuhteiden muoto ja laajuus.

Riskienhallintapolitiikan määritteleminen

Riskienhallintapolitiikan oln ilmaistava selkeästi organisaation tavoitteet riskienhallinnalle sekä sitoutuminen siihen (SFS-ISO 2011, 28). SFS-ISO (2011, 28-30) mukaan standardin riskienhallintapolitiikka kattaa

- organisaation riskienhallinnan perusteet
- organisaation tavoitteiden ja toimintaperiaatteiden ja riskienhallintapolitiikan väliset yhteydet
- riskienhallintaan liittyvät vastuuta ja velvollisuudet
- eturistiriitojen käsittelytapa
- sitoutuminen tarvittavien resurssien varaamiseen riskienhallinnasta vastaavien tahojen käyttöön
- riskienhallinnan tason mittaus- ja raportointikeinot
- sitoutuminen riskienhallintapolitiikan puitteiden katselmointiin ja kehittämiseen sekä säännöllisin väliajoin että reaktioina tapahtumiin tai olosuhteiden muuttumiseen.

Vastuut ja velvollisuudet

Organisaation on varmistettava, että organisaatiossa on määritelty vastuut ja velvollisuudet, valtuudet sekä riittävä osaaminen riskienhallintaan. Näihin kuuluvat osaaminen ris-

kienhallintaprosessin toteuttamiseen ja ylläpitämiseen sekä mahdollisten hallintakeinojen riittävyyden, vaikuttavuuden ja tehokkuuden varmistaminen. (SFS-ISO 2011, 30.)

Sisällyttäminen organisaation prosesseihin

Riskienhallinta on sisällytettävä kaikkiin organisaation käytäntöihin ja prosesseihin tarkoituksenmukaisella, vaikuttavalla ja tehokkaalla tavalla. Riskienhallintaprosessi ei ole erillinen prosessi, vaan se on liitettävä osaksi organisaation prosesseja. Sen olisi etenkinkin oltava osa toimintaperiaatteiden kehittämistä, liiketoimintasuunnittelua strategista suunnittelua, katselmuksia ja muutoksenhallintaprosesseja. Organisaation kattavalla riskienhallintasuunnitelmalla varmistetaan, että riskienhallintapolitiikka toteutetaan ja sisällytetään kaikkiin organisaation käytäntöihin ja prosesseihin. (SFS-ISO 2011, 30.)

Resurssit

SFS-ISO (2011, 30) mukaan organisaation on kohdennettava tarvittavat resurssit riskienhallintaan ja otettava huomioon

- ihmiset ja heidän taitonsa, kokemuksensa ja pätevyytensä riskienhallintaprosessissa kussakin vaiheessa tarvittavat resurssit
- organisaation riskienhallintaan käytettävät, prosessit, menetelmät ja työkalut
- dokumentoidut prosessit ja menettelyt
- tiedon ja tietämyksen hallintajärjestelmät
- koulutusohjelmat.

Sisäisten viestintä- ja raporttimallien laatiminen

Organisaation on luotava sisäisen viestinnän ja raportoinnin mallit, joilla vahvistetaan vastuuta ja riskien omistajuutta (SFS-ISO 2011, 32). SFS-ISO (2011, 32) mukaan mallien olisi varmistettava, että

- riskienhallinnan puitteiden tärkeimmistä osista ja myöhemmistä muutoksista tiedotetaan asianmukaisesti
- puitteista, niiden vaikuttavuudesta ja tuloksista raportoidaan riittävästi organisaation sisällä
- riskienhallinnan soveltamisesta saatua olennaista tietoa on saatavilla sopivilla tasoilla ja sopivina ajankohtina
- tiedonvaihtoon sisäisten sidosryhmien kanssa on olemassa prosesseja.

Ulkoisten viestintä- ja raportointimallien laatiminen

Organisaation on laadittava suunnitelma siitä kuinka se aikoo viestiä ulkoisten sidosryhmien kanssa (SFS-ISO 2011, 32). SFS-ISO (2011, 32) mukaan suunnitelmaan sisältyy

- asiaankuuluvien ulkoisten sidosryhmien osallistaminen ja vaikuttavan tiedon vaihtamisen varmistaminen
- lakien, viranomaisten ja hallintoelinten vaatimustenmukainen ulkoinen raportointi
- palautteen antaminen ja raportointi viestinnästä ja tiedonvaihdosta
- viestinnän hyödyntäminen lisäämään luottamusta organisaatioon
- viestintä sidosryhmien kanssa kriisi- tai poikkeustilanteessa.

Riskienhallinnan toteuttaminen

Riskienhallinnan toteutuminen tapahtuu organisaatioissa sekä puitteiden että riskienhallintaprosessin toteuttamisen avulla. Seuraavissa kappaleissa on kuvattu näiden standardissa määritelty sisältö.

Riskienhallinnan puitteiden toteuttaminen

SFS-ISO (2011, 32) mukaan standardin riskienhallinnan puitteita toteuttaessaan organisaation on tehtävä seuraavat toimet:

- Määriteltävä sopiva puitteiden toteuttamisen aikataulu ja strategia.
- Sovellettava riskienhallintapolitiikkaa ja –prosessia organisaation prosesseihin.
- Noudatettava lakien ja viranomaisten vaatimuksia.
- Varmistettava, että päätöksenteko, kuten tavoitteiden määrittäminen ja asettaminen, on samansuuntainen riskienhallintaprosessin tulosten kanssa.
- Järjestettävä tiedotus- ja koulutustilaisuuksia.
- Viestittävä ja vaihdettava tietoa sidosryhmien kanssa varmistaakseen, että sen riskienhallinnan puitteet ovat edelleen tarkoituksenmukaisia.

Riskienhallintaprosessin toteuttaminen

Riskienhallinta on toteutettava varmistamalla, että riskienhallintaprosessia sovelletaan riskienhallintasuunnitelman mukaisesti. Prosessia on sovellettava kaikilla organisaation tasoilla ja tehtäväalueilla osana sen käytäntöjä ja prosesseja. (SFS-ISO 2011, 32.) Riskienhallintaprosessi on kuvattu omassa aliluvussaan.

Puitteiden seuranta ja katselmointi

SFS-ISO (2011, 32) mukaan varmistuakseen, että riskienhallinta on vaikuttavaa ja tukee jatkuvasti organisaation suorituskykyä, on sen tehtävä seuraavat toimet:

- Mitattava riskienhallinnan tasoa ja verrattava sitä indikaattoreihin, joiden soveltuvuutta katselmoidaan säännöllisin väliajoin.
- Mitattava säännöllisesti riskienhallintasuunnitelman toteutumista ja mahdollisia poikkeamia siitä.
- Katselmoitava säännöllisesti, ovatko riskienhallinnan puitteet, riskienhallintapolitiikka ja –suunnitelma edelleen asianmukaisia, kun otetaan huomioon organisaation ulkoinen ja sisäinen toimintaympäristö.
- Raportoitava riskeistä, riskienhallintasuunnitelman edistymisestä ja siitä, kuinka hyvin riskienhallintapolitiikkaa noudatetaan.
- Katselmoitava riskienhallinnan puitteiden vaikuttavuutta.

Puitteiden jatkuva kehittäminen

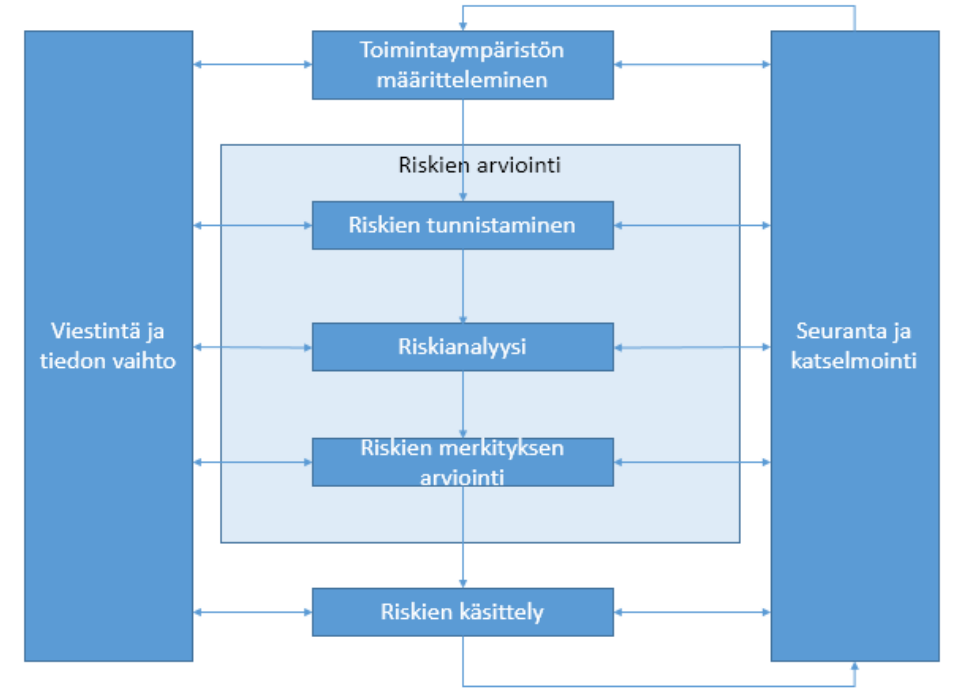
Seurannan ja katselmoinnin tulosten perusteella on päätettävä kuinka riskienhallinnan puitteita, riskienhallintapolitiikkaa ja –suunnitelmaa voidaan kehittää. Näiden päätösten on johdettava organisaation riskienhallinnan ja sen riskienhallintakulttuurin kehitykseen.(SFS-ISO 2011, 34.)

2.5.4 ISO 31000 riskienhallintaprosessi

SFS-ISO (2011, 34) mukaan riskienhallintaprosessi on

- olennainen osa johtamista
- sisällytetty organisaation kulttuuriin ja käytäntöihin
- mukautettu organisaation liiketoimintaprosesseihin sopivaksi.

Riskienhallintaprosessi kattaa seuraavassa kuviossa kuvatut toiminnot (kuvio 30).



Kuvio 30 ISO 31000 riskienhallintaprosessi (SFS-ISO 2011, 34.)

Viestintä ja tiedonvaihto

Ulkoisten ja sisäisten sidosryhmien kanssa on viestittävä ja vaihdettava tietoa kaikkien riskienhallintaprosessin vaiheiden aikana. Ulkoisella ja sisäisellä viestinnällä ja tiedonvaihdolla on varmistettava, että riskienhallintaprosessin toteuttamisesta vastaavat ahot ja sidosryhmät ymmärtävät päätöksenteon perusteet ja syyt siihen, miksi tiettyjä toimenpiteitä tarvitaan. (SFS-ISO 2011, 34-36).

Sidosryhmien kanssa viestiminen ja tiedon vaihtaminen on tärkeää, koska sidosryhmät tekevät olettamuksia riskistä omien riskiä koskevien näkemystensä perusteella. Koska näkemyksillä voi olla huomattavaa vaikutus tehtyihin päätöksiin, näkemykset olisi otettava huomioon päätöksentekoprosessissa. (SFS-ISO 2011, 36.)

Toimintaympäristön määritteleminen

Määrittelemällä toimintaympäristön organisaatio ilmaisee sen tavoitteet, määrittelee ulkoiset ja sisäiset muuttujat, jotka on otettava huomioon riskien hallinnassa, sekä merkittävyyden arvioinnissa käytetyt riskikriteerit. Monet näistä muuttujista ovat samanlaisia kuin puitteiden suunnittelussa tarkastellut muuttujat. Muuttujia on kuitenkin tarkasteltava yksityiskohtaisemmin sen osalta, kuinka ne liittyvät riskienhallintaprosessin soveltamisalaan. (SFS-ISO 2011, 36.) Toimintaympäristön määritteleminen voidaan jakaa eri osioihin. Osiot on kuvattu seuraavassa kuviossa (kuvio 31).

Kuvio 31 ISO 31000 riskienhallintaprosessin toimintaympäristön määrittelyn osat (SFS-ISO 2011, 36-40)

Ulkoisen toimintaympäristön määritteleminen

Ulkoinen toimintaympäristö on se ulkoinen ympäristö, jossa organisaatio pyrkii saavuttamaan tavoitteensa. Ulkoisen toimintaympäristön ymmärtäminen on tärkeää, jotta voidaan varmistaa, että ulkoisten sidosryhmien tavoitteet ja huolenaiheet otetaan huomioon riskikriteerien laatimisessa. (SFS-ISO 2011, 36.) Ulkoiseen toimintaympäristöön kuuluvat tekijät on lueteltu riskien puitteiden suunnittelu luvussa.

Sisäisen toimintaympäristön määritteleminen

Sisäinen toimintaympäristö on se sisäinen ympäristö, jossa organisaatio pyrkii saavuttamaan tavoitteensa. Riskienhallintaprosessin olisi oltava samansuuntainen organisaation

kulttuurin, prosessien, rakenteen ja strategian kanssa. Sisäinen toimintaympäristö kattaa kaikki organisaation sisäiset tekijät, jotka voivat vaikuttaa tapaan, jolla organisaatio hallitsee riskejä. (SFS-ISO 2011, 36-38.) Sisäiseen toimintaympäristöön kuuluvat tekijät on lueteltu riskien puitteiden suunnittelu luvussa.

Riskienhallintaprosessin toimintaympäristön määritteleminen

Organisaation tai riskienhallintaprosessin kattamien organisaation osien, toimintojen tavoitteet, strategiat, laajuus ja muuttujat on määriteltävä. Organisaation riskienhallinnassa on otettava huomioon tarve perustella siihen käytettävät resurssit. Lisäksi resurssit, vastuut, valtuudet ja tallenteet on määriteltävä. Riskienhallintaprosessin toimintaympäristö vaihtelee organisaation tarpeiden mukaan. Siihen voi sisältyä määrittelyt, joiden pitäisi auttaa varmistamaan, että riskienhallintaan sovellettava toimintamalli soveltuu olosuhteisiin, organisaatioon ja sen tavoitteiden saavuttamiseen vaikuttaviin riskeihin.(SFS-ISO 2011, 38). SFS-ISO (2011, 38) mukaan määrittelyssä on oltava

- riskienhallintatoimintojen tavoitteet lyhyellä ja pitkällä aikavälillä
- riskienhallintaprosessin vastuutahot
- suoritettavien riskienhallintatoimintojen laajuus ja yksityiskohtaisuus sekä erityisesti mukaan sisällytettävät tai pois jätettävät asiat
- toiminnon, prosessin tai toiminnon sekä organisaation muiden projektien, prosessien tai toimintojen väliset suhteet
- riskienarviointimenetelmät
- tapa, jolla suorituskykyä ja vaikuttavuutta arvioidaan riskienhallinnassa
- päätökset, jotka on tehtävä
- tarvittavat tutkimukset, niiden laajuus, tavoitteet ja rajaukset sekä niihin tarvittavat resurssit.

Riskikriteerien määritteleminen

Organisaation olisi määriteltävä kriteerit, joita käytetään riskien merkityksen arvioinnissa. Kriteerien olisi kuvastettava organisaation arvoja, tavoitteita ja resursseja. Osa kriteereistä voi perustua lakien ja viranomaisten vaatimuksiin sekä muihin organisaatiota sitoviin velvoitteisiin. Riskikriteerien olisi oltava yhtäpitäviä organisaation riskienhallintapolitiikan kanssa. Ne olisi määriteltävä jokaisen riskienhallintaprosessin alussa ja niitä olisi tarkasteltava jatkuvasti. (SFS-ISO 2011, 40.)

Riskien arviointi

Riskien arviointi on kokonaisvaltainen prosessi, joka kattaa riskien tunnistamisen, riskianalyysin ja riskin merkityksen arvioinnin (SFS-ISO 2011, 40). Riskien arviointi jakautuu riskien tunnistamiseen, riskianalyysiin ja riskien merkityksen arviointiin. Vaiheet on kuvattu seuraavassa kuviossa (kuvio 32).

Kuvio 32 ISO 31000 riskien arviointi (SFS-ISO 2011, 40-42)

Riskien tunnistaminen

Organisaation olisi tunnistettava riskin lähteet, vaikutusalueet, tapahtumat ja niiden syyt sekä mahdolliset seuraukset. Tapahtumissa on huomioitava myös olosuhteiden muutokset. Riskien tunnistamisen tavoitteena on luoda kattava luettelo riskeistä niiden tapahtumien perusteella, jotka voivat mahdollistaa tai estää tavoitteiden saavuttamisen tai parantaa, haitata, nopeuttaa tai viivästyttää sitä. On tärkeää tunnistaa riskit, jotka liittyvät jonkin mahdollisuuden hyödyntämättä jättämiseen. Riskien tunnistaminen mahdollisimman kattavasti on ratkaisevan tärkeää, sillä riski, jota ei tunnisteta tässä vaiheessa, ei ole mukana myöhemmässä analyysissa. (SFS-ISO 2011, 40.)

Organisaation olisi käytettävä sellaisia riskien tunnistamisen työkaluja ja menetelmiä, jotka soveltuvat sen tavoitteisiin ja kykyihin sekä sen kohtaamiin riskeihin. Olennainen ja ajantasainen tieto on tärkeää riskien tunnistamisen kannalta. Tiedon olisi soveltuvin osin sisällettävä myös taustatiedot. Riskien tunnistamisessa oli oltava mukana henkilöitä, joilla on tarvittava tietämys. (SFS-ISO 2011, 40.)

Riskianalyysi

Riskianalyysiin kuuluu käsityksen muodostaminen riskistä. Riskianalyysi on lähtökohta riskin merkityksen arvioinnille ja päätöksille siitä, tarvitseeko riskejä käsitellä ja mitkä ovat sopivimmat riskienkäsittelystrategiat ja –menetelmät. Riskianalyysi voi myös antaa lähtötietoja päätöksentekoon, kun on tehtävä valintoja sellaisten eri vaihtoehtojen välillä joihin sisältyy erityyppisiä ja eritasoisia riskejä. (SFS-ISO 2011, 42.)

Riskianalyysiin sisältyy riskien syiden ja lähteiden, niiden myönteisten ja haitallisten seurausten sekä seurausten tapahtumisen todennäköisyyden tarkastelu. Seurauksiin ja tapahtumistodennäköisyyteen vaikuttavat tekijät olisi tunnistettava. Riskiä analysoidaan määrittelemällä seuraukset ja niiden tapahtumistodennäköisyydet sekä muut riskiin liittyvät ominaisuudet. Tapahtumalla voi olla useita seurauksia, ja se voi vaikuttaa moniin tavoitteisiin. Käytössä olevat hallintakeinot ja niiden vaikuttavuus ja tehokkuus olisi myös otettava huomioon. (SFS-ISO 2011, 42.)

Riskien merkityksen arviointi

Riskien merkityksen arvioinnin tarkoitus on auttaa tekemään päätöksiä riskianalyysin tulosten perusteella siitä, mitä riskejä on tarpeen käsitellä ja mikä on niiden käsittelyn toteuttamisen tärkeysjärjestys. Riskien merkityksen arviointiin kuuluu analyysiprosessin aikana havaitun riskitason vertaaminen toimintaympäristön määrittelemisen yhteydessä määriteltyihin riskikriteereihin. Tämän vertailun perusteella voidaan päättää riskien käsittelyn tarpeesta. (SFS-ISO 2011, 42.)

Riskien käsittely

Riskien käsittelyyn sisältyy yhden tai useamman riskienkäsittelytavan valitseminen ja valittujen vaihtoehtojen toteuttaminen. Riskienkäsittelytavat luovat tai muuttavat hallintakeinoja. (SFS-ISO 2011, 42). SFS-ISO (2011, 42) mukaan riskienkäsittely on toistuva prosessi, johon kuuluvat

- riskien käsittelyn arviointi
- päätös siitä, onko jäännösriskien taso siedettävä
- jos jäännösriskien tasoa ei pidetä siedettävänä, uuden riskien käsittelyn aloittaminen
- riskien käsittelyn vaikuttavuuden arviointi.

Edellä mainitut vaiheet sisältyvät kahteen päävaiheeseen, jotka on kuvattu seuraavassa kuviossa (kuvio 33).

Kuvio 33 ISO 31000 Riskienkäsittelyn vaiheet (SFS-ISO 2011, 44.)

Riskien käsittelyn vaihtoehdot eivät välttämättä ole toisensa poissulkevia tai kaikkiin olosuhteisiin soveltuvia (SFS-ISO 2011, 42). SFS-ISO (2011, 42-44) mukaan vaihtoehtoja voivat olla

- riskin torjuminen päättämällä olla aloittamatta tai jatkamatta riskin aiheuttavaa toimintaa
- riskin ottaminen tai lisääminen jonkin mahdollisuuden hyödyntämisen takia
- riskin lähteen poistaminen
- todennäköisyyden muuttaminen
- seurausten muuttaminen
- riskin jakaminen toisen osapuolen tai osapuolten kanssa esimerkiksi sopimusten tai rahoittamisen kautta
- säilyttäminen tietoon perustuvalla päätöksellä.

Riskienkäsittelytavan valinta

Kun riskinkäsittelytavoista valitaan sopivinta, niiden toteutumiseen vaatimia kustannuksia ja työmäärää verrataan niistä saataviin hyötyihin ottaen huomioon lakien ja viranomaisten vaatimukset. Myös muut vaatimukset, kuten yhteiskuntavastuu ja ympäristönsuojelu tulee ottaa huomioon. Päätöksenteossa olisi myös otettava huomioon riskit, jotka voivat vaatia riskin käsittelyä, joka ei ole taloudellista perusteltua. Tällaisia ovat esimerkiksi vakavat, mutta harvinaiset riskit eli riskit joilla on pieni todennäköisyys, mutta hyvin haitalliset vaikutukset. (SFS-ISO 2011, 44.)

Joitakin riskin käsittelyn vaihtoehtoja voidaan tarkastella ja soveltaa joko yksittäin tai yhdessä. Useiden käsittelytapojen käyttäminen yhdessä on yleensä hyödyllistä. Käsittelytapoja valitessaan organisaation olisi huomioitava sidosryhmien arvot ja näkemykset ja sopivimmat tiedonvälitystavat organisaation ja sidosryhmien välillä. (SFS-ISO 2011, 44.)

Riskienhallintasuunnitelmassa olisi selkeästi yksilöitävä, missä tärkeysjärjestyksessä yksittäiset riskinkäsittelytoimenpiteet toteutetaan. Riskin käsittely voi itsessään aiheuttaa uusia riskejä. Riskinkäsittelytoimenpiteiden epäonnistuminen tai tuloksettomuus voi olla merkittävä riski. Seurannan täytyy olla olennainen osa riskienkäsittelysuunnitelmaa, jotta toimenpiteet varmasti pystyisivät vaikuttavina. Riskin käsittely voi aiheuttaa seurausriskejä, joita täytyy arvioida, käsitellä, seurata ja katselmoida. Seurausriskit olisi sisällytettävä samaan riskinkäsittelysuunnitelmaan kuin alkuperäinen riski, eikä niitä saisi käsitellä uutena riskinä. Näiden riskien välinen yhteys olisi tunnistettava ja säilytettävä. (SFS-ISO 2011, 44.)

Riskinkäsittelysuunnitelman laatiminen ja toteuttaminen

Riskinkäsittelysuunnitelmien tarkoituksena on dokumentoida, kuinka valitut käsittelyvaihtoehdot toteutetaan (SFS-ISO 2011, 44). SFS-ISO (2011, 44) mukaan riskinkäsittelysuunnitelmissa olisi kuvatta

- riskinkäsittelytapojen valintaperusteet, kuten niistä odotettavat hyödyt
- suunnitelman hyväksymisestä vastuussa olevat tahot ja sen toteuttamisesta vastaavat tahot
- ehdotetut toimenpiteet
- resurssivaatimukset, myös poikkeustilanteisiin varautuminen
- toiminnan tason mittarit ja rajoitukset
- raportointi- ja seurantavaatimukset
- ajoitus ja aikataulu.

Riskinkäsittelysuunnitelmat olisi yhdistettävä organisaation johtamisprosesseihin, ja niistä olisi keskusteltava asiaan liittyvien sidosryhmien kanssa. Päätöksentekijöiden ja muiden sidosryhmien olisi oltava tietoisia riskin käsittelyn jälkeisen jäännösriskien luonteesta ja laajuudesta. Jäännösriski olisi dokumentoitava ja sitä olisi seurattava, katselmoitava ja tarvittaessa käsiteltävä uudelleen. (SFS-ISO 2011, 44-46.)

Seuranta ja katselmointi

Sekä seurannan että katselmoinnin olisi oltava suunniteltu osa riskienhallintaprosessia. Niihin olisi kuuluttava säännöllisiä tarkastuksia tai valvontaa. Seuranta ja katselmointi voi olla määrävälein tapahtuvaa tai tilannekohtaista. Seurantaan ja katselmointiin liittyvät vastuut olisi määriteltävä selvästi. (SFS-ISO 2011, 46.)

Organisaation seuranta- ja katselmointiprosessin olisi katettava kaikki riskienhallinta prosessin osa-alueet(SFS-ISO 2011,46). SFS-ISO (2011, 46) mukaan kattava prosessi tarvitaan seuraavista syistä:

- Voidaan varmistaa, että hallintakeinot ovat vaikuttavia ja tehokkaita sekä rakenteeltaan että toiminnaltaan.
- Saadaan lisätietoja ja voidaan parantaa riskin arviointia.
- Voidaan analysoida tapahtumia, kuten läheltä piti -tilanteet, muutoksia, kehityssuuntia, onnistumisia ja epäonnistumisia ja oppia niistä.
- Havaitaan ulkoisen ja sisäisen toimintaympäristön muutokset myös riskikriteerien ja itse riskien muuttuminen, mikä voi edellyttää riskien käsittelyn ja tärkeysjärjestyksen uudelleentarkastelua.
- Uudet riskit tunnistetaan.

Riskienkäsittelysuunnitelmien toteuttamisen edistyminen toimii myös suorituskyvyn mittarina. Tuloksia voidaan hyödyntää organisaation yleisen suorituskyvyn hallinnassa, mittauksissa ja ulkoisessa ja sisäisessä raportoinnissa. Seurannan ja katselmoinnin tulokset olisi tallennettava ja niistä olisi raportoitava soveltuvin osin ulkoisesti ja sisäisesti. Niitä olisi myös käytettävä riskienhallinnan puitteiden katselmoinnin lähtötietoina. (SFS-ISO 2011, 46.)

Riskienhallintaprosessin tallenteet

Riskienhallintatoimintojen olisi oltava jäljitettäviä. Riskienhallintaprosessin tallenteet ovat menetelmien ja työkalujen sekä koko prosessin kehittämisen lähtökohta. (SFS-ISO 2011, 46.) SFS-ISO (2011, 46) mukaan tallenteiden luomista koskevissa päätöksissä olisi otettava huomioon seuraavaa:

- Millaisia jatkuvan oppimisen tarpeita organisaatiossa on.
- Millaista hyötyä tiedon uudelleen käyttämisestä on johdolle.
- Mitä kustannuksia ja toimia tallenteiden luominen ja ylläpito vaatii.
- Millaisia tallenteita laki, viranomaiset ja organisaation toiminta edellyttävät.
- Kuinka tallenteita pääsee tarkastelemaan, kuinka helposti löytää tarvitsemansa ja millaisia tallennusvälineitä käytetään.
- Mikä on tallenteiden säilytysaika.
- Kuinka arkaluonteisia tiedot ovat.

2.6 VAHTI-ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa

Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä VAHTI on julkaissut useita tietoturvallisuuden ohjeita joita valtionhallinnossa noudatetaan. Vuonna 2003 VAHTI julkaisi ohjeistuksen riskien arvioinnoista valtionhallinnossa.

2.6.1 Johtaminen, tietoturva ja riskienhallinta

Tietoturvallisuus on osa johtamistoimintaa. Tietoturvallisuuden ensisijaisena tavoitteena on tarjottavien palvelujen perustana olevan tietoaineiston ja käytössä olevan tietotekniikan

turvallisuuden sekä toimintakyvyn ja käytettävyyden varmistaminen kaikissa oloissa. Tietoturvallisuuden perustana on tunnistaa ja arvioida organisaation toimintaan liittyvät tietoriskit, jonka pohjalta tehdään päätökset mitä toimenpiteitä pitää toteuttaa. Riskejä hallittaessa lähtökohdaksi on otettava organisaation toiminnan kehittäminen, kuten esimerkiksi toimintatavat, osaaminen ja johtaminen. Sen jälkeen tulevat tekniset suojauskeinot. (VAHTI 2003, 10.)

Johdolla tulee olla oikea kuva organisaation toimintaan kohdistuvista tietoriskeistä ja tietoturvallisuuden tasosta. Toimintaan ja palvelujen tietoturvallisuuteen kohdistuvien riskien arviointiin tarvitaan järjestelmällinen riskianalyysimenettely. (VAHTI 2003, 10.) VAHTI (2003, 10) mukaan riskianalyysin tarkoituksena on

- selvittää toiminnan ja palveluiden tietoturvatarpeet ja vaatimukset
- arvioida ulkoiset ja sisäiset riskit
- selvittää säädöksistä ja määräyksistä johtuvat vaatimukset
- arvioida toiminnan ja tietotekniikan muutoksien vaikutukset tietoturvallisuuteen
- selvittää sidosryhmien odotukset
- edellä mainittujen perusteella määritellä tietoturvallisuuden tarpeet, periaatteet ja toteutustapa.

2.6.2 Riskien arvioinnin merkitys ja organisointi

Riskienhallinnalla on selkeät päävaiheet. Ensin tunnistetaan uhat ja arvioidaan niiden merkitys. Sen jälkeen suunnitellaan riskien torjunta ja tarvittavat toimenpiteet. Kolmannessa vaiheessa suunnitellaan miten vahingon sattuessa toimitaan ja miten siitä toivutaan. Tämän jälkeen tilannetta seurataan. Mahdollinen toteutunut riski analysoidaan ja tapahtuneesta otetaan opiksi. (VAHTI 2003, 15.)

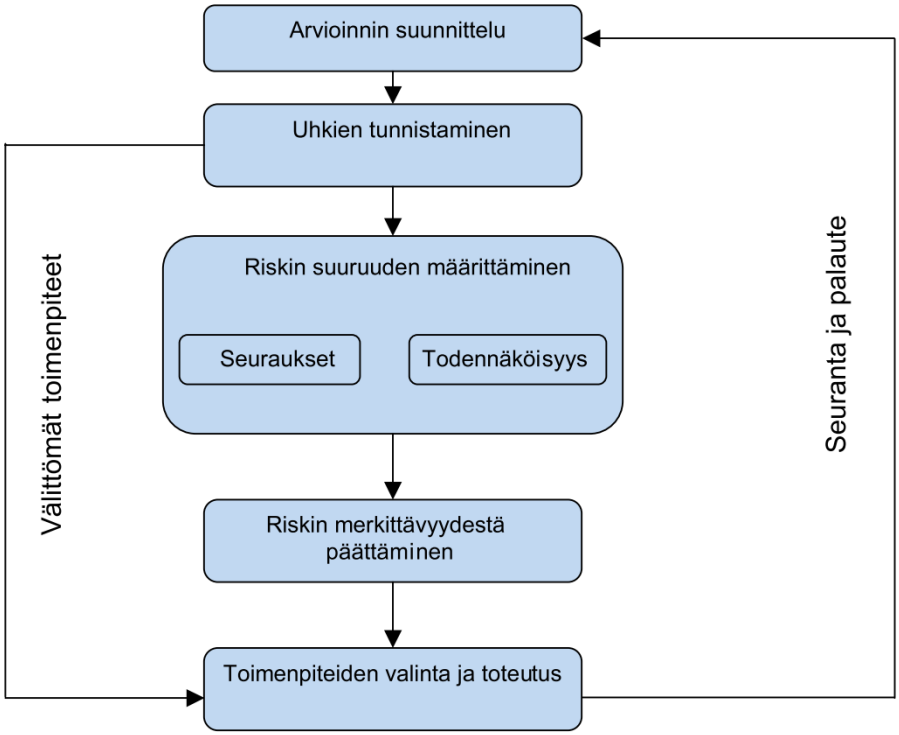
Riskien arvioinnin merkitys

Riskien arvioinnilla tarkoitetaan niitä järjestelmällisiä toimenpiteitä, joilla pyritään tunnistamaan tietoturvallisuuden uhkia ja haavoittuvuuksia sekä arvioimaan mahdollisesti toteutuvien uhkien seurauksia. Käytettävät menetelmät ja työvälineet voivat olla samoja kuin muidenkin riskien arvioinnissa käytetään. (VAHTI 2003, 15.) VAHTI (2003, 15) mukaan riskien arvioinnissa pyritään vastaamaan siihen

- mitä kaikkea voi sattua
- miksi
- mitä siitä voi seurata
- miten suuri on aiheutuva riski.
- mitkä riskit ovat suurimmat.

Riskien arviointi osana riskienhallintaa

Riskien arviointiin sisältyy myös tulosten raportointi perusteluineen (VAHTI 2003, 15). Riskien arvioinnin ja hallinnan vaiheet on esitetty seuraavassa kuviossa (kuvio 34).



Kuvio 34 Riskien arvioinnin ja hallinnan vaiheet (Murtonen 2003; VAHTI 2003, 16)

Kriittinen ja ennakkoluuloton asenne on hyvä uhkien tunnistamisen ja riskien arvioinnin lähtökohta. Lisäksi tarvitaan apuvälineitä, joilla varmistetaan tarkastelun kattavuus ja järjestelmällisyys. Uhkien tunnistaminen voidaan aloittaa karkeilla kartoitusmenetelmillä. Niillä saadaan kokonaiskuva tilanteesta ja löydetään ne riskialueet, joita on seuraavassa vaiheessa tarkoituksenmukaista tutkia yksityiskohtaisemmilla menetelmillä. Tunnistaminen etenee yleisestä yksityiskohtaisempaan. Välillä on syytä arvioida kokonaistilaanne uudelleen karkealla kartoitusvälineellä. (VAHTI 2003, 16.)

Riskien arvioinnin suunnittelu ja toteutus

Riskien arvioinnin suunnittelu edesauttaa sen sujuvaa toteutusta. Hyvän suunnittelun avulla riskien arvioinnin toteutus helpottuu ja nopeutuu. Arviointi kannattaa pyrkiä pitämään mahdollisimman yksinkertaisena. Riskien arviointi kannattaa tehdä ryhmätyönä, johon osallistuu organisaation toiminnan tuntevia henkilöitä (VAHTI 2003, 17.) VAHTI (2003, 17) mukaan analyysin onnistumisen edellytyksenä on sitä varten nimetty vastuullinen henkilö, jonka tehtävänä on

- kohteesta tarvittavan tiedon hankkiminen

- työryhmän kokoaminen
- työryhmän perehdyttäminen analyysimenetelmään
- työryhmäkokousten vetäminen
- tulosten raportointi ja tiedottaminen.

Yhteistyössä työryhmässä käsitellään analyysin laajuus ja rajaus, laaditaan toteutussuunnitelma ja kokousaikataulu sekä suunnitellaan jatkotoimenpiteiden organisointi (VAHTI 2003, 17).

Riskien arvioinnin ensimmäisenä tehtävänä on tunnistaa suojattavat kohteet, jotka ovat organisaation toiminnalle tärkeitä ja joita ilma organisaatio ei voi toimia. Tallaisia suojattavia kohteita ovat esimerkiksi tietoaineistot, turvaluokitellut asiakirjat, holvit, asiakastilat, laitehuoneet, toimistohuoneet, neuvottelutilat, arkistot, paperien hävitys, tietojärjestelmät, sovellukset ja tietoliikenneyhteydet. (VAHTI 2003, 17.)

Varsinainen analysointi tehdään työryhmässä. Sen suositeltava koko on vetäjän lisäksi 3-6 henkeä. Ryhmään valitaan henkilöitä, joilla on hyvä käsitys kohteen toiminnasta, valmius keskustella asioista rakentavassa hengessä ja joille on varattu riittävästi aikaa osallistua analyysiprojektiin. Tärkeää on, että ryhmässä ovat kattavasti mukana kaikki tarvittavat tahot (VAHTI 2003, 18.)

Riskien arvioinnin organisointi

Riskien arvioinnin tulee olla säännöllistä ja jatkuvaa toimintaa. Riskien arviointia voidaan käyttää toiminnan suunnittelussa, projekteissa, tietotekniikkahankkeissa, toiminnan tarkastuksessa ja päivittäisessä johtamisessa. Keskeistä on laaja-alainen riskien arviointi ja hallinta. (VAHTI 2003, 18)

Tietoturvallisuuden vastuiden tulee olla laaja-alaisesti huomioitu organisaatiossa (VAHTI 2003, 18). Eri tahoja, joilla on vastuista tietoturvallisuusriskien arvioinnissa, on kuvattu seuraavassa taulukossa (taulukko 13).

Taulukko 13 Vahti tietoturvallisuusriskien arvioinnin tehtäviä ja vastuita (VAHTI 2003, 18-19)

Tehtävä	Vastuut
Ylin johto	- Vastaa kokonaisvastuun osana tietoturvallisuuden toteutumisesta - Sisällyttää tietoturvallisuuden osaksi riskienhallintaa - Luo edellytykset ja takaa tietoturvallisuuden toteuttamiseksi tarvittavat resurssit - Hyväksyy tietoturvapolitiikan ja siihen liitty-

	vät periaatteet – Edellyttää toimintojen tietoturvapriorisointia – Asettaa vaatimukset raportoinnille
Tietohallintojohto	– Valmistelee tietohallintoon ja tietotekniikkaan liittyvän tietoturvapolitiikan – Ohjaa organisaation tietoturvallisuuden kehittämistoimenpiteitä – Varmistaa tietoturvallisuuden toteutumisen tietohallinnossa – Huolehtii riskien arvioinnista tietojärjestelmäkehityksessä ja tietotekniikkahankkeissa – Arvioi elintärkeiden tietojärjestelmien haavoittuvuutta – Käynnistää arvioinnin esiintuomat kehittämistoimenpiteet
Tietoturvallisuusjohto	– Osallistuu tietoturvapolitiikan ja -periaatteiden määrittelyyn – Kehittää tietoturvallisuutta turvallisuuspolitiikan mukaisesti – Ohjaa tietoturvallisuuden käytännön toteutusta ja siihen liittyvää riskienhallintaa – Luo ja valitsee menettelyt tietoriskien arvioimiseksi – Hankkii arvioinnissa tarvittava asiantuntemuksen – Kouluttaa toiminnasta vastaavan henkilöstön käyttämään arviointimenetelmiä – Osallistuu asiantuntijana riskien arviointiin
Operatiivinen johto	– Vastaa toimialansa tietoturvallisuuden kehittämistoimenpiteiden toteuttamisesta – Ottaa huomioon tietoturvavaatimukset johtaessaan toimialaansa
Esimiehet	– Toteuttavat tietoturvatoimenpiteitä asetettujen tavoitteiden mukaisesti – Raportoivat tietoturvallisuudesta ja siihen kohdistuvista uhkista ja häiriöistä
Tietoturva-asiantuntijat	– Avustavat johtoa ja yksiköitä tietoturvallisuuden edellyttämien asiantuntijat toimenpiteiden kehittämisessä ja siihen liittyvässä päätöksenteossa – Toteuttavat osaltaan päätetyt tietoturvatoimenpiteet – Toimivat asiantuntijoina riskien arvioinnissa
Tietopalveluista ja asiakirjahallinnosta vastaavat	– Raportoivat havaitsemistaan uhkista ja häiriöstä asiakirjahallinnosta – Osallistuvat tarvittaessa oman alansa asiantuntijoina riskien arviointiin
Tietojärjestelmien pääkäyttäjät	– Seuraavat tietojärjestelmien toimintaa tietoturvallisuuden kannalta – Raportoivat tietoturvallisuutta vaarantavista uhkista ja häiriöistä – Osallistuvat tarvittaessa oman alansa asiantuntijoina riskien arviointiin

Käyttäjät	– Raportoivat tietoturvallisuutta vaarantavista uhkista ja häiriöistä – Osallistuvat tarvittaessa oman alansa asiantuntijoina riskien arviointiin

2.6.3 Uhkien määrittely ja tunnistaminen

Uhkien tunnistamiseen on olemassa eri menetelmiä, joita voidaan käyttää rinnakkain (VAHTI 2003, 25). VAHTI (2003, 25) perusteella menetelmää valittaessa on otettava huomioon

- tiedon keruu
- menetelmän ominaisuudet ja sopivuus siihen ympäristöön, jossa sitä on tarkoitus käyttää
- tulosten esitystapa ja kattavuus
- tulosten selkeys ja yksiselitteisyys
- käytön helppous
- menetelmän omat turvaominaisuudet
- raportointimahdollisuudet.

Uhkien tunnistamismenetelmiä

Riskianalyysimenetelmillä voidaan uhkien tunnistettaessa ottaa huomioon monia luonteeltaan erilaisia tekijöitä ja tarkastella yksityiskohtaisesti niiden välisiä riippuvuussuhteita. Analyysissä tarkasteltava kohde jaetaan yleensä osiin ja riskejä tunnistetaan osakohtaisesti. Usein tunnistuksessa käytetään apuna tarkistuslistoja tai avainsanaluetteloita. (VAHTI 2003, 25.) VAHTI (2003, 25-26) mukaan uhkien ja vaarojen tunnistamiseen on kehitetty useita menetelmiä. Seuraavissa kappaleissa esitellään osa menetelmistä.

Potentiaalisten ongelmien analyysi

Potentiaalisten ongelmien analyysi POA on tehokas uhkien tunnistusmenetelmä. Uhkien tunnistaminen edellyttää avointa mieltä ja eri kokemusten yhdistämistä. Tavallinen keskustelu tai tarkistuslistojen käyttö ei täytä näitä vaatimuksia. POA on tehokas menetelmä riskien luovaan ideointiin ja käsittelyyn työryhmässä. Potentiaalisten ongelmien analyysissa on useita vaiheita. Analyysi laaditaan ryhmätyönä vastuulisen vetäjän johdolla. Kohteen koosta riippuen joudutaan pitämään useampiakin analyysikokouksia, joiden tyypillinen kesto on 2-4 tuntia. POA aloitetaan valitsemalla ja rajaamalla tarkasteltava kohde. Valintaperusteet ja kohteen rajaukset on hyvä esitellä tarkastelun loppuraportissa. Valittua kohdetta tarkastellaan usean osatekijän kautta. Esimerkiksi tietojärjestelmää voidaan tarkastella arkkitehtuurin, tietojen käytön, sovelluksien, palvelinten, tietoliikenteen, fyysisen ympäristön sekä tähän liittyvän henkilöstön kautta. (VAHTI 2003, 26.)

Uhkapuut

Uhkapuut on menetelmä, jossa uhkat jaetaan järjestelmällisesti pieniin osiin. Menetelmässä tietoturvaa koskevia uhkia jaetaan pienempiin osiin niin kauan kuin se on mahdollista. Näin syntyvä puumalli kuvaa rakenteellisesti kaikkia tietoturvaa koskevia uhkia. Uhkapuiden rakentaminen vaatii tarkastelun kohteen selkeää rajausta ja huolellista tarkastelun kohteena olevan toiminnon tai tietojärjestelmän analyysia (Suominen 2003, 86; VAHTI 2003, 26).

Skenaariomenetelmä

Skenaarioanalyysissä käydään läpi erilaisia tapauksia, joiden avulla pyritään tunnistamaan mahdollisia uhkia. Analyysi aloitetaan skenaarioiden luomisella. Tähän vaiheeseen otetaan mukaan henkilöstöä eri puolelta organisaatiota sekä eri alueiden erityisosaajia. Skenaarioiden laadinnassa on hyvä hyödyntää tietoja aiemmin sattuneista tietoturvavahingoista tai läheltä piti –tilanteista. Apuna voidaan käyttää myös tietoturvaan liittyvää yleistä aineistoa. Analyysin seuraavassa vaiheessa laadittujen tapausten pohjalta pyritään saamaan kuva suojausten nykytilasta sekä mahdollisista tietoturvapuitteista. (Suominen 2003, 88; VAHTI 2003, 27.)

Haavoittuvuusanalyysi

Haavoittuvuudella tarkoitetaan riskien hallintaan liittyvää epävarmuutta, joka uhkaa organisaation toimintaa. Haavoittuvuusanalyysin näkökulma on tulevaisuuspainotteinen. Analyysissa pyritään tarkastelemaan, miten jatkossa selvitään. Myös kokemuksista otetaan opiksi. Tarkastelemalla itselle ja muille sattuneita tilanteita ja vahinkoja saadaan vinkkejä omista vahvuuksista ja heikkouksista. Haavoittuvuusanalyysissä voidaan tarkastella toimintaa kokonaisuutena. Analyysissä tunnistetaan ne osa-alueet, joihin liittyvät suurimmat riskit ja selvittää riskejä tarkemmin ja toteuttaa riskejä vähentäviä toimenpiteitä. (VAHTI 2003, 27-28.)

Tarkistuslistat

Tarkistuslistojen avulla voidaan uhka kerrallaan miettiä, liittyykö tämä oman organisaation toimintaan. Tarkistuslista on hyvä väline karkeaan uhkien tunnistamiseen ja ongelmakohtien paikallistamiseen. Tarkistuslistoja voidaan käyttää muistilistoina, kun mietitään eri uhkien vaikutusta organisaatiossa. Tarkistuslistat eivät ole koskaan täydellisiä. Listoja käytettäessä on syytä miettiä, kattavatko ne organisaation toimintaan liittyvät keskeiset uhat. (VAHTI 2003, 29.)

2.6.4 Riskien suuruuden arviointi

Riskin suuruuteen vaikuttavat mahdollisten seurausten vakavuus ja todennäköisyys. Uhkia löytyy usein niin paljon, että kaikkia ongelmia on mahdoton hoitaa yhdellä kertaa. Tärkeää onkin tunnistaa ne isoimmat riskit, jotka kiireisemmin vaativat ratkaisua. Tämän vuosi määritellään ensin riskin suuruus arvioimalla uhkan seurauksena mahdollisesti syntyvien vahinkojen suuruus ja todennäköisyys. Riskin suuruuden arviointi antaa perusteet toimenpiteiden suunnittelulle ja kohdistamiselle. (VAHTI 2003, 41.)

Uhkan todennäköisyyden arviointi

Uhkien todennäköisyyksien luokitteluun voidaan käyttää asteikkoa joka on yhdistelmä sanallista arviota ja numerollista arviota. (VAHTI 2003, 41.) Asteikko on esitelty seuraavassa taulukossa (taulukko 14).

Taulukko 14 VAHTI Uhkien todennäköisyyksien arviointiasteikko (VAHTI 2003, 41-42)

Uhkan todennäköisyysaste	Todennäköisyys arvo	Todennäköisyyden kuvaus
Korkea	**3**	– Toiminto tai järjestelmä on heikosti valvottua – Toimintoon tai järjestelmään pääsy on helppoa – Toimintoa tai järjestelmää kohtaan on suurta mielenkiintoa – Toiminnon ohjeistusta ei ole – Tapahtuma ilmenee kerran kuukaudessa – Uhkan toteuttaminen on mahdollista suurelle määrälle käyttäjiä (oma henkilöstö, yhteistyökumppanit, ulkopuoliset)
Keskimääräinen	**2**	– Toiminto on osittain valvottua – Toiminnon ohjeistus on puutteellista – Tapahtuma ilmenee 1-2 kertaa vuodessa – Uhkan toteutuminen on mahdollista tietylle käyttäjäryhmälle (atk-tuki)
Alhainen	**1**	– Toiminto on hyvin valvottua ja siihen pääsy on hallittua – Toiminto on hyvin ohjeistettu – Toimintoa kohtaan ei ole mielenkiintoa – Tapahtuma ilmenee kerran vuodessa – Uhkan toteuttaminen on mahdollista vai yksittäisille työntekijöille (asiantuntijat)
Ei merkitystä	**0**	– Todennäköisyys on tasan nolla. Tämä uhka ei voi toteutua missään olosuhteissa

Seurausten vakavuuden arviointi

Seurausten vakavuuden arviointi kattaa mahdollisesti esiintyvän haitallisen tapahtuman vaikutusten analysoinnin. Kuten todennäköisyyksien arvioinnissa, seurausten vakuutta

voidaan arvioida asteikon avulla. (VAHTI 2003, 42.) Asteikko on esitelty seuraavassa taulukossa (taulukko 15).

Taulukko 15 VAHTI Uhkien vakavuuksien arviointiasteikko (VAHTI 2003, 42-43)

Uhkan vakavuus-aste	Vakavuusarvo	Vakavuuden kuvaus
Erittäin vakavat	**3**	– Seuraukset koskevat kaikkia tietojen tai palveluiden käyttäjiä – Uhkan toteutuminen aiheuttaa välittömiä toimenpiteitä – Uhkan toteutuminen aiheuttaa raportoinnin ministeriölle ja tiedotusvälineille – Uhkan toteutuminen aiheuttaa toiminnan keskeytymisen tunneista useisiin päiviin – Uhkan toteutuminen aiheuttaa suuria taloudellisia kustannuksia – Uhkan toteutuminen aiheuttaa vakavan häiriön organisaation toiminnassa (useiden avainhenkilöiden menetys) – Uhkan toteutuminen aiheuttaa luottamuksellisuuden menetyksen – Toiminta on lainsäädännön velvoitteiden vastaista
Vakavat	**2**	– Seurauksilla on vaikutusta organisaation sisällä, esimerkiksi yksittäisten työntekijöiden työmäärät kasvavat (avainhenkilön menetys) – Seuraukset koskevat useita tietojen tai palveluiden käyttäjiä – Seurauksilla on vaikutus organisaation toimintaan (saatava kuntoon tunneissa) – Uhkan toteutuminen aiheuttaa tiedotteen tekemisen – Uhkan toteutuminen aiheuttaa merkittäviä taloudellisia kustannuksia
Vähäiset	**1**	– Seuraukset koskevat muutamia tietojen tai palveluiden käyttäjiä – Uhkan toteutuminen ei aiheuta välittömästi toimenpiteitä – Uhkan toteutuminen aiheuttaa sisäisen raportoinnin – Uhkan toteutuminen aiheuttaa vähäisiä taloudellisia kustannuksia – Toiminnan keskeytyminen on muutaman minuutin pituinen

Riskin suuruus

Käytännön apuvälineenä riskin arviointiin voidaan käyttää riskitaulukkoa. Taulukossa seurausten vakavuudelle ja uhkan todennäköisyydelle on kolme eri tasoa. Uhkien arviointien perusteella valitaan ensiksi seurausten vakavuus ylimmältä riviltä. Sen jälkeen valitaan tapahtuman todennäköisyys ensimmäisestä sarakkeesta. Riskin suuruus saa valintojen

leikkauksessa määritellyn arvon välillä 1-5. Pienimmillään arvo 1 merkitsee merkityksetöntä riskiä ja suurimmillaan arvo 5 merkitsee sietämätöntä riskiä. (VAHTI 2003, 43.) Seuraava taulukossa (taulukko 16) on kuvattu riskin kriittisyyden arvioinnissa avuksi käytettävää riskitaulukkoa.

Taulukko 16 VAHTI Riskitaulukko (VAHTI 2003, 43.)

Kriittisyys		**Seurausten vakavuus**		
		Vähäinen (1)	Vakava (2)	Erittäin vakava (3)
Uhkan todennäköisyys	Korkea (3)	3. Kohtalainen riski	4. Merkittävä riski	5. Sietämätön riski
	Keskimääräinen (2)	2. Vähäinen riski	3. Kohtalainen riski	4. Merkittävä riski
	Alhainen (1)	1. Merkityksetön riski	2. Vähäinen riski	3. Kohtalainen riski

Jatkoarviointi

Analyysia voidaan jatkaa merkittävimpien uhkien seurausten ja tapahtumistaajuuden kvantitatiivisella arvioinnilla, mikäli tarvitaan tarkempia arvioita päätöksenteon pohjaksi. Uhkien todennäköisyyksien arviointi perustuu tällöin esimerkiksi komponenttien vioittumistietoihin ja ihmisten toiminnan virhetietoihin. Seurausten kuvaamiseen voidaan käyttää laskentamenetelmiä, jotka kuvaavat järjestelmän käyttäytymistä häiriötilanteessa. (VAHTI 2003, 44.)

2.6.5 Toimenpiteiden priorisointi ja määrittely

Tunnistettuja riskejä voidaan hallita monilla keinoilla. Ensisijaisesti on pyrittävä estämään vahinkojen syntyminen tai vähentämään niiden seurauksia. Tarvittavat toimenpiteet riippuvat riskien suuruudesta. Toimenpiteiden suunnittelussa voidaan käyttää avuksi taulukkoa. (VAHTI 2003, 45.) Toimenpidetaulukko (taulukko 17) on kuvattu alla.

Taulukko 17 VAHTI Toimenpiteiden määrittelytaulukko (VAHTI 2003, 45-46)

Riskin suuruus	**Toimenpiteet**
Merkityksetön riski	– Toimenpiteitä ei tarvita
Vähäinen riski	– Toimenpiteitä ei välttämättä tarvita. – Harkitaan parempia ratkaisuja, jotka eivät aiheuta lisäkustannuksia. – Tilannetta seurataan ja varmistetaan, että riski pysyy hallinnassa.
Kohtalainen riski	– Ryhdyttävä toimiin riskin pienentämiseksi. Toimenpiteiden toteutukselle voidaan suunnitella sopiva aikajänne. – Toimenpiteiden kustannuksia on mietittävä tarkasti. – Jos riskiin liittyy erittäin haitallisia seu-

	rauksia, kuten vakava henkilövahinko tai tulipalo, on tarpeen selvittää todennäköisyys tarkemmin.
Merkittävä riski	– Riskin pienentäminen on välttämätöntä. Toimenpiteet tulee aloittaa nopeasti. – Riskialtista toimintaa ei pidä aloittaa ennen kuin riskiä on pienennetty. – Riskialtista toimintaa voidaan jatkaa, mutta kaikkien on tunnettava riski ja toiminta pitää saada loppumaan nopeasti.
Sietämätön riski	– Riskin poistaminen on välttämätöntä. Toimenpiteet tulee aloittaa välittömästi. – Riskialtista toimintaa ei pidä aloittaa. – Riskialtis toiminta pitää keskeyttää, kunnes riski on poistettu.

Riskien arvioinnin tavoitteena on löytää tehokkaimpia toimenpiteitä tietoturvallisuuden parantamiseen. Riskin suuruutta voidaan käyttää perusteena toimenpiteiden kohdistamiseen. Suurimpien riskien poistaminen tai pienentäminen tulee olla etusijalla toimenpiteitä toteutettaessa. Riskien suuruusjärjestys ei ole kuitenkaan suoraan toimenpiteiden järjestys. Toimenpiteiden valinnassa pitää päätyä kokonaisuuden kannalta parhaaseen ratkaisuun. (VAHTI 2003, 46.)

Riskienhallinnan keinot

Kun riskien todennäköisyys ja vakavuus on arvioitu, voidaan suunnitella ja päättää keinoista riskien hallitsemiseksi (VAHTI 2003, 21). Riskejä voidaan hallinta monin keinoin. Keskeiset toimintavaihtoehdot on kuvattu seuraavassa taulukossa (taulukko 18).

Taulukko 18 VAHTI keskeiset riskienhallinnan keinot (VAHTI 2003, 21)

Hallintakeino	Kuvaus
Riskin välttäminen	Mahdollista vain, jos ko. toiminnasta pidättäydytään kokonaan.
Riskin poistaminen	Yksittäinen riski voidaan mahdollisesti poista kokonaan. Poistaminen saattaa aiheuttaa uusia riskejä.
Riskin pienentäminen	Ensisijaisesti on pyrittävä estämään vahinkojen syntyminen tai vähentämään niiden seurauksia. Erilaisilla kontrolleilla pyritään vähentämään seurausten vakavuutta tai tapahtuman todennäköisyyttä.
Riskin siirtäminen	Siirtäminen voidaan tehdä sopimuksilla tai vakuuttamalla.
Riskin pitäminen omalla vastuulla	Osa riskeistä joudutaan tai kannattaa pitää omalla vastuulla. Tällöin otetaan tietoinen riski siitä, että uhka voi toteutua.

Riskien pienentämiseksi voidaan tehdä erinäisiä toimia. Näitä on kuvattu seuraavassa taulukossa (taulukko 19).

Taulukko 19 VAHTI Toimenpiteitä riskien pienentämiseksi (VAHTI 2003, 21-22)

Toimenpideluokka	Kuvaus
Tekniset toimenpiteet	Laite- tai työtilaratkaisut, konesuojauksen kehittäminen, tekniset varmistukset, hälytinjärjestelmät tai huollon ja kunnossapidon parannukset.
Organisaation toimintaan liittyvät toimenpiteet	Yhtenäisistä pelisäännöistä sopiminen, toimintaohjeiden laatiminen, valvonnan tai seurannan kehittäminen, tiedonkulun ja työsuunnittelun parantaminen tai vastuista sopiminen.
Yksilöiden toiminnan parantamisen toimenpiteet	Uusien työvälineiden hankinta, ohjeistus, perehdyttäminen ja koulutus, uudet työaika- tai työparijärjestelyt.

Kaikkia riskejä ei voida poistaa. Riskienhallintatoimenpiteet on syytä aloittaa suurimmiksi arvioiduista riskeistä ja ulottaa niin laajalle kuin mahdollista. Riskienhallintaa liittyy aina arviointi toimenpiteiden kustannuksista. On mietittävä kuinka paljon riskien pienentäviin toimenpiteisiin voidaan panostaa. (VAHTI 2003 22.)

2.6.6 Jatkokehitys- ja seurantasuunnitelmat

Riskien arvioinnissa laadittujen toimenpide-ehdotusten toteuttamiseksi tulee analyysin lopuksi sopia, mitä ehdotuksia ja miten niitä ryhdytään viemään eteenpäin. Samalla sovitaan toimenpiteille vastuuhenkilöt ja karkea aikataulu. Edistymistä seurataan sopivin välein pidettävissä seurantakokouksissa. (VAHTI 2003, 47.) Riskien hallinnasta voidaan tehdä suunnitelma taulukkomuodossa. Esimerkki hallintasuunnitelmataulukosta (taulukko 20) on esitetty alla.

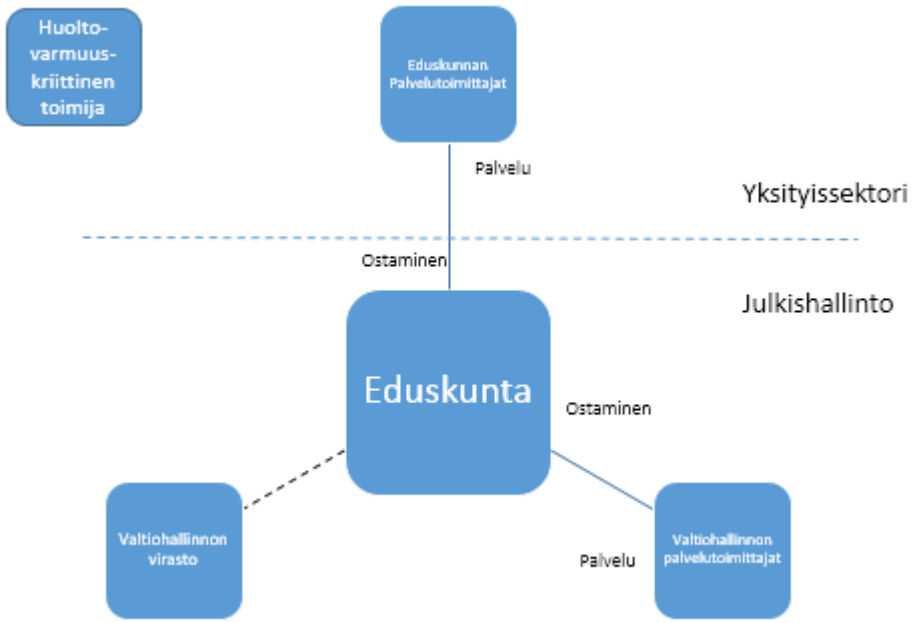
Taulukko 20 VAHTI riskin hallintasuunnitelma (VAHTI 2003, 47)

Riski	WWW-palvelun tietomurto
Tavoite	Tavoitteena on sekä riskin todennäköisyyden että seurausten vakavuuden pienentäminen
Syy riskin olemassaoloon	Käyttöjärjestelmässä on haavoittuvuuksia. Testauksessa ei ole löydetty kaikkia aukkoja, joita hyökkääjä voi hyödyntää
Toimenpide-ehdotus	Toimintaympäristön tapahtumia seurataan. Palvelimen ohjelmisto päivitetään usein. Hankitaan seurantavälineitä joilla mahdollinen murto voidaan havaita.
Aikataulu ja vastuuhenkilö	Toiminnan seuranta on jatkuvaa. Hankitaan tarvittavat ohjelmistot kahden kuukauden aikana. Vastuuhenkilö N.N.

Suunnitellut toimenpiteet on saatettava asianomaisten tietoon. Sekä johtoa, että kohteen henkilöstöä tulee informoida riskianalyysin tuloksista ja kertoa jatkotoimenpiteistä. Tiedottaminen voidaan hoitaa organisaation normaalin tiedotuskäytännön mukaisesti. (VAHTI 2003, 47-48.)

2.7 Muiden organisaatioiden riskienhallinta

Verkostoituneessa yhteiskunnassa riskienhallinta on noussut edellytykseksi organisaatioiden toiminnalle. Eduskunnan kanslia ei ole tästä poikkeus. Voidakseen kehittää riskienhallintaa on tiedettävä tavoitteet ja taso mihin pyritään. Tässä yhtenä menetelmänä on vertailu muiden organisaatioiden toimintatapoihin. Teoriataustaa vasten vertailu suoritettiin haastattelujen avulla. Haastateltavaksi valittiin julkishallinnon ja yksityissektorin toimijoita. Julkishallinnosta haastateltiin valtiohallinnon viraston ja valtionhallinnon palveluntoimittajaa. Yksityissektorilta haastateltiin eduskunnan palveluntarjoajaa ja huoltovarmuuskriittistä organisaatiota. Valinnoilla pyrittiin saada kattavat haastattelut aikaan organisaatioista jotka liittyvä suoraan tai edustavat samaa kuin eduskunta ja organisaatiota joille riskienhallinta on erittäin tärkeää oman toiminnan kannalta. Näiden suhde ja rooli eduskunnan kansliaan on esitetty seuraavassa kuviossa (kuvio 35).



Kuvio 35 Teoriataustaan haastateltujen organisaatioiden suhde eduskuntaan

Haastattelut tehtiin teemahaastatteluina, haastattelukysymykset on esitetty liitteessä 1 haastatteluteemat.

2.7.1 Eduskunnan palveluntarjoaja

Eduskunnan palveluntarjoajana käyttöpalveluille toimii Elisa Appelsiini Oy. Haastateltavan henkilönä oli tietoturvapäällikkö Kirill Filatov. Haastattelun yhteenveto johtopäätöksineen on esitetty seuraavassa taulukossa (taulukko 21).

Taulukko 21 Elisa Appelsiini Oy riskienhallinta (Filatov 18.12.2014)

Teema	Tulos	Johtopäätös
Mitä riskienhallinnalla nyt ymmärretään	Riskienhallinta on siirtynyt kohti kokonaisriskien hallintaa konsernitasolla ja prosessitason riskienhallintaan. Osa riskienhallinnasta on vielä lähellä tekemistä ja ei huomioi kokonaisuutta. Organisaatiokulttuuri on vahvasti tekemislähtöistä ja pyrkii ketteryyteen, tällä selkeä vaikutus riskienhallinnan toteutukseen.	Riskienhallinnan tulisi huomioida kokonaisuudet ja pyrkiä toimimaan prosessitasolla sekä käytännön tasolla. Organisaatiokulttuurilla on merkittävä vaikutus riskienhallinnan toteutukselle, kulttuuri olisi saatava myönteiseksi riskienhallinnalle.
Mitä riskienhallinnalla pitäisi saada tiedoksi	Riskienhallinnalla on kaksi tavoitetta, organisaation jatkuvuuden toteutuminen sekä asiakkaiden sopimusvelvoitteiden täyttäminen. Riskienhallinnalla on saatava selville keskeisten järjestelmien mahdolliset ongelmat, niin omassa organisaatiossa kuin asiakkaan järjestelmissä. Asiakkaalla on kuitenkin vastuu omien järjestelmiensä turvallisuudesta ja riskeistä.	Riskienhallinnan on huomioitava organisaation tavoitteet ja ulkoiset velvoitteet. Organisaation on harjoitettava säännöllistä riskienarviointia ja järjestelmien tärkeyden arviointia. Verkostossa ostavan osapuolen on huolehdittava riskienhallinnasta. Riskienhallinnassa tulisi olla yhteiset liityntäpisteet.
Miten ja mitä tulisi mitata (raportointi: mitä, kuka, kenelle, kuinka usein, miten jatkoseuranta, kuka valvoo…)?	Riskienhallinnasta raportoidaan konsernin tasolla keskeisistä riskeistä. Yritystasolla riskejä seurataan liiketoiminnoittain kootusti. Liiketoiminnat seuraavat omia riskejään vastuualueillaan. Mittarit riippuvat eri liiketoiminta-alueista, teknologiakeskeisissä liiketoiminnoissa keskitytään järjestelmäkohtaisiin riskeihin ja muissa toiminnoissa esimerkiksi projektikohtaisiin riskeihin.	Mittarit riskienhallinnalle on muokattava organisaation kypsyyden mukaan. Alussa on syytä mitata riskienhallinnan suorittamista. Kypsemmällä tasolla on kehitettävä jalostuneempia mittareita riskienhallinnan tehokkuuden mittaukseen. Mittauksen toimivuuden edellytys on oman toiminnan ja sen erityispiirteiden ymmärtäminen.

	Mittarit muodostuvat pitkälti toiminnon luonteesta niiden kypsyydestä.	
Mitä odotuksia rajoille / reagointipisteille	Liiketoiminnan kannalta tärkeisiin järjestelmiin tai hankintoihin sekä projekteihin on kiinnitettävä tarkemmin huomiota kuin muihin.	Organisaation on tunnistettava sille kriittiset järjestelmät ja niiden sidokset. Riskinsietokykyä on alennettava kriittisissä kohteissa.
Mitä erityispiirteitä tietohallintoon / palvelutuotantoon liittyy	Tietohallinnon toimintamalli on pidetty kevyenä. Keskeiset tuotantojärjestelmät on tunnistettu ja niihin liittyvää riskienhallintaa tehdään säännöllisesti. Toimintaa ohjaa vahvasti asiakkaan tekemät sopimukset ja yhteistyön taso.	Onnistumisen kannalta on palveluorganisaatiossa tunnistettava asiakkaan toiminta ja siihen liittyvät odotukset. Asiakkaan on ymmärrettävä mitä on ostanut ja miten valvoa sitä mitä on ostanut.
Muut erityiset riskienhallintaan liittyvät asiat	Yhteistyö on keskeisessä roolissa. Tämä takaa onnistuneen riskienhallinnan.	On ymmärrettävä verkoston erityisominaisuudet riskienhallinnassa ja pidettävä aktiivisesti yllä keskustelukanavia asiakkaan ja palveluntuottajan välillä.

2.7.2 Valtiohallinnon palvelutuottaja

Valtionhallinnon palveluntuottajana toimii Valtion tieto- ja viestintätekniikkakeskus VALTORI. Haastateltavina henkilöinä olivat riskienhallintajohtaja Kimmo Rousku ja tietoturvapäällikkö Tommi Simula. Haastattelun yhteenveto johtopäätöksineen on esitetty seuraavassa taulukossa (taulukko 22)

Taulukko 22 Valtion tieto- ja viestintätekniikkakeskus VALTORI riskienhallinta (Rousku 10.2.2015; Simula 9.1.2015)

Teema	Haastateltava R. Tulos	Haastateltava S. Tulos	Johtopäätös
Mitä riskienhallinnalla nyt ymmärretään	Toimintaan ja strategisia tavoitteita uhkaavat epäsuotuisat tai kielteiset asiat ja tapahtumat, joista nostetaan uhkien arvioimisella tunnistettuja, hallintaan ja seurantaan otettuja riskejä.	Riskienhallinta on organisaation toimintaa ohjaava menettely, jolla tunnistetaan ja priorisoidaan toimintaa uhkaavat asiat ja tapahtumat, sekä mahdollistetaan päätöksenteko toimenpiteistä niiden käsittelemiseksi	Riskienhallinta on osa organisaation johtamista. Riskienhallinnalla on oltava keskustelukanava johtoon.
Mitä riskienhallinnalla pitäisi saada tie-	Mitkä ovat ne sellaiset uhat, jotka mei-	Riittävät tiedot toimintaa uhkaavista	Riskienhallinnan pitää pystyä tunnis-

doksi	dän pitää tunnistaa ja ottaa hallintaan. Toisesta näkökulmasta riskienhallinnasta pitäisi saada tietoon organisaatioon päin seuraavaa: – Miten organisaatiossa riskienhallinta toimii? – Miksi sitä tehdään? – Miten sitä tehdään? Lisäksi tarvitaan esimerkkejä sen toiminnasta eli vaikuttavuudesta mittareiden kautta.	riskeistä ja niiden vaikutuksista, jotta voidaan toteuttaa tarvittavat toimenpiteet niiden saattamiseksi hyväksyttävälle tasolle. Keinoina toimivat esimerkiksi pienentämällä riskejä kehitystoimenpitein tai välttämällä liian suuren riskin muodostavaa toimintaa.	tamaan oleelliset riskit toiminnalle ja löytää keinot niiden hallitsemiseksi. Riskienhallinnan on myös sisällytettävä menetelmät raportoida toiminnasta organisaation laajuisesti.
Miten ja mitä tulisi mitata (raportointi: mitä, kuka, kenelle, kuinka usein, miten jatkoseuranta, kuka valvoo…)?	Mittareina voidaan käyttää seuraavia: – tunnistettujen uhkien määrä – käsiteltyjen riskien määrä – sovittujen toimenpiteiden määrä – sovittujen toimenpiteiden vaikuttavuus – riski-tasojen muuttuminen ylös tai alas – historiatiedot Raportoinnin tehdään sovittujen vastuiden mukaisesti. Käytössä on vuosikellossa 4 kohtaa, 2 kertaa arviointi osana seuraavan vuo toiminnan suunnittelua, sekä 2 kertaa arvioidaan sovittujen toimenpiteiden tila.	Mitä mitataan: yleisesti riskienhallintaprosessin toimivuutta ja vaikuttavuutta sekä hallintatoimenpiteiden statusta. Kuka mittauksen tekee: riskienhallinnan toimenpiteistä vastaavat henkilöt, muun muassa riskienhallinta, turvallisuus, talous ja operatiivinen toiminta. Kenelle raportoidaan: riskien omistajille ja hallintatoimenpiteiden päätöksenteosta vastaaville henkilöille sekä muille organisaation osille ja sidosryhmille, joihin toimenpiteet vaikuttavat. Kuinka usein raportoidaan: riittävällä frekvenssillä päätöksenteon kannalta, huomioitava esimerkiksi vuosibudjetoinnin ajankohdat. Jatkoseuranta ja	Mittarit on sovittava mittamaan sekä prosessin toimivuutta että sillä aikaansaatuja vaatimuksia. Raportointi ja riskienhallinnan seuranta on vastuutettava selkeästi. Riskienhallinnan on huomioitava muun organisaation toiminta ja aikataulutettava toimintansa sen mukaisesti. Riskienhallinta on koko organisaation vastuulla, ei vain riskienhallintaprosessin kehityksestä vastaavalla osalla.

		valvonta: riskienhallintaorganisaatio valvoo prosessin toimintaa, muut organisaation osat vastuullaan olevien riskiarviointien toteuttamista ja hallintatoimenpiteiden edistymistä. Esimerkiksi talousosasto seuraa talousriskejä, palveluorganisaatio seuraa palveluun liittyviä tietoriskejä.	
Mitä odotuksia rajoille / reagointipisteille	Riskienhallinnan toimivuus ja reagoinnin dynaamisuuden tavoittaminen vie oman aikansa ja edellyttää jo aika toimivaa, pitempään aidosti toiminnassa ollutta kypsynyttä toimintamallia. Alussa toiminta tapahtuu enemmän tai vähemmän improvisoitua. Viestintää koko organisaatio, että kaikista asioista kannattaa reagoida – ei odoteta mitään riskienhallintasessiota. Riskienhallinnan kehittäminen ja palveluiden normaali tuotantotoiminta pitää selkeästi erottaa.	Johto määrittää hyväksyttävät riskitasot, jotka ylittyessään edellyttävät toimenpiteitä ja eskalointi tapahtuu eri tasoille määriteltyjen kriteerien perusteella. Hallintatoimenpiteille määritellään toteutusaikataulu, jonka ylitys aiheuttaa eskaloinnin.	Riskienhallinta ja erityisesti reagointipisteet kehittyvät riskienhallinnan prosessin kehittyessä. Kuitenkin johdon olisi määriteltävä jo alussa riskinottokyky, jotta riskeihin voitaisiin reagoida. Seurannan kautta tapahtuu reagointia, mutta myös osana normaalia palvelutuotantoa olisi ryhdyttävä toimenpiteisiin heti ongelmia havaittaessa.
Mitä erityispiirteitä tietohallintoon / palvelutuotantoon liittyy	Oman tietohallinnon ja asiakaspalvelutuotannon erot voi olla haastava tunnistaa.	Tietohallinnolla on keskeinen rooli organisaation toimintaan kohdistuvien tietoriskien hallinnassa. Tietohallinto vastaa organisaation toimintaa tukevien ICT-palvelujen ja –ratkaisujen tuottamisesta ja niihin koh-	Palveluita tuotettaessa on tunnistettava asiakkaan toiminnalle kriittiset järjestelmät ja pystyttävä reagoimaan niihin kohdistuviin ongelmatilanteisiin. Tietohallinnon on kuitenkin arvioitava myös oman toiminnan kannalta kriittiset riskit.

		distuvien hallinta-toimien hyväksynnästä.	
Muut erityiset riskienhallintaan liittyvät asiat	Palveluissa riskienhallinnan pitäisi viedä osaksi palveluiden vuosikelloa, jotta sen toiminta olisi hallittua ja ohjattua.	Ei erityisiä havaintoja.	Riskienhallinta on oltava määrämuotoista kaikissa organisaation toiminnan osissa.

2.7.3 Valtion virasto

Valtion virastona toimii Valtiokonttori. Haastateltavana henkilönä oli riskienhallintajohtaja Juha Pietarinen. Haastattelun yhteenveto johtopäätöksineen on esitetty seuraavassa taulukossa (taulukko 23).

Taulukko 23 Valtiokonttorin riskienhallinta (Pietarinen 5.2.2015)

Teema	Tulos	Johtopäätös
Mitä riskienhallinnalla nyt ymmärretään	Keskittyy tällä hetkellä operatiivisiin ja vahinkoriskeihin. Riskienhallinta ei ole vielä sillä kypsyystasolla millä sen pitäisi olla. Toiminta virastossa on hyvin laaja-alaista ja poikkeavat toisistaan merkittävästi, joka vaikuttaa riskienhallintaan ja erityisesti sen johtamiseen. Kypsyystasot vaihtelevat riskienhallinnassa, osa toiminnoista on luonnostaan ennakoivampaa ja vahvasti säädeltyä, kun taas osa toiminnoista ei taas vaadi vahvaa hallintaa.	Riskienhallinnan tulisi olla huomioida organisaation toiminta ja pyrkiä luomaan yhteistä mallia esimerkiksi raportoinnille ja seurannalle. Yksi malli ei välttämättä täysin sovi kaikkeen organisaation toimintaan, mutta viitekehys auttaa harmonisoimaan riskienhallintaa.
Mitä riskienhallinnalla pitäisi saada tiedoksi	Riskienhallinnan kautta tulisi saada tiedoksi mitkä ovat tavoitteita uhkaavat riskit. Riskienhallinnan ei tulisi yksioikoisesti keskittyä vain vahinkoriskien hallintaan, vaan nimenomaan strategisten tavoitteiden saavuttamiseen. Julkishallinnossa tämä tarkoittaa virastolle asetettuja velvoitteita ja uusien esimerkiksi sähköisten palveluiden tuomien hyötyjen saamista.	Organisaation on tunnistettava sille asetetut tavoitteet ja riskienhallinnalla pyrittävä hallitsemaan näitä uhkaavia riskejä. Riskienhallinnan tulisi myös huomioida myös strategisten riskien hallinta operatiivisten ja vahinkoriskien ohella.
Miten ja mitä tulisi mitata (raportointi: mitä, kuka, ke-	Riskienhallinnan kehityksen alussa on syytä mitata ris-	Mittaristo on oleellinen osa riskienhallinnan toimivuu-

nelle, kuinka usein, miten jatkoseuranta, kuka valvoo…)?	kienhallintaprosessin toimivuutta. Jatkossa kannattaa mitata toimenpiteiden tehokkuutta ja vaikuttavuutta. Tehokkuuden ja vaikuttavuuden mittarit toimivat samalla prosessin toimivuuden mittareina.	den varmistamista. Mittareita on kehitettävä samalla kun riskienhallinta kehittyy organisaatiossa,
Mitä odotuksia rajoille / reagointipisteille	Reagointipiste kannattaa asettaa aina arvioitavan kohteen kriittisyyden mukaisesti. Mitä kriittisempi kohde, sen tarkempaa tarkastelua se vaatii. Toimintaympäristön arvioinnissa tulisi siis huomioida miten arvioitava kohde palvelee organisaation toimintaa. Kriittisyysluokituksen kautta voidaan löytää tarvittavat reagointirajat. (tähänkin yksinkertainen malli, esimerkiksi koriajattelu kolmeen luokkaan)	Organisaatioiden tulisi tehdä kriittisyysluokittelu omista palveluistaan ja siihen liittyvistä järjestelmistä. Jo yksinkertainen malli kriittisyyden arviointiin on riittävä. Esimerkiksi jakamalla palvelut kolmeen luokkaan, voidaan saavuttaa jo toimiva malli.
Mitä erityispiirteitä tietohallintoon liittyy	Tietohallinnon tulee tunnistaa roolinsa toimintaa tukevana organisaationa. Toisin sanoen, miten tietojärjestelmät, tietoliikenne ja perusinfra tukevat muun organisaation toimintaa ja reagoitava näihin liittyviin uhkiin ja riskeihin.	Organisaation on tunnistettava palveluiden ja siihen liittyvien järjestelmien riippuvuudet. Riippuvuuksien tunnistamisen kautta voidaan osaltaan varmistaa riskienhallinnan kattavuus.
Muut erityiset riskienhallintaan liittyvät asiat	Riskienhallinta edellyttää yhteistyötä koko organisaation laajuisesti.	Organisaation laajuinen kommunikaatio on edellytys riskienhallinnan onnistumiselle.

2.7.4 Huoltovarmuuskriittinen organisaatio

Huoltovarmuuskriittisenä organisaationa toimii Jyväskylä Energia. Haastateltavan henkilönä oli riskienhallintajohtaja Kari Helislahti. Haastattelun yhteenveto johtopäätöksineen on esitetty seuraavassa taulukossa (taulukko 24).

Taulukko 24 Jyväskylän Energian riskienhallinta (Helislahti 24.2.2015)

Teema	Tulos	Johtopäätös
Mitä riskienhallinnalla nyt ymmärretään	Riskienhallinnan tulisi olla yksinkertaista ja helposti	Riskienhallinnan mallin tulisi olla riittävän yksinkertainen,

	lähestyttävää. Riskienhallinnassa tällä hetkellä keskitytään liikaa analysointiin ja unohdetaan varsinainen riskienhallinta eli toimenpiteet. Liian monimutkainen riskienhallinnanmalli saa äärimmäisissä tapauksissa organisaation luopumaan riskienhallinnasta.	mutta toimiva. Uhista tulee päästä toimenpiteisiin mahdollisimman nopeasti, helposti käytettävillä työkaluilla ja tätä tukevilla menetelmillä.
Mitä riskienhallinnalla pitäisi saada tiedoksi	Riskienhallinnan keskeisenä osana ovat toimenpiteet. Näiden löytäminen keskeisten riskien hallitsemiseksi on riskienhallinnan tarkoitus. Jokaisen organisaation on mahdollista löytää sille merkitykselliset riskit oppimisen kautta.	Riskienhallintakulttuurin luominen on pohjatyötä riskienhallinnan edistämiselle. Kulttuuria voidaan edistää jakamalla riskienhallintaa pienempiin osiin organisaation eri osien tarpeiden mukaan. Kulttuuri edistyy tekemisen ja oppimisen kautta.
Miten ja mitä tulisi mitata (raportointi: mitä, kuka, kenelle, kuinka usein, miten jatkoseuranta, kuka valvoo…)?	Toimenpiteet on vastuutettu operatiiviselle tasolle, joka raportoi niistä esimiehelle. Nämä puolestaan raportoivat riskienhallinnasta omille esimiehilleen, josta muodostetaan riskienhallinnan kokonaiskuva. Raportoinnin kohteina ovat esimerkiksi toimenpiteiden toteutumisaste tai riskianalyysien tekeminen. Myös strategisten projektien riskit kuten talous, aikataulu ja kannattavuus voidaan ottaa mukaan yhdeksi mittariksi.	Riskienhallinnan seurannan ja toteuttamisen vastuut on määriteltävä organisaation läpi johdosta operatiiviselle tasolle. Tälle on luotava edellytykset riskienhallintamallilla.
Mitä odotuksia rajoille / reagointipisteille	Reagointipisteet voidaan määritellä kohteen mukaan. Samoin raportointiväli voidaan määritellä kohteen mukaan. Kriittisimpiä kohteita on seurattava tarkemmin kuin muita. Näiden määrittelyssä voidaan käyttää puolueetonta tahoa, joka voi analysoida mitkä riskit ovat tärkeitä.	Organisaation on tunnistettava kriittiset toimintansa ja tavoitteensa. Näiden seuranta on oltava tarkemmalla tasolla kuin muiden kohteiden riskit ja hallintatoimenpiteet. Ulkopuolisesta näkökulmasta voi olla hyötyä riskien analysoinnissa, mutta lopullinen vastuu on aina organi-

	Tämä edellyttää toiminnan tuntemista ja luottamusta ulkopuoliseen tahoon.	saatiolla.
Mitä erityispiirteitä tietohallintoon liittyy	Tietohallinto on kriittinen tukitoiminto organisaatiolle. Kriittisten järjestelmien osalta on riskienhallinnan oltava kunnossa ja huomioitava tietoriskit. Tietohallinnossa usein korostuu projektien riskienhallinta. Lähes kaikki toiminta tietohallinnossa on nykyisin projektimuotoista, erityisesti uusien järjestelmien käyttöönoton kohdalla. Tietohallinnossa on myös tunnistettava riippuvaisuudet palvelutoimittajista. Tietohallinnon tuotantomalli on tyypillisesti osittainen tai kokonaan ulkoistettu malli.	Tietohallinnon on kommunikoitava substanssin tai johdon kanssa, jotta palveluiden ja niihin liittyvät järjestelmät saadaan priorisoitua. Tietohallinnon on tehtävä verkostonsa kanssa riskienhallintaa. Tietohallinnolla olisi oltava oma malli riskienhallinnalle, jotta se huomioisi tarpeeksi oman organisaation toiminnan.
Muut erityiset riskienhallintaan liittyvät asiat	Riskienhallinnan tulisi pyrkiä mahdollisimman käytännönläheiseen toimintaan. Käytännönläheisyys vaatii yksinkertaiset työkalut ja näitä tukevat toiminnat.	Riskienhallinnan kehityksessä on noudatettava kypsyysmallia. Yksinkertaisten menetelmien avulla organisaatio oppii riskiajattelua ja tämä edesauttaa riskikulttuurin kehitystä.

2.8 Yhteenveto riskienhallinnasta

Riskienhallinta on menestyvän organisaation keinoja hallita epävarmuuksia ja huomata mahdollisuuksia toiminnassaan. Edellisissä luvuissa on esitelty riskienhallinnan teoriataustaa kirjallisuuden ja kolmen keskeisen viitekehyksen avulla. Nämä toimivat tärkeänä lähteenä eduskunnan tietohallintotoimiston riskienhallinnan kehityksen kannalta tarpeiden ohella. Teoriataustasta on muodostettu synteesi taulukkomuodossa (taulukko 25).

Taulukko 25 Yhteenveto riskienhallinnasta

Tekijä	Kuvaus tai tavoitteet	Keinot	Viittaus
Riskienhallinnan motivaatio	Auttaa organisaatiota saavuttamaan varmemmin tavoitteensa. Pyrkiä vähentämään epävarmuustekijöiden toteutumista ja niiden vaikutuksia.	Organisaation analyysi omasta toiminnastaan. Aikaisemmat tapahtumat ja niiden seuraukset.	Kirjalisuuskatsaus Riskienhallinnan tavoitteet luku 2.3.1 ja Riskien raportointi luku 2.3.6. COSO yleisesittely luku 2.4

	Täyttää organisaatiolle asetetut ja odotetut vaatimukset.	Ulkopuoliset vaatimusten tai odotusten tunnistaminen esimerkiksi lainsäädäntö ja asiakasodotukset.	ISO 31000 periaatteet luku 2.5.2 Haastattelut luvut 2.7.1 – 2.7.4.
Riskienhallinnan kehittäminen ja sen hyödyt	Kehittämisen perustana yrityksen kyky ja halu riskinottoon. Mahdollisuus vaikuttaa kilpailukykyyn positiivisesti. Johdon rooli keskeinen kehittämisessä. Riskienhallinnalla mahdollista tehostaa organisaation työskentelyä. Riskienhallinta yhtenäistää toimintatapoja.	Määritellään riskienhallinnan periaatedokumenteissa. Määritelty riskitasot ja tunnistetut riskit päätöksenteon tukena. Mahdollisuuksien tunnistaminen riskienhallinnan avulla ja myyntiargumenttina käyttäminen. Organisaation johto määrittelee vastuut ja antaa tukensa kehittämiselle. Samalla johto sitoutuu itse riskienhallinnan kehittämiseen. Riskienhallinta laittaa organisaation miettimään riskejä yhdessä keskustellen. Organisaatioyksikköjen välinen kommunikaatio parantuu. Lisäksi riskejä mietitään yhteistyökumppanien kanssa, joka edistää kommunikaatiota ja yhteisen tavoitteen muodostamista toiminnalle. Prosessimainen toimintatapa vaikuttaa koko organisaation toimintaan ja luo turvallisuuskulttuurin lisäksi pohjaa prosessikulttuurille.	Kirjallisuuskatsaus luku Riskienhallinnan tavoitteet luku 2.3.1, Riskienhallinta prosessina luku 2.3.2 ja Riskienhallinnan kehittäminen luku 2.3.6 COSO Sisäinen ympäristö luku 2.4.2 COSO Tavoitteenasettelu luku 2.4.3 COSO roolit ja vastuut luku 2.4.10 ISO 31000 periaatteet luku 2.5.2 ISO 31000 puitteet luku 2.5.3 ISO 31000 riskienhallintaprosessi luku 2.5.4 VAHTI riskien arvioinnin merkitys ja organisointi luku 2.6.2 Haastattelut luku 2.7.2, 2.7.4
Riskienhallinnan toteutustapa	Toistuva, mitattava, määrämuotoinen toteutustapa eli prosessi.	Standardien ja hyvien käytäntöjen hyödyntäminen.	Kirjallisuuskatsaus luku Riskienhallinnan tavoitteet luku 2.3.1, Riskienhallinta prosessina luku

	Ennakoiva toimintamalli, joka tunnistaa mahdolliset ongelmat. Tunnistamisen jälkeen analysoi, hallitsee ja seuraa riskejä. Riskienhallinta raportoi toiminnastaan organisaatiossa ja sidosryhmille. Kehittyvä malli, joka mukautuu organisaatioiden muutoksiin. Huomioi myös mahdollisuudet eikä ainoastaan ongelmat.	Toimii osana organisaation toiminnan suunnittelua Analysointiin, hallintakeinojen määrittelyyn sekä seurantaan avustavien työkalujen määrittely. Raportointimallien määrittely osaksi riskienhallinnan viitekehystä sekä keskitetyn riskisalkun luonti. Organisaation toiminnan kehittämiseen panostaminen ja prosessitoiminnan hyötyjen ymmärtäminen sekä prosessin katselmointiin panostaminen kehityksen varmistamiseksi. Arvioinnissa huomioitava strategiset riskit, joiden hallintakeinoilla voi olla positiivisia vaikutuksia organisaation toimintaan, uusina innovaatioina tai muina hyötyinä.	2.3.2, Riskien arviointi luku 2.3.3, Riskienhallintakeinot luku 2.3.4, Riskien raportointi luku 2.3.5 ja Riskienhallinnan kehittäminen luku 2.3.6 COSO yleisesittely luku 2.4 COSO tapahtumien tunnistaminen luku 2.4.4 COSO riskien arviointi luku 2.4.5 COSO riskeihin vastaaminen luku 2.4.6 COSO valvontatoimenpiteet luku 2.4.7 COSO tieto ja viestintä luku 2.4.8 COSO seuranta luku 2.4.9 ISO 31000 puitteet luku 2.5.3 ISO 31000 riskienhallintaprosessi 2.5.4 VAHTI Riskienarvioinnin merkitys ja organisointi luku 2.6.2 VAHTI Uhkien määrittely ja tunnistaminen luku 2.6.3 VAHTI Riskien suuruuden arviointi luku 2.6.4 VAHTI Toimenpiteiden priorisointi ja määrittely luku 2.6.5 VAHTI Jatkokehitys- ja seurantasuunnitelmat luku 2.6.6 Haastattelut luku 2.7.1-2.7.4.
Riskienhallinnan käyttöönotto	Käyttöönotossa huomioitava organisaatiokulttuuri.	Asteittainen kypsyysmallin mukainen käyttöönotto. Ensin määriteltävä perusvaatimukset ja toteutettava yksinkertainen riskien	Kirjallisuuskatsaus Riskienhallinnan kehittäminen luku 2.3.6 ja Riskienhallinnan käyttöönotto luku 2.3.7

		arviointi. Seuraavaksi prosessin määrittely ja lopulta integrointi osaksi päivittäistä toimintaa.	COSO sisäinen ympäristö luku 2.4.2 COSO roolit ja vastuut luku 2.4.10 ISO 31000 periaatteet luku 2.5.2
	Kehitystyölle määriteltävä selkeät tavoitteet ja aikataulu.	Riskienhallinnan kehitys toteutettava projektina, jossa selkeästi määritellyt tavoitteet, aikataulu ja vastuut.	ISO 31000 puitteet luku 2.5.3 ISO 31000 riskienhallintaprosessi luku 2.5.4
	Riskienhallinta vietävä osaksi muita prosesseja.	Riskienhallinnan huomioitava muut prosessit ja luotava näihin kiinnityskohdat. Esimerkiksi sisäisen tarkastuksen prosessit, liiketoiminnan suunnitteluprosessit, projektiprosessit ja muut prosessit.	VAHTI riskien arvioinnin merkitys ja organisointi luku 2.6.2 Haastattelut luku 2.7.1-2.7.4
	Riskienhallinnan kehitysvastuu on määriteltävä	Kehitysprojektissa määriteltävä selkeä omistajuus riskienhallinnan kehitykselle. Kehitysvastaava ei voi kuitenkaan tehdä johdon puolesta päätöksiä	
	Riskienhallinnan toteutus ja päätöksenteko on määriteltävä.	Riskienhallinnan toteutus on määriteltävä organisaatiossa kaikille. Päätöksenteko on johdon vastuulla	
Riskienhallinnan onnistumiskriteerit	Organisaation sitoutuminen riskienhallintaan kaikilla tasoilla. Riskienhallintakulttuurin luominen organisaatioon. Huomioi organisaation kypsyysasteen riskienhallinnassa.	Johdon valtuutus riskienhallinnalle. Selkeiden vastuiden määrittely. Organisaation johdon ja henkilöstön koulutus. Riskienhallinnan asteittainen käyttöönotto organisaatiossa. Työkalujen pitäminen yksinkertaisina.	Kirjallisuuskatsaus luku Riskien arviointi luku 2.3.3, Riskienhallintakeinot luku 2.3.4, Riskienhallinnan kehittäminen luku 2.3.6 ja Riskienhallinnan tason arviointi luku 2.3.8 COSO sisäinen ympäristö luku 2.4.2 COSO tavoitteenasettelu luku 2.4.3 COSO tapahtumien tunnistaminen luku

	Merkityksellisten tapahtumien onnistunut tunnistaminen	Operatiivisessa toiminnassa kerätyn opin mukaan tuominen riskienhallintaan tekijöiden kautta. Historiatiedon kerääminen tapahtumista. Organisaation tavoitteiden selkeä määrittely.	2.4.4 COSO riskien arviointi luku 2.4.5 COSO riskeihin vastaaminen luku 2.4.6 COSO valvontatoimenpiteet luku 2.4.7 COSO seuranta luku 2.4.9 COSO rooli ja vastuut luku 2.4.10
	Oikein suhteutetut hallintakeinot riskeihin ja toimintaan nähden	Organisaation riskinottokyvyn tunnistaminen arvioinneissa.	ISO 31000 periaatteet luku 2.5.2 ISO 31000 puitteet luku 2.5.3
	Keskittyminen hallintatoimenpiteisiin ja niiden säännölliseen seurantaan. keskeinen osa, ei pelkkä analyysi.	Seurannan kautta painotus hallintatoimenpiteisiin, lisäksi tarvitaan keskitetty näkymä riskeihin.	ISO 31000 luku 2.5.4 VAHTI Riskien arvioinnin merkitys ja organisointi luku 2.6.2
	Integrointi osaksi organisaation toimintaa.	Vuosikellojen määritteleminen sekä palveluiden ja muun toiminnan seurantaan yhdistäminen.	VAHTI Uhkien määrittely ja tunnistaminen luku 2.6.3 VAHTI Riskien suuruuden arviointi luku 2.6.4
	Kattaa organisaation toiminnan keskeiset kriittiset toiminnot tavoitteiden saavuttamisen kannalta.	Analysoi organisaation ulkoisen toimintaympäristön ja sisäisen toimintamallin sekä toimintaajatuksen sekä johtaa näistä kriittiset menestystekijät organisaation toiminnalle. Lisäksi huomioi organisaatiolle asetetut tavoitteet analyyseissä.	VAHTI Toimenpiteiden priorisointi ja määrittely luku 2.6.5 VAHTI Jatkokehitys-seurantasuunnitelmat luku 2.6.6 Haastattelut luvut 2.7.1 – 2.7.4
	Yhteistyökumppaneiden huomioiminen ja sitouttaminen riskienhallintaan.	Yhteistyökumppaneiden osallistaminen riskienhallintaan yhteistyötoimintamallilla sekä sopimusteitse.	
	Riskienhallinta on oltava tehokasta.	Säännöllinen tason mittaus riskienhallinnan prosessin mittareilla sekä vertaismittauksella ulkopuolisiin tahoihin.	

3 Eduskunnan kanslian tietohallinnon riskienhallinnan kehittäminen

Opinnäytetyön kehittämistehtävän kohteena oli eduskunnan kanslian tietohallintotoimiston riskienhallinnan kehittäminen. Tavoitteena oli kehittää malli, jolla tietohallintotoimisto voisi määrämuotoisesti riittävällä laajuudella hallita riskejään. Malli toteutettiin riskienhallinnan puitekuvauksena, jota varten määriteltiin riskienhallinnan periaatteet, kuvattiin riskienhallinnan puitteet ja luotiin riskienhallinnan käsikirja, joka sisälsi prosessikuvauksen, menetelmäkuvaukset, riskienarvioinnin työkalut sekä koulutusmateriaalit. Malli testattiin käsittelemällä aikaisemmin havaitut riskit työstämällä ne riskisalkkuun sekä tekemällä kokonaan uusi riskienarviointi keskeiselle tietojärjestelmälle. Kaikki dokumentaatio myös hyväksytettiin toimiston johtoryhmässä.

Kehitystehtävällä lähdettiin ratkomaan ongelmaa siitä, minkälaisella mallilla tietohallintotoimiston pitäisi hallita riskejään. Lisäksi tutkittiin, minkälaisia tarpeita tietohallintotoimistolla on riskienhallinalle ja miten riskejä tulisi tunnistaa, priorisoida ja analysoida sekä hallita toimistossa. Tutkimusmenetelminä käytettiin konstruktiivista tutkimusta mallin luomiseen. Tukevina menetelminä käytettiin haastatteluja ja dokumenttianalyysia.

Kehittämistehtävä suoritettiin toimiston sisäisenä projektina, jossa projektipäällikkönä toimi tietoturvapäällikkö ja projektin omistajana tietohallintopäällikkö. Tietohallintopäällikkö toimi samalla tutkimuksen ohjaajana organisaatiossa. Seuraavissa aliluvuissa on kuvattu tarkemmin miten kehittämistehtävä tehtiin, perustellaan menetelmävalinnat sekä esitellään tutkimuksessa kehitetty malli ja sen testauksen tulokset.

3.1 Menetelmäkuvaukset ja perustelut niiden käyttämiselle

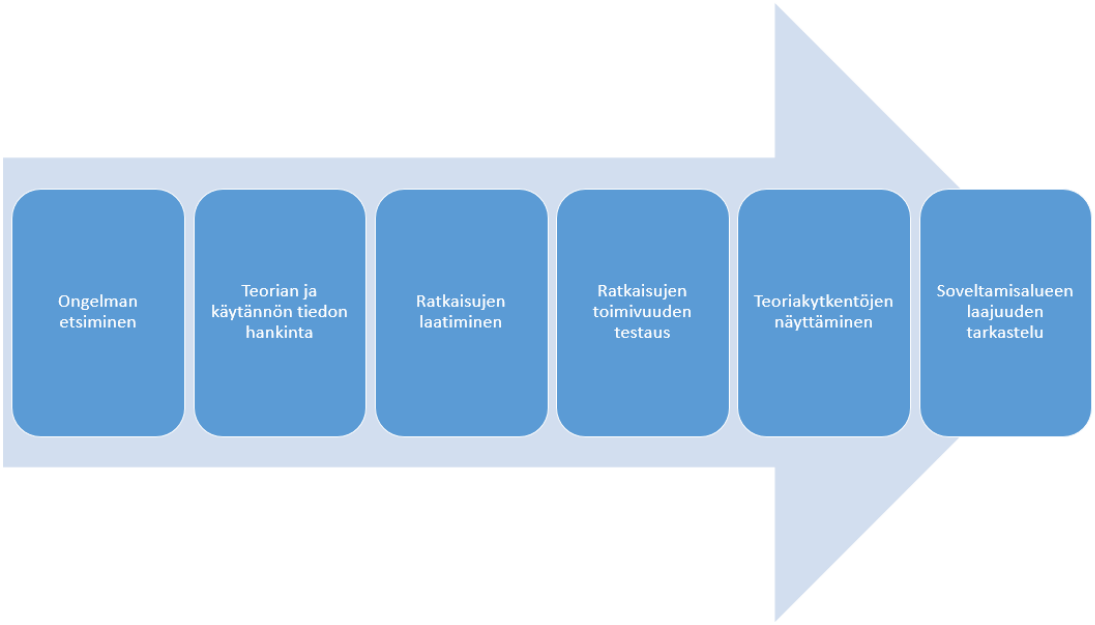
Tutkimusmenetelmänä kehitystyössä käytetään konstruktiivista tutkimusotetta. Tietohallintotoimiston käytännön johtamisessa ja aiemmin tehdyssä riskianalyysissa tuli esille selkeä tarve kehittää toimiston riskienhallintaa. Riskienhallinnalle nykytila oli matalalla kypsyysasteella, joka myös käytännössä toi esille tarpeen uudelle toimintatavalle. Konstruktiivisessa tutkimusotteessa luodaan uusi toimintamalli ja testataan tätä käytännössä. Kehitystehtävän tavoitteena oli luoda uusi malli tietohallintotoimiston riskienhallintaan ja testata mallin toimivuutta käytännössä. Konstruktio oli riskienhallinnan puitteet ja toimintamalli sen toteuttamiseksi mukaan lukien sitä tukevat työkalut ja dokumentaatio.

Jos kehittämistehtävänä on luoda jonkinlainen konkreettinen tuotos tai esimerkiksi suunnitelma, mittari tai malli sopii lähestymistavaksi konstruktiivinen tutkimus. Konstruktiivisella tutkimusotteella pyritään ratkaisemaan tosielämän ongelma innovatiivisella konstruktiolla ja tuottamaan tieteenalalle uutta kontribuutiota. Kyse on uudenkaltaisen todellisuuden

rakentamisesta tutkimustiedon pohjalta. Uuden rakenteen luomiseksi tarvitaan olemassa olevaa teoreettista tietoa ja uutta käytännöstä kerättävää tietoa. Ratkaisun on oltava uudenlainen ja teoreettisesti perusteltu. Konstruktiivinen tutkimus on paikallaan, kun ongelmanratkaisuun tarvitaan myös teoreettista tietämystä. Kohdeorganisaatio saa konstruktiivisessa tutkimuksessa puolueettoman ja teoreettiseen tietämykseen perustuvan ratkaisun ongelmaan. (Lukka 2001; Ojasalo ym. 2014, 65-66.)

Kehittämistehtävän tavoitteena oli luoda tietohallintotoimistolle soveltuva riskienhallintamalli, joka toimisi myös käytännössä. Tämän varmistamiseksi on luotua mallia testattava. Lisäksi on huomioitava toimiston tarpeet riskienhallinnalle. Konstruktiiviseen tutkimukseen kuuluu ratkaisun testaaminen sekä käytännön tiedon hankinta. Koska nyt luotiin ensimmäistä kertaa näin laaja riskienhallinnan malli, on selvää, että sitä on jatkokehitettävä tietohallintotoimiston riskienhallinnan kypsyysasteen kasvaessa. Siten kyseessä on pitkäaikainen sitoutuminen malliin ja sen kehittämiseen. Konstruktiivisen tutkimuksen luonteisiin kuuluu myös toimeksiantajan sitoutuminen kehitystyöhön sekä madaltaa mahdollista jatkokehitystä käyttämällä samoja menetelmiä.

Konstruktiivinen tutkimus on suunnittelua ja käsitteellistä mallintamista sekä toteutusta ja testaamista. Konstruktiivinen tutkimusote sisältää kehitetyn konstruktion toteuttamisyrityksen, jolla mitataan sen toimivuutta. Konstruktiivinen eli suunnittelutieteellinen tutkimus pyrkii vastaamaan kysymyksiin voidaanko rakentaa tietty innovaatio ja kuinka hyödyllinen innovaatio on. Jatkokehityksestä huomioiden konstruktiivinen tutkimus madaltaa teoreettisen tutkimuksen ja käytännön kehitystyön välistä kuilua, mikä lisää omaa tutkimusosaamista myöhemmissä kehittämishankkeissa. Tutkimusotteessa tutkija ja kohdeorganisaation edustajat tekevät läheistä yhteistyötä, jossa odotetaan tapahtuvan kokemuksellista oppimista. Toimeksiantajan on sitouduttava kehittämiseen, se ei saa olla vain yhden avaintyötekijän tai johtajan ajatus. (Järvinen & Järvinen 2004, 103; Lukka 2001; Ojasalo ym. 2014, 65-66.) Konstruktiivisen tutkimukseen prosessin vaiheet on kuvattu seuraavassa kuviossa (kuvio 36).



Kuvio 36 Konstruktiivisen tutkimuksen prosessi (Kasanen, Lukka & Siitonen 1991; Ojasalo ym. 2014, 67)

Konstruktiivisessa tutkimuksessa tavoitteena on kehittää organisaatioon jotain uutta. Tällöin kannattaa kerätä tarvittava aineisto monin tavoin. Havainnointi, ryhmäkeskustelut, kysely ja haastattelu ovat tyypillisiä menetelmiä konstruktiivisessa lähestymistavassa. Lisäksi yhteistyö organisaation kanssa on oleellista. Kehitystarpeet on syytä tuntea hyvin tarkoin. Konstruktiivisen tutkimuksen tekijä tai kehittäjä on aina myös muutosagentti, jonka rooli vaikuttaa voimakkaasti kohdeympäristössä. (Ojasalo ym. 2014, 68.)

Virkani tietoturvapäällikkönä edellyttää läheistä toimintaa IT-palveluiden toimittajien sekä erityisesti tietohallintotoimiston asiantuntijoiden kanssa, jotka ovat vastuussa IT-palveluntuottajien ohjaamisesta. Lisäksi osallistun tietotohallintotoimiston johtamiseen toimiston johtoryhmän jäsenenä. Konstruktiivinen tutkimusote soveltuu hyvin tähän toimintamalliin ja ei tuota ongelmia sen vaativan yhteistyön suhteen.

Tutkimuksessa käytettiin teorian ja käytännön tiedon hankintamenetelminä haastatteluja ja dokumenttianalyysia. Haastateltavilta saatiin kerättyä tietohallinnon tarpeet riskienhallinnalle sekä muiden organisaatioiden toteutustavat riskienhallinnalle. Dokumenttianalyysillä arvioitiin riskienhallinnan nykytilanne ja tietohallintotoimistolle asetetut vaatimukset. Lisäksi kerättiin teoriataustaa kirjallisuudesta ja tutkimuksista.

Haastattelu sopii hyvin moniin kehitystehtäviin, sillä haastattelulla saadaan nopeasti kerättyä syvällisesti tietoa kehittämisen kohteesta (Ojasalo ym. 2014, 106). Haastattelut toteu-

tettiin puolistrukturoituina haastatteluina joihin oli mietitty haastatteluteemat etukäteen. Tällä tavalla haluttiin antaa mahdollisuus keskustelulle, mutta myös antaa raamit keskustelun aiheessa pysymiselle. Ojasalo ym. (2014, 108) mukaan haastattelun tavoitteena on kehittämistehtävän ratkaisua edistävän aineiston kerääminen. Haastattelussa haastattelija ohjaa käytävää keskustelua. Haastattelija on kysyjä ja tiedon kerääjä ja haastateltava vastaaja ja tiedon antaja. Haastattelu toteutettiin kahden haastattelijan voimin, joista toinen keskittyi pelkästään muistiinpanojen tekemiseen. Haastatteluaineistot analysointiin teemoittain ja niistä muodostettiin kooste. Teemoittelussa tarkastellaan aineistossa esiintyviä ilmiöitä tai asioita jotka ovat useammalle haastateltavalle yhteisiä (Ojasalo ym. 2014, 110).

Dokumenttianalyysin avulla tunnistettiin ulkopuoliset vaatimukset riskienhallinnalle kuten esimerkiksi tietohallintolinjaus. Lisäksi dokumenttianalyysin avulla arvioitiin nykyinen riskienhallinta ja –arviointimenetelmä. Sisällön analyysi tehtiin pelkistämällä se osiin haastatteluteemojen, teoriataustan vaatimusten ja asetettujen vaatimusten mukaisesti. Ojasalo ym. (2014, 136-138) mukaan dokumenttianalyysissa pyritään tekemään päätelmiä kirjalliseen muotoon saatetusta erityisesti verbaalisesta symbolisesta tai kommunikatiivisesta aineistosta. Tavoitteena on analysoida dokumentteja järjestelmällisesti ja luoda sanallinen ja selkeä kuvaus tulkittavasta ja kehitettävästä asiasta. Analyysin tarkoituksena on informaatioarvon lisääminen. Sillä luodaan selkeyttä aineistoon, jotta voidaan tehdä siitä luotettavia johtopäätöksiä.

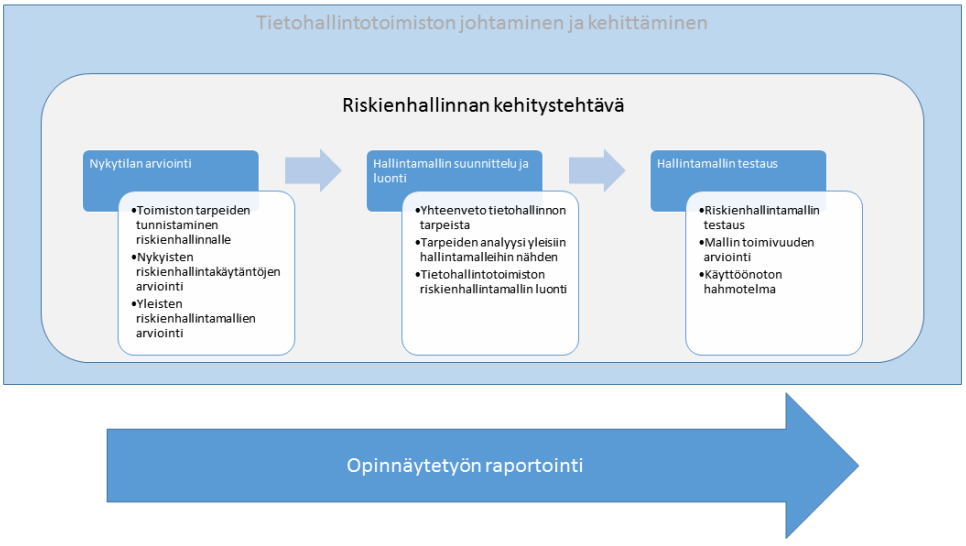
Teorian, tietohallintotarpeiden kartoittamisen ja nykytilan arvioinnin pohjalta muodostettiin konstruktiona riskienhallinnan malli, jonka toimivuutta testattiin tietohallintotoimistossa. Tutkimusprosessin vaiheet ja sen kytkökset kehittämistehtävää on kuvattu seuraavissa luvuissa.

3.2 Tutkimusprosessi ja kytkökset kehittämistehtävään

Konstruktiivisen tutkimuksen prosessissa tunnistetaan aluksi relevantti ongelma jolla on mahdollisuuksia teoreettiseen kontribuutioon, selvitetään yhteistyömahdollisuudet pitkäaikaiseen yhteistyöhön, hankintaan teoriatausta, kehitetään innovaatio ja testataan sen toimivuus. Testauksen jälkeen tarkastellaan ratkaisun soveltuvuutta ja tunnistetaan ja analysoidaan teoreettinen kontribuutio. (Lukka 2001.) Järvinen ja Järvisen (2004, 104) mukaan konstruktiivinen tutkimus on jaoteltavissa kolmeen osioon: kohteen suunnittelu, prosessin suunnittelu ja toteutuksen suunnittelu. Kohteen suunnittelu on lopputuloksen suunnittelua ja määrittelyä, prosessin suunnittelussa suunnitellaan miten periaatteessa eri resursseja käyttäen lopputulos saadaan aikaan ja toteutuksen suunnittelussa suunnitellaan käytän-

nön toimenpiteet miten alkutilasta päästää haluttuun lopputilaan. Lisäksi innovaation rakentaminen ja käyttö tulee arvioida, koko elinkaari ideasta ensimmäiseen toteutukseen, käyttöön ja lopulta hävitykseen asti(Järvinen & Järvinen 2004, 105).

Riskienhallinnan mallin kehittämistehtävän tarve syntyi eduskunnan kansliassa käynnistetystä riskienhallinnan käyttöönotosta ja sen mukana tehdystä tietohallintotoimiston riskianalyysista. Riskianalyysin havaintona oli, ettei tietohallintotoimisto ole määrämuotoisesti kehittänyt tai ohjannut tietoturvallisuuttaan määrittelemällä toimintatapoja siihen. Tietohallintoon oli perustettu tietoturvapäällikön virka, jonka toimenkuvana on kehittää hallinnollista tietoturvaa. Riskianalyysin perusteella tietohallintotoimiston johtoryhmä päätti, että riskienhallinnan kehittäminen on ensimmäinen askel kohti määrämuotoista tietoturvan hallintaa kohden. Kehittämistyön pohjana toimi käytössä oleva riskienhallintakäytäntö. Tämä ei kuitenkaan antanut mallia kokonaisvaltaisemmalle riskienhallintamallille. Tätä varten tarvittiin vahvasti teoriaan pohjautuva uusi toimintatapa. Kehittämistehtävä jaettiin kolmeen päävaiheeseen. Vaiheet olivat nykytilan arviointi, hallintamallin suunnittelu ja luonti sekä hallintamallin testaus. Tämän rinnalla tehtiin opinnäytetyöraportointia. Vaiheet sisältöineen on kuvattu seuraavassa kuviossa (kuvio 37)



Kuvio 37 Kehitystehtävän vaiheistus

3.2.1 Nykytilan arviointi

Nykytilan arviointi vaati tutkimusaiheen tarkempaa tutkimista. Tutkimisen kohteina olivat tietohallintotoimiston tarpeiden tunnistaminen, tietohallintotoimiston riskienhallinnan nyky-

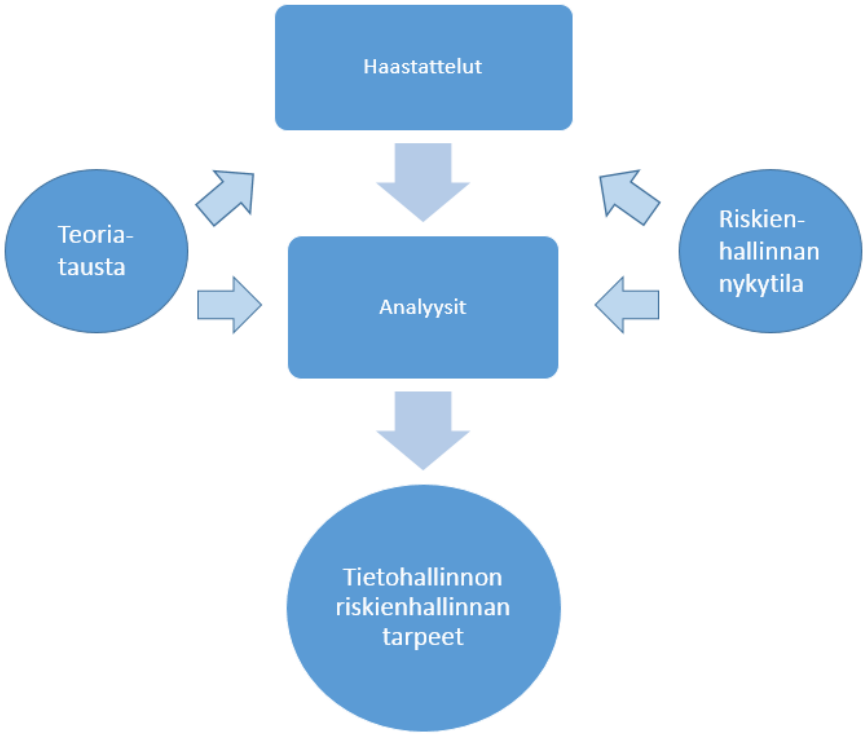
tilan arviointi sekä riskienhallinnan teoriataustan keräämistä. Näistä muodostettiin pohjavaatimukset toimiston riskienhallintamallin toteutukselle.

Tutkimusaiheen syvällisen tuntemuksen hankkiminen muistuttaa kenttätutkimusta. Havainnointien, haastattelujen ja kirjallista aineisto analysoimalla pyritään saavuttamaan syvällinen ymmärrys organisaation lähtötilanteesta. Tavoitteena on myös varmistaa tietoisuus alan aiemmista teorioista. Tämä mahdollistaa myöhemmässä vaiheessa tunnistamaan ja analysoimaan tutkimuksen teoreettista kontribuutiota. (Lukka 2001.) Järvinen ja Järvinen (2004, 108) kuvaavat tuntemuksen hankkimista osana tavoitetilan kuvausta joka tehdään osana innovaation toteuttamista. Tavoitetila heijastaa innovaation ja suunnittelijoiden ja päättäjien arvoja. Tavoitetilaa kuvaava malli on normatiivinen ja se esittää miten asioiden pitäisi olla. Järvisen ja Järvisen (2004, 109) esittämän mallin mukaan tavoitetila kuvataan spesifiointiprosessin avulla. Tieteen näkökulmaa painottamalla tulee perusteellisen kirjallisuustutkimuksen avulla varmistua, että innovaatio on ainutlaatuinen tai tekee huomattavan parannuksen olemassa olevaan innovaatioon. Käytännön innovaatioissa on usein useita osapuolia joilla on omia toiveita tavoitetilan suhteen. Eri osapuolten näkemykset tulisi huomioida siten, että eri osapuolet pyrkivät ristiinkouluttamaan toisiaan tavoitetilan vaatimusten suhteen

Toimiston tarpeiden tunnistaminen riskienhallinnalle

Toimiston tarpeiden tunnistaminen tehtiin haastatteluilla. Haastateltavina olivat tietohallintotoimiston johtoryhmän jäsenet paitsi tutkimuksen tekijä tietoturvapäällikkö. Toimiston johtoryhmän jäsenet toimivat esimiesroolissa asiantuntijoille ja suunnittelijoille sekä projektipäälliköille. Päälliköiden näkemys riskienhallinnan kehittämisestä oli keskeinen tarpeiden tunnistamisen kannalta. Samalla haastatteluilla aloitettiin johtoryhmän sitouttaminen uuden riskienhallintamallin käyttöönoton tueksi. Haastattelut toteutettiin jokaiselle johtoryhmän jäsenelle omana puolistrukturoituna teemahaastatteluna. Haastatteluteemat on esitetty liitteessä 1.

Puolistrukturoitu haastattelu sisältää sekä strukturoituja kysymyksiä että avoimia keskusteluteemoja. Haastattelu on tehokas ja tärkeä tiedonhankintamenetelmä. Uutta tietoa voidaan välittömästi tarkentaa vastaanoton jälkeen johon ei ole mahdollisuutta kirjalliseen materiaaliin tutustuttaessa, (Järvinen & Järvinen 2004, 145-146.) Seuraavassa kuviossa (kuvio 38) on esitetty tarpeiden keräämisen vaiheet ja siihen vaikuttaneet tekijät.



Kuvio 38 Tietohallintotoimiston riskienhallinnan tarpeiden kerääminen

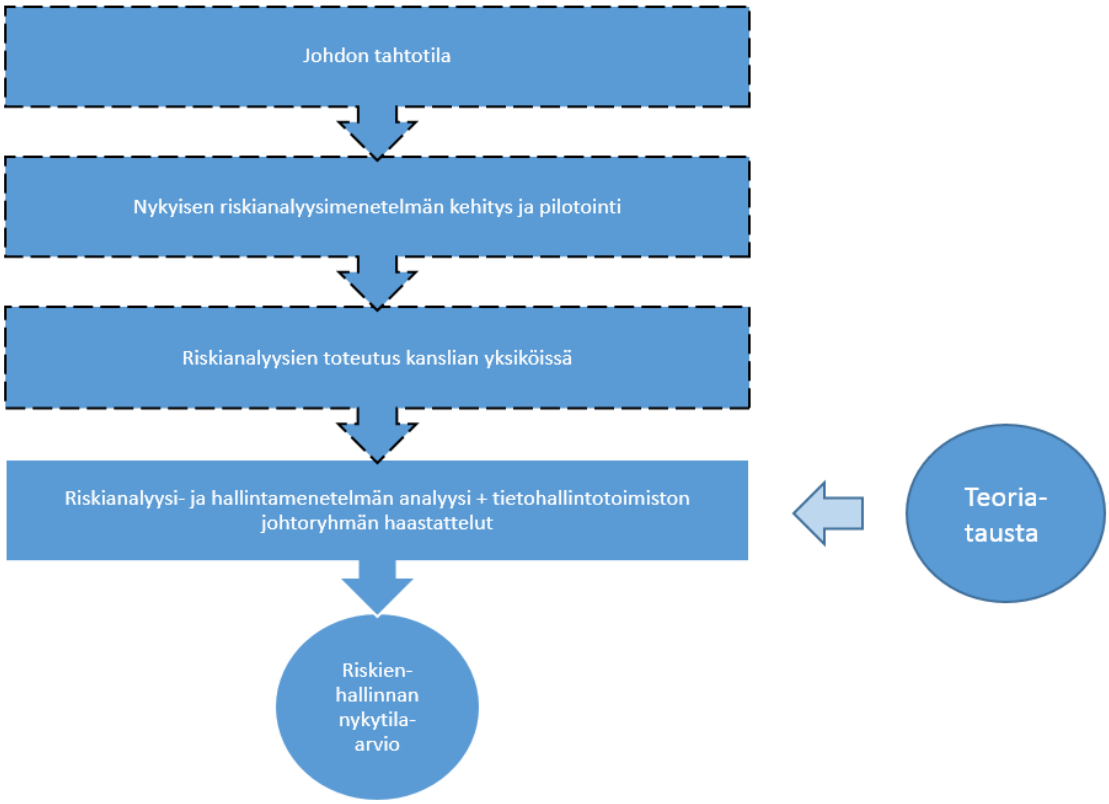
Haastattelun teemoihin ja tulosten analyyseihin vaikuttivat sekä teoriatausta että nykytilan analyysi.

Nykyisten riskienhallintakäytäntöjen arviointi

Nykyisten riskienhallintakäytäntöjen arviointi perustui eduskunnan kansliassa käytössä olevan menetelmän arviointiin. Arviointiin saatiin myös materiaalia tietohallintotoimiston johtoryhmän haastatteluista. Yhtenä haastatteluteemana oli riskienhallinnan nykytila tietohallintotoimistossa.

Eduskunnan kansliassa oli aloitettu yhteisen riskianalyysimenetelmän käyttö vuonna 2014. Sitä oli edeltänyt sisäisen tarkastuksen havaintoihin perustunut eduskunnan kanslian kansliatoimikunnan päätös käynnistää riskienhallinta kaikissa yksiköissä. Turvallisuusyksikkö pilotoi mallia ensin ja 2014 kevään aikana samalla menetelmällä analysoitiin koko kanslian riskit. Samaa menetelmää käytettiin tietohallintotoimiston riskien analysoimiseen. Nämä askeleet riskienhallinnan kehityksessä oli otettu ennen tätä tutkimusta.

Riskienhallinnan nykytilan arviointi perustui edellä mainittuihin haastatteluihin ja käytössä olevan menetelmän arviointiin. Nykytilan arvioinnin vaiheet on esitelty seuraavassa kuviossa (kuvio 39). Katkoviivalla esitetyt vaiheet eivät kuuluneet tämän tutkimuksen piiriin.



Kuvio 39 Tietohallintotoimiston riskienhallinnan nykytilan arviointi

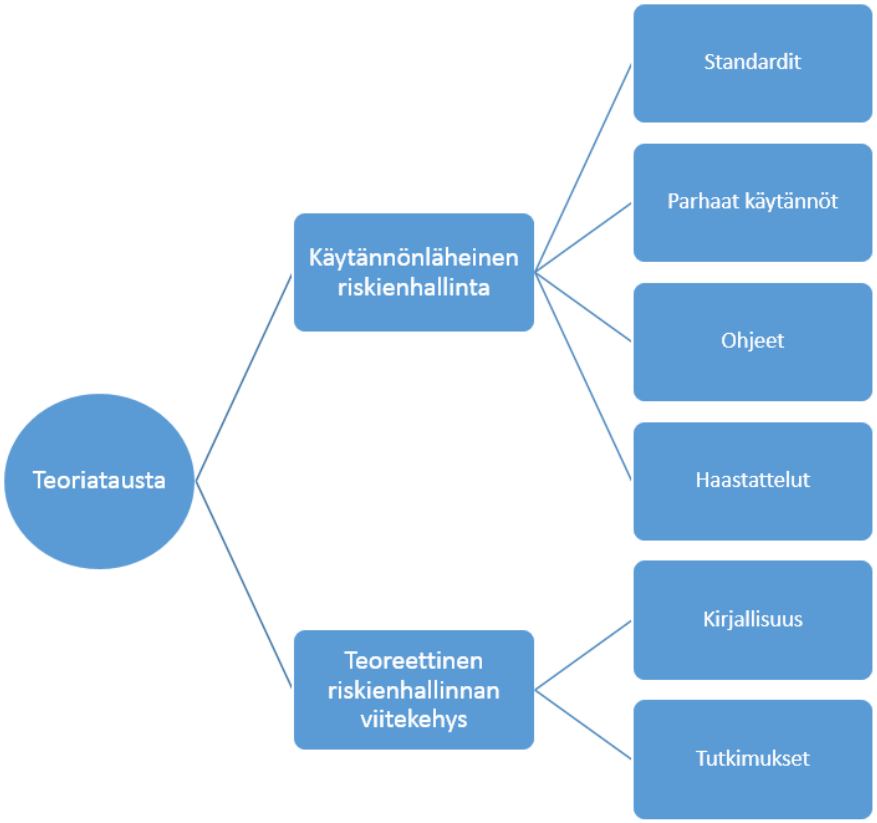
Arvioinnissa vertailtiin nykyistä riskianalyysimenetelmää teoriataustan tuomaan viitekehykseen riskienhallinnan toteutuksesta. Myös johtoryhmän haastatteluissa tuodut seikat otettiin huomioon arviossa. Analyysimenetelmänä oli dokumenttianalyysi, jossa nykytilaa kuvaava dokumentaatio purettiin teoriataustan perusteella muodostettuihin näkemyksiin riskienhallinnan sisällöstä ja verrattiin niiden toteutumista nykytilassa. Ojasalo ym. (2014, 139-140) mukaan pelkistämisen tarkoituksena on selkeyttää ja tiivistää aineistoa tunnistamalla ja rajaamalla pieni määrä näkökulmia. Pelkistämällä tuotetaan myös uutta tietoa. Abstrahoinnin avulla pyritään muodostamaan yleiskäsitteet pelkistämällä ja muodostamalla oleellinen tieto tutkimukselle. Tulkintavaiheessa muodostetaan analyysin perusteella johtopäätökset.

Analyysin jälkeen tehtiin tulkinta analyysin tuloksista ja esitettiin ne johtopäätöksinä riskienhallinnan nykytilasta. Ojasalo ym. (2014, 143-144) mukaan tulkinta ei tarkoita samaa kuin analyysi. Tutkimus ei ole vielä valmis kun tulokset on analysoitu, vaan tutkijan tehtävänä on tulkita tulokset. Tulkinnassa tutkija tuo kohdeilmiöstä esiin jotain uutta. Kehittäjän on pyrittävä laatimaan eri havainnoista ja osatuloksista synteesejä, jotka kokoavat yhteen keskeiset tulokset ja antavat selkeästi pelkistetyn ja perustellun vastauksen asetettuihin

kysymyksiin. Johtopäätökset tai kehittämistyön suositukset laaditaan näiden synteesien perusteella. Nykytilan arvioinnin tulokset on esitelty luvussa 3.4.

Yleisten riskienhallintamallien arviointi

Yleisten riskienhallintamallin arviointi sisälsi teoriataustan keräämisen riskienhallinnasta. Teoriataustassa käytettiin lähteinä kirjallisuutta ja tutkimuksia, jotka muodostivat teoreettisen viitekehyksen riskienhallinnalle. Käytännönläheinen riskienhallinta muodostui COSO ERM kokonaisvaltaisen riskienhallinnan viitekehyksestä, ISO 31000 riskienhallinnan standardista ja Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI julkaisemaa ohjeesta riskienhallinnan toteutukselle. Näitä täydennettiin haastatteluilla riskienhallinnan toteutuksista muissa organisaatioissa. Teoriataustan kokoonpano on esitelty seuraavassa kuviossa (kuvio 40).



Kuvio 40 Tutkimuksen teoriataustan koostumus

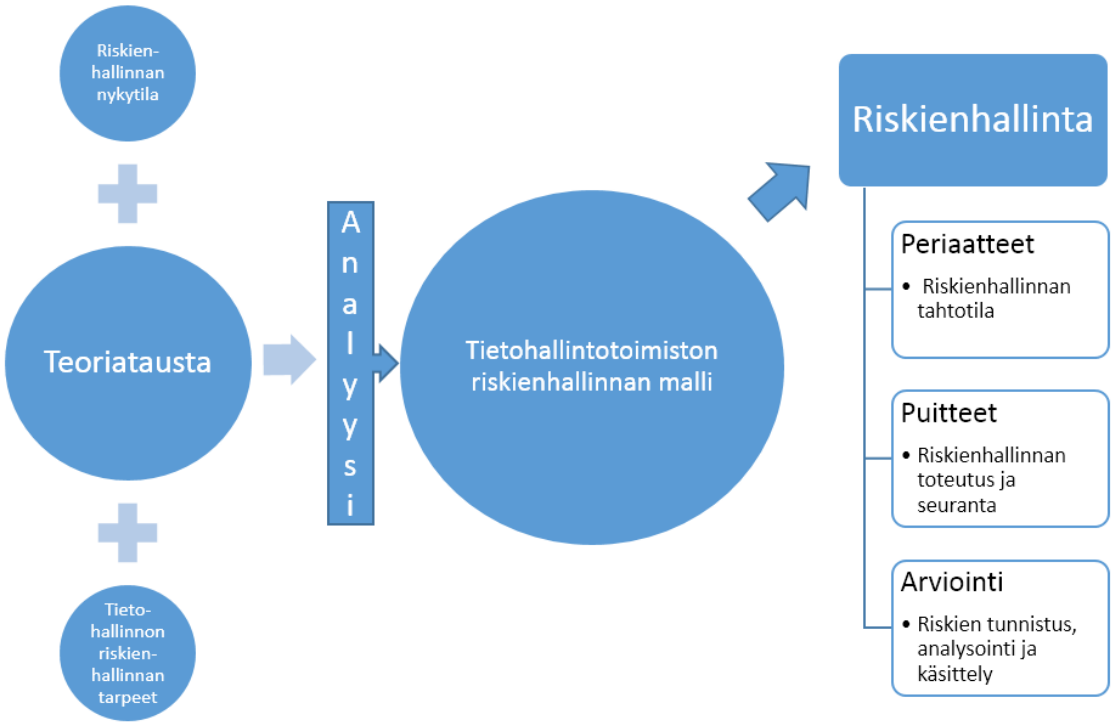
Kerätyistä materiaaleista muodostettiin synteesi, joka on esitelty luvussa 2.8. Menetelmänä synteesin muodostuksessa käytettiin dokumenttianalyysia, kuten nykytilan arvioinnissa ja tarpeiden tulosten muodostamisessa.

3.2.2 Hallintamallin suunnittelu ja luonti

Hallintamallin suunnittelu ja luonti -vaiheessa koostettiin yhteen edellisessä vaiheessa koottu materiaali, analysointiin se ja näiden pohjalta luotiin malli riskienhallinnan toteuttamiselle tietohallintotoimistossa. Kehitetty malli oli tutkimuksen konstruktio, jonka toimivuutta testattiin käytännössä.

Vaihe on kriittinen, jos konstruktiota ei pystytä kehittämään, ei projektia ole syytä jatkaa. Vaihe on luova ja heuristinen, joten tarjolla on hyvin vähän yleispäteviä ohjeita. Konstruktion tulee olla innovatiivinen, pelkkää aiempien konstruktioiden soveltamista ei voida pitää konstruktiivisen tutkimusotteen tuloksena. (Lukka 2001.) Järvinen ja Järvisen (2004, 109-111) kuvaavat konstruktion muodostamisen implementointiprosessina, jossa voidaan käyttää erilaisia ongelmanratkaisun heuristiikkoja, kuten ongelmanreduktio heuristiikka. Tässä heuristiikassa jaetaan pääongelma pienempiin osaongelmiin ja pyritään ratkaisemaan osaongelmat ja sillä tavoin pääongelman. Muita tavoitetilan saavuttamiskeinoja ovat valmisosan hankinta täyttämään asetetut vaatimukset sekä rinnakkaiset spesifiointi- ja implementointiprosessit.

Tietohallintotoimiston tarpeet riskienhallinnalle koostettiin yhteen ja analysoitiin teoriataustaa sekä nykytilaa vasten. Analyysin perusteella luotiin hallintamalli tietohallintotoimiston Seuraava kuvio (kuvio 41) kuvaa mallin luontia ja karkeaa sisältöä.



Kuvio 41 Riskienhallintamallin luonti ja sisältö

Yhteenveto tietohallintotoimiston tarpeista

Yhteenveto tietohallintotoimiston tarpeista tehtiin johtoryhmän haastattelujen perusteella. Yhteenvetoa vasten analysoitiin koostettu haastattelumateriaali. Analyysissa purettiin haastatteluiden tulokset teemoittain sekä tehtiin teemakohtainen yhteenveto. Yhteenvedoista tehtiin johtopäätökset johtoryhmän näkemyksistä riskienhallinnalle tietohallintotoimistossa. Johtopäätökset tarpeista on esitelty tutkimuksen tuloksia esittelevässä luvussa 3.4 ja liitteessä 2.

Tarpeiden analyysi yleisiin hallintamalleihin nähden

Tietohallintotoimiston tarpeet riskienhallinnalle yleisiin riskienhallintamalleihin nähden tehtiin analysoimalla toimiston tarpeiden analyysin tulkinnat vertaillen niitä yleisten riskienhallintamallin analyysin tuloksiin nähden. Tämän tuloksena saatiin lähtökohta tietohallintotoimiston riskienhallinnan mallin kehitykselle. Tulokset on esitelty luvussa 3.4.

Tietohallintotoimiston riskienhallintamallin luonti

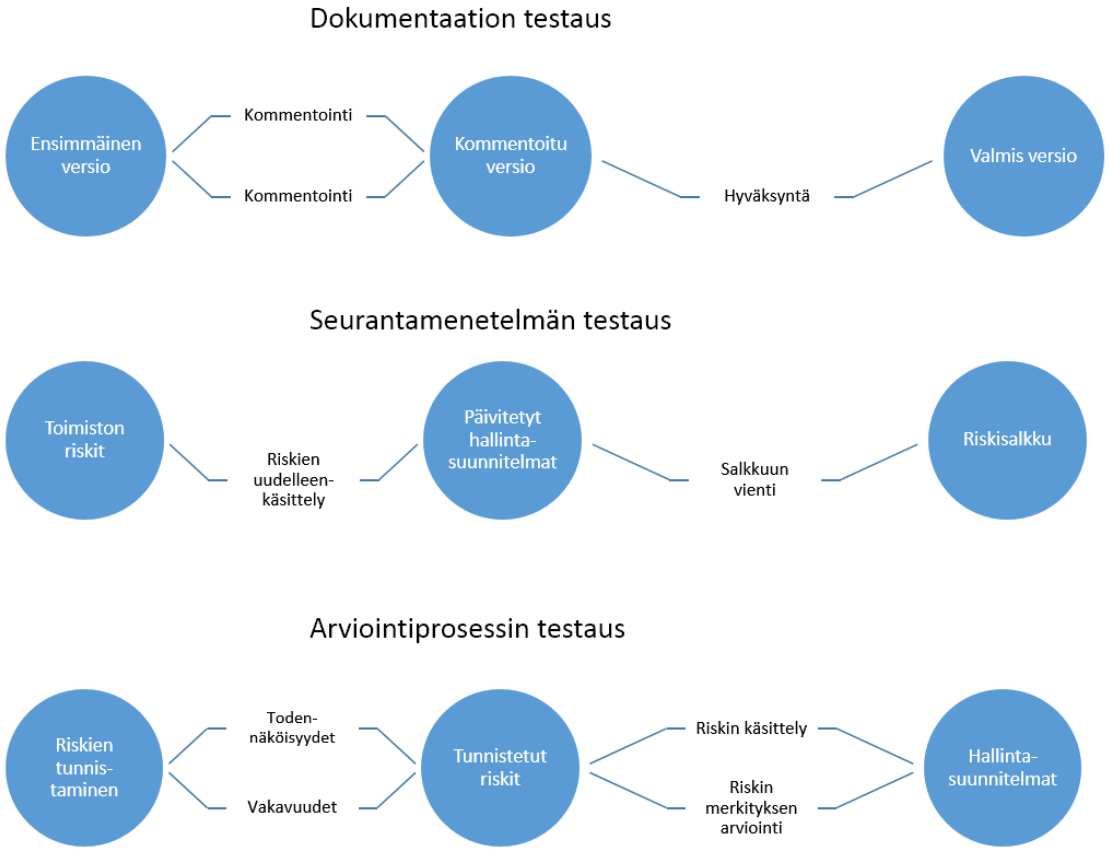
Tietohallintotoimiston riskienhallintamalli luotiin edellisissä vaiheissa tehtyjen analyysien perusteella. Riskienhallintamalli pohjautui vahvasti teoriataustaan huomioiden toimiston tarpeet ja nykytilan riskienhallinnassa. Malli koostuu riskienhallinnan periaatteista, riskienhallinnan puitteiden kuvauksesta, riskienhallinnan prosessikuvaksesta ja riskienhallinnan käsikirjasta. Lisäksi kehitettiin riskianalyysin työkaluja, riskienseurannan työkaluja ja riskienhallinnan koulutusmateriaalia. Kehitetty ja testattu malli on esitelty luvussa 3.4 ja liitteissä 3,4,5, 6, 7, 8, 9 ja 10.

3.2.3 Hallintamallin testaus

Kehitetyn konstruktion testi on konstruktiivisen tutkimuksen tärkeimmistä piirteistä, konstruktion testaus testaa samalla tutkimusprosessin toimivuutta. Jos innovoitu konstruktio läpäisee testin, on mielekästä arvioida sen toimivuutta muissa organisaatioissa. Vaikka testi epäonnistuisi, on hyvä arvioida kuinka epäonnistumiset voidaan välttää muissa organisaatioissa. Toimivuuden arviointi perustuu määrittelyvaiheessa luotuihin odotuksiin. Mitä yksityiskohtaisempi tavoitetilan kuvaus on, sitä paremmin voidaan arvioida onko se toteutettavissa ja millaiset ovat hyödyt ja muut sivuvaikutukset (Järvinen & Järvinen 2004, 113; Lukka 2001.)

Riskienhallintamallin testaus

Riskienhallintamallia testattiin dokumentaation osalta kommenttikierrosten ja hyväksyntöjen kautta tietohallintotoimiston johtoryhmällä sekä testaamalla riskianalyysityökalua tekemällä riskianalyysi Active Directory -tietojärjestelmälle sekä seurantatyökaluja käsittelemällä tietohallintotoimiston tunnistettuja riskejä. Testausprosessi on havainnollistettu seuraavassa kuviossa (kuvio 42).



Kuvio 42 Riskienhallintamallin testaus

Dokumentaatio testattiin kommentoinnin kautta. Tietohallintotoimiston johtoryhmä käsitteli dokumentaatiot osana toimiston johtoryhmän kehityspäiviä. Dokumentit käsiteltiin ensin johtoryhmän jäsenten suoralla kommentoinnilla ja sen jälkeen yhteisellä kommentointilaisuudessa helmikuussa ja maaliskuussa 2015. Dokumentit hyväksyttiin maaliskuussa 2015.

Riskienhallintamallin seurantamenetelmää testattiin käsittelemällä uudelleen tietohallintotoimiston aikaisemman mallin mukaisesti tunnistetut ja käsitellyt riskit. Riskit ja erityisesti niiden hallintasuunnitelmat käsiteltiin uuden riskienhallintamallin mukaisesti. Päivitetyt hallintasuunnitelmat ja riskit vietiin seurantaa varten kehitettyyn riskisalkkuun. Päivitetyistä hallintasuunnitelmista ja näihin liittyvistä vastuista tiedotettiin mallin mukaisesti. Riskisalk-

ku käsiteltiin tietohallintotoimiston johtoryhmän kokouksessa huhtikuussa 2015 ja asetettiin suunnitelmien mukaiseen seurantaan.

Riskienarviointiprosessi testattiin arvioimalla Active Directory –tietojärjestelmän riskit kolmessa työpajassa huhtikuussa 2015. Työpajat pidettiin yhdessä tietohallintotoimiston asiantuntijoiden ja palveluntarjoajan edustajien kanssa. Työpajoissa testattiin riskienhallintakäsikirjan, koulutusmateriaalin sekä riskienarviointityökalujen toimivuus. Ensimmäinen työpaja aloitettiin lyhyellä koulutuksella riskienhallintaan ja keskityttiin riskien tunnistamiseen. Toisessa työpajassa arvioitiin riskien todennäköisyydet ja vakavuudet. Kolmannessa työpajassa arvioitiin riskien merkitykset ja käsiteltiin merkitykselliset riskit muodostamalla niille hallintasuunnitelmat. Lopuksi hallintasuunnitelmat vietiin koko toimiston riskisalkkuun ja asetettiin hallintamallin mukaiseen seurantaan.

Mallin toimivuuden arviointi

Tutkimuksen lopussa analysoidaan teoreettinen kontribuutio. Tämä on tutkimuksen kannalta väistämätön ja ratkaiseva vaihe. Tutkijan on osoitettava teoreettinen kontribuutio joko reflektoimalla konstruktiota teoriataustaan ja osoittamalla sen uutuus tai analysoimalla riippuvuussuhteita tutkimusprosessissa. (Lukka 2001.) Järvinen ja Järvisen (2004, 115) mukaan uuden innovaation tieteellinen meriitti vaatii rakentamisprosessin kuvauksen yksityiskohtaisesti, perustella valinnat ja päätökset. Ratkaisun alkuperäisyys ja paremmuus muihin tunnettuihin ratkaisuihin nähden tulee myös osoittaa.

Tietohallintotoimiston riskienhallintamallin toimivuutta arvioitiin testauksen jälkeen. Arviointi tehtiin asetettuihin tavoitteisiin nähden. Arvioinnissa vertailtiin kehitetyn dokumentaation sisältöä ja sen kommentointia ennen hyväksyntää. Seurantamenetelmän arviointi tehtiin vertailemalla aikaisemmin tunnistettuja riskejä ja niiden seurantaa uuden menetelmän mukaiseen seurantaan. Arvioinnissa myös huomioidaan johtoryhmän kommentit seurannasta. Arviointiprosessia arvioidaan vertaamalla aikaisempaan menetelmään ja uuden mallin mukaiseen menetelmään. Toimivuuden arvioinnin tulokset on esitelty tämän raportin luvussa 3.4.5 ja tutkimuksen johtopäätökset luvussa 4.1.

Käyttöönoton hahmotelma

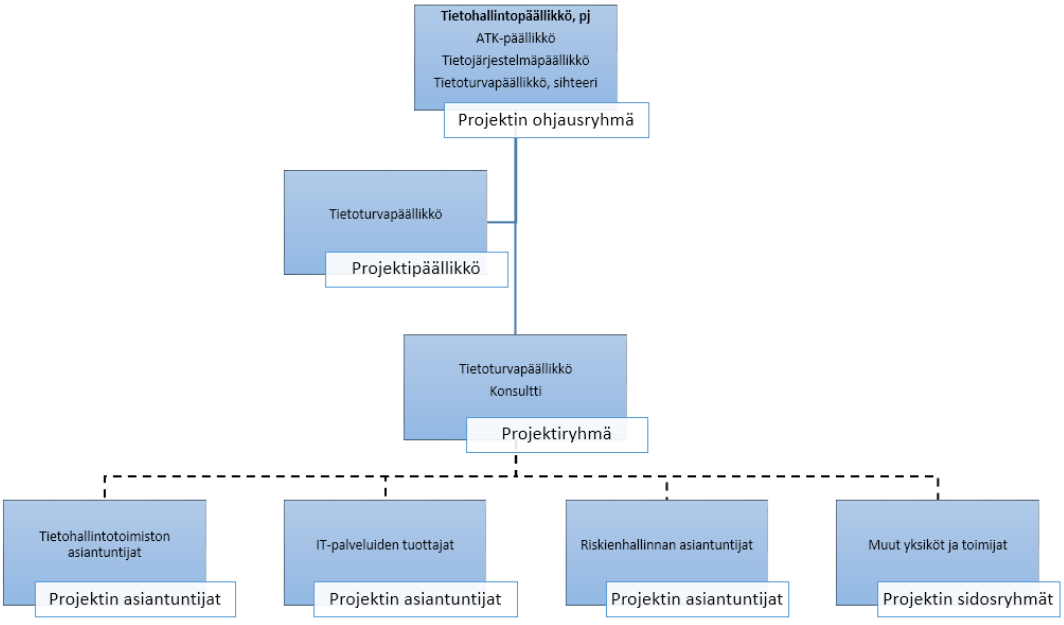
Riskienhallintamallin käyttöönoton hahmotelma toteutettiin osana riskienhallinnan käsikirjaa ja sen liitteenä olevaa vuosisuunnitelmaa ja vuosikelloa. Nämä on esitelty liitteessä 7 riskienhallinnan käsikirja. Lisäksi käyttöönottoa hahmotellaan luvussa 4.3.

3.3 Kehitystyön toteutus

Kehitystyö toteutettiin tietohallintotoimiston sisäisenä kehitysprojektina, jonka avulla toteutettiin toimintatapojen kehitys. Projektin toteutuksessa noudatettiin tietohallintotoimiston projektimallia. Kehitystyö toteutettiin kolmessa vaiheessa, jonka rinnalla tehtiin opinnäytetyön tutkimustyön raportointia jatkuvana työnä kehitystyön edetessä. Projekti toteutettiin loppuvuoden 2014 ja kevään 2015 aikana.

3.3.1 Kehitystyön organisointi

Kehitystyön projektin omistajana oli tietohallintotoimisto ja sen toimistopäällikkö toimiva tietohallintopäällikkö. Ohjausryhmänä toimi tietohallintotoimiston johtoryhmä, jolle raportoitiin projektin edistymisestä ja joka toimi ylimpänä päätöksentekijänä projektissa. Kehitystyön projektin projektipäällikkönä toimi tietoturvapäällikkö. Projektin toteutuksesta vastasi tietoturvapäällikkö, jonka käytettävissä oli tarpeen mukaan ulkopuolinen konsultti. Projektiryhmän ulkopuolisina asiantuntijoina olivat tietohallintotoimiston asiantuntijat ja suunnittelijat sekä IT-palveluita tuottavat palvelutalojen asiantuntijat ja muiden organisaatioiden riskienhallinnan asiantuntijat. Projektin sidosryhminä toimivat eduskunnan kanslian muut yksiköt ja muut toimijat. Alla oleva kuvio (kuvio 43) kuvaa kehitystyön organisointia.



Kuvio 43 Kehitystyön projektiorganisaatio

Kehitystyö toteutettiin pääosin tietohallintotoimiston sisäisenä virkatyönä. Ulkopuolista konsulttia käytettiin tukemaan ja kommentoimaan kehitystyötä.

3.3.2 Kehitystyön vaiheet ja aikataulut

Kehitystyö jaettiin kolmeen vaiheeseen: nykytilan arviointi, hallintamallin suunnittelu ja luonti sekä hallintamallin testaus. Opinnäytetyön raportointia tehtiin koko kehitystyön ajan. Kehitystyön projektin vaiheiden sisältö on kuvattu luvussa 3.2. Kehitystyön tulokset raportoitiin opinnäytteenä tehtävän työelämän kehittämistehtävän raportissa osana tätä dokumenttia. Aikataulullisesti projekti toteutettiin syksy 2014 – kesä 2015 aikavälillä.

3.3.3 Kehitystyön ohjaus

Kehitystyön edistymistä seurattiin tietohallintotoimiston projektimallin mukaisesti. Projektipäällikkö toimitti edistymisraportit ohjausryhmän käyttöön, jossa ne käsiteltiin. Projektissa oli 4 ohjauspistettä mukaan lukien aloitus- ja lopetuskokoukset. Edistymisraporteissa esiteltiin tehtävien edistyminen, taloudellinen edistyminen ja kustannus käyttö. Ohjausryhmä käsitteli myös muutosehdotukset. Opinnäytetyötä ohjattiin omilla ohjaustapaamisilla projektin rinnalla.

3.4 Tutkimuksen tulokset

Tämä luku esittelee tutkimuksen tulokset vaiheittain. Tulokset vastaavat tutkimuskysymyksiin. Tutkimuskysymykset ja niihin vastaavat tulokset on esitetty seuraavassa taulukossa (taulukko 26).

Taulukko 26 Tutkimuksen tulokset

Tutkimuskysymys	Tulos
Millaisella mallilla eduskunnan tietohallintotoimiston tulisi hallita sen toimintaa liittyviä riskejä?	Tutkimuksen tuloksena kehitettiin kolmitasoinen malli, joka määrittelee riskienhallinnan toiminnan tietohallintotoimistossa. Luvun 3.4.2 aliluku tietohallintotoimiston riskienhallinnan viitekehys ja sitä seuraavat aliluvut esittelevät sisällön tarkemmin.
Mitä riskienhallinnan tarpeita eduskunnan tietohallintotoimistolla on?	Tutkimuksen tuloksena ovat johtoryhmän haastattelut sekä haastatteluiden ja nykytilan analyysin perusteella tehty tarvekooste. Tulokset on esitelty luvussa 3.4.1 tietohallintotoimiston riskienhallinnan nykytilan arviointi ja luvun 3.4.2 aliluvussa Analyysi tietohallintotoimiston tarpeista riskienhallinnalle.
Miten eduskunnan tietohallintotoimisto tunnistaa, analysoi ja priorisoi riskejään?	Tutkimuksen tuloksena ovat riskienhallinnan käsikirja ja riskiarviointityökalu. Tulokset on esitelty luvun 3.4.2 aliluvuissa riskienhallinnan käsikirja ja riskienhallinnan työkalu.

Tulokset on jaoteltu nykytilan arvioon ja tarvekartoitukseen, kehitettyyn tietohallintotoimiston riskienhallinnan malliin sekä tuotetun mallin testauksen tulokset. Kaikki tulokset on esitelty tämän luvun aliluvuissa.

3.4.1 Tietohallintotoimiston riskienhallinnan nykytilan arviointi

Nykytilan arviossa analysoitiin eduskunnan kanslian käytössä olevaa riskienhallintaa teoriataustaan nähden. Tietohallintotoimiston tarpeet riskienhallinnalle kartoitettiin haastattelemalla toimiston johtoryhmän jäsenet. Yleisten mallien arviointi tehtiin luomalla kerätystä tiedosta synteesi.

Riskienhallinnan nykytilan arvio

Nykytilan arviointi tehtiin analysoimalla sitä teoriataustasta johdettuun synteesiin purkamalla se vastaaviin osiin ja analysoimalla niiden toteutumista. Analyysin lopputuloksena ovat johtopäätökset nykytilan soveltuvuudesta riskienhallinnan toteuttamiseksi tietohallintotoimistossa. Nykyinen riskienhallintamalli on kuvattu luottamuksellisessa liitteessä 12. Nykyisen riskienhallintamallin analyysi on esitetty seuraavassa taulukossa (taulukko 27).

Taulukko 27 Nykyisen riskienhallinnan analyysi

Riskienhallinnan tekijä	Nykytilan toteutus	Johtopäätös
Riskienhallinnan motivaatio - Tavoitteiden saavuttaminen - Epävarmuustekijöiden tunnistaminen ja vaikutusten pienentäminen - Vaatimustenmukaisuus	Riskienhallintaa on käsitelty eduskunnan kanslian johtoryhmässä ja tilintarkastuksen yhteydessä. Riskienhallinnan kautta halutaan tunnistaa ja hallita paremmin operatiivisia riskejä. Vaatimuksenmukaisuustavoitteet näkyvissä sisäisten vaatimusten kautta.	Nykytilassa on olemassa motivaatio riskienhallinnalle. Johtoryhmä on valtuuttanut riskienhallinnan kehittämistyön ja käyttöönoton. Yksikkötason riskienhallinnan motivaatio riskienhallinnalle ei vielä ilmeistä, todennäköisesti vaatii riskikulttuurin kehittymistä.
Riskienhallinnan kehittäminen ja sen hyödyt. - Riskinottokyky - Johdon keskeinen rooli - Organisaation toiminnan tehostaminen - Yhtenäiset toimintatavat	Johdolle raportoidaan vuosittain riskienhallinnasta Kehitetty yhtenäinen malli riskien tunnistamiseen ja hallintakeinojen listaamiseen.	Eduskunnan kanslian riskienottokyky ei ole selkeästi tunnistettavissa nykymallista. Johdon sitoutuminen tulee esille mallin käynnistämisen yhteydessä ja vuosittaisessa raportoinnissa. Organisaation toiminnan tehostamisesta ei voida vielä tehdä johtopäätöksiä. Yhtenäistetyt toimintatavat

		riskien tunnistamiseen olemassa. Näiden laajentaminen muuhun toimintaan ei ole todennettavissa
Riskienhallinnan toteutustapa - Toistuva, mitattava määrämuotoinen - Ennakoiva toimintamalli - Tunnistaa, analysoi, hallitsee ja seuraa riskejä - Raportoi toiminnastaan organisaatiossa ja sidosryhmille - Kehittyvä malli mukautuu organisaation muutoksiin - Huomioi myös mahdollisuudet	Nykytilassa määritelty toistuvuus kerran vuoteen ja arvioinneissa käytettävät uhka- sekä vakavuusluokat. Nykytilassa tunnistetaan ja analysoidaan riskejä. Riskeistä raportoidaan turvallisuus yksikölle, joka koostaa ne yhteiseksi raportiksi.	Riskienhallinnalle ei ole määritelty mittareita tai muita vastuullisia toimistoittain. Määrämuotoisuus kattaa vain riskientunnistamisen keinot. Nykytilassa ei ole huomioitu riskienhallintatoimenpiteiden seurantaa. Raportointimalli ei kata organisaation laajuista tiedottamista. Raportointi on lähinnä yksisuuntaista. Nykytilassa ei ole määritelty kehitystä eikä organisaation mahdollisuuksien tunnistamista. Operatiivisten riskien osalta mahdollisuuksien tunnistaminen on myös vaikea toteuttaa.
Riskienhallinnan käyttöönotto - Huomioi organisaatiokulttuurin - Määritellyt tavoitteet ja aikataulu - Integrointi osaksi muita prosesseja - Kehitysvastuu määriteltävä - Riskienhallinnan toteutusvastuut ja päätöksenteko määriteltävä	Nykytila huomioi organisaation aloittamalla riskienhallinnan kevyellä mallilla. Tavoitteena operatiivisten riskien tunnistaminen ja aikatauluna vuosittainen tapahtuma. Integrointi määritelty osaksi toiminnan suunnittelua. Kehitysvastuita ei määritelty. Toteutus- ja päätöksentekovastuu määritelty yksiköille	Käyttöönotossa on huomioitu riskienhallinnan kypsyystason riskienhallinnalle. Malli ei kuitenkaan tarjoa kehitysaskeleita riskienhallinnan tai kulttuurin kehittämiselle. Käyttöönoton tavoitteet varsin yleisluontoiset, mutta huomioiden kulttuurin, eivät käytännön tavoitteet ole vielä selvillä. Taustoituksessa olisi voinut määritellä riskienhallinnan toteuttamisen motivaatiot. Integrointi osaksi nykyisiä toimintatapoja on suppea. Yleiseen malliin on hankala luoda yksikkötason integrointia. Esimerkkejä integraatiosta olisi syytä antaa. Selkeä kehitysvastuu puuttuu nykyisestä toimintamallista. Vastuut toteutuksesta ja päätöksenteosta hyvin yleisellä tasolla, ei anna selkei-

		tä vaatimuksia miten tulisi toteuttaa.
Riskienhallinnan onnistumiskriteerit - Sitoutuminen - Riskienhallintakulttuurin luonti - Organisaation kypsyyden huomiointi - Tapahtumien tunnistaminen - Oikein suhteutetut hallintakeinot	Organisaatio sitoutuminen johdon tasolla selkeää. Riskienhallintakulttuuri ei vielä olemassa. Organisaation kypsyys huomioitu aloittamalla riskienhallinta kevyellä mallilla. Tapahtumien tunnistamista ei ohjeistettu. Hallintakeinojen suhteuttaminen ohjattu riskikartan avulla.	Johdon sitoutuminen on olemassa jolloin siltä osin riskienhallinnan käyttöönotolle on hyvät olosuhteet. Yksiköiden sitoutuminen toimintaan on epäselvää ja yksiköiden omalla vastuulla. Varsinaista mallia sitoutumisen varmistamiseksi ei ole. Riskienhallintakulttuurin luomiseksi ei ole määritelty keinoja kuten tietoiskuja seminaareja tai koulutuksia. Organisaation kypsyys on huomioitu, joka auttaa käyttöönotossa. Kehitysaskeleet kuitenkin epäselviä kun organisaation kypsyys kasvaa riskienhallinnan toteutuksen kautta. Tapahtumien tunnistamiseen tarvitaan apukeinoja, nykyinen malli ei välttämättä kattava vaikka uhkaluokat on määritelty. Hallintakeinojen suhteuttaminen esimerkiksi kriittisten järjestelmien osalta ei toteudu nykyisellä mallilla. Keinot voivat olla liian keveitä tai järeitä.

Yhteenvetona voidaan todeta, että vaikka nykyinen malli luo pohjan riskienhallinnan käynnistämiselle eduskunnan kansliassa, ei se ole kuitenkaan riittävän kattava teoriataustaan nähden. Nykyisellä mallilla on pystytty tunnistamaan riskejä sekä muodostamaan näille hallintatoimenpiteitä. Hallintakeinoille ei kuitenkaan määritellä aikatauluja eikä seurantaa. Hallintatoimien riittävyydestä ja vaikuttavuudesta ei saada riittävää kuvaa nykymallilla.

Riskienhallinnan kokonaistoimivuudelle ei ole määritelty seurantakeinoja nykymallissa. Täten ei ole tietoa siitä, onko se riittävällä tasolla. Mallilla ei ole myöskään määritelty kehitysvastuuta. Organisaation toiminnan muuttuessa ja riskienhallinnan kyvykkyyden kasvaessa, tulisi mallin mukautua tehokkaampaan toimintaan. Integraatio nykyiseen toimintaan ei tule riittävästi esille nykymallissa. Ilman selkeätä integraatiota normaaliin toimintaan

riskienhallinta saattaa muuttua irralliseksi toiminnaksi, jolla ei ole omistajaa ja se voi jäädä jopa tekemättä.

Nykymallista voidaan hyödyntää uhkaluokkia, riskien vaikutusten luokitusta sekä todennäköisyyksien luokituksia. Lisäksi riskien suuruuden määrittelemää riskikarttaa voidaan hyödyntää jatkossa. Uuden mallin käytössä näitä ominaisuuksia on syytä hyödyntää, jotta säilytettäisiin yhteensopivuus kanslian muiden yksiköiden ja toimintojen riskienarvioinnin kanssa.

Tietohallintotoimiston tarpeet riskienhallinnalle

Tietohallintotoimiston tarpeet riskienhallinnalle kartoitettiin haastattelemalla toimiston johtoryhmä. Haastatteluissa kartoitettiin tietohallintotoimiston johtoryhmän näkemyksiä riskienhallinnan nykytilasta ja tarpeista riskienhallinnalle. Johtoryhmä on riskienhallinnassa avainasemassa. Johtoryhmä toimii esimiesasemassa henkilöstölle ja omalla sitoutumisellaan antaa viestin riskienhallinnan tärkeydestä. Haastateltavina olivat tietohallintopäällikkö, tietojärjestelmäpäällikkö ja ATK-päällikkö.

Haastattelut toteutettiin yksilöhaastatteluina käyttämällä teemoja. Haastattelun teemoja olivat

- riskienhallinnan nykytila
- riskienhallinnan tavoitetila
- riskienhallinnan raportointitarpeet
- riskienhallinnan reagointipisteet
- tietohallinnon riskienhallinnan erityispiirteet
- muut riskienhallinnan tarpeet.

Haastattelun teemat on tarkemmin kuvattu liitteessä 1 haastatteluteemat.

Haastatteluista tehtiin muistiinpanot ja näistä muodostettiin yhteenveto. Yhteenvetoon lisättiin tietohallintotoimistolle asetetut tavoitteet tietohallintolinjauksista. Nämä analysoitiin ja tuloksista tehtiin johtopäätökset riskienhallinnan kehittämistarpeista. Yhteenveto haastatteluista ja johtopäätökset on esitetty seuraavassa taulukossa (taulukko 28). Haastattelut on kokonaisuudessaan esitetty liitteessä 2 yhteenvetotaulukko tietohallintotoimiston haastatteluista.

Taulukko 28 Yhteenveto tietohallintotoimiston johtoryhmän haastatteluista

Teema	Yhteenveto	Johtopäätökset
Nykytila	Toimittajariippuvuutta liikaa Kattavuus puutteellista, riskienhallinta ei ole määrämuo-	Nykyinen riskienhallinta ei toimi kattavasti ja toimissa on liikaa vaihtelua

	toista tekemistä Ajanpuute aiheuttaa vain reaktiivista toimintaa Riskien hallinta jää tekemättä	tai niiden toteuttamisesta puuttuu yhtenäinen oma arviointimalli.
Tavoitetila	Prosessi riskien hallinnalle eli riskienhallinnan malli Kattavuus palvelutuotannon ja projektinhallinnan riskejä koskien Proaktiivisuutta mallien avulla	Riskienhallinnan periaatteet on luotava. Riskien arviointiprosessi on kuvattava.
Raportointi	Säännöllisyyttä lisättävä (vuosikellomainen käsittely) Vertailukelpoisuus eri riskien välisesti riskiluokkien sisällä (kriittisyydet)	Riskienhallintaan vaaditaan yhtenäinen säännöllinen raportointimalli, joka perustuu riskienhallinnan periaatteisiin.
Reagointipisteet	Proaktiivisuutta korostettava Malli ja vertailukelpoisuuden mahdollistavat mittarit/taulukot Monitoimittajuuteen liittyvien riskien tunnistaminen	Riskienarviointiprosessiin on luotava reagointia helpottamaan case-tyyppisiä esimerkkejä tyypillisimmistä riskeistä ja niiden merkityksestä (todennäköisyys ja vaikutus).
Tietohallinnon erityispiirteet	Riskienhallinnan yhteinen ja yhtenäinen malli Palveluiden riskienhallinnan malli huomioi koko talon	Riskienhallinta on toteutettava yhtenäisten riskienhallinnan periaatteiden mukaan. Tietohallinnossa otetaan käyttöön ja sovelletaan koko organisaatioon vaikuttavia yhtenäisiä periaatteita. Tietojärjestelmien hankintaan ja niihin liittyvissä projekteissa riskejä on arvioitava laajemmin kuin vain tietohallinnon riskeinä.
Muut riskienhallinnan tarpeet	Projektien riskienhallinnan kattavuus Eduskunnan erityispiirteet yhteiskunnassa (mm. julkisuusnäkökulma)	Projektinhallintaan on laadittava riskienhallintaa varten yhtenäinen malli. Järjestelmätoimittajien riskienhallintamallit eivät yksistään riitä eduskunnan tarpeisiin.

Yhteenvetona voidaan todeta, että nykyinen riskienhallintamalli koetaan teoreettisena eikä se ole luonteva osa normaalia toimintaa. Riskienhallintaa tehdään, mutta se ei ole määrämuotoista tai riittävän kattavaa. Riskeihin pääasiassa reagoidaan ja tehdään korjaavia ja selvitystöitä ennakoinnin sijaan. Odotuksena riskienhallinnalle on määrämuotoinen tapa

tunnistaa ja käsitellä riskejä ennakoivasti. Riskienhallintaan halutaan toimintamalli ja sitä tukevat työkalut. Riskienhallinta pitäisi olla osa toimiston kaikkia palveluita.

Yleisten riskienhallintamallien arviointi

Yleisiin riskienhallintamalleihin arvioitiin teoriataustan tiedot ja muodostettiin näitä synteesi. Synteesi on esitelty tämän raportin luvussa 2.8 yhteenveto riskienhallinnasta.

3.4.2 Tietohallinnon riskienhallintamallin luonti

Tietohallintotoimiston riskienhallinta malli perustui nykytilan arvion ja tarvekartoitukseen sekä teoriataustaan. Näiden perusteella muodostettiin, suunniteltiin ja luotiin tietohallintotoimiston riskienhallinnan malli.

Analyysi tietohallintotoimiston tarpeista riskienhallinnalle

Riskienhallinnan nykytilaa ja tarpeita verrattiin teoriataustan teemoihin riskienhallinnan toteutuksesta. Näistä tehtiin analyysin pohjalta johtopäätökset joista johdetaan kehityksen toimenpiteet. Analyysin tulokset on esitetty seuraavassa taulukossa (taulukko 29).

Taulukko 29 Riskienhallinnan tarpeiden analyysi

Teoriataustan teema	Nykytila	Tarvekartoitus	Johtopäätös
Riskienhallinnan motivaatio	Ylimmän johdon motivaatio on olemassa	Motivaatio on olemassa tietohallintotoimiston johtoryhmässä	Tarvittava motivaatio löytyy riskienhallinnan kehitykselle ja toteuttamiselle
Kehittäminen ja hyödyt	Voidaan hyödyntää osia nykyisestä mallista	Riskienhallintaa halutaan hyödyntää osana toimiston palveluita ja johtamista.	Riskienhallintaa pitää kehittää systemaattisempaan suuntaan, jotta sitä voitaisiin käyttää halutulla tavalla.
Toteutustapa	Nykytila ei riittävän kattava eikä täytä yleisesti asetettuja tavoitteita	Riskienhallinnalla on pystyttävä ennakoivasti parantamaan toimistojen palveluiden toimintavarmuutta. Riskejä on pystyttävä ennakoimaan.	Riskienhallinta on tuotava osaksi normaalia toimintaa toimistossa. Toiminnalle on luotava selkeä malli, työkalut ja ohjeet sekä tuettava henkilöstöä toteutuksessa.
Käyttöönotto	Nykytila antanut pohjan riskienhallinnalle, mutta jatkokehitystä ei ole määritelty. Käyttöönotolle on	Riskienhallinnassa on huomioitava tietojärjestelmien kriittisyys koko eduskunnan toiminnalle. Riskienhallinnassa	Suunnitellussa mallissa on huomioitava sidosryhmät sekä pystyttävä reagoimaan kriittisiin järjestelmiin. Samalla on kuitenkin säilytet-

	luotu mahdollisuus.	on huomioitava toimiston tuotantotapa ja saatava toimittajat mukaan riskienhallintaan.	tävä yhteensopivuus kanslian muiden yksiköiden riskienhallintaan. Käyttöönotossa on sitoutettava henkilöstö ja toimittajat mukaan hallintamalliin ja tapoihin.
Onnistumiskriteerit	Onnistumiskriteerit löytyvät sitoutumisessa. Organisaation kypsyys on huomioitu kevyellä aloituksella	Johdon tahtotila on olemassa, asiantuntijat tekevät jo omissa tehtävissään riskienhallintaa. Integrointi osaksi toimintaprosesseja on saatava aikaiseksi	Riskienhallinnalle on määriteltävä tahtotila ja vastuut. Riskienhallinnan toteuttamista on tuettava koulutuksilla ja toimivilla työkaluilla. Riskienhallinnalle on luotava sitä tukeva toimintakulttuuri

Riskienhallintamallin kehityksessä on edellisten tulosten perusteella huomioitava seuraavat seikat:

- Riskienhallinta on toteutettava yhtenäisten riskienhallinnan periaatteiden mukaan.
- Riskienhallinnan kokonaisprosessi on kuvattava ja määriteltävä riskienhallinnan puitteet.
- Riskienarviointiprosessi on kuvattava nykyistä tarkemmin.
- Riskienarviointia varten on laadittava tarkemmat ohjeet ja työkalut.
- Ohjeissa olisi luotava arviointia helpottamaan esimerkkejä tyypillisimmistä riskeistä ja niiden merkityksestä.
- Riskienhallintaan tarvitaan yhtenäinen, säännöllinen raportointimalli, joka perustuu riskienhallinnan periaatteisiin.
- Raportoinnin on katettava toimiston kaikki riskit.
- Riskienhallinnan toimintaa on arvioitava säännöllisesti.
- Riskienhallinnalle on määriteltävä toteutus-, seuranta- ja kehitysvastuut.
- Riskienhallinnan on katettava koko toimiston toiminta.
- Riskienhallintaa on koulutettava säännöllisesti koko toimiston henkilöstölle.
- Riskienhallintamallin on oltava yhteensopiva koko eduskunnan kanslian riskienhallintamallin kanssa.

Toimenpiteet riskienhallinnan kehittämiselle

Tarpeiden analyysin ja nykytilan arvion sekä teoriataustan perusteella voidaan päätellä seuraavat toimenpiteet tarpeiden täyttämiseksi. Riskien hallinnan kehittämistoimien pääkohdat eduskunnan tietohallintotoimistossa ovat

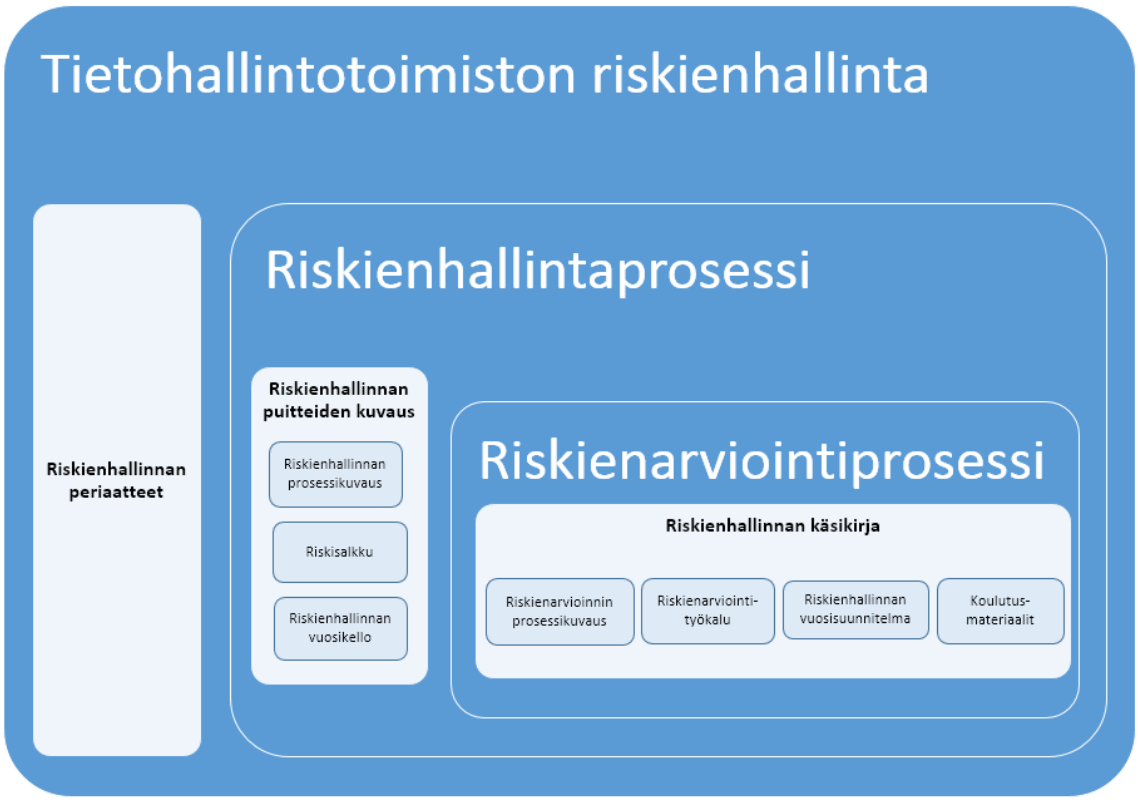
- tietohallintotoimiston riskienhallinnan viitekehyksen luominen
- riskienhallinnan periaatteiden kuvaaminen
- riskienhallinnan puitteiden kuvaaminen
- riskienhallinnan prosessin kuvaaminen

- riskienarvioinnin työkalujen kehittäminen ja ohjeistus sekä koulutusmateriaalin luonti
- riskienhallintamallin testaaminen
- riskienhallintamallin toimivuuden arviointi.

Riskienhallinnan nykyisestä menettelystä voidaan ottaa käyttöön riskienarviointia tukevat uhkaluokat, todennäköisyysasteikko, vakavuusasteikko ja riskien merkityksen arviointia tukeva riskikartta.

Tietohallintotoimiston riskienhallinnan viitekehys

Tietohallintotoimiston viitekehys koostuu useista käsitteistä, dokumenteista ja työkaluista. Käsitteitä ovat tietohallinnon riskienhallinta, riskienhallintaprosessi ja riskienarviointiprosessi. Dokumentteja ovat riskienhallinnan periaatteet, riskienhallinnan puitekuvaus ja riskienhallinnan käsikirja. Työkaluja ovat riskienhallinnan prosessikuvaus, riskisalkku, riskienhallinnan vuosikello, riskienarvioinnin prosessikuvaus, riskienarviointityökalu, riskienhallinnan vuosisuunnitelma ja koulutusmateriaalit. Näiden suhde toisiinsa on kuvattu seuraavassa kuviossa (kuvio 44).



Kuvio 44 Tietohallintotoimiston riskienhallinnan viitekehys

Tietohallintotoimiston riskienhallinta kattaa kaiken riskienhallintatoiminnon toimistossa. Keskeisin dokumentti, jossa määritellään riskienhallinnan sisältö ja tahtotila, on riskinhallinnan periaatteet. Riskienhallintaprosessi sisältää riskienhallinnan puitekuvauksen, joka kuvaa kokonaisprosessin ja sen ylläpidon. Työkaluina tällä tasolla on riskisalkku, jonka

avulla riskienhallinnan kokonaiskuvaa seurataan sekä riskienhallinnan vuosikello, joka määrittelee toistuvat tapahtumat riskienhallinnassa. Samalla tasolla on myös riskienhallinnan prosessikuvaus, joka visualisoi prosessin toiminnan.

Riskienarviointiprosessi kuvaa kuinka riskienarviointeja tehdään tietohallintotoimistossa. Riskienhallinnan käsikirja kuvaa menetelmät riskienarviointien tekemiselle ja riskien seurannalle. Työkaluina tällä tasolla ovat riskienarvioinnin työkalu, koulutusmateriaalit sekä riskienhallinnan vuosisuunnitelma, joka määrittelee tarkemmalla tasolla mitä toimenpiteitä kuluvalla vuodella tulee riskienhallinnassa tehdä. Tällä tasolla on myös riskienarvioinnin prosessikuvaus. Dokumenttien ja työkalujen sisältö on kuvattu seuraavissa aliluvuissa.

Riskienhallinnan periaatteet

Tietohallintotoimiston riskienhallinnan periaatteet -dokumentti kuvaa riskienhallinnan tahtotilaa sekä määrittelee korkealla tasolla riskienhallinnan linjauksen. Periaatteet-dokumentti on tämän raportin liitteenä, Liite 3 Eduskunnan tietohallintotoimiston riskienhallinnan periaatteet.

Periaatteet luotiin ohjaamaan riskienhallintaa toimistossa. Periaatteiden avulla toimiston johto sitoutuu riskienhallintaprosessiin ja velvoittaa muun henkilöstön noudattamaan riskienhallinnan määrittelemiä toimintatapoja. Seuraavassa taulukossa (taulukko 30) on kuvattu periaatteiden sisältö tiivistetysti. Samassa taulukossa tehdään kytkentä teoriataustaan, nykytilan arvioon ja tarpeisiin.

Taulukko 30 Riskienhallinnan periaatteiden sisältö ja kytkökset teoriaan, nykytilan ja toimiston tarpeisiin

Sisältö	Kuvaus	Teoriatausta viittaukset	Nykytila	Tarpeet
Johdanto ja riskienhallinnan tavoitteet	Määrittelee riskienhallinnan tehtävän ennaltaehkäisevänä toimintana.	Kirjallisuuskatsaus riskienhallinnan prosessi luku 2.3.2 ja riskienhallinnan kehittäminen luku 2.3.6 COSO ERM sisäinen ympäristö luku 2.4.2, ISO 31000 riskienhallinnan periaatteet ja puitteet luvut 2.5.2 ja 2.5.3.	Vastaa tarpeeseen yksiköiden sitoutumisen varmistamisesta.	Vastaa määrämuotoisuuden ja sitoutumisen tavoitetta. Määrittelee riskienhallinnan ennakoivaksi
Riskienhallin-	Velvoittaa mal-	Kirjallisuuskat-	Vastaa tarpee-	Vastaa tarpee-

nan periaatteet	lin noudattamiseen. Määrittelee riskienhallinnan osaksi normaalia toimintaa ja koskee kaikkea toimiston toimintaa.	saus riskienhallinnan kehittäminen luku 2.3.6 COSO ERM sisäinen ympäristö luku 2.4.2 ISO 31000 riskienhallinnan periaatteet 2.5.3. Haastattelut palveluntarjoaja luku 2.7.1, valtiohallinnon palvelutuottaja luku 2.7.2, valtion virasto luku 2.7.3 ja huoltovarmuuskriittinen organisaatio luku 2.7.4	seen määrämuotisesta toiminnasta ja sen periaatteista.	seen määrämuotisesta toiminnasta ja sen periaatteista.
Riskienhallinnan roolit ja vastuut	Kuvaa prosessin roolit ja vastuut	Kirjallisuuskatsaus riskienhallinnan kehittäminen luku 2.3.6 sekä riskienhallinnan käyttöönotto luku 2.3.7 COSO tieto ja viestintä luku 2.4.8 sekä roolit ja vastuut luku 2.4.10 ISO 31000 riskienhallinnan puitteet luku 2.5.3. VAHTI riskien arvioinnin merkitys ja organisointi luku 2.6.2. Haastattelut valtiohallinnon palvelutuottaja luku 2.7.2 ja huoltovarmuuskriittinen	Vastaa tarpeeseen selkeistä vastuista ja rooleista	Vastaa tarpeeseen selkeistä vastuista ja rooleista

		organisaatio luku 2.7.4		
Riskienhallinnan toteutusprosessi	Kuvaus toteutusprosessista sekä riskinsietokyvystä	Kirjallisuuskatsaus riskienhallinta prosessina luku 2.3.2 ja riskien arviointi luku 2.3.3 COSO Sisäinen ympäristö luku 2.4.2, tavoitteenasettelu luku 2.4.3, tapahtumien tunnistaminen 2.4.4 riskien arviointi 2.4.5 ja riskeihin vastaaminen 2.4.6. ISO 31000 riskienhallinnan puitteet luku 2.5.3 ja riskienhallintaprosessi luku 2.5.4. VAHTI Riskien arvioinnin merkitys ja organisointi luku 2.6.2. Haastattelut palveluntarjoaja luku 2.7.1 ja valtiohallinnon palvelutuottaja luku 2.7.2	Vastaa tarpeeseen laajentaa riskienhallintaa koko toimintaan sekä määrittelee riskienottokyvyn.	Vastaa tarpeeseen kattavasta riskienhallinnasta ja määrämuotoisesta toiminnasta sekä määrittelee arviointiprosessin
Ohjeet ja koulutus	Määrittele miten koulutetaan riskienhallintaa	Kirjallisuuskatsaus riskienhallinnan käyttöönotto 2.3.7 COSO tieto ja viestintä luku 2.4.8. ISO 31000 puitteet luku 2.5.3 ja riskienhallintaprosessi luku 2.5.4. Haastattelut huoltovar-	Vastaa tarpeeseen riskienhallintakulttuurin luomiselle	Vastaa tarpeeseen yhdenmukaisesta riskienhallintamallista

		muuskriittinen organisaatio luku 2.7.4		
Riskienhallinnan periaatteiden ja prosessin toimivuuden seuranta ja valvonta	Kuvaa säännöllinen tarkastellun periaatteet mallin toimivuudesta.	Kirjallisuuskatsaus riskienhallinta prosessina luku 2.3.2 ja riskienhallinnan käyttöönotto 2.3.7 sekä riskienhallinnan tason arviointi luku 2.3.8. COSO valvontatoimenpiteet luku 2.4.7 ja seuranta luku 2.4.9. ISO 31000 puitteet luku 2.5.3. Haastattelut palveluntarjoaja luku 2.7.1, valtiohallinnon palvelutuottaja luku 2.7.2, valtion virasto luku 2.7.3 ja huoltovarmuuskriittinen organisaatio luku 2.7.4.	Vastaa tarpeeseen kehityksen organisoinnista ja mallin toimivuuden arvioinnista.	Vastaa tarpeeseen yhtenäisestä mallista riskienhallinnalle.
Tiedottaminen	Määrittelee tiedottamistarpeen riskienhallintamallista	Kirjallisuuskatsaus riskienhallinta prosessina luku 2.3.2 ja riskien raportointi luku 2.3.5 sekä riskienhallinnan käyttöönotto luku 2.3.7. COSO tieto ja viestintä luku 2.4.8. ISO 31000 puitteet luku 2.5.3 ja riskienhallintaprosessi luku 2.5.4. Haastattelut	Vastaa tarpeeseen riskienhallintakulttuurin luomiselle.	Vastaa tarpeeseen yhdenmukaisesta riskienhallintamallista

		palveluntarjoaja luku 2.7.1, valtiohallinnon palvelutuottaja luku 2.7.2 ja valtion virasto luku 2.7.3		
Riskienhallinnan käsitteet	Riskienhallinnan yhteinen sanasto	Kirjallisuuskatsaus riskienhallinnan käyttöönotto luku 2.3.7. COSO tieto ja viestintä luku 2.4.8. ISO 31000 puitteet luku 2.5.3 ja riskienhallintaprosessi luku 2.5.4.	Vastaa tarpeeseen riskienhallintakulttuurin luomiselle.	Vastaa tarpeeseen yhdenmukaisesta riskienhallintamallista

Riskienhallinnan puitteet

Tietohallintotoimiston riskienhallinnan puitteet –dokumentti kuvaa riskienhallinnan kokonaistoteutusmallin tietohallintotoimistossa. Dokumentti kuvaa miten riskienhallinta on toteutettu tietohallintotoimistossa ja mitkä tekijät siihen vaikuttavat. Riskienhallinnan puitteet -dokumentti on tämän raportin liitteenä, Liite 4 Eduskunnan tietohallintotoimiston riskienhallinnan puitteet. Puitteiden kuvauksella huolehditaan siitä, että toiminta on määrämuotoista ja käytettävä ajantasainen. Puitteet kuvaavat miten riskienhallintaa johdetaan tietohallintotoimistossa. Seuraava taulukko (taulukko 31) kuvaa periaatteiden sisällön tiivistetysti ja esittää kytkökset teoriataustaan, nykytilan arvioon ja toimiston tarpeisiin.

Taulukko 31 Riskienhallinnan puitekuvaus ja kytkennät teoriaan, nykytilan ja toimiston tarpeisiin

Sisältö	Kuvaus	Teoriatausta viittaukset	Nykytila	Tarpeet
Johdanto, valtuudet ja sitoutuminen	Kuvaus riskienhallinnan kytkennästä kokonaisuuteen ja johdon valtuutuksesta ja sitoutumisesta	Kirjallisuuskatsaus riskienhallinnan kehittäminen luku 2.3.6 ja riskienhallinnan käyttöönotto luku 2.3.7 COSO sisäinen ympäristö luku 2.4.2.	Vastaa kehitysvastuun ja muiden vastuiden tarkempaan vaatimukseen. Määrittelee yksikkötasolla sitoutumisen.	Määrittelee yhtenäistä toimintamallia

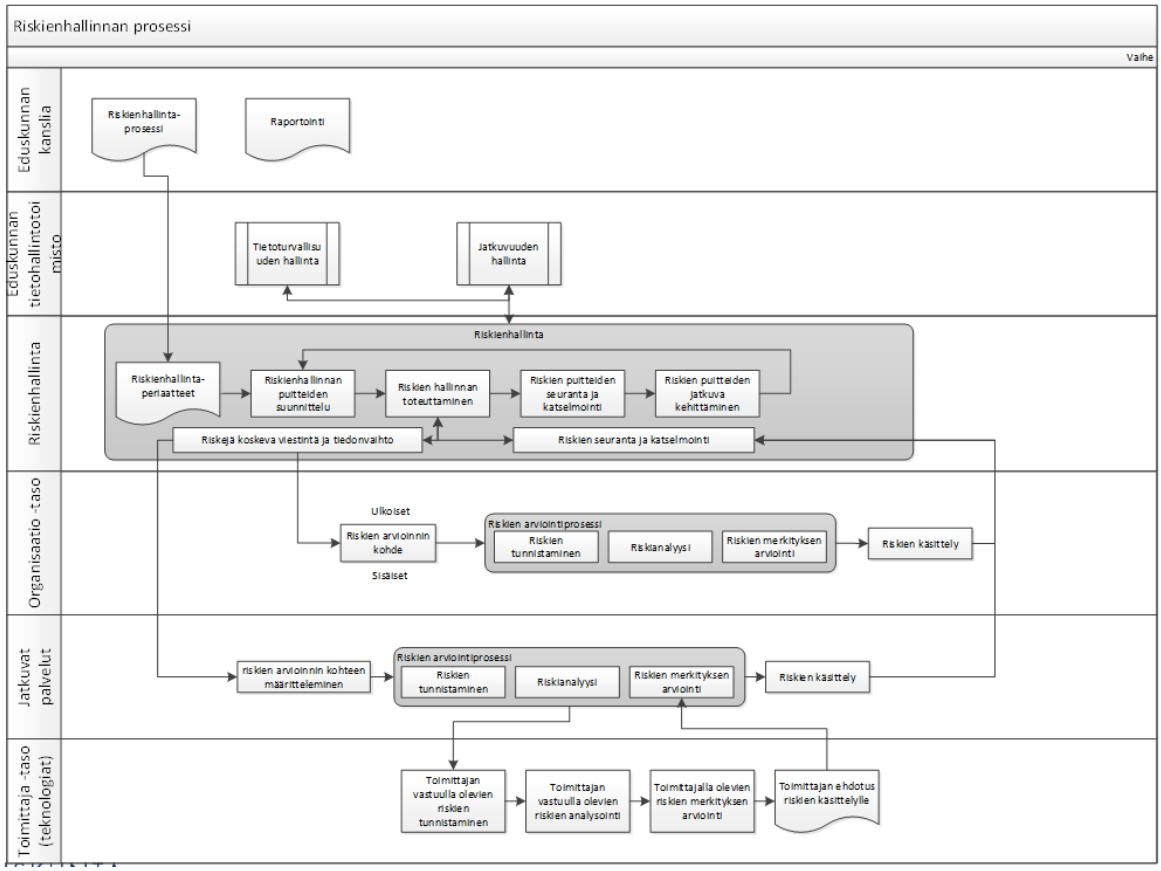
		ISO 31000 puitteet luku 2.5.3. VAHTI riskien arvioinnin merkitys ja organisointi luku 2.6.2. Haastattelut valtiohallinnon palvelutuottaja luku 2.7.2 ja huoltovarmuuskriittinen organisaatio luku 2.7.4.		
Puitteiden suunnittelu	Määrittelee toimiston toimintaympäristön, periaatteet, vastuut ja velvollisuudet, riskienhallinnan toteuttamisen ja viestinnän.	Kirjallisuuskatsaus riskienhallinta prosessina luku 2.3.2, riskienhallinnan kehittäminen luku 2.3.6 ja riskienhallinnan käyttöönotto luku 2.3.7. COSO sisäinen ympäristö luku 2.4.2, tapahtumien tunnistaminen luku 2.4.4, riskien arviointi luku 2.4.5, valvontatoimenpiteet luku 2.4.7, tieto ja viestintä luku 2.4.8, roolit ja vastuut luku 2.4.10. ISO 31000 puitteet luku 2.5.3 ja riskienhallintaprosessi luku 2.5.4. VAHTI riskien arvioinnin merkitys ja organisointi luku 2.6.2.	Vastaa tarpeisiin riskienhallinnan seurannasta ja kokonaisvaltaisuudesta. Integroi riskienhallintaa muuhun toimintaan.	Määrittelee yhtenäisen toimintatavan riskienhallinnalle.
Riskienhallintapuitteiden ja	Puitteiden toteutuksen sito-	Kirjallisuuskatsaus riskienhal-	Vastaa tarpeeseen laajentaa	Määrittelee määrämuotoista

riskienhallinta-prosessin toteuttaminen	minen periaatteisiin ja vuosikelloon. Prosessin toteuttamisen sitominen käsikirjaan	linta prosessina luku 2.3.2. COSO sisäinen ympäristö luku 2.4.2, tapahtumien tunnistaminen luku 2.4.4, valvontatoimenpiteet 2.4.7, tieto ja viestintä luku 2.4.8 ja roolit ja vastuut luku 2.4.10. ISO 31000 puitteet luku 2.5.3 ja riskienhallintaprosessi luku 2.5.4. Haastattelut valtiohallinnon palvelutuottaja luku 2.7.2, valtion virasto luku 2.7.3	riskienhallinnan kattavuutta.	toimintaa.
Riskienhallinnan puitteiden katselmointi ja mittarit	Määrittelee puitteiden katselmointitavat ja riskienhallinnan toimivuuden mittarit.	Kirjallisuuskatsaus riskienhallinta prosessina luku 2.3.2 ja riskienhallinnan tason arviointi luku 2.3.8. COSO seuranta luku 2.4.9. ISO 31000 puitteet luku 2.5.3. Haastattelut eduskunnan palveluntarjoaja luku 2.7.1, valtionhallinnon palvelutuottaja luku 2.7.2, valtion virasto luku 2.7.3, huoltovarmuuskriittinen organisaatio luku 2.7.4	Vastaa tarpeeseen toimivuuden arvioinnista ja mittareista.	Vastaa tarpeeseen yhtenäisestä toimintamallista ja riskienhallinnan laajuuden kasvattamisesta.
Riskienhallinnan puitteiden kehittäminen	Määrittelee vastuut riskienhallinnan kehittä-	Kirjallisuuskatsaus riskienhallinnan kehittä-	Vastaa tarpeeseen kehitysvastuista.	Vastaa tarpeeseen yhtenäisestä toiminta-

	misestä.	minen luku 2.3.6 ja riskienhallinnan käyttöönotto 2.3.7 COSO roolit ja vastuut luku 2.4.10. ISO 31000 puitteet luku 2.5.3. VAHTI riskien arvioinnin merkitys ja organisointi 2.6.2. Haastattelut valtionhallinnon palveluntarjoaja luku 2.7.2		mallista.

Riskienhallinnan prosessikuvaus

Riskienhallinnan puitekuvauksen kanssa samalla tasolla on kuvattu riskienhallinnan kokonaisprosessi. Prosessikuvaus visualisoi miten riskienhallinnan kokonaisprosessi toimii tietohallintotoimistossa. Prosessi on kuvattu seuraavassa kuviossa (kuvio 45). Prosessi löytyy myös tämän raportin liitteestä, liite 10 Riskienhallinnan kokonaisprosessi. Prosessin vaiheiden tekstikuvaukset ovat osa puitekuvausta ja riskienhallinnan käsikirjaa, liitteet 4 ja 7.



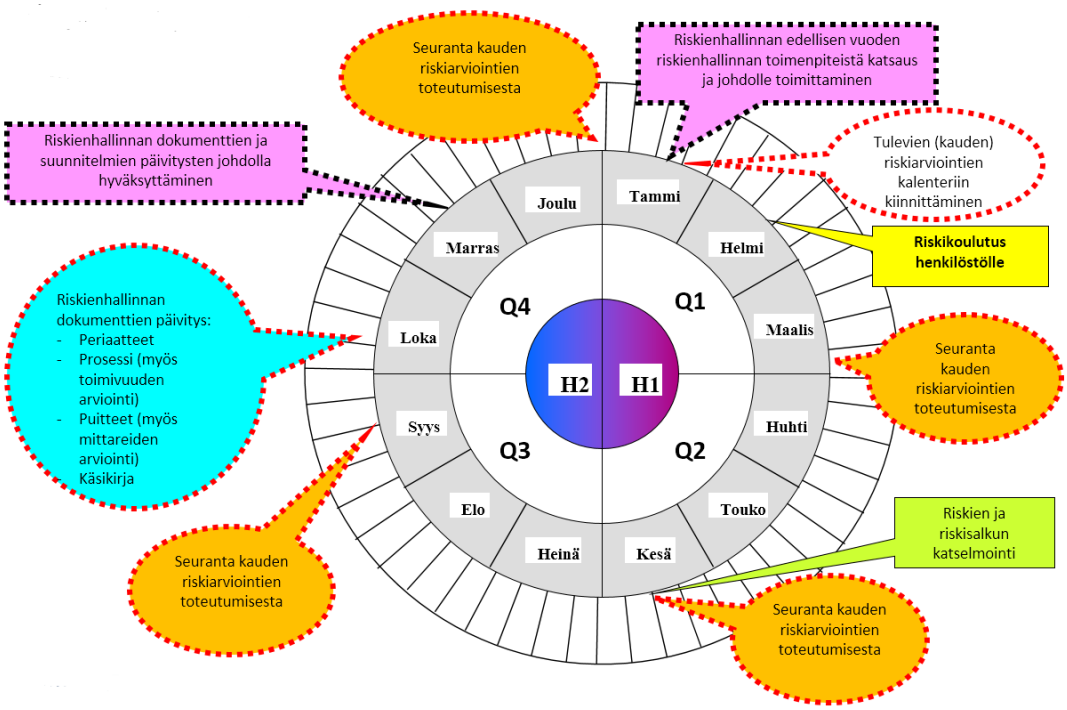
Kuvio 45 Eduskunnan tietohallintotoimiston kokonaisriskienhallintaprosessi

Riskisalkku

Riskisalkku toimii koko toimiston riskiseurannan välineenä. Riskisalkkuun kerätään kaikki toimiston riskit suuruusjärjestyksessä. Seurannan tavoitteena ja tehtävänä on varmistaa, että riskeille suunnitellut toimenpiteet toteutuvat sovitulla tavalla. Seurantaa tehdään toimiston johtoryhmässä neljännesvuosittain. Johtoryhmä päättää toimenpiteistä joita riskisalkun perusteella tehdään. Salkkuun kirjataan riski, todennäköisyys, vaikutus, kriittisyys, riskin suuruus, tavoiteaikataulu hallintatoimille, vastuuhenkilö, toimenpiteiden status ja uhkaluokka. Riskisalkun malli on tämän raportin liitteenä, liite 9 riskisalkku.

Riskienhallinnan vuosikello

Riskienhallinnan vuosikello määrittelee miten kokonaisprosessi ylläpidetään ja miten riskienhallinnan toimivuutta seurataan. Vuosikellossa määritellään johtoryhmän tekemän toimenpideseurannan ajankohdat, riskiarviointien sopimisajankohta, koulutusajankohta, riskien ja salkun katselmointiajankohta, dokumenttien päivitysajankohta, dokumenttien hyväksyntäajankohta sekä vuosiraportin ajankohdan. Seuraavassa kuviossa (kuvio 46) on esitetty riskienhallinnan vuosikello. Vuosikello on tämän raportin liitteenä, liite 11 riskienhallinnan vuosikello.



Kuvio 46 Riskienhallinnan vuosikello

Riskienhallinnan käsikirja

Riskienhallinnan käsikirja kuvaa tietohallintotoimiston riskienhallinnan prosessiin liittyvät käytännön toimet. Käsikirjaan on liitetty useita apuvälineitä riskienarviointien ja käsittelyn tueksi sekä seurantaan ja koulutukseen liittyvää materiaalia. Riskienhallinnan käsikirja on tämän raportin liitteenä, liite 7 riskienhallinnan käsikirja.

Seuraava taulukko (taulukko 32) kuvaa käsikirjan sisällön tiivistetysti ja esittää kytkökset teoriataustaan, nykytilan arvioon ja toimiston tarpeisiin.

Taulukko 32 Riskienhallinnan käsikirja ja kytkennät teoriaan, nykytilan ja toimiston tarpeisiin

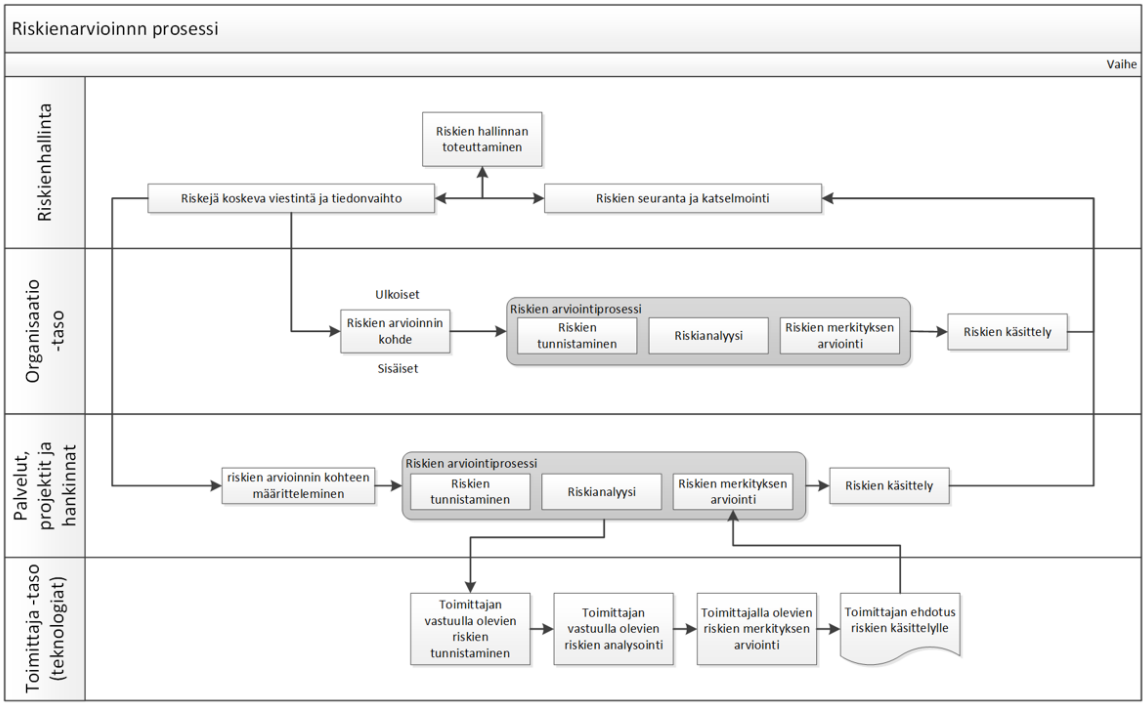
Sisältö	Kuvaus	Teoriatausta viittaukset	Nykytila	Tarpeet
Johdanto, riskienhallinta- ja arviointiprosessi	Esittelee käsikirjan sisällön, riskienhallinnan viitekehyksen ja riskienarvioinnin toteutuksen ja vastuut	Kirjallisuuskatsaus riskienhallinta prosessina luku 2.3.2, riskienhallinnan kehittäminen luku 2.3.6 ja riskienhallinnan käyttöönotto 2.3.7	Vastaa tarpeeseen laajentaa riskienhallintaa	Vastaa tarpeeseen määrämuotoisesta, kattavasta riskienhallinnasta.

		COSO riskien arviointi luku 2.4.5 ja roolit ja vastuut luku 2.4.10. ISO 31000 puitteet luku 2.5.3. VAHTI riskien arvioinnin merkitys ja organisointi luku 2.6.2 Haastattelut valtiohallinnon palvelutuottaja luku 2.7.2 ja huoltovarmuuskriittinen organisaatio luku 2.7.4		
Riskien arviointi ja liitteet 1, 4,5,6,7 ja 8 liite 1 riskienhallinnan RACI-taulukko liite 4 riskien käsittelyn esimerkkejä ja hyviä käytäntöjä liite 5 uhkaluokat liite 6 riskien vaikutusluokat liite 7 todennäköisyyksien luokitus liite 8 riskikartta	Esittelee miten riskien arviointi tehdään tietohallintotoimistossa	Kirjallisuuskatsaus riskien arviointi luku 2.3.3 ja riskienhallintakeinot luku 2.3.4. COSO tapahtumien tunnistaminen luku 2.4.4, riskien arviointi luku 2.4.5 ja riskeihin vastaaminen luku 2.4.6. ISO 31000 riskienhallintaprosessi luku 2.5.4. VAHTI riskien arvioinnin merkitys ja organisointi luku 2.6.2, uhkien määrittely ja tunnistaminen luku 2.6.3, riskien suuruuden arviointi luku 2.6.4, toimenpiteiden priorisointi ja määrittely luku 2.6.5.	Nykytilasta käytetään uhkaluokkia, vaikuttavuusluokkia ja todennäköisyysluokkia sekä riskikarttaa yhteensopivuuden säilyttämiseksi kanslian muuhun riskienhallintaan nähden. Tarkentaa toimenpiteitä mitä tehdään itse riskien arvioinnissa. Vastaa myös tarpeeseen tapahtumien tunnistamisen apukeinoista.	Kuvaa arviointiprosessin, antaa apuvälineitä kuten case-esimerkkejä riskeistä. Määrittelee yhtenäisen riskienarviointimallin.
Riskien hallinta,	Määrittelee mal-	Kirjallisuuskat-	Vastaa tarpee-	Määrittelee

seuranta, katselmointi ja viestintä	lin riskien seurannalle ja arviointien katselmoinnille sekä periaatteet viestinnälle ja tiedonvaihdolle.	saus riskienhallinta prosessina luku 2.3.2, riskien raportointi luku 2.3.5 COSO valvontatoimenpiteet luku 2.4.7, tieto & viestintä luku 2.4.8 ja seuranta luku 2.4.9. ISO 31000 puitteet luku 2.5.3 ja riskienhallintaprosessi luku 2.5.4. VAHTI jatkokehitys- ja seurantasuunnitelmat luku 2.6.6. Haastattelut eduskunnan palveluntarjoaja luku 2.7.2, valtionhallinnon palveluntuottaja luku 2.7.2, valtion virasto luku 2.7.3 ja huoltovarmuuskriittinen organisaatio luku 2.7.4.	seen riskienhallintatoimenpiteiden seurantaan sekä raportoinnista organisaation laajuudelta	määrämuotoisen toiminnan. Määrittelee yhtenäisen säännöllisen raportointimallin, joka perustuu riskienhallinnan periaatteisiin
Riskienhallinnan vuosikello ja riskienhallinnan toimenpiteet ja liitteet 2 ja 3 liite 2 riskienhallinnan vuosikello liite 3 riskienhallinnan toimenpiteet	Määrittelee toimenpiteiden syklit ja tapahtuma-ajat sekä tarkentaa vuosittaiset tapahtumat	Kirjallisuuskatsaus riskienhallinta prosessina luku 2.3.2, riskien raportointi luku 2.3.5 COSO seuranta luku 2.4.9. ISO 31000 puitteet luku 2.5.3 ja riskienhallintaprosessi luku 2.5.4. Haastattelut valtionhallinnon palveluntarjoaja luku 2.7.2.	Vastaa tarpeeseen integroida riskienhallina osaksi toimiston muuta toimintaa ja säännöllisen seurannan	Määrittelee säännöllisen riskienhallintamallin

Riskienarviointiprosessi

Tällä tasolla kuvataan myös riskienarviointiprosessi. Riskienarviointiprosessi kuvaa miten riskienarviointiprosessit tietohallintotoimistossa tehdään. Prosessin vaiheet on kuvattu riskikäsikirjassa. Seuraava kuvio (kuvio 47) kuvaa riskienarviointiprosessia.



Kuvio 47 Riskienarviointiprosessi

Riskienarvioinnin työkalu

Riskienarvioinnin työkalu yhtenäistää riskienarviointiprosessia tietohallintotoimistossa. Arvioinnin lisäksi se toimii seurannan ja katselmointien apuna sekä kerää historiatietoa riskeistä. Jokaisesta arvioitavasta kohteesta täytetään oma arviointityökalu. Työkalu on tämän raportin liitteenä, liite 8 riskienarviointityökalu. Työkalu käyttöohjeet on kuvattu riskienhallinnan käsikirjassa.

Riskienarviointityökaluun täytetään esitiedot sivulle arvioitava kohde, määritellään kohteen toimintaympäristö, arvioitavan kohteen riippuvuudet muulle toiminnalle ja riippuvuudet muusta toiminnasta, kohteen kriittisyys toiminnalle sekä käytetäänkö riskiasteikkoa sellaisenaan vai vaatiiko se soveltamista. Tässä vaiheessa voidaan hyödyntää periaatteissa kuvattua toimintaympäristöä sekä käsikirjan liitteenä olevaa riskikarttaa.

Riskien arviointi tehdään aktiiviset riskit välilehdelle, jolle kuvataan riskit ja niiden syyt, arvioidaan todennäköisyydet ja vakavuudet. Työkalu laskee automaattisesti riskien kriittisyysarvon ja päättelee riskin suuruuden. Kriittisyysarvo ei kerro suoraan riskin suuruutta,

sen avulla voidaan erottaa toisistaan saman suuruusluokan riskit toisistaan. Riskin suuruus määräytyy riskikartan avulla työkalussa automaattisesti kolmeen luokkaan: korkeat riskit, kohtalaiset riskit tai matalat riskit. Riskin suuruus määrittelee jatkokäsittelyn tarpeen, yleislinjaus on määritelty riskienhallinnan periaatteissa, korkeat ja kohtalaiset riskit otetaan käsittelyyn aina. Myös matalat riskit otetaan käsittelyyn, jos ne liittyvät arvioitavan kohteen kriittisiin riippuvuuksiin tai arvioitava kohde on kokonaisuudessaan kriittinen eduskunnan toiminnalle.

Aktiiviset riskit välilehdelle kuvataan riskienhallintasuunnitelma eli riskin hallintaan liittyvät toimenpiteet ja tavoitetila. Samalle kuvataan riskin omistaja eli toimenpiteiden seurannasta vastaava henkilöä ja toimenpiteiden aikataulu sekä tarkistuspiste. Myös uhkaluokka merkitään työkaluun seurantaa varten. Aktiiviset riskit välilehteä käytetään riskin toimenpiteiden seurantaan sekä katselmointiin. Tältä välilehdeltä siirretään myös tiedot kokonaisseurantaa varten toimiston riskisalkkuun.

Historiatietoihin siirretään jokaisen muutoksen jälkeen tiedot arviointivälilehdeltä ja päivitetään seurantakaaviot vastaamaan tilannetta. Näitä tietoja käytetään arvioitaessa riskien toimenpiteiden vaikutuksia ja toteutumista riskienhallinnan mittauksen osana.

Riskienhallinnan vuosisuunnitelma

Riskienhallinnan vuosisuunnitelman avulla ajoitetaan riskienhallinnan vuosittaiset. Riskienhallinnan vuosikello määrittelee tapahtumien ajankohdat, vuosisuunnitelma taas määrittelee toimenpidetasolla mitä kunakin vuonna tehdään. Kaikkia toimenpiteitä ei tehdä joka vuosi, toimenpiteet on jaoteltu parittomille ja parillisille vuosille seuraavan taulukon mukaisesti (taulukko 33).

Taulukko 33 Toimenpiteiden jakautuminen vuosille

	Parittomina vuosina	Parillisina vuosina
Riskienhallinnan periaatteet - Muutostarpeiden arviointi - Muutosehdotusten laatiminen - Johdolla hyväksyttäminen	X	X
Riskienhallinnan periaatteet - Johdon/avainhenkilöiden haastattelut	X	
Riskienhallinnan puitteet - Prosessin toimivuus - Prosessin päivittäminen - Mittariston päivittäminen	X	X

- Johdolla hyväksyttäminen		
Riskienhallinnan käsikirja - Dokumentin ja vuosikellon päivittäminen - Esimerkkien arviointi ja päivittäminen - Johdolla hyväksyttäminen	X	X
Riskienhallinnan koulutus koko eduskunnan tietohallintotoimiston henkilöstölle		X
Riskienhallinnan tietoiskut henkilöstölle	X	
Riskiarviointien toteutus - Kohteiden valinta - Vuosikelloon päivittäminen - Seuranta ja katselmointi	X	X
Riskisalkun seuranta - Riskisalkun läpikäynti johtoryhmässä - Huom! Tämä tehdään neljännesvuosittain.	X	X

Vuosisuunnitelmassa taas määritellään tarkemmalla tasolla miten toimenpiteitä tehdään.

Vuosisuunnitelman tyhjä esimerkki on kuvattu seuraavassa taulukossa (taulukko 34).

Taulukko 34 Riskienhallinnan vuosisuunnitelmaesimerkki

	Toteutuksesta vastaa	Toteutusajankohta	Toteutukseen osallistujat
Riskienhallinnan periaatteet - Muutostarpeiden arviointi - Muutosehdotusten laatiminen - Johdolla hyväksyttäminen			
Riskienhallinnan periaatteet - Johdon/avainhenkilöiden haastattelut			
Riskienhallinnan puitteet - Prosessin toimivuus - Prosessin päivittäminen - Mittariston päivittäminen - Johdolla hyväksyttäminen			
Riskienhallinnan käsikirja - Dokumentin ja vuosikellon päivittäminen - Esimerkkien arviointi ja päivittäminen - Johdolla hyväksyttäminen			

Riskienhallinnan koulutus koko eduskunnan tietohallintotoimiston henkilöstölle				
Riskienhallinnan tietoiskut henkilöstölle				
Riskiarviointien toteutus - Kohteiden valinta - Vuosikelloon päivittäminen - Seuranta ja katselmointi	**Arviointikohde:**			
Riskisalkun seuranta - Riskisalkun läpikäynti johtoryhmässä - Huom! Tämä tehdään neljännesvuosittain.				

Riskienhallinnan koulutusmateriaalit

Riskienhallinnan koulutus on keskeinen osa toimintamalliin sitouttamista. Riskienhallintaa varten on luotu oma koulutusmateriaali. Koulutusmateriaali on tämän raportin liitteenä, liite 6 riskienhallinnan koulutusmateriaali.

3.4.3 Riskienhallintamallin testaus

Riskienhallintamallia testattiin tietohallintotoimistossa kolmella keinolla. Dokumentaatio testattiin käsittelemällä ja hyväksymällä ne tietohallintotoimiston johtoryhmässä. Riskisalkun ja seurannan toimivuutta testattiin käsittelemällä tietohallintotoimiston tunnistetut riskit uuden mallin mukaisesti ja lisäämällä käsitellyt riskit riskisalkkuun sekä hyväksymällä ne tietohallintotoimiston johtoryhmässä. Riskien arviointiprosessia testattiin tekemällä Active Directory tietojärjestelmästä riskien arviointi ja käsittelemällä tunnistetut riskit kehitetyillä työkaluilla. Lopuksi riskit lisättiin seurantaan riskisalkkuun. Seuraavissa luvuissa on esitelty testauksen tulokset.

Dokumenttien testaus

Dokumentaation pohjatyöt luotiin yksilötyönä. Tämän jälkeen ne käytiin läpi työpajatyöskentelynä konsultin kanssa viimeistellen ne johtoryhmän kommentointiin. Kun dokumentit oli saatu valmiiksi johtoryhmän kommentointiin, tiedotettiin niistä toimiston johtoryhmän jäsenille. Johtoryhmän jäsenet kävivät läpi dokumentit yksilötyönä ja valmistelivat kommenttinsa. Dokumentit ja niihin liittyvät kommentit käytiin läpi johtoryhmän kehityspäivinä. Kehityspäivien yhteydessä hyväksyttiin muokattuina kommenttien perusteella. Hyväksy-

misen jälkeen ne julkaistiin intranetissa ja tiedotettiin toimistokokouksissa sekä sähköpostilla henkilöstölle. Hyväksytyt dokumentit myös jaeltiin sidosryhmille soveltuvin osin. Dokumenttien hyväksymisaikataulut on kuvattu seuraavassa taulukossa (taulukko 35).

Taulukko 35 Dokumentaation testaus

Dokumentti	Liite	Ensimmäinen versio	Kommentointi	Hyväksyntä
Riskienhallinnan periaatteet	Liite 3	13.2.2015	13.2.-24.3.2015	24.3.2015
Riskienhallinnan prosessi	Liite 10	27.2.2015	27.2.-24.3.2015	24.3.2015
Riskienhallinnan puitekuvaus	Liite 4	13.2.2015	13.2.-24.3.2015	24.3.2015
Riskienhallinnan vastuutaulukko	Liite 5	13.2.205	13.2.-24.3.2015	24.3.2015
Riskienhallinnan käsikirja	Liite 7	1.4.2015	1.4.-14.4.2015	14.4.2015
Riskienhallinnan vuosikello	Liite 11	1.4.2015	1.4.-14.4.2015	14.4.2015

Tietohallintotoimiston johtoryhmä hyväksyi kaikki dokumentit ylläkuvatussa aikataulussa. Tästä johtuen katsotaan dokumenttien läpäisseen testauksen ja saaneen hyväksynnän. Hyväksytyt dokumentit ovat tämän raportin liitteenä.

Riskienarvioinnin työkalu, riskisalkku ja koulutusmateriaalit kehitettiin samalla menetelmällä kuin dokumentaatio. Näitten testaus tehtiin käyttämällä työkaluja käytännössä. Seuraavissa luvuissa on kuvattu näitten testaus.

Riskisalkun testaus

Riskisalkkua varten käsiteltiin tietohallintotoimiston aikaisemmin tunnistetut riskit uudelleen. Käsittelyssä käytettiin työkaluina riskienarvioinnin työkalua sekä riskisalkkua. Testaus tehtiin riskienhallinnan käsikirjan avulla.

Ensimmäisessä vaiheessa aikaisemmista riskikuvauksista purettiin esille konkreettinen riski ja syy riskiin. Samalla tarkistettiin pitääkö alkuperäinen riski sisällään useita riskejä. Riskien määrä pysyi tarkastuksesta huolimatta samana. Tässä vaiheessa myös tunnistettiin syy riskiin ja kirjattiin se ylös arviointityökaluun. Myös uhkaluokat tarkistettiin, niiden vaihtamiseen ei ollut tarvetta. Toisessa vaiheessa tarkastettiin riskien arvioinnin tulokset vaikuttavuuden ja todennäköisyyden osalta. Näihin ei tehty muutoksia käsittelyssä. Riskien kriittisyydet ja suuruudet pysyivät arvioissa samoina.

Kolmannessa vaiheessa määriteltiin riskien perusteella hallinnalle tavoitetila ja hallintatoimenpiteet, joilla tavoitteeseen päästään. Nämä tarkentuivat selkeästi edellisistä arvioista

parantuneen arviointitietojen vuoksi. Hallintatoimenpiteiden määrittelyn jälkeen tarkennettiin vastuuhenkilöt ja toimenpiteiden aikataulut. Vastuut määriteltiin henkilötasolle niissä riskeissä, joissa ne olivat olleet ryhmillä ja aikataulut tarkennettiin päivämäärätasolle.

Viimeisessä riskityökalun täyttövaiheessa tarkistettiin toimenpiteiden statustiedot vastuuhenkilöiltä. Statustiedot eivät olleet muuttuneet edellisen tarkistuskerran jälkeen. Tämän jälkeen päivitettiin historiatiedot ajantasaiseksi seurantaa varten ja siirrettiin riskit riskisalkkuun. Riskisalkkuun siirrettiin

- riskitunniste
- riskin kuvaus
- todennäköisyys
- vaikutus
- riskin kriittisyys
- riskin suuruus
- vastuuhenkilö
- toimenpiteiden tavoiteaikataulu
- toimenpiteiden statustieto.

Riskityökalua käytti ja siirron riskisalkkuun teki tietoturvapäällikkö yhdessä ATK-päällikön, tietojärjestelmäpäällikön ja tietohallintopäällikön kanssa. Lopputuloksen katselmoi ja hyväksyi tietohallintotoimiston johtoryhmä 14.4.2015. Salkku voidaan katsoa toimivaksi työkaluksi, koska se saavutti johtoryhmän hyväksynnän ja otettiin tuotantokäyttöön.

Alkuperäinen riskiarvio on tämän raportin liitteenä, luottamuksellinen liite 13 tietohallintotoimiston nykyiset riskit. Tietohallintotoimiston käsitellyt riskit ovat tämän raportin liitteenä, luottamuksellinen liite 14 tietohallintotoimiston käsitellyt riskit. Tietohallintotoimiston riskisalkku on tämän raportin liitteenä, luottamuksellinen liite 16

Riskienarvioinnin testaus

Riskienarviointiprosessi testattiin tekemällä keskeiseen tietojärjestelmään Active Directory –hakemistopalveluun riskienarviointi. Testaus tehtiin kolmessa työpajassa riskienhallintakäsikirjan avulla. Työpajoihin osallistuivat tietoturvapäällikkö, sovellustiimin projektipäällikkö ja perustietotekniikkatiimin projektipäällikkö. Käyttöpalvelutoimittajan edustajina olivat palvelupäällikkö sekä palvelusta vastaava järjestelmäasiantuntija. Erillisiä palvelutoimittajan työpajoja ei järjestetty. Riskienarvioinnin työpajat pidettiin 15.4., 24.4. ja 30.4.2015. Riskienarviointiin liittyi myös esivalmistelu, joka tapahtui riskienhallinnan käsikirjaan ja koulutusmateriaaliin tutustamalla sekä arvioitavan kohteen esitietojen täyttäminen. Tietoturvapäällikkö täytti esitiedot, jotka käytiin ensimmäisessä työpajassa läpi. Työpajojen jälkeen tietoturvapäällikkö siirsi riskit riskisalkkuun ja kävi ne läpi palvelun omistajan, ATK-päällikön kanssa.

Ensimmäisessä työpajassa käytiin läpi koulutusmateriaali tiivistetysti ennen varsinaista riskienarviointia. Tämä toimi samalla koulutusmateriaalin testauksena. Lyhyen katsauksen jälkeen siirryttiin varsinaiseen riskienarviointiin. Ensimmäisenä työpajan teemana oli riskien tunnistaminen. Apuna tunnistamisessa käytettiin riskienhallinnan käsikirjan esimerkkejä ja uhkaluokkia. Uhkaluokkia käytettiin keskustelun teemana ja keskustelusta poimittiin riskit ylös. Kun kaikki teemat oli käyty läpi, tarkistettiin vielä käsikirjan esimerkit tunnistettaisiinko näitten avulla lisää riskejä. Riskit tarkennettiin käytännön tasolle ja kirjattiin uhkaluokkineen riskityökaluun.

Seuraava työpaja aloitettiin lyhyellä kertauksella edellisessä työpajassa havaituista riskeistä. Lisäriskejä ei tunnistettu joten tästä siirryttiin toisen työpajan teemaan, joka oli riskien analysointi. Ensimmäiseksi analysoitiin tunnistettujen riskien syyt. Analysointi tehtiin keskustelemalla ja tulokset kirjattiin ylös hallintatyökaluun. Kirjaamalla riskien syyt, voidaan näille helpommin muodostaa hallintasuunnitelmat. Seuraavaksi analyysissä arvioitiin riskien todennäköisyys ja toteutumisen vaikutukset asteikolla 1-5. Asteikko on kuvattuna riskienhallinnan käsikirjassa. Jokainen kirjattu riski käsiteltiin ensin todennäköisyyden ja sitten vaikutuksen osalta. Riskityökalu laski automaattisesti riskin kriittisyyden ja riskin suuruuden.

Viimeisessä työpajassa arvioitiin riskien merkitys ja päätettiin toimenpiteiden tarpeellisuudesta. Esitiedoissa tunnistettiin järjestelmän kriittisyys toiminnalle sekä keskeiset järjestelmän toimintaan liittyvät riippuvuudet. Näihin liittyvien riskien osalta tehtiin hallintasuunnitelmat samalla tapaa kuin kohtalaiset riskit myös matalille riskeille. Muilta osin matalat riskit otettiin seurantaan ja muita toimenpiteitä ei niille suunniteltu. Muut riskit valittiin käsittelyyn riskienhallinnan periaatteiden mukaisesti eli korkeita riskejä ei siedetä jolloin toimenpiteet tähtäävät niiden pienentämiseen, siirtämiseen tai poistamiseen. Kohtalaiset riskit pyritään pienentämään siirtämään tai poistamaan, jos tässä ei onnistuta, seurataan niitä aktiivisesti.

Samassa työpajassa jatkettiin riskien käsittelyllä. Hallintatoimenpiteet suunniteltiin määrittelemällä ensin tavoitetila johon pyritään. Tämän jälkeen keskusteltiin keinoista miten riskiä hallitaan, onko keinoina riskin pienentäminen, poistaminen tai siirtäminen. Toimenpiteiden keinon valinnan jälkeen keskusteltiin onko se riittävä vai pitäisikö jäljelle jäävää jäännösriskiä arvioida vielä uudelleen. Jäännösriskien todettiin olevan riittävällä tasolla toimenpiteiden suorittamisen jälkeen, joten uudelleenarviointeja ei tehty. Toimenpiteet kirjattiin aktiiviset riskit –välilehdelle. Tarkkoja toimenpidekuvauksia riskeille ei tehty, jos hallinta vaatii suunnittelua ja toteutusta suunnittelun jälkeen kirjattiin nämä toimenpiteiksi.

Riskien tilannekatsauksessa päivitetään hallintasuunnitelmien edistymistä. Suunnitelmaan merkittiin myös riskin omistaja eli toimenpiteiden seurannasta vastaava henkilö, toimenpiteiden valmistumisaikataulu sekä tarkastuspiste. Kaikki riskit käsiteltiin samalla tavalla.

Työpajojen jälkeen tietoturvapäällikkö siirsi käsitellyt riskit toimiston riskisalkkuun seurantaa varten. Riskiarvioinnin tulokset käsiteltiin myös kohteen omistajan, ATK-päällikön, kanssa yhdessä. Tässä päätettiin miten riskeistä tiedotetaan. Tulokset päätettiin jakaa toimiston sisällä ja palvelutoimittajalle, mutta vain palveluun nimetyille henkilöille, jotka ovat turvaselvitettyjä ja allekirjoittaneet vaitiolovakuutuksen. Muuta tiedotusta ei tehdä. ATK-päällikkö seuraa Active Directoryn riskien edistymistä kokonaisuutena riskienhallintasuunnitelmien mukaisesti ja tietoturvapäällikkö kaikkien riskien edistymistä vuosikellon mukaisesti. Seuraava kokonaistilanteen tarkastus on syyskuussa 2015.

Työkalut voidaan katsoa toimiviksi ja testaus onnistuneeksi. Järjestelmään liittyviä riskejä tunnistettiin, niiden vaikutukset ja suuruudet analysointiin, hallintatoimenpiteet päätettiin aikatauluineen ja vastuuhenkilöineen. Kohteen omistaja hyväksyi tulokset ja ne siirrettiin seurantaan. Testaukseen liittymät materiaalit ovat tämän raportin liitteinä, liite 6 koulutusmateriaali sekä luottamukselliset liitteet, liite 15 Active Directory riskit ja liite 16 Tietohallintotoimiston riskisalkku.

3.4.4 Riskienhallintamallin hyödyntäminen

Riskienhallintamallia voidaan testausten tulosten perusteella hyödyntää tietohallintotoimistossa. Riskienhallintamallista hyötyjen saaminen vaatii toimistolta sitoutumista sen toteuttamiseen. Ottaen huomioon lähtötilanteen, on mallin käyttämisestä saatavissa nopeasti hyötyjä. Mallin toiminta kehittyy ajan myöstä ja sen kehittämisestä on huolehdittava samalla tavalla kuten mistä tahansa muusta toimintamallista. Jatkuvalla kehittämisellä ja mittaamisella riskienhallintamalli pystyy jatkossakin antamaan tukea toiminnan johtamiseen.

Palvelut

Palveluiden näkökulmasta riskienhallinta antaa tietohallintotoimistolle mahdollisuuden ennakoida palveluissa mahdollisesti esiintyviä häiriötilanteita ja toimenpiteillä pienentää niiden esiintymistä ja mahdollisia vaikutuksia. Tuotannossa olevien palveluiden osalta arvioitava kohde tunnetaan hyvin ja toteutuksen mahdolliset heikkoudet saadaan kirjattua ylös ja hallintaan. Uudesta palvelusta on saatavilla kehitysvaiheessa tehtyjä havaintoja. Nämä tiedot voidaan hyödyntää riskienarvioinnissa. Uusien palveluiden osalta riskienhal-

linnan tukena voivat olla vielä projektin aikaiset ja hankinnan aikaiset riskienarvioinnit ja riskienhallinnantoimenpiteet.

Projektit

Projektien riskienhallintaan tai hankintojen riskienhallintaan sopivuudesta ei mallista kuitenkaan saatu varmuutta. Kehityksen aikana tietohallintotoimiston sen hetkiset projektit olivat jo pitkällä käyttöönottovaiheessa, jolloin suurin osa riskeistä oli hallinnassa tai mahdollisista ongelmatilanteista oli jo selvitty. Myöskään hankintoja ei tehty kehitystyön aikana. Oletettavasti malli kuitenkin soveltuu riskienhallintaan myös näissä tapauksissa. Riskienhallinnan perusta on arvioida epävarmuuksia ja muodostaa näille hallintakeinoja. Projektien riskienhallinta perinteisesti perustuu talouden, aikataulujen ja laadun kontrollointiin. Näille määritellään vaikutusten todennäköisyydet ja vaikutukset sekä hallintakeinot. Sama toimintamalli on myös nyt kehitetyssä riskienhallintamallissa. Malli siis oletettavasti toimisi ja laajentaisi projektinhallinnan riskienhallintaa. Seuranta eroaisi jatkuvan palvelun riskien seurannasta. Projektin riskejä seurataan projektipäällikön toimesta ja ne on liitetty projektin ohjaukseen. Projektissa on todennäköisesti myös tarvetta arvioida riskejä tiheämmällä tahdilla kuin jatkuvissa palveluissa. Projektin toimintaympäristö muuttuu nopeammin kuin jatkuvan palvelun ympäristö. Riippuen projektimallista on riskejä syytä arvioida aina vaiheen loppuessa tai kehityskierroksen lopussa, kun päästään lähelle lopullista tuotosta.

Hankinnat

Hankinnoissa vaatimukset ovat keskeisessä roolissa. Riskienhallinnassa on mahdollista tunnistaa hankintoihin liittyviä riskejä kehitetyn mallin avulla ja muodostaa näistä vaatimuksia hankittavalle kohteelle. Edellytyksenä on hankittavan kohteen toiminnan tunteminen, mutta tämä on hankintojen kannalta oleellinen vaatimus muutenkin. Uusissa hankinnoissa ei päästä yksityiskohtaiselle tasolle riskienhallinnassa, mutta jo yleisellä tasolla voidaan tunnistaa oleellisia riskejä jotka hankinnoissa tulisi huomioida. Hankinnat jotka liittyvät jonkin olemassa olevan palvelun päivittämiseen, voivat hyödyntää palvelutuotannon aikaisia riskiarviointeja vaatimusten muodostamisessa. Vaikka kehittämisen aikana ei tehty merkittäviä hankintoja, on oletettavaa, että mallia voidaan hyödyntää seuraavan suuremman hankinnan aikana osana vaatimusmäärittelyä.

Seuranta

Riskienhallintamalli tuo tietohallintotoimistoon kokonaan uuden toimintamallin riskien seurantaan. Aikaisemmassa mallissa riskejä on käytännössä seurattu kerran vuodessa toiminnan suunnittelun yhteydessä. Seuranta on integroitavissa toiminnan muuhun seuran-

taan joko sisäiseen prosessiin tiimikokousten yhteyteen tai palvelutoimittajien kanssa tehtävään palvelunseurantaan. Seurantaa joudutaan todennäköisesti tekemään molemmilla tavoilla. Teknisten korjaavien toimenpiteiden tekeminen on palveluntoimittajien vastuulla ja tietohallintotoimiston omiin prosesseihin liittyvät toimenpiteet ovat sisäisen kehityksen kautta tehtäviä toimenpiteitä. Organisaatioon liittyvien riskien seuranta tehdään tietohallintotoimiston johtoryhmän toimesta sisäisesti. Koska nämä rakenteet ovat jo olemassa, seurannan järjestäminen ei vaadi ylimääräisiä järjestelyjä. Seuranta pystytään järjestämään sopimalla kokousten sisältö ja ajankohta. Seurannan toimivuus on rakenteiden puolesta todennäköisesti korkealla tasolla ja siten hyödynnettävissä tietohallintotoimiston toiminnassa.

Mallin toimivuuden seuranta ja kehittäminen

Kehitetty malli vaatii seurantaa ja jatkokehittämistä. Avainhenkilönä mallin toimivuuden seurannan ja kehittämisen kannalta on mallista vastaava henkilö, tietohallintotoimiston riskienhallintamallin vastuiden mukaisesti tietoturvapäällikkö. Kehitysprosessista on vastannut tietoturvapäällikkö, jolloin sen hyödyntäminen ja soveltuminen tietohallintotoimistoon on huomioitu alusta alkaen. Varmuus mallin seurannan ja kehittämisen hyödyntämisen mahdollisuuksista saadaan, kun mallia on käytännössä toteutettu ja kehitetty seurannan perusteella. Tämä toteutuu käyttöönoton edetessä.

3.4.5 Tulosten ja kehitysprosessin arviointi

Tulokset onnistuivat varsin hyvin. Ne pohjautuivat vahvasti teoriataustaan ja huomioivat nykyisen toimintatavan ja tarpeet. Kehitetyllä mallilla pystyttiin käsittelemään olemassa olevat riskit tarkemmalle tasolle ja liittämään ne riskisalkkuun seurantaan. Uusia riskejä pystyttiin myös tunnistamaan, analysoimaan ja käsittelemään kehitetyllä mallilla.

Tulosten onnistuminen

Riskienhallinnan dokumentit eli periaatteet, puitekuvaus ja käsikirja voidaan katsoa onnistuneiksi tuotoksiksi. Ne hyväksyttiin johtoryhmän toimesta ja testattiin riskienarvioinnin testauksen yhteydessä. Samalla testattiin riskiarviointityökalu ja riskien seurantaan keskittynyt riskisalkku. Myös koulutusmateriaali testattiin arviointien yhteydessä. Riskienhallinnan prosessin kehitystä ja seurantaa ei tässä vaiheessa pystytty todentamaan testauksen avulla. Myös vuosikello ja vuosisuunnitelma jäivät testaamatta. Näitä varten olisi prosessia pitänyt käyttää pidemmän aikaa, kuin tutkimuksessa oli mahdollista toiminnan varmistamiseksi.

Kehitysprosessin onnistuminen

Kehitysprosessi oli hyvin pitkälti tietoturvapäällikön vastuulla. Eduskunnan kanslia valmistautui kehitysprosessin aikana peruskorjaukseen liittyviin muuttoihin, vaaleihin ja uusien tietojärjestelmien käyttöönottoihin. Tämä antoi kehitystyölle raamit, joka käytännössä tarkoitti, että kehitystyö oli kokonaan tietoturvapäällikön vastuulla. Kehitystyö sai kuitenkin tukea tietohallintotoimiston johtoryhmältä, joka ohjasi kehitystyötä sekä toimi kommentointiroolissa. Prosessissa käytettiin myös kommentoijan roolissa ulkopuolista konsulttia.

Kehitysprosessi onnistui olosuhteet ja resurssit huomioon ottaen hyvin. Tietoturvapäällikkö pystyi keskittymään kehitystyöhön varaamalla kokonaisia päiviä kehitystyöhön. Mallin kehittäminen pohjautui vahvasti teoriataustaan, jolloin sen merkitys korostui. Teoriataustan kerääminen aloitettiin välittömästi kehitystyön alussa, jotta se olisi käytettävissä riskienhallinmallin kehitystyön aikana mahdollisimman varhaisessa vaiheessa. Mallin hahmottelu tapahtui samaan aikaan teorian keräämisen kanssa, nämä etenivät rinnakkaisina väylinä. Tämä mahdollisti iteratiivisen toimintamallin ja mallin uudelleentarkastelun perustuen kerättyyn tietoihin, kun teoriatausta kasvoi.

Prosessiin sitoutuminen tapahtui johtoryhmän kautta. Johtoryhmällä oli kommentoinnin kautta keskeinen rooli kehitystyön tulosten hyväksynnässä sekä toimiston tarpeiden keräämisessä. Käyttöönoton kannalta olisi ollut toivottavaa toimiston henkilöstön laajempi osallistuminen, joka olisi antanut mahdollisuuden sitouttaa mallin käyttöön laajemmin kuin vain testausten osalta. Tämä puute on kuitenkin kompensoitavissa koulutuksilla ja mallin käyttämisellä tuotannossa.

Itse projekti noudatti tietohallintotoimiston projektimallia. Projektin organisaatio oli kuitenkin varsin pieni, joten ehkä kevyempi malli olisi soveltunut läpivientiin. Kevyempi projektimalli on vasta kehitteillä, joten sitä ei ollut saatavilla. Projektia kuitenkin seurataan ja ohjataan molemmissa malleissa samalla tavalla, raportointikäytännöissä on eroa. Projektimalli kuitenkin toimi tässäkin tapauksessa.

Oma rooli kehitystyössä

Oma roolini kehitystyössä oli hyvin keskeinen. Toimin tietoturvapäällikkönä kehitysvastuullisena sekä projektipäällikkönä. Kehitetyn riskienhallintamallin jatkon kannalta toimin myös vastuullisena kehittäjänä ja käyttöönotosta vastaavana resurssina. Nämä huomioiden olin sitoutunut mallin kehitystyöhön ja olen sitoutunut mallin käyttämiseen ja jatkon kehittämiseen. Kehitystyössä pystyin keskittymään riskienhallintamallin kehittämiseen varsin hyvin. Ainoana varsinaisena resurssina ajankäyttö oli ajoittain haasteellista. Tässä auttoi töiden

priorisointi ja aikataulujen varsin helppo siirto, ainoana resurssina ei tarvinnut suuria järjestelyjä aikataulujen muutoksille ja tilavarauksille.

Tutkijana minulla oli mahdollisuus päästä näkemään tietohallintotoimiston toimintaa organisaation sisältä ja vaikuttaa kehitystyöllä organisaation toimintaan. Organisaatio antoi myös itse sisältöä kehitystyöhön ja ei pyrkinyt liikaa vaikuttamaan kehitettävään riskienhallinnan malliin. Tietohallintotoimisto luotti minuun tutkijana ja kehitystyön tekijänä. Tietohallintotoimiston johtoryhmän tuki oli tutkijana minulle keskeinen, ilman sitä ei tutkimusta olisi voinut tehdä. Johtoryhmä osallistui riskienhallintamallin kehittämiseen sekä antoi resurssit sen tekemiseen. Empirian vaativan käytännön työn lisäksi minulla oli aikaa käytettävissä teoriataustan kasaamiseen.

Pääsin kehitystyössä vaikuttamaan kaikkiin osa-alueisiin ja luomaan uutta toimintamallia tietohallintotoimistolle. Vaikka koko kehitystyö oli yksin vastuullani, pääsin kuitenkin tekemään yhteistyötä toimiston johdon ja henkilöstön kanssa. Tämä loi kehittämistyöhön kumppanuuden ilmapiirin ja uuden toiminnan luoman autenttisuuden, kun pyrittiin ratkaisemaan aitoa ongelmaa, joka oli tutkimuksen käynnistävänä tekijänä. Oma roolini oli tässä olla kehittäjä ja konsultti samaan aikaan. Vahva teoriatausta taas toi minulle tutkijan roolin, joka näkyy kehitetyssä mallissa, joka nojautuu teoreettiseen taustaan ja nykytilan sekä tarpeiden arviointiin.

3.4.6 Yhteenveto

Tutkimustehtävässä kehitettiin eduskunnan tietohallintotoimistolle riskienhallinnan malli. tutkimusmenetelmänä käytettiin konstruktiivista tutkimusotetta, kehityksellä haluttiin luoda käytännön mallien toimiston riskien hallitsemiseksi. Kehitystehtävä jaettiin kolmeen vaiheeseen: nykytilan arviointi, hallintamallin suunnittelu ja luonti sekä hallintamallin testaus.

Nykytilan arvioinnissa analysoitiin riskienhallinnan nykykäytännöt, toimiston tarpeet riskienhallinnalle sekä yleiset riskienhallintamallit. Nykykäytäntöjen analyysi tehtiin dokumenttianalyysillä käytössä olevasta riskienhallintamenetelmästä, toimiston tarpeet tunnistettiin haastattelemalla tietohallintotoimiston johtoryhmä ja yleiset riskienhallinnan menetelmät arvioitiin tekemällä teoriataustasta synteesi.

Hallintamallin suunnittelussa ja luonnissa tehtiin yhteenveto tietohallinnon tarpeista, analysoitiin tarpeet yleisiin malleihin nähden ja kehitettiin näiden pohjalta tietohallintotoimiston riskienhallintamalli. Tarpeiden yhteenvedossa todettiin, että nykyinen riskienhallintamalli soveltuu pääosin riskienarviointiin, mutta tarve on laajemmalle hallittavalle kokonaisuudelle, johon sisältyy arviointien lisäksi seuranta ja kehitys. Teoriataustan perusteella menes-

tyvä riskienhallinta vaatii myös johdon sitoutumisen ja riskienhallintakulttuurin luomisen sekä selkeät rakenteet riskienhallinnalle. Näiden tietojen pohjalta kehitettiin tietohallintotoimiston riskienhallintamalli joka jakautuu kolmeen tasoon: riskienhallinta yleisesti, riskienhallintaprosessi ja riskienarviointiprosessi. Yleisellä tasolla määritellään riskienhallinnan tahtotila ja vastuut riskienhallinnan periaatteilla. Riskienhallintaprosessin tasolla määritellään kuinka riskienhallintaa toteutetaan ja kuinka sitä ohjataan sekä seurataan. Määrittelevänä dokumenttina tällä tasolla on riskienhallinnan puitekuvaus. Seurantaa tehdään riskisalkulla ja säännöllisyyttä ajastetaan vuosikellolla. Riskienarviointiprosessissa taas tehdään riskienarvioinnit. Tällä tasolla riskienhallintakäsikirja määrittelee toimenpiteet miten arviointeja tehdään. Lisäksi riskienarvioinnin työkalu auttaa tekemään arvioinnit sekä koulutusmateriaalit tukevat arviointien suorittamisia.

Hallintamallin testauksessa testattiin mallin toimivuus ja arvioitiin sen hyödynnettävyys toimistossa. Tietohallintotoimiston johtoryhmä kommentoi ja hyväksyi kaikki riskienhallintaan liittyvät dokumentit. Riskienhallinnan seurannan toimivuus testattiin käsittelemällä aiemmat riskiarvioinnit uudelleen ja siirtämällä ne salkkuun sekä hyväksyttämällä ne johtoryhmällä. Riskienarvioinnin testaus tehtiin tekemällä alusta saakka riskienarviointi Active Directory –järjestelmälle. Testausten perusteella luodut dokumentaatiot ovat toimivia ja otettavissa käyttöön tietohallintotoimistossa. Lisäksi seuranta vaikutti toimivalta ja hyväksyttiin johtoryhmän toimesta käyttöön. Riskienarviointiprosessi pystyi myös tuottamaan onnistuneen riskienarvioinnin ja myös tämä prosessi hyväksyttiin käyttöön.

Testausten pohjalta arvioitiin, että kehitetty malli on hyödynnettävissä tietohallintotoimistossa. Mallin kehitys tapahtuu kun sitä on käytetty jonkin aikaa. Tässä vaiheessa ei siis varmuudella voida sanoa kuinka hyvin malli toimii jatkossa toimiston toimintatapojen muutosten yhteydessä, mutta säännöllinen mallin toimivuuden seuranta ja muokkaukset oletettavasti pitävät mallin toimivana myös tulevaisuudessa.

Kehitysprosessi, joka noudatti tietohallintotoimiston omaa projektimallia, todettiin myös toimivaksi. Projektin vähäiset resurssit olisivat voineet muodostua ongelmaksi, mutta nämä vältettiin toimiston johdon sitoutumisen ja töiden priorisoinnin avulla. Tutkijan rooli oli myös keskeinen ja tärkeä uuden toiminnan luomisessa. Erityisesti teoriatausta vaikutti vahvasti kehitettyyn malliin, joten tutkijan rooli oli tärkeä mallin kehittämisessä.

4 Yhteenveto ja arviointi

Riskienhallinnan merkitys organisaatiolle on yksi menestyksekkään organisaation tekijöistä. Riskienhallinta osana muuta organisaation tekemää laatutyötä parantaa ja tehostaa organisaation toimintaa. Lähes kaikki organisaatiot tekevät riskienhallintaa jollakin tavalla, joko suunnitellusti omana toimintonaan tai osana muuta organisaation tekemää työtä. Riskienhallinnalle on selkeä tarve olemassa, jotta organisaatiot voivat hallita epävarmuustekijöitä.

Tämä opinnäytetyönä tehty kehitystehtävä lähti kehittämään eduskunnan tietohallintotoimistolle riskienhallintamallia toimiston riskien aiheuttamien epävarmuustekijöiden hallitsemiseksi. Tutkimuskysymyksenä oli selvittää millaisella mallilla eduskunnan tietohallintotoimiston tulisi hallita sen toimintaan liittyviä riskejä. Lisäksi tavoitteena oli selvittää mitä riskienhallinnan tarpeita tietohallintotoimistolla on ja miten tietohallintotoimisto tunnistaa, analysoi ja priorisoi riskejään.

Tarve kehitystyölle oli havaittu osana toimiston tekemää riskianalyysia omasta toiminnastaan. Riskienhallinta ei ollut sillä tasolla kuin sen haluttiin olevan. Kehitystarpeita oli erityisesti prosessimaisessa toiminnassa ja riskienhallinnan vaikuttavuuden seurannassa ja arvioinnissa. Lopputuloksen haluttiin olevan kokonaisvaltainen malli, joka tukisi tietohallintotoimiston johtamista.

Tietoturvapäällikkö luonnosteli kehitystyön projektisuunnitelman ja käynnisti sen sisäisenä hankkeena. Kehitystyössä kartoitettiin riskienhallinnan nykytilanne sekä toimiston tarpeet riskienhallinnalle. Lisäksi huomioitaisiin keskeiset riskienhallinnan toteutusmallit, koottaisiin kattava lähdemateriaali ja haastateltaisiin muiden organisaatioiden riskienhallintavastaavia riskienhallinnan toteutusmalleista. Näiden pohjalta luotaisiin tietohallintotoimistolle riskienhallintamalli.

Teoriatausta koottiin lähdekirjallisuudesta ja parhaista käytännöistä, standardeista ja ohjeista. Hyvin nopeasti tuli selville, että lähdemateriaalit yhtenäisesti korostivat prosessimaisen riskienhallinnan tärkeyttä onnistuneelle riskienhallintamallille. Säännöllinen arviointi ja seuranta ovat riskienhallinnan onnistumisen kannalta tärkeimmässä roolissa. Riskienhallinnan tavoitteet saavutetaan suunniteltujen toimenpiteiden avulla, joita tulee seurata. Itse riskienhallinnan ohjaaminen vaatii myös määritellyt toimintatavat tukemaan riskienhallinnan toteuttamista. Organisaation sitoutuminen ja kulttuuri vaikuttavat myös riskienhallinnan onnistumiseen.

Toimiston tarvekartoitus toteutettiin samanaikaisesti teoriataustan keräämisen kanssa. Tarvekartoitus tehtiin haastattelemalla tietohallintotoimiston johtoryhmä. Haastattelun tuloksina toimiston tarpeiksi tunnistettiin määrämuotoinen riskienhallinnan malli, joka tukisi palveluiden tuottamista, kehittämistä ja hankintoja. Myös tarve konkreettisille työkaluille oli oleellinen havainto.

Riskienhallinnan nykytilan arvio tehtiin analysoimalla käytettävissä olevaa dokumentaatiota riskianalyyseistä. Analyysissä todettiin nykyisen toimintamallin tukevan riskienarviointiprosessia ja hyödynnettävissä näiltä osin arvioinnissa. Nykyinen toimintatapa kuitenkin tarvitsee täydennystä erityisesti toimenpiteiden seurantaan ja riskienhallintamallin jatkokehittämiseen.

Teoriataustan, toimiston tarpeiden ja nykytilan analyysin perusteella kehitettiin tietohallintoimistolle kolmitasoinen riskienhallinnan malli. Ylimmällä tasolla määritellään riskienhallinnan tahtotila ja johdon sitoutuminen sekä riskienhallinnan periaatteet. Seuraavalla tasolla määritellään riskienhallinnan prosessi, vastuut ja kuvataan riskienhallinnan puitteet. Yksityiskohtaisimmalla tasolla kuvataan riskienarvioinnin menetelmät riskienhallinnan käsikirjassa. Malli koostuu dokumentaatiosta ja käytännön työkaluista. Dokumentit ovat riskienhallinnan periaatteet, riskienhallinnan puitekuvaus, riskienhallinnan käsikirja, riskienhallinnan vuosikello sekä koulutusmateriaali. Työkaluja ovat riskisalkku toimiston riskien seurantaan ja riskienarvioinnin työkalu kohdekohtaiseen riskienarviointiin ja toimenpiteiden seurantaan.

Dokumentaatio testattiin hyväksyttämällä ne tietohallinnon johtoryhmässä. Ennen hyväksymistä johtoryhmä kommentoi dokumentteja. Käytännön työkaluista riskisalkkua testattiin käsittelemällä aikaisemmat riskit uudelleen ja viemällä ne riskisalkkuun seurantaan ja hankkimalla hyväksyntä sille johtoryhmästä. Riskienarviointityökalu ja koulutusmateriaali testattiin arvioimalla sopivan kohteen riskit alusta asti. Samalla testattiin riskienhallinnan käsikirjan ja koulutusmateriaalien toimivuutta.

Testit osoittivat, että dokumentaatio ja niissä määriteltävä malli on hyväksyttävissä ja otettavissa käyttöön tietohallintotoimistossa. Kaikki dokumentit hyväksyttiin ja otettiin käyttöön. Riskisalkkuun pystyttiin viemään arvioidut riskit seurantaan. Riskienarvioinnin kohteen riskit voitiin arvioida riskienhallintakäsikirjassa määritellyllä tavalla käyttämällä riskienarvioinnin työkalua. Koulutusmateriaali myös toimi, arvioinnissa osattiin toimia oikein ja saatiin tuloksia aikaiseksi. Riskienhallintamallin toimivuuden seurannan ja siitä johdettavaa kehitystä ei voitu testata tutkimuksessa.

Testien perusteella malli on hyödynnettävissä tietohallinnon toiminnon osana. Nykyiset toimintamallit mahdollistavat riskienhallinnan integroitumisin osaksi normaalia toimintaa ilman, että ylimääräisiä toimintatapoja tulisi kehittää tai nykyisiä muuttaa paljon. Tutkijan roolissa pääsin hyvin toimimaan osana tietohallintotoimiston organisaatiota ja vaikuttamaan sen toimintaan. Toimisto ei myöskään pyrkinyt liikaa vaikuttamaan tutkimuksen tuloksiin.

4.1 Johtopäätökset

Tutkimuksessa oli päätavoitteena selvittää, minkälaisella mallilla eduskunnan tietohallintotoimiston tulisi hallita riskejään. Tutkimuksen kehitystehtävässä päädyttiin luomaan malli, joka määrittelee ylätasolla riskienhallinnalle selkeät suuntaviivat ja määrittelee riskienhallinnan osaksi toimiston normaalia toimintaa. Ylätasolla määritellään riskienhallinta määrämuotoiseksi toiminnaksi, jonka toteuttamiseen osallistuvat kaikki tietohallintotoimistossa työskentelevät. Seuraavilla tasoilla tarkennetaan toimintatavat ja käytännön tasolla tehtävä riskienhallinta.

Kehitettyyn riskienhallinnan malliin päädyttiin teoriataustan, tarvehaastatteluihin ja nykytilan arvion kautta. Teoriataustan mukaan riskienhallinnan tulee olla prosessi jonka toteuttamiseen koko organisaatio on sitoutunut. Organisaation sitoutuminen tapahtuu johdon sitoutumisen kautta. Tietohallintotoimiston riskienhallinnan mallissa määritellyt riskienhallinnan periaatteet ilmaisevat johdon sitoutumisen riskienhallintaan. Prosessimainen lähestymistapa on toteutettu määrittelemälle riskienhallinnan toteutuksen puitteet ja käytännön työkalut riskienhallinnan puitekuvauksessa ja käsikirjassa. Tarvehaastatteluissa tuli esille tarve määrämuotoisesta käytännönläheisestä riskienhallinnasta. Näihin tarpeisiin vastattiin edellä mainittujen dokumenttien lisäksi kehittämällä riskienarvioinnin työkalut ja ohjeet käytännön esimerkkeineen riskeistä. Nykytilan arvio päätyi lopputulokseen, että nykyinen malli on sovellettavissa riskienarviointiin, mutta ei sovellu prosessimaiseen määrämuotoiseen riskienhallintaan.

Testausten perusteella malli on toimiva ja antaa paremman näkymän kokonaistilanteesta. Mallilla pystyttiin havaitsemaan uusia riskejä ja kirjaamaan ylös jo aiemmin tunnistettuja riskejä tarkemmalla tasolla kuin aikaisemmin. Riskienhallintamalli ja siihen kuuluvat työkalut mahdollistivat tarkemman tason analyysin riskeistä sekä helpottivat toimenpiteiden seurantaa. Myös kriittisten riskien tunnistaminen helpottui. Lisäksi malli antoi suunnitelmallisuutta riskienhallinnan toteutuksiin ja ennakointimahdollisuuden riskienarviointien toteutuksiin.

Johtopäätöksenä voidaan vetää, että riskienhallinnan mahdollisimman kattava ja tehokas toiminta vaatii riskienhallinnan kokonaisvaltaisen mallin luomista, joka kattaa organisaation kaiken toiminnan. Mallissa voidaan hyödyntää riskienhallinnan olemassa olevia käytäntöjä soveltuvin osin. Nykykäytännöt tulee kuitenkin analysoida huolellisesti, jotta voidaan tunnistaa hyödynnettävät osat. Kehityksessä on myös huomioitava organisaation tarpeet, jotta riskienhallintamalli on mahdollisimman toimiva ja sovellettavissa osaksi normaalia toimintaa. Lisäksi jos organisaatiolla on jonkinlainen malli olemassa riskienarviointiin, voidaan tämän toimintakykyä huomattavasti tehostaa luomalla selkeä, määrämuotoinen malli riskienhallintaan ja sen toteutukseen.

Tutkimuksen toisena kysymyksenä oli selvittää, minkälaisia tarpeita tietohallintotoimistolla on riskienhallinnalle. Tarpeiden selvittäminen toteutettiin haastatteluilla. Haastattelut teemoitettiin aloittamalla nykytilan arviosta päätyen tietohallintotoimiston erityistarpeisiin. Haastattelujen analysoinnin jälkeen tuloksena päädyttiin siihen, että riskienhallinta koettiin nykymallissa teoreettisena eikä käytännön tason toiminnassa näkyvänä. Riskienhallinnan pitäisi näkyä kaikessa toimiston toiminnassa toimiston johtamisesta sen tarjoamiin palveluihin saakka. Lisäksi tietohallintotoimiston keskeinen rooli tietojärjestelmiin liittyvien palveluiden tuottajana on kriittisyydeltään ja tuotantomallissaan käyttämien ulkoistusten kautta poikkeava muista saman osaston toimistoista, joka tulisi huomioida riskienhallinnassa.

Johtopäätöksenä tästä voidaan tehdä, että kriittisten toimintayksiköiden kuten tietohallintotoimiston riskienhallinnan tulee olla mahdollisimman kattavaa ja määrämuotoista. Kriittiset kohteet tulisi pystyä tunnistamaan ja käsittelemään niiden riskit tarkemmin kuin ei kriittisten kohteiden. Lisäksi riskienhallinnan tulee huomioida tuotantomalli ulkoistustilanteissa ja määritellä riskienhallinta siten, että ulkoistuskumppanit ovat osa sitä.

Kolmantena kysymyksenä oli selvittää miten tietohallintotoimisto tunnistaa, analysoi ja priorisoi riskejään. Toimintatapaa selvitettiin nykymallia analysoimalla ja teoriatausta ja toimiston tarpeet huomioiden. Analyysin tuloksena kehitystyössä päädyttiin siihen, että nykymallista on säilytettävä yhteensopivuuden vuoksi osia. Kanslian yhteisessä riskienhallintamallissa on määritelty riskien todennäköisyys ja vaikutusten vakavuus sekä riskiluokat, jotka ovat yhteensopivuuden vuoksi oltava samoja koko organisaatiossa. Muilta osin parannuksia tehtiin kaikille osa-alueille kehittämällä riskienarviointityökalua, luomalla tätä tukevaa ohjeistusta ja panostamalla koulutukseen. Testauksen perusteella riskienarviointien laatu ja analysointikyky parani aikaisempaan malliin verrattuna.

Johtopäätöksenä tästä voidaan tehdä, että riskienarviointikyvykkyyden nostamiseksi ja laadukkaampien tulosten aikaansaamiseksi, on käytännön työkaluihin ja tukimateriaaleihin

panostettava. Riskienarviointeja voi tehdä hyvinkin kevyellä mallilla, mutta riskienhallinnan ohjeistus, koulutusmateriaali ja työkalut vaikuttavat lopputuloksiin positiivisesti. Erityisesti tulosten laatu paranee silloin kuin ne on viety tarvittavalle yksityiskohtien tasolle käytännön esimerkein varustettuina. Tietohallintotoimistossa riskienarviointeja tekevät henkilöt ovat asiantuntijoita ja pystyvät omaksumaan vaadittavan ajattelutavan nopeasti, mutta ennalta määritelty toimintatapa nopeuttaa orientoitumista ja helpottaa sekä nostaa toteutusten laatua melko raskaassa riskienarviointiprosessissa.

4.2 Tutkimuksen arviointi ja suositukset

Kehittämistehtävänä toteutettu konstruktiivinen tutkimus onnistui tavoitteissaan. Riskienhallinnan malli saatiin toteutettua ja testattua tietohallintoimistossa. Mallissa myös pystyttiin huomioimaan toimiston tarpeet. Vaikka tutkimuksellisesti myös mallin toimimattomuus on tulos, antaa onnistunut testaustulos hyvän lähtökohdan mallin käyttöönotolle. Kehittämismenetelmä ja sen aikana kerätyn materiaalin tiivistelmä on dokumentoitu tähän raporttiin. Näiden pohjalta tutkimustyö on mahdollista toteuttaa uudelleen.

Huomioitavaa on kuitenkin, että tietohallintotoimiston lähtötilanne ei ole enää sama kuin tutkimuksen alussa. Avainhenkilöt ovat kommentoineet ja hyväksyneet tässä tutkimuksessa kehitetyn mallin. Tämä on vaikuttanut avainhenkilöiden näkemyksiin tarpeista ja todennäköisesti samaa tulosta tarvekartoituksissa ei enää saataisi. Tekemällä tarvekartoituksen jossain muussa eduskunnan kanslian yksikössä voisi tuottaa samankaltaisen tutkimustuloksen kuin tietohallintotoimistosta saatiin. Siinä tapauksessakin olisi huomioitava erilaiset toimintatavat ja palveluiden tuotantomallit, jotka vaikuttaisivat lopputulokseen. Tarvekartoitus on tämän tutkimuksessa vaikeimmin toistettavia alueita erilaisista toimintaympäristöistä ja niihin vaikuttavista seikoista johtuen. Menetelmänä haastattelu on kuitenkin toistettavissa ja tulokset samalla tavalla analysoitavissa.

Riskienhallinnan nykytilan arvio tuottaisi oletettavasti samankaltaisen lopputuloksen kuin nyt tehty arvio. Tämä pohjautui pitkälti dokumenttianalyysiin, johon ulkopuoliset ympäristötekijät eivät vaikuta. Analyysin tekijä on kuitenkin tietohallintotoimiston organisaatiossa töissä, jolloin voidaan olettaa, että tällä on vaikutusta lopputulokseen. Ulkopuolinen taho olisi voinut painottaa eri näkökulmia ja päätyä arviossaan jonkin verran erilaiseen tulokseen. Isoja poikkeamia ei todennäköisesti olisi kuitenkaan esiintynyt, riskienhallinnan kypsyystaso ei ole kautta organisaation kovin korkealla.

Teoriataustan yhteenveto tuottaisi todennäköisesti samankaltaisen tuloksen kuin tässä tutkimustyössä saatiin aikaiseksi. Kaikki teoriataustan lähdemateriaalit painottivat samaa prosessimaista lähestymistä riskienhallinnassa. Merkittäviä eroja kirjallisuuden, käytäntö-

jen ja asiantuntijahaastattelujen välillä ei syntynyt. Lähdemateriaalit tuntuivat täydentävän toisiaan eikä varsinaisia ristiriitoja syntynyt. Tämä antaa kuvan, että riskienhallinnan parhaasta toimintamalleista on varsin yhtenäinen näkemys vallalla. Tämä myös tukee näkemystä siitä, että toistettaessa kehitystehtävän konstruktio olisi varsin samankaltainen kuin nyt kehitetty.

Kehitetty malli pohjautui vahvasti teoriataustaan, jonka synteesi olisi todennäköisesti samankaltainen jos tutkimus tutkimusta toistettaisiin. Tutkijan toiminta organisaation osana ei siten vaikuttaisi merkittävästi lopputulokseen verrattuna siihen jos tutkija olisi ollut ulkopuolinen. Myös testauksen lopputulos ei tämän tulkinnan mukaan eroaisi siten merkittävästi tässä tutkimuksissa päädytyistä tuloksista. Tutkijalla oli vapaus tehdä omia tulkintojaan ja kehittää mallia tutkimuksen pohjalta ilman, että kohdeorganisaatio olisi vahvasti pyrkinyt vaikuttamaan lopputuloksiin.

Tutkimuksen tulosten ja kehitetyn mallin voidaan olettaa olevan luotettavia ja käyttöönotettavissa. Suosituksena on, että tietohallintotoimisto ottaa kehitetyn riskienhallintamallin käyttöön ja omaksuu sen osaksi normaalia toimintamalliaan. Malliin on rakennettu säännöllinen toimivuuden arviointi ja sen pohjalta tehtävä jatkokehitysmahdollisuus. Nämä ominaisuudet auttavat mallia mukautumaan tietohallintotoimiston toiminnan muutoksiin sekä riskienhallinnan kypsyyden kasvun kautta tuleviin muutostarpeisiin. Mitä nopeammin malli otetaan käyttöön, sitä nopeammin luodaan myös riskienhallinnalle myönteinen kulttuuri. Riskienhallintakulttuuri on yksi menestystekijöistä toimivalle riskienhallinnalle.

Prosessimainen toimintatapa mahdollistaa laadun parantamisen riskienhallinnan toteutuksissa, joka heijastuu koko organisaation toimintaan. Tietohallintotoimisto pystyy jo heti käyttöönoton alkuvaiheessa saamaan nopeita etuja ennustettavuuden parantuessa sekä ennakoimaan mahdollisia heikkouksia toiminnassaan ja tarjoamissaan palveluissa. Myös selkeästi määritellyt vastuut mallin toteuttamisesta, seurannasta ja kehittämisestä parantavat toimiston suorituskykyä palveluiden tarjoamisessa. Riskienarviointii sisäänrakennetulla toimintaympäristön analyysi auttaa tunnistamaan kriittisiä järjestelmiä ja riippuvuuksia, joka on taas hyödynnettävissä esimerkiksi jatkuvuuden hallinnassa.

4.3 Jatkokehitys

Tietohallintotoimiston riskienhallinnan malli on elinkaarensa alussa. Mallin vaikutuksia toimiston toimintaan tai riskienhallintaan ei vielä tiedetä. Jatkokehityksenä olisi arvokasta tutkia miten kehitetty malli vaikuttaa toimiston suoritukseen ja miten sitä voisi edelleen kehittää palvelemaan organisaation tarpeita. Tutkimuksessa voi verrata saman organisaation yksikköjä toisiinsa tai eri organisaatioiden samassa tilanteessa olevien yksiköiden

tilannetta. Tilannetta olisi hyvä arvioida riskienhallintakulttuurin kehittymisen ja riskienhallintamallin kehittymisen näkökulmista. Arviointikeinoina voi käyttää riskienhallinnan mittaustulosten vaikutuksia kehitykseen ja tehdä haastattelututkimus riskienhallintaan osallistuneiden parissa. Näiden perusteella havaituista mahdollisista eroista voi arvioida riskienhallinnan onnistumisia ja tehdä muutosehdotuksia nykyiseen toimintamalliin. Tällä tavalla on mahdollista saada laajempi näkökulma kehittymiseen kuin vain oman yksikön toimintaa arvioimalla.

Jatkokehitysmahdollisuuden tarjoaa myös mallin laajentaminen organisaation kokonaisvaltaisen riskienhallinnan malliksi. Koko organisaation riskienhallinnassa tulisi panostaa raportointiin ja seurantaan erityisesti. Yksikkötasoille voidaan antaa mallia riskienhallinnan toteuttamiseen, mutta organisaatioyksiköiden riskienhallintamalli erityisesti riskienarvioinnin ja riskinottokyvyn osalta vaihtelee. Olisi tutkittava voitaisiinko yleistä riskienhallintamallia valmiiksi muuntaa yksikkökohtaiseksi ennen sen käyttöönottoa, jos tiedetään organisaatioyksikön toimintatapa ja onko tällaisesta muuntamisesta hyötyä riskienhallinnan tehokkuuteen. Myös riskienarvioinnin tulosten tulkintaa olisi tutkittava. Yksikkökohtaisten tulosten erojen huomioiminen seurannan kokonaisuudessa ja silti säilyttää yhdenmukainen tapa tunnistaa riskit, joita tulisi organisaatiotasolla seurata, vaatisi erillisiä toimintamalleja tulosten tulkintaan. Riskienhallinnan tuloksia ei suoraan voi verrata toisiinsa yksikköjen välillä erilaisista tarpeista ja toimintaympäristöstä sekä tuotantomallista johtuen. Yksiköissä tunnetaan oman toiminnan riskit ja voidaanko niitä ylhäältä käsin seurata ja vaikuttaa niihin. Toisaalta onko mahdollista tunnistaa yksikkötasolla riskejä jotka vaikuttavat koko organisaation toimintaan esimerkiksi riippuvuuksien kautta. Näihin kysymyksiin olisi jatkotutkimuksissa hyvä löytää vastauksia. Koko organisaation riskienhallinnan tuloksista pitäisi pystyä jalostamaan tietoa esimerkiksi yhteisistä tekijöistä, jotka vaikuttavat useammassa yksikössä. Jalostetusta tiedosta olisi erityisen kiinnostavaa tutkia mahdollisia piiloriskejä. Piiloriskit voivat aiheutua riippuvuuksista eri yksiköiden toiminnasta, joita ei välttämättä tunnisteta yksikkötasoisissa riskiarvioinneissa. Piiloriskit pitäisi myös pystyä hallitsemaan ja niille pitäisi pystyä löytämään omistaja. Koko organisaation kattava riskienhallintamallin kehittäminen tuo useita kiinnostavia jatkokehityskohteita esille.

Lähteet

Arnell, J. 2010. Viestintäviraston kokonaisvaltaisen riskienhallinnan kehittäminen. Opinnäytetyö Ylempi AMK. Laurea Leppävaara. Espoo. Luettavissa: http://urn.fi/URN:NBN:fi:amk-201002262580. Luettu 8.2.2015

COSO 2004a. The Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management – Integrated Framework. AICPA. New York.

COSO 2004b. The Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management – Integrated Framework Application Techniques. AICPA. New York.

Eduskunnan kanslian ohjesääntö 13.2.1987/320

Eduskunta 2015a. Tietoa eduskunnasta. Luettavissa: https://www.eduskunta.fi/FI/tietoaeduskunnasta/Sivut/default.aspx. Luettu: 27.4.2015.

Eduskunta 2015b. Eduskunnan hallinto. Luettavissa: https://www.eduskunta.fi/FI/tietoaeduskunnasta/Organisaatio/Sivut/default.aspx. Luettu: 27.4..2015.

Eduskunta 2013. Eduskunnan tietohallintolinjaus 2013-2016.

Elinkeinoelämän keskusliitto 2014. Yritysturvallisuus. Luettavissa: http://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/. Luettu: 25.11.2014

Filatov, K. 18.12.2014. Tietoturvapäällikkö. Elisa Appelsiini Oy. Haastattelu. Helsinki

Hallikas, J., Karvonen, I., Lehtinen, E., Ojala, M., Pulkkinen, U., Tuominen, M., Uusi-Rauva, E. & Virolainen, V-M. 2001.Riskienhallinta yhteistyöverkostossa. MET-julkaisuja nro 14/2001. Metalliteollisuuden Kustannus Oy. Helsinki.

Helislahti, K. 24.22015. Riskienhallintajohtaja. Jyväskylän Energia. Haastattelu. Helsinki

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15. uudistettu painos. Tammi. Helsinki.

Holmberg, J. 7.11.2013. Finanssineuvos Riskienhallinta ja sisäinen valvonta johtamisen työkaluina. Valtiovarainministeriö / valtiovarain controller –toiminto. Seminaariesitys. Helsinki. Luettavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20131010Valtio/03_Vahti_riskienhallintaseminaari_07112013.pdf.

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. 2013. Johda riskejä – käytännön opas yrityksen riskienhallintaan. Finanssi- ja vakuutuskustannus Oy FINVA. Helsinki.

Järvinen, P. & Järvinen, A. 2004. Tutkimustyön metodeista. Opinpajan kirja. Tampere.

Kahra, H., Kuusela, H. & Kanto, A. 2005. Taloudellisen riskin hallinta. Teoksessa Kuusela, H. & Ollikainen, R. (toim.) Riskit ja riskienhallinta, s. 72-87. Tampere University Press. Tampere.

Kasanen, E., Lukka, K. & Siitonen, A. 1991. Konstruktiivinen ote liiketaloustieteessä. Liiketaloudellinen aikakauskirja, 40, 3, s. 301-329.

Kuusela, H. & Ollikainen, R. 2005. Riskit ja riskienhallinta-ajattelu. Teoksessa Kuusela, H. & Ollikainen, R. (toim.) Riskit ja riskienhallinta, s. 15-54. Tampere University Press. Tampere.

Leino, M., Steiner, M-L. & Wahlroos 2005. Corporate Governance ja riskienhallinta. Teoksessa Kuusela, H. & Ollikainen, R. (toim.) Riskit ja riskienhallinta, s. 123-147. Tampere University Press. Tampere.

Lukka, K. 2001. Konstruktiivinen tutkimusote. Luettavissa: https://metodix.wordpress.com/2014/05/19/lukka-konstruktiivinen-tutkimusote/. Luettu: 9.3.2015.

Marchetti, A. 2012. Enterprise Risk Management Best Practices: From Assessment to Ongoing Compliance. John Wiley & Sons, Inc.. Hoboken, New Jersey. USA.

Murtonen, M. 2003. Riskien arviointi työpaikalla. Työkirja. Sosiaali- ja terveysministeriö, työsuojeluosasto. Tampere.

Ojasalo, K., Moilanen, T. & Ritalahti J.2014. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. Sanoma Pro Oy. Helsinki.

Pietarinen, J. 5.2.2015. Riskienhallintajohtaja. Valtiokonttori. Haastattelu. Helsinki

PricewaterhouseCoopers Oy 2004a. 7th Annual Global CEO Survey. Managing Risk: An assessment of CEO Preparedness.

PricewaterhouseCoopers Oy 2004b. Enterprise Risk Management (ERM) Benchmarking Survey 2004.

Rousku, K. 10.2.2015. Riskienhallintajohtaja. Valtion tieto- ja viestintätekniikkakeskus Valtori. Sähköposti

Scherf, A. 2012. Riskienhallinta osaksi eduskunnan kanslian johtamista. Opinnäytetyö Ylempi AMK. Laurea. Espoo

SFS-ISO 2011a. SFS-ISO 31000 RISKIENHALLINTA. PERIAATTEET JA OHJEET Risk management. Principles and guidelines. Teoksessa SFS-käsikirja 828 Riskienhallinta ja toimitusketjun turvallisuuden hallintajärjestelmät. s. 213 -264 (1-52). SFS. Helsinki

SFS-ISO 2011b. SFS-OPAS 73 RISKIENHALLINTA. SANASTO Risk management. Vocabulary. Teoksessa SFS-käsikirja 828 Riskienhallinta ja toimitusketjun turvallisuuden hallintajärjestestelmät. s. 265-283 (1-19). SFS. Helsinki

Simula, T. 9.1.2015. Tietoturvapäällikkö. Valtion tieto- ja viestintätekniikkakeskus Valtori. Sähköposti

SRHY 2015. Suomen riskienhallintayhdistys SRHY-riskienhallinta. Luettavissa: http://pk-rh.fi/. Luettu: 30.1.2015

Suominen, A. 1994. Yritysten riskienhallintakäyttäytyminen ja vakuutuspolitiikka liikkeenjohdon toiminnan osana. Turun kauppakorkeakoulun julkaisuja. Turku

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

Turvallisuus- ja puolustusasiain komitean sihteeristö 2013. Suomen kyberturvallisuusstrategia Valtioneuvoston periaatepäätös 24.1.2013. Turvallisuus- ja puolustusasiain komitean sihteeristö. Helsinki.

Turvallisuuskomitea 2014. Ministeriöiden kyberturvallisuustehtävät. Luettavissa: http://www.turvallisuuskomitea.fi/index.php/fi/materiaalia/julkaisut/ministerioiden-kyberturvallisuustehtavat. Luettu 23.11.2014

VAHTI 2003. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Valtiovaraiministeriö. Helsinki. Luettavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53828/53827_fi.pdf. Luettu: 24.1.2015

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681. Luettavissa: http://www.finlex.fi/fi/laki/ajantasa/2010/20100681. Luettu: 23.11.2014

Virolainen, V-M. & Hallikas, H. 2005. Toimittajaverkostoihin liittyvä riskienhallinta. Teoksessa Kuusela, H. & Ollikainen, R. (toim.) Riskit ja riskienhallinta, s. 218-241. Tampere University Press. Tampere..

VTT 2007. Keskeisten termien määritelmiä. Luettavissa: http://www.vtt.fi/proj/riskianalyysit/riskianalyysit_maaritelmia.jsp. Luettu: 22.11.2014

Liitteet

Liite 1. Haastatteluteemat

Johdanto teemaan keskustellen

- Toiminnan vaatimusten ja yleisten linjausten mukainen riskienhallinta
- Riskienhallinta käytännössä toiminnan eri tasoilla
- Riskienhallinnan ulottaminen koko organisaatioon

Riskienhallinnan nykytila

- Mitä riskienhallinnalla nyt ymmärretään?
- Mitä riskienhallinnan kautta pitäisi saada tiedoksi?

Riskienhallinta ja mittarit

- Mitä ja miten tulisi mitata (raportointi: mitä, kuka, kenelle, kuinka usein, miten jatkoseuranta, kuka valvoo…)?
- Mitä odotuksia on rajoille / reagointipisteille, joiden jälkeen tulisi puuttua asioihin?

Riskienhallinta tietohallinnossa / palveluntarjoajalle

- Mitä erityispiirteitä tietohallintoon liittyy?
- Muut erityiset riskienhallintaan liittyvät asiat?

Liite 2. Yhteenvetotaulukko tietohallintotoimiston haastatteluista

Teema	Haastateltava 1	Haastateltava 2	Haastateltava 3	Yhteenveto	TH-linjaukset	Jatkotoimet riskienhallinnalle
Nykytila ja tavoitetila						
Nykytila	- Teoreettista - Ei ole prosesseissa - Ei kata asiantuntija-tasoa	- Ei ole kattavaa - Jää keskeneräiseksi (vain arviointi) - Reaktiivista - Toimittajariippuvuus	- Tietoriskit ulkoistettu tietohallinnolle - Riskien hallinta jää tekemättä (aika ja osaaminen voi puuttua) - Toimittajariippuvuus - Testaus rajallista	- Toimittajariippuvuutta liikaa - Kattavuus puutteellista → ei ole määrämuotoista tekemistä - Ajanpuute → vain reaktiivisuus - Riskien hallinta jää tekemättä	Kansanedustajien ja eduskunnan työn nykyistä parempi tukeminen tietotekniikalla ja edellytysten luominen tietojohtamiseen. Tavoitteisiin liittyy olennaisesti sähköisen asioinnin ja käsittelyn sekä tietoliikenneverkon aiempaa monimuotoisemman käytön edistäminen.	Nykyinen riskienhallinta ei toimi kattavasti ja toimissa on liikaa vaihtelua tai niiden toteuttamisesta puuttuu yhtenäinen oma arviointimalli.
Tavoitetila	- Prosessitasolle yllettävä - Proaktiivisuus - Katettava sekä ohjaamisen että tekemisen tasot	- Selkeä prosessi - Tunnetuimmat riskit kartoitettava ja käsittelyn mallinnus - Hallinnan malli	- Palveluhallinta (liiketoimintanäkökulma) ○ Jatkuvuus ○ Kannattavuus ○ Tarpeeseen vastaaminen - Projektinhallintaan liittyvät riskit kattavasti	- Prosessi riskien hallinnalle → riskienhallinnan malli - Kattavuus palvelutuotannon ja projektinhallinnan riskejä koskien - Proaktiivisuutta mallien avulla		Riskienhallinnan periaatteet on luotava. Riskien arviointiprosessi on kuvattava.

Teema	Haastateltava 1	Haastateltava 2	Haastateltava 3	Yhteenveto	TH-linjaukset	Jatkotoimet riskienhallinnalle
Mittarit						
Raportointi	- Tavoitteellista - Säännöllistä	- Järjestelmät vuosikellomaisesti - Kanslia vuosittain (vuosikello myös) - Projektit yhtenäisesti (sama malli)	- Yleiset riskiluokat ○Ulkoiset riskit ○Kustannusriskit ○Aikatauluriskit ○Teknologiariskit	- Säännöllisyyttä lisättävä (vuosikellomainen käsittely) - Vertailukelpoisuus eri riskien välisesti riskiluokkien sisällä (kriittisyydet)	Eduskunnan tietohallinto järjestää ja tuottaa asiakkailleen eduskunnan toiminnan edellyttämät tieto- ja viestintätekniikan palvelut laadukkaasti, tehokkaasti ja taloudellisesti. Palveluja kehitetään innovatiivisesti valituilla alueilla kehityksen kärjessä.	Riskienhallintaan vaaditaan yhtenäinen säännöllinen raportointimalli, joka perustuu riskienhallinnan periaatteisiin.
Reagointipisteet	- Priorisointi - Proaktiivisuus	- Etukäteismallit - Proaktiivisuus - Riippuvuudet useista tekijöistä/osapuolista (monitoimittajatoteutus)	- Kattavuutta enemmän (tarkistuspisteitä enemmän) - Käyttötapauksia myös riskien näkökulmasta	- Proaktiivisuutta korostettava - Malli ja vertailukelpoisuuden mahdollistavat mittarit/taulukot - Monitoimittajuuteen liittyvien riskien tunnistaminen		Riskienarviointiprosessiin on luotava reagointia helpottamaan case-tyyppisiä esimerkkejä tyypillisimmistä riskeistä ja niiden merkityksestä (todennäköisyys ja vaikutus).

Teema	Haastateltava 1	Haastateltava 2	Haastateltava 3	Yhteenveto	TH-linjaukset	Jatkotoimet riskienhallinnalle
Tietohallinnon erityistarpeet						
Tietohallinnon erityistarpeet	- Huoltokatkojen suunnittelu ja ajoitus (koko talon huomioon ottaminen) - Muutoshallinta kattavaksi	- Kokonaisarkkitehtuuri tarvitaan - Pystyttävä irtautumaan toimittajariippuvuudesta (ettei kaikessa mennä vain toimittajan ehdoilla)	- Yhteinen malli ja menetelmä riskien hallintaan	- Riskienhallinnan yhteinen ja yhtenäinen malli - Palveluiden riskienhallinnan malli huomioi koko talon	Keskeisenä tavoitteena on myös tietohallinnon organisaation ja toiminnan kehittäminen. Toiminnan kehittämisen yksi merkittävä alue on projektityöskentelyn kehittäminen ja oman projektityömallin käyttöönotto.	Riskienhallinta on toteutettava yhtenäisten riskienhallinnan periaatteiden mukaan. Tietohallinnossa otetaan käyttöön ja sovelletaan yhtenäisiä periaatteita. Tietojärjestelmien hankintaan ja niihin liittyvissä projekteissa riskejä on arvioitava laajemmin kuin vain tietohallinnon riskeinä.
Muut riskienhallinnan tarpeet	- Projektien riskienhallinta ja hankintojen riskienhallinta	- Eduskunnan erityispiirre yhteiskunnassa (mm. julkisuusnäkökulma)	- Projektinhallinta - Tasojen mukaan arviointi o Organisatorinen o Strateginen - Hankinnat (vrt. toimittaja- tai palvelukohtaisuus)	- Projektien riskienhallinnan kattavuus - Eduskunnan erityispiirteet yhteiskunnassa (mm. julkisuusnäkökulma)	Tavoitteisiin liittyy olennaisesti sähköisen asioinnin ja käsittelyn sekä tietoliikenneverkon aiempaa monimuotoisemman käytön edistäminen.	

Liite 3. Eduskunnan tietohallintotoimiston riskienhallinnan periaatteet

Riskienhallinnan periaatteet

Päivämäärä	Versio	Muuttaja	Muutos / toimenpiteet	Tila
13.2.2015	0.9	Antti Laulajainen	Dokumentin valmistelu hyväksyttäväksi.	luonnos
24.3.2015	1.0	Antti Laulajainen	Tarkennettu vastuut ja hyväksytty toimiston johtoryhmässä	hyväksytty

Sisällysluettelo:

(POISTETTU LIITTEESTÄ)

1 Johdanto

Näillä riskienhallinnan periaatteilla edesautetaan eduskunnan tietohallintotoimiston kykyä tuottaa palveluita eduskunnan ydintoimintojen ja keskeisten tehtävien tueksi. Riskienhallinnan periaatteet auttavat osaltaan eduskunnan tietohallintotoimistoa sen strategisissa tehtävissä.

2 Riskienhallinnan tavoitteet

Eduskunnan tietohallintotoimiston riskienhallinnan tavoitteena on eduskunnan toimintaa häiritsevien riskien ennaltaehkäiseminen. Riskienhallinnan tavoitteisiin kuuluu toimintaan kohdistuvien uhkien tunnistaminen ja riskien hallitseminen.

Eduskunnan tietohallintotoimiston riskienhallinnan tavoitteina on suunnitelmallisesti huolehtia riskien tunnistamisesta, analysoinnista, arvioinnista sekä käsittelystä eduskunnan tietohallintotoimiston toiminnassa, järjestelmähankkeissa sekä niihin liittyvässä projektinhallinnassa ja kumppanitoiminnassa.

3 Riskienhallinnan periaatteet

Eduskunnan tietohallintotoimiston riskienhallinta toteutetaan yhteneväisesti eduskunnan kanslian yleisten riskienhallintaperiaatteiden mukaisesti.

Riskienhallinta on säännöllistä, ennakoivaa, järjestelmällistä, jäsenneltyä ja ajantasaista sekä tilannekohtaisesti toiminnan kriittisyyden huomioon ottavaa.

Riskienhallinta on osa eduskunnan tietohallintotoimiston toimintaa ja päätöksentekoa sekä toiminnan kehittämistä. Riskienhallinta kattaa muun toiminnan ohella myös palvelutuotannon, järjestelmähankinnat ja niihin liittyvät projektit.

Riskienhallintaan osallistuminen kuuluu kaikille eduskunnan tietohallintotoimiston tehtävissä toimiville työntekijöille mukaan lukien tietohallintotoimistolle töitä tekevät ulkopuoliset henkilöt.

Riskienhallintaprosessi toteutetaan palvelutuotannossa sopimusten mukaisessa laadunhallinnassa sekä hankkeiden projektisuunnitelmissa.

4 Riskienhallinnan roolit ja vastuut

Riskienhallinnasta kokonaisvaltaisesti vastaa eduskunnan turvallisuusjohtaja.

Eduskunnan tietohallintotoimiston riskienhallinnasta vastaa tietohallintopäällikkö.

Riskienhallinnan seurannasta ja kehittämisestä vastaa tietoturvapäällikkö.

Tietohallintotoimiston organisaatiotasoisesta riskienhallinnasta vastaa tietohallintotoimiston johtoryhmä.

Palvelutuotantoon ja hankkeisiin liittyvästä riskienhallinnan ohjauksesta ja seurannasta vastaavat atk-päällikkö ja tietojärjestelmäpäällikkö. Riskienhallinnasta käytännön tasolla vastaavat palvelupäälliköt, suunnittelijat, asiantuntijat ja hankkeiden projektipäälliköt.

5 Riskienhallinnan toteutusprosessi

Riskienhallinta toteutetaan riskienarviointiprosessissa riskienhallinnan periaatteiden mukaisesti. Riskienhallinnan periaatteet ja riskien arviointiprosessissa käytettävät riskirajat arvioidaan vuosittain.

Riskienarviointi prosessi kattaa riskien tunnistamisen, analysoinnin, merkitysten arvioinnin sekä riskien käsittelyn. Riskien tunnistamisen yhteydessä riskit kartoitetaan eli tunnistetaan ja kuvataan. Riskianalyysissä tarkastellaan riskien luonnetta ja määritellään riskien taso arvioimalla todennäköisyys ja vaikutus. Riskien merkityksen arvioinnissa arvioidaan onko riski tai jäännösriski hyväksyttävällä tai siedettävällä tasolla. Riskien käsittelyssä riskejä poistetaan, pienennetään, siirretään tai päätetään sietää riski.

Riskien sieto ja käsittely:

- Punaisia eli korkeita riskejä ei siedetä eikä niitä sallita. Kaikille punaisille eli korkeille riskeille tehdään suunnitelma niiden poistamiseksi, pienentämiseksi tai siirtämiseksi.

- Oranssien eli kohtalaisten riskien osalta selvitetään voidaanko riski poistaa tai voidaanko riskiä pienentää. Kaikki oranssit eli kohtalaiset riskit, joita ei voi poistaa tai riskin suuruutta ei voida pienentää riittävästi, kuvataan ja niitä seurataan aktiivisesti.

- Vihreät eli alhaiset riskit kuvataan ja niiden merkitystä arvioidaan tarvittaessa. Pääsääntöisesti vihreille eli alhaisille riskeille ei tehdä poisto- tai pienentämistoimenpiteitä.

Riskienhallinnassa tulee ottaa lisäksi huomioon se, että pienten riskien yhteisvaikutus voi olla pahimmillaan suurempi kuin yksit-

täisten riskien suuruus (ns. kerrannaisvaikutus tai riippuvuuksista aiheutuvat vaikutukset).

Riskienarvioinnissa arvioinnin kohteen kriittisyys tulee ottaa huomioon ja tarvittaessa reagoidaan myös alemman tason riskeihin laatimalla niille hallintatoimenpiteet.

6 Ohjeistus ja koulutus

Riskienhallinnan ohjeet löytyvät riskienhallinnan käsikirjassa, joka käydään läpi vuosittain. Riskienhallinnan käsikirjaa päivitetään tarvittavilta osin vuosittaisen läpikäynnin perusteella.

Riskienhallinnan periaatteet perehdytetään henkilöstölle.

7 Riskienhallinnan periaatteiden ja prosessien toimivuuden seuranta ja valvonta

Riskienhallinnan periaatteet käydään vuosittain läpi. Riskienhallinnan prosessin toimivuus ja kehitystarpeet kartoitetaan ja päivitetään riskienhallinnan periaatteiden läpikäynnin yhteydessä.

Riskienhallinnan prosessin toimivuutta seurataan ja mitataan.

8 Tiedottaminen

Riskienhallinnan periaatteiden päivityksistä ja muutoksista tiedotetaan henkilöstölle ja sopimuskumppaneille sekä sidosryhmille.

9 Riskienhallinnan käsitteet

Riskienhallinta luo toiminnalle lisäarvoa uhkien tunnistamisen ja riskien käsittelyn kautta riskejä pienentäen tai poistaen.

Riskeillä tarkoitetaan toimintaan liittyviä epävarmuuden ja uhkien vaikutuksia tavoitteisiin niin myönteisesti kuin kielteisesti.

Riskienhallinnan periaatteet sisältävät riskienhallinnan suunnittelun, toteutuksen, raportoinnin ja kehittämisen.

Riskienhallintaprosessi on riskienhallinnan periaatteiden, menettelyjen ja käytäntöjen järjestelmällinen soveltaminen riskien tunnistamiseen, analysointiin, arviointiin, käsittelyyn, seurantaan ja katselmointiin.

Riskien arviointi on prosessi, joka kattaa riskien tunnistamisen, analysoinnin, merkitysten arvioinnin.

Riskien tunnistaminen on prosessi, jossa riskit havaitaan ja kuvataan.

Riskianalyysi on prosessi, jossa pyritään ymmärtämään riskin luonne ja määrittelemään riskitaso.

Riskien merkityksen arviointi on prosessi, jossa riskianalyysin tuloksia verrataan riskikriteereihin ja arvioidaan, onko riski tai sen suuruus hyväksyttävä tai siedettävä.

Riskien hallintakeinot ovat riskeihin vaikuttavia ja riskejä muuttavia toimenpiteitä.

Jäännösriskit ovat jäljellejääviä riskejä, joita ei voida tai haluta poistaa. Niitä voidaan myös kutsua hyväksytyiksi riskeiksi tai riskeiksi, joita ollaan valmiita ottamaan.

Liite 4. Eduskunnan tietohallintotoimiston riskienhallinnan puitteet

Riskienhallinnan puitteet

Päivämäärä	Versio	Muuttaja	Muutos / toimenpiteet	Tila
13.2.2015	0.9	Antti Laulajainen	Dokumentin valmistelu hyväksyttäväksi.	luonnos
24.3.2015	1.0	Antti Laulajainen	Tietohallintotoimiston johtoryhmän hyväksyntä	hyväksytty

Sisällysluettelo:

(POISTETTU LIITTEESTÄ)

1 Johdanto

Tällä riskienhallinnan puitteiden kuvauksella edesautetaan eduskunnan tietohallintotoimiston kykyä ja mahdollisuuksia ohjata toimintaansa liittyvien riskien hallintaa. Riskienhallinta viedään osaksi organisaation toimintaa ja johtamiskulttuuria. Riskienhallintaan kuuluu riskienhallinnan puitteiden suunnittelu, riskienhallinnan toteuttaminen, riskienhallinnan puitteiden seuranta ja katselmointi sekä riskienhallinnan puitteiden jatkuva kehittäminen. Riskienhallinta kattaa vastuiden ja valtuuksien määrittelyn, riskienhallintaan käytettävien resurssien varaamisen sekä mittareiden ja tavoitteiden määrittelyn.

2 Valtuudet ja sitoutuminen

Eduskunnan kansliatoimikunta vahvistaa riskienhallinnan periaatteet turvallisuusjohtajan esityksestä. Eduskunnan turvallisuusjohtaja huolehtii koko eduskunnan kattavista riskienhallintaperiaatteista sekä niiden soveltamisesta eduskunnan kansliatoimikunnan päätösten mukaisesti.

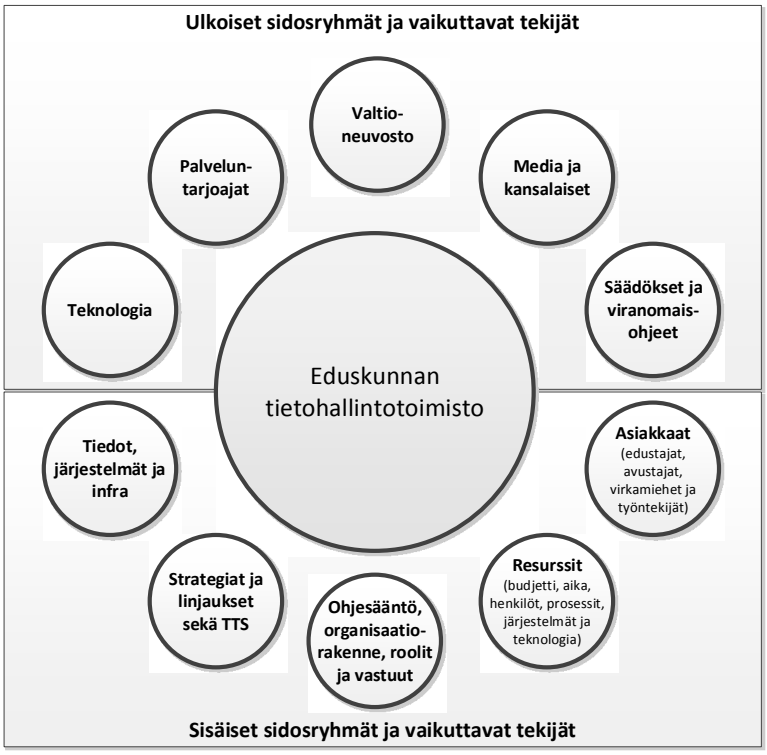
Eduskunnan tietohallintotoimiston päällikkö huolehtii riskienhallintaperiaatteiden laadituttamisesta sekä niiden esittelystä hallintojohtajalle.

Eduskunnan tietohallintotoimiston johtoryhmä päättää riskienhallintaperiaatteiden linjauksista sekä riskienhallintaan käytettävistä resursseista.

Eduskunnan tietoturvapäällikkö vastaa eduskunnan tietohallintotoimiston riskienhallintaperiaatteiden ja niihin liittyvien mittareiden ja tavoitteiden laatimisesta ja kehittämisestä sekä käytäntöön viemisestä.

3 Riskienhallinnan puitteiden suunnittelu

3.1 Toimintaympäristö



Eduskunnan tietohallintotoimiston toimintaympäristöön kuuluvat ulkoiset sidosryhmät ovat:

- Säädökset ja viranomaisohjeet, jotka otetaan huomioon eduskunnan toiminnassa
- Media ja kansalaiset, joiden tiedusteluihin vastataan ja tarvittaessa tarjotaan informaatiota sekä medialle tarjottavat palvelut
- Valtioneuvosto ministeriöineen
- Palveluntarjoajat, joita ovat mm. ulkoistuskumppaneita tai sovellustoimittajia
- Teknologia ja tekninen kehitys, uudet teknologiat ja tietohallinnon tarpeisiin tai käyttöön mahdollisesti soveltuvat palvelut ja ratkaisut

Eduskunnan tietohallintotoimiston toimintaympäristöön kuuluvat sisäiset sidosryhmät ovat:

- Asiakkaat, joihin kuuluvat kansanedustajat sekä näiden avustajat, virkamiehet ja eduskunnan muut työntekijät
- Resurssit, joiden avulla palveluita tuotetaan ja kehitetään
- Eduskunnan kanslian ohjesääntö, joka ohjaa eduskunnan tietohallintotoimiston toimintaa ja vastuita

- Strategiat ja linjaukset sekä talouden ja toiminnan suunnittelu, joissa kuvataan tarkemmin toiminnan tavoitteet sekä tehtävät

- Tiedot, järjestelmät ja infra, joilla tietohallintotoimisto tuottaa eduskunnassa tarvittavat ICT-palvelut

3.2 Riskienhallintaperiaatteiden määrittely

Eduskunnan tietohallintotoimiston riskienhallinnan periaatteet perustuvat eduskunnan kanslian hyväksymiin ja päättämiin riskienhallinnan periaatteisiin, jotka on muodostettu eduskunnan kanslian tavoitteiden ja toimintaperiaatteiden mukaisesti.

Eduskunnan tietohallintotoimiston riskienhallinnan periaatteet on julkaistu ja niissä on kuvattu riskienhallintaan liittyvät vastuut ja velvollisuudet.

Eduskunnan tietohallintotoimiston riskienhallinnan periaatteita katselmoidaan vuosittain ja päivitetään tarvittavilta osin.

3.3 Vastuut ja velvollisuudet

Eduskunnan tietohallintotoimiston riskeistä kokonaisvastuu kuuluu tietohallintopäällikölle. Riskien omistajina toimivat vastuualueillaan ATK-päällikkö ja tietojärjestelmäpäällikkö, joille valtuudet riskien käsittelyyn antaa tietohallintopäällikkö.

Riskienhallintaprosessissa riskien käsittelystä vastaavat projektipäälliköt, sovellusasiantuntijat ja tekniset asiantuntijat sekä sovellussuunnittelijat ja tekniset suunnittelijat, joille valtuudet riskien käsittelyyn antavat ATK-päällikkö ja tietojärjestelmäpäällikkö.

Riskien hallinnan puitteiden kehittämisestä, toteuttamisesta ja ylläpidosta vastaa eduskunnan tietoturvapäällikkö.

Riskienhallinnan vastuut kuvataan tarkemmin erillisessä taulukossa (RACI-taulukko).

3.4 Riskienhallinta eduskunnan tietohallintotoimistossa

Riskienhallinta toteutetaan osana toiminnan ja talouden suunnittelua sekä palveluiden ja projektien hallintaa. Riskienhallintaa ohjataan riskienhallinnan käsikirjan ja riskisalkun avulla.

Resursointitarpeet ja tarvittavien resurssien varaaminen sekä resurssien osaamisen kehittäminen otetaan huomioon toiminnan ja talouden suunnittelussa.

Riskienhallinnan kehittäminen toteutetaan tietoturvan vuosikellon mukaisesti.

3.5 Riskienhallinnan puitteista viestintä

Riskienhallinnan puitteiden tärkeimmistä osista ja muutoksista tiedotetaan koko eduskunnan tietohallintotoimiston henkilöstölle.

4 Riskienhallinnan puitteiden ja riskienhallintaprosessin toteuttaminen

Riskienhallinnan puitteet toteutetaan riskienhallinnan periaatteiden ja tietoturvan vuosikellon mukaisesti.

Riskienhallinnan prosessi on kuvattu erikseen. Riskienhallinnan prosessissa noudatetaan riskienhallinnan käsikirjaa.

5 Riskienhallinnan puitteiden katselmointi ja mittarit

Riskienhallinnan puitteiden tehokkuutta ja toimivuutta arvioidaan jatkuvasti. Riskienhallinnan puitteet katselmoidaan vuosittain. Katselmoinnin yhteydessä arvioidaan riskienhallinnan prosessin onnistumista ja vaikutuksia puitteisiin.

Riskienhallinnan puitteiden tehokkuuden mittareita ovat:

- riskienhallinnan toteutumiset (riskienhallinnan käsikirja)
    - riskienhallinnan käsikirjan kannalta suunnitelmallisuuden (riskiarviointien) toteutuminen vuositasolla
- riskien käsittely (riskisalkku)
    - riskeille tehtävät toimenpiteet
        - toimet käynnistämättä/käynnistetty/toteutettu
        - aika (pitkittyykö, pysytäänkö tavoitteissa)
    - toimenpiteiden vaikutukset
- riskienhallinnan dokumentaation ajantasaisuus
    - katselmoinnit ja päivitystarpeiden tunnistaminen
    - päivitysten/muutosten toteuttaminen
- riskienhallinnan koulutukset/perehdytykset
    - vuosittainen valmennus/ tietoisuuden kehittäminen
    - muutoksiin perehdyttäminen

Riskienhallintaprosessin toimivuutta seurataan ja tulokset arvioidaan. Tuloksia käytetään riskienhallinnan puitteiden katselmoinnin lähtötietoina.

6 Riskienhallinnan puitteiden kehittäminen

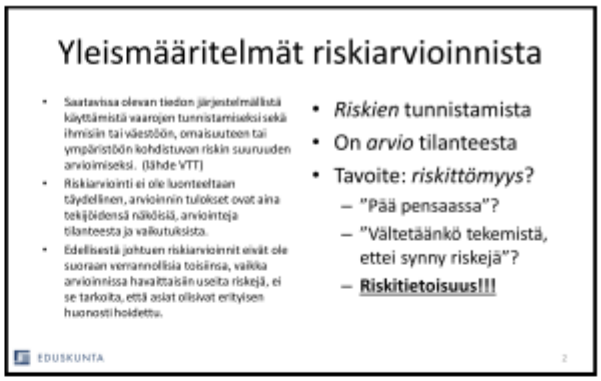
Eduskunnan tietoturvapäällikkö johtaa riskienhallinnan puitteiden kehittämistä ja arvioi katselmoinnin kautta saatuja tuloksia ja havaintoja laatien niiden perusteella riskienhallinnan puitteiden kehitystoimet ja kehitysehdotukset. Toteutettavaksi ehdotetuista kehitystoimista päätöksen tekee eduskunnan tietohallintotoimiston päällikkö.

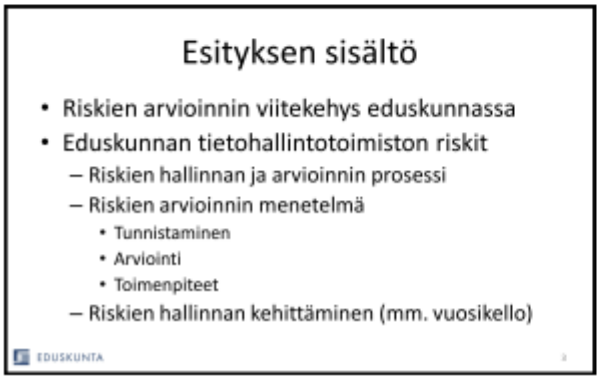
Liite 5. Eduskunnan tietohallintotoimiston riskienhallinnan vastuutaulukko

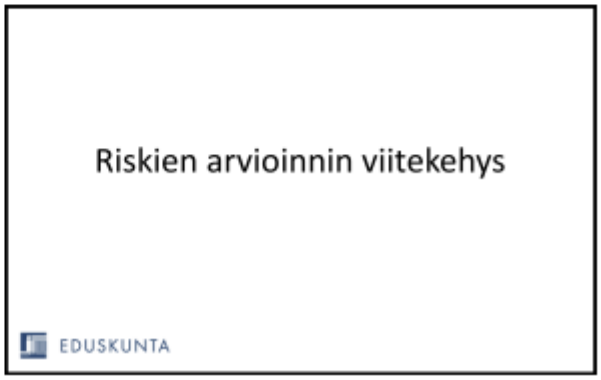
	Eduskunnan turvallisuus-johtaja	Eduskunnan hallintojohtaja	Tietohallinto-päällikkö	Eduskunnan tietohallinto-toimiston johtoryhmä	Tietoturva-päällikkö	ATK-päällikkö	Tietojärjestelmä-päällikkö	Projektipäälli-köt,palvelupäällik öt, asiantun-tijat ja suunnit-telijat	Palvelun-tarjoajat
Eduskunnan tietohallintotoimiston riskienhallinnan periaatteet	I, C	I	A, C	I	R	C	C	I	I
Eduskunnan tietohallintotoimiston riskienhallinnan puitteet -dokumentti	I, C	I	A	I	R	C	C	I	
Puitteiden suunnittelu									
Riskienhallinnan toteuttaminen									
Puitteiden seuranta ja katselmointi									
Puitteiden jatkuva kehittäminen									
Eduskunnan tietohallintotoimiston riskisalkku	I	I	A	I	R	R	R	I	
Eduskunnan tietohallintotoimiston riskienhallinnan prosessin kuvaus	I, C	I	A	I	R	C	C	I	I
Eduskunnan tietohallintotoimiston riskienhallinnan käsikirja	I, C	I	A	I	R	C	C	I	I
Eduskunnan tietohallintotoimiston palveluiden riskienhallinnan prosessi käytännössä									

Toimintaympäristön määritteleminen					C	A	A	R	I, C
Riskienarviointiprosessi					C	A	A	R	R
Riskien tunnistaminen					C	A	A	R	R
Riskianalyysi					C	A	A	R	R
Riskien merkityksen arviointi					C	A	A	R	R
Riskien käsittely			I, C		C	A	A	R	I, C
Seuranta ja katselmointi			I		A	R	R	C	R
Viestintä ja tiedonvaihto			I		A	R	R	C	R
Eduskunnan tietohallintotoimiston organisaation riskienhallinnan prosessi käytännössä									
Toimintaympäristön määritteleminen			A		R	R	R	I	
Riskienarviointiprosessi			A		R	R	R	I	
Riskien tunnistaminen			A		R	R	R	I	
Riskianalyysi			A		R	R	R	I	
Riskien merkityksen arviointi			A		R	R	R	I	
Riskien käsittely			A		R	R	R	I	
Seuranta ja katselmointi			A		R	R	R	I	
Viestintä ja tiedonvaihto			A		R	R	R	I	
R = responsible (vastuullinen), R-henkilö suorittaa annetun tehtävän tai on osa suoritustiimiä, jokaisella tehtävällä on ainakin yksi R-henkilö									
A = accountable (vastuussa oleva), A-henkilö valvoo, että tehtävä tulee valmiiksi, jokaisella tehtävällä on vain yksi A-henkilö									
C = consulted (neuvoja), C-henkilöltä voidaan kysyä ohjeita ja neuvoja, jokaisella tehtävällä voi olla nolla – rajaton määrä C-henkilöä									
I = informed (tiedotettava), I-henkilöä tiedotetaan tehtävän suorittamisesta, jokaisella tehtävällä voi olla nolla – rajaton määrä I-henkilöä									

Liite 6. Riskienhallinnan koulutusmateriaali







Taustalla: Operatiivisten riskien hallinta eduskunnan kansliassa (25.11.2013)

- Riskikartta
  - Punaiset, oranssit ja vihreät riskit
- Riskiluokat
- Liitteissä mm.
  - Vaikutuksen arviointi –taulukko
  - Todennäköisyyden arviointi –taulukko

Riskikartta – riskien suuruudet

- Vaikutus x Todennäköisyys
  - Esim. 4 x 2 = 8 (kohtalainen)
- Riskien suuruudet:
  - Korkea riski = **punainen**
  - Kohtalainen riski= oranssi
  - Alhainen riski= vihreä

Käytettävät riskiluokat

Riskiluokka	Sisältö
Operatiivinen johtaminen ja prosessit	• strategia ja päätöksenteko • toimintaprosessi • projektinhallinta • tiedonkulku • lakien, määräysten ja sopimusten mukaisuus
Henkilöt	• henkilöstö (määrä, osaaminen, motivaatio) • etiikka • virka- ja työsuhteiden hallinta
Järjestelmät	• toimitilat, fyysinen turvallisuus • tietojärjestelmät • toiminnan infrastruktuuri • tietoturvallisuus
Ulkoiset tekijät	• rikollisuus • luonnonilmiöt

Uhkakuvia riskiluokkien näkökulmasta

- Operatiivisen johtamisen riskit
  - Heikosti johdettu ja ohjeistettu toiminta
  - **Seuraukset:** Viiveet, virheet ja laadun heikkeneminen
- Lakien ja määräysten noudattamatta jättämisen riskit
  - Sanktiot
  - **Seuraukset:** Eduskunnan julkisen kuvan heikentyminen
- Avainosaamiseen liittyvät riskit
  - Johtamisen puutteet
  - Kehittymissuunnitelmien laadinnan puutteet
  - **Seuraukset:** Virheet ja toimintakatkokset

Vaikutuksen arviointi

Asteikko	Euroa		[illegible]		[illegible]		[illegible]
5 – Vakava	> 1 milj.	ja/tai	[illegible]	ja/tai	[illegible]	ja/tai	[illegible]
4 – Merkittävä	100.000–1 milj.	ja/tai	[illegible]	ja/tai	[illegible]	ja/tai	[illegible]
3 – Huomattava	10.000–100.000	ja/tai	[illegible]	ja/tai	[illegible]	ja/tai	[illegible]
2 – Kohtalainen	1.000–10.000	ja/tai	[illegible]	ja/tai	[illegible]	ja/tai	[illegible]
1 – Vähäinen	[illegible]						

EDUSKUNTA [illegible]

Todennäköisyyden arviointi

Riskin arvioitu toteutumistodennäköisyys ottaen huomioon nykyiset hallintakeinot	Kuvaus
5 – Toteutuu seuraavan 1 vuoden aikana.	[illegible]
4 – Toteutuu seuraavan 2 vuoden aikana.	[illegible]
3 – Toteutuu seuraavan 5 vuoden aikana.	[illegible]
2 – Toteutuu seuraavan 10 vuoden aikana.	[illegible]
1 – Toteutuu seuraavan 20 vuoden aikana.	[illegible]

EDUSKUNTA

Riskien hallinta ja arviointi eduskunnan tietohallintotoimistossa

EDUSKUNTA

Tietohallintotoimiston tavoitteet

- Tietohallintolinjauksen 2013 - 2016 keskeinen tavoite on kansanedustajien ja eduskunnan työn nykyistä parempi tukeminen tietotekniikalla ja edellytysten luominen tietojohtamiseen.
- Tähän tavoitteeseen liittyy olennaisesti sähköisen asioinnin ja käsittelyn sekä tietoliikenneverkon aiempaa monimuotoisemman käytön edistäminen.
- Keskeisenä tavoitteena on myös tietohallinnon organisaation ja toiminnan kehittäminen. Toiminnan kehittämisen yksi merkittävä alue on projektityöskentelyn kehittäminen ja oman projektityömallin käyttöönotto.
- Eduskunnan kiinteistöjen peruskorjauksen aikana tietohallinnon palvelut tuotetaan luotettavasti. Peruskorjauksessa toteutetaan yhtenevästi infraverkko (tietoturva-kiinteistö-AV).

- Eduskuntatyön tukeminen
- Digitaalisen asioinnin edistäminen
- Toiminnan kehittäminen
- Palveluiden luotettavuus

- *Vrt. voiko jokin vaarantaa edellisiä tavoitteita?*

EDUSKUNTA

Tietohallintotoimiston visio

- Eduskunnan tietohallinto järjestää ja tuottaa asiakkaalleen eduskunnan toiminnan edellyttämät tieto- ja viestintätekniikan palvelut laadukkaasti, tehokkaasti ja taloudellisesti
- Toiminnassaan tietohallinto toteuttaa eduskunnan kanslian strategioita päämääriä. Tämä näkyy erityisesti tietoteknisen infrastruktuurin ja palvelujen toimintavarmuuden kehittämisessä.
- Palveluja kehitetään innovatiivisesti valituilla alueilla kehityksen kärjessä.
- Tietohallintolinjauksen tavoite on suunnata eduskunnassa kehittämisen rajallisia resursseja siten, että tietohallinto omalta osaltaan mahdollistaa eduskunnan kanslian palvelujen tuottamisen ja toiminnan kehittämisen.

- **Laadukkuus, tehokkuus ja taloudellisuus**
- **Infrastruktuurin ja palveluiden toimintavarmuuden kehittäminen**
- **Innovatiivisuus palvelujen kehittämisessä**

- *Vrt. voiko jokin vaarantaa edellisiä tavoitteita?*

EDUSKUNTA 13

Tietohallintotoimiston riskienhallinta – yleistä

- Tietohallintotoimiston riskienarviointi toimii johtamisen välineenä, laadun varmistajana sekä tietoturvan yhtenä peruspilareista
- Havaintojen perusteella voidaan tehdä suunnitelmia ja päätöksiä palveluissa, projekteissa sekä toimiston johtamisessa
- Tietoturvanhallintamalli ja tietoturvapäällikkö avustaa analyysien tekemisessä

- **Laadun varmistaminen**
- **Suunnittelun ja päätöksenteon tukeminen**
- **Myös tietoturvallisuuden hallinnan tuki**

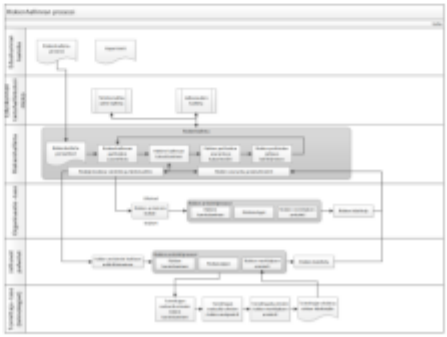
- *Vrt. voiko jokin vaarantaa edellisiä tavoitteita?*

EDUSKUNTA 14

Tietohallintotoimiston riskienhallinnan kokonaiskuva

EDUSKUNTA 15

PROSESSI



EDUSKUNTA 16

Riskien arvioinnin menetelmä

- Kolme päävaihetta:
  - Riskien arvioinnin kohteen määritteleminen
  - Riskienarviointi (prosessi)
  - Riskien käsittely

EDUSKUNTA 17

Riskien arvioinnin kohteen määritteleminen

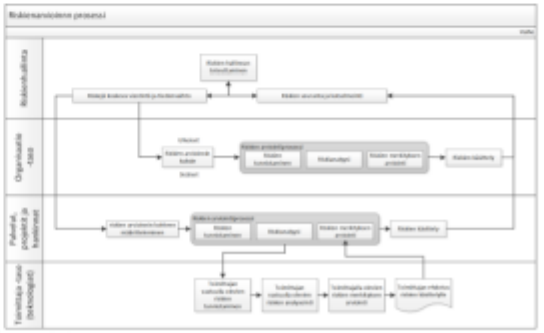
- Rajaukset
  - **Arvioitava kohde**
- Toimintaympäristö
- Riippuvuudet ja vaikutukset
  - Merkitys muille
  - Riippuvuus muista
- Kohteen kriittisyys
- Arviointityökalu

EDUSKUNTA 18

Riskien arviointi

- Vaiheittain työpajat:
  - Riskien tunnistamistyöpaja, toimintaan kohdistuvien riskien tunnistaminen
  - Riskien arviointi, vahingon suuruus ja toteutumisen todennäköisyys
  - Toimenpiteistä päättäminen ja seuranta, riskien omistajuudet ja aikataulut

EDUSKUNTA 19



EDUSKUNTA 20

Riskien tunnistaminen

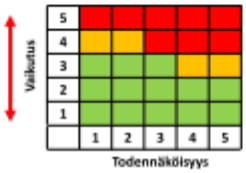
- Riskien tunnistaminen ja kirjaaminen
- Keskeiset kysymykset:
  - Miten riski voi toteutua ja mitä toteutumisesta seuraa?
  - Mikä on riskin syy?
  - Mitä on mahdollisesti tapahtunut aiemmin?

- Riskien tunnistamisessa on tavoitteena löytää toiminnan tavoitteiden toteutumista estävät tai haittaavat uhkatekijät
- Tavoitteena on tunnistaa mahdollisimman konkreettinen riski, jotta uhkan muodostamalle riskille voidaan määritellä hallintatoimenpiteitä
- Tunnistamisen apuna käytetään riskiluokkia mahdollisimman laajan näkökulman muodostamiseksi sekä esimerkkitapauksia

Apuna esimerkkejä

Riskien vaikutusten arviointi

- Asteikko 1-5:
  - Vakavin vaikutus 5
  - Pienin vaikutus 1
- Vaikutusten arviointi:
  - Euromääräinen vahinko
  - Toimimattomuuden (tilat ja järjestelmät) haitta
  - Mainetappio
  - Tavoitteissa epäonnistuminen



Riskien todennäköisyyksien arviointi

- Asteikko 1-5, tapahtuu:
  - Seuraavan 1 vuoden aikana 5
  - Seuraavan 2 vuoden aikana 4
  - Seuraavan 5 vuoden aikana 3
  - Seuraavan 10 vuoden aikana 2
  - Seuraavan 20 vuoden aikana 1
- Todennäköisyyden arviointi:
  - Aikaisemmat tapahtumat
  - Ennakoitu kehittyminen
  - Nykyiset riskienhallintakeinot
  - Kontrolleissa onnistuminen

Toimenpiteet riskeille

- Riskien hallitsemisen toimenpiteet
- Riskien omistajuus
- Riskien käsittely
- Riskien hallintasuunnitelma

Riskien hallitsemisen toimenpiteet

- Tunnistettujen ja analysoitujen riskien hallitsemiseksi päätetään toimenpiteistä
- Ensimmäisessä tarkastelussa päätellään ovatko riskit merkityksettömiä ja hallinnassa
- Jos näin ei ole, mietitään tarvittavat toimenpiteet riskien hallitsemiseksi
- Tämä muodostaa riskienhallintasuunnitelman

Riskien omistajuus

- Jokaiselle riskille nimetään omistaja
  - Riskeille tehtäville toimenpiteille nimetään omistaja
  - Riskin omistaja vastaa toimenpiteiden tekemisestä
- Toimenpiteiden varmistamiseksi
  - Säännöllinen seuranta
  - Säännöllinen raportointi

Riskien käsittelyn toimenpiteet

- Korkeat riskit
  - Vaativat nopeita toimenpiteitä
  - Toimenpiteet aloitetaan välittömästi
- Kohtalaiset riskit
  - Vaativat toimenpiteitä ja seurantaa
  - Pitkittyessään voivat nousta korkeiksi riskeiksi
- Matalat riskit
  - Voivat edellyttää toimenpiteitä
  - Osa riskeistä voidaan hyväksyä ja sietää
- Otettava huomioon myös arvioidun kohteen kriittisyys

Riskien hallintasuunnitelma

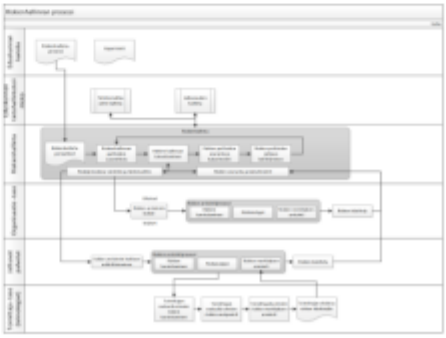
- Toimenpiteiden edistymistä seurataan säännöllisesti
- Tavoiteaikataulut riskien käsittelylle
- Tietohallintotoimiston riskien kokonaistilannetta seurataan neljännesvuosittain
- Korkeiden riskien seuranta tiheämmällä tahdilla
- Riskeille suunniteltujen toimenpiteiden seuranta
  - Riskien omistajat raportoivat tietoturvapäällikölle ja kohteen omistajalle
  - Tietoturvapäällikkö koostaa edistymisraportin
- Em. toimet ovat varsinaista riskienhallintaa!

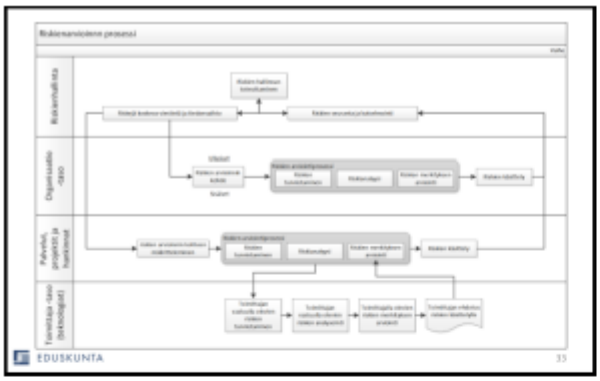
Riskienhallinnan kehittäminen, vuosikello ja vuosisuunnitelma

Riskienhallinnan prosessi

- Riskianalyysi ei ole kertaluonteinen tapahtuma
- Riskejä pitää tarkastella säännöllisesti, uhkakuvat muuttuvat sekä tavoitteet
- Myös sidosryhmien vaikutukset sekä muut muutokset toimintaympäristössä vaikuttavat riskeihin

PROSESSI





Riskienhallinnan kehitys

- Riskienhallinnan kehittämisestä vastaa tietoturvapäällikkö
- Kehityksessä noudatetaan kypsyysmallia: *"Tekemällä oppii"* –malli käytössä
- Riskienhallinnan työkalujen kehittäminen:
  - Visuaalisuuden kehittäminen
  - Käyttäjäystävällisempi toteutus
  - Raportointimenetelmien tehokkuus

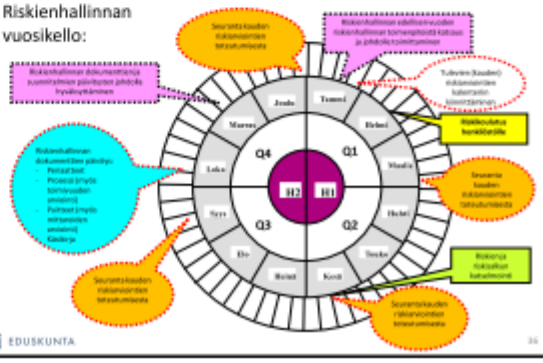
EDUSKUNTA 34

Toimenpiteiden ajoitus

- Riskienhallinnan vuosikello määrittelee vuosittain tehtävät toimenpiteet
- Vuosisuunnitelma tarkentaa toimenpiteiden sisällön ja ajankohdan

EDUSKUNTA 35

Riskienhallinnan vuosikello:



EDUSKUNTA 36

Riskienhallinnan kehittämisen vuosisuunnitelma

- Riskienhallinnan
  - Periaatteet
  - Puitteet
  - Käsikirja
  - Koulutus ja tietoiskut
- Riskiarviointien toteutus
- Riskisalkun seuranta

EDUSKUNTA 37

Lisätietoja:
Antti Laulajainen, tietoturvapäällikkö

EDUSKUNTA

Liite 7. Riskienhallinnan käsikirja

RISKIENHALLINNAN KÄSIKIRJA

Päivämäärä	Versio	Muuttaja	Muutos / toimenpiteet	Tila
1.4.2015	0.9	Antti Laulajainen	Dokumentin valmistelu hyväksyttäväksi.	luonnos
7.4.2015	1.0	Antti Laulajainen	Hyväksytty toimiston johtoryhmässä	hyväksytty

Sisällysluettelo:

(POISTETTU LIITTEESTÄ)

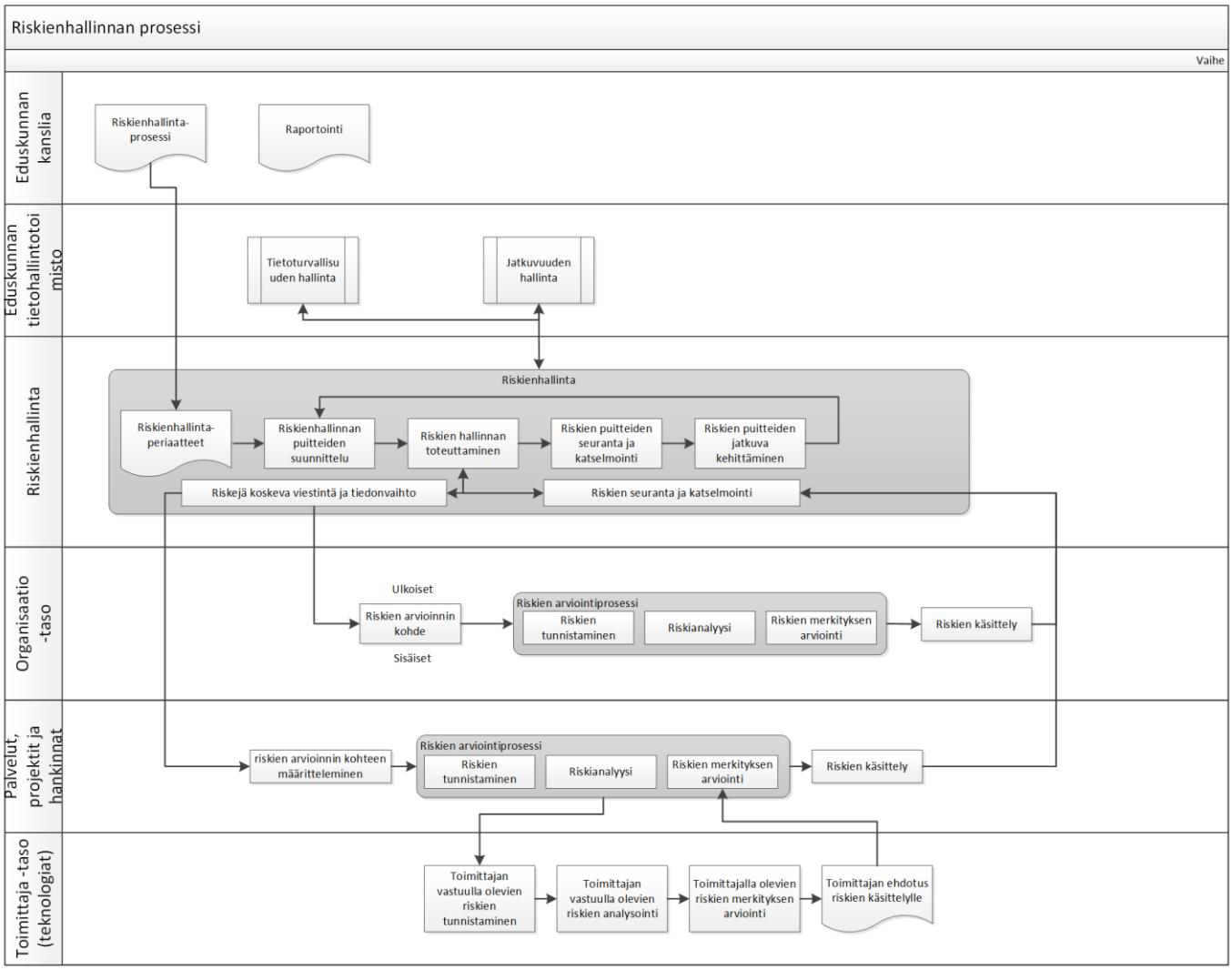
1 Johdanto

Tämä riskienhallinnan käsikirja kuvaa eduskunnan tietohallintotoimiston riskienhallinnan prosessiin liittyvät käytännön toimet sekä sisältää esimerkkejä riskien käsittelyyn.

2 Riskien hallinta- ja arviointiprosessi

2.1 Riskien hallinnan viitekehys

Riskienhallintaa toteutetaan eduskunnan tietohallintotoimistossa sovittujen riskienhallinnan periaatteiden mukaisesti. Riskienarviointia ohjataan eduskunnan tietohallintotoimistossa sovittujen riskienhallinnan periaatteiden pohjalta kuvattujen riskienhallinnan puitteiden avulla.

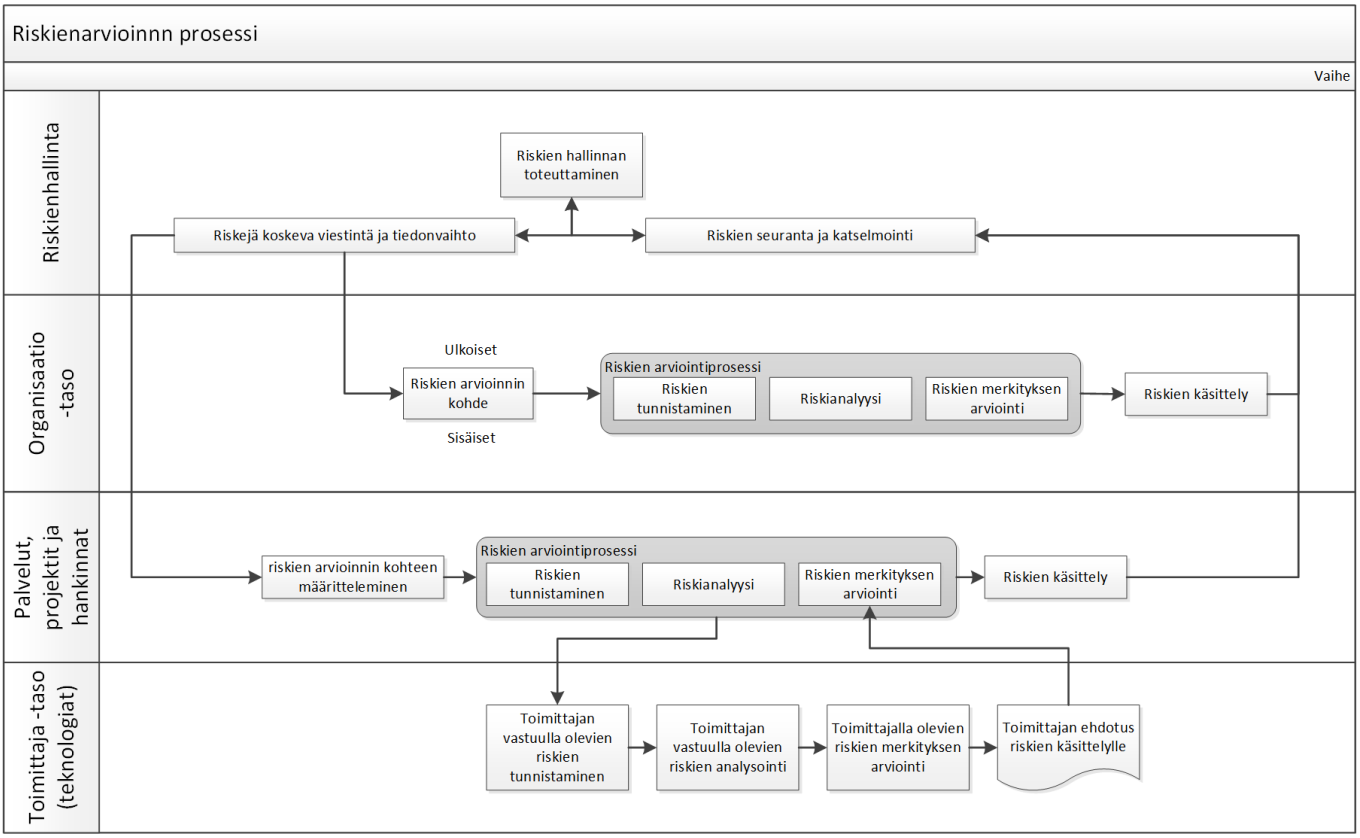


Kuva 1. *Riskienhallinnan kokonaiskuva.*

2.2 Riskien arvioinnin toteutus ja vastuut

Riskien arviointia toteutetaan seuraavilla tasoilla:

- Tietohallintotoimiston oman organisaation ja toiminnan riskien arviointi.
- Tietohallintotoimiston tarjoamat palvelut, projektit ja hankinnat eli tietohallintotoimiston kohdekohtaiset riskienarvioinnit.
- Palvelutoimittajiin ja näiden tuottamiin palveluihin (mm. käyttöpalvelu-, tietoliikenne-, sovellus-, infra- ja asiantuntijapalvelut) kohdistuva riskienarviointi.



Kuva 2. *Riskienarviointiprosessin kokonaiskuva.*

Riskien arviointien toteutusvastuut:

- Tietohallintotoimiston johtoryhmän toteuttaa eduskunnan tietohallintotoimiston organisaation riskien arvioinnit.
- Suunnittelijat ja projektipäälliköt toteuttavat palveluiden, projektien ja hankintojen riskiarvioinnit.
- Suunnittelijat ja projektipäälliköt toteuttavat myös palvelutoimittajiin ja näiden tarjoamiin palveluihin kohdistuvat riskiarviointien toteuttamiset yhteistyössä toimittajan edustajien kanssa.

- Eduskunnan tietoturvapäällikkö osallistuu tarvittaessa riskiarviointien suorittamiseen.

Riskienhallintaan ja riskien arviointiin liittyvät vastuut on kuvattu tarkemmin liitteenä olevassa vastuutaulukossa, liite 1 (RACI-mallin mukainen).

3 Riskien arviointi

3.1 Erityistä riskien arvioinnissa

Riskien arvioinnissa on otettava huomioon seuraavia erityisiä näkökulmia:

- Organisaation riskien arviointi
    - Henkilöstöön ja resursseihin liittyvät näkökulmat
    - Budjettiin ja talouden ja toiminnan suunnitteluun liittyvät näkökulmat
    - Tietohallintotoimiston tavoitteet ja linjaukset
- Palveluiden, projektien ja hankintojen riskien arviointi
    - Henkilöstön osaamiseen ja resurssien käytettävyyteen liittyvät näkökulmat
    - Kohteen kriittisyys ja riippuvuudet
    - Alihankinta- ja kumppanuussopimukset
    - Vaatimustenmukaisuus
- Palvelutoimittajien riskien arviointi
    - Teknologioihin ja tietoturvallisuuteen liittyvät vaatimukset
    - Palveluprosesseihin liittyvät näkökulmat
    - Palvelutaso- ja turvallisuussopimukset
    - Tietoliikenteeseen liittyvät näkökulmat
    - Tietoihin liittyvät näkökulmat
    - Käyttäjien tunnistamiseen liittyvät näkökulmat

Tarvittaessa riskien arviointi ulotetaan kattamaan myös muiden kuin eduskunnan tietohallintotoimiston omiin palveluihin liittyvien tahojen omistamiin järjestelmiin ja tuottamiin palveluihin.

3.2 Riskien arviointi

Riskien arvioinnin vaiheet ovat:

- Riskien arvioinnin kohteen määrittely
- Riskien tunnistaminen
- Riskien analysointi
- Riskien merkityksen arviointi
- Riskien käsittely

3.2.1 Riskiarvioinnin kohteen määrittely

Riskiarvioinnin kohteen osalta arvioidaan siihen vaikuttavat asiat ja mahdolliset rajaukset. Kohteen määrittelyn yhteydessä käydään läpi myös kriteeristö ja sen sovellettavuus. Riskien arvioinnissa käytettävän kriteeristön sovellettavuutta arvioitaessa ja määriteltäessä tulee ottaa huomioon arvioinnin kohteen tärkeys eduskunnan toiminnalle tai eduskunnan tietohallintotoimistolle.

Riskien arvioinnin toteuttamisesta vastaava kirjaa ennen riskien arvioinnin toteuttamista työkaluun lähtötiedot välilehdelle:

- Riskien arvioinnin kohde (esim. organisaation osa tai toiminto).
- Riskien arvioinnin kohteen toimintaympäristön määrittelyn. Toimintaympäristöön kuuluvat sekä ulkoiset (teknologia, palveluntarjoajat, valtioneuvosto, media ja kansalaiset sekä säädökset ja viranomaisohjeet) että sisäiset (asiakkaat, resurssit, ohjesääntö, strategiat ja linjaukset sekä tiedot, järjestelmät ja infra) sidosryhmät ja vaikuttavat tekijät, jotka on tarkemmin kuvattu riskienhallinnan puitteet –dokumentissa.
- Tietohallintotoimiston tavoitteiden ja riskienhallinnan periaatteiden mukaisuus sekä arvioinnissa käytettävän asteikon sopivuus eli käykö asteikko sellaisenaan vai sovelletaanko sitä kohteen riskien arvioinnissa.
- Kriittiset riippuvuudet eli riskien arvioinnin kohteelle välttämättömät asiat ja osapuolet sekä riskien arvioinnin kohteesta riippuvat asiat ja osapuolet.

3.2.2 Riskien arviointi: tunnistaminen, analysointi ja merkityksen arviointi

Riskien arvioinnissa ensin tunnistetaan riskit, jonka jälkeen suoritetaan riskianalyysi ja tämän jälkeen suoritetaan riskien merkityksen arviointi eli:

- riskien tunnistamisen yhteydessä kirjataan
    - jokainen havaittu riski
    - kuvaus riskistä tai sen seurauksista
    - riskiluokka
- tunnistamisen apuna käytetään esimerkkejä riskeistä ja yleistä uhkaluokitusta. Esimerkit ja uhkaluokat ovat tämän dokumentin liitteissä 4 ja 5

- riskien analysoinnin yhteydessä arvioidaan ja kirjataan riskikohtaisesti
    - syyt riskin olemassaoloon
    - riskin todennäköisyys
    - riskin vaikutukset
- riskin todennäköisyyden ja vaikutusten suuruuden arvioinnista käytetään asteikkoa 1-5. Vaikutusten ja todennäköisyyksien luokitusten kuvaukset ovat tämän dokumentin liitteissä 6 ja 7.
- riskien merkityksen arvioinnissa käydään riskikohtaisesti läpi
    - riskin suuruudet (todennäköisyys ja vaikutukset)
    - siedetäänkö riski vai edellytetäänkö riskin osalta toimenpiteitä
- riskien suuruuden ja merkityksen arvioinnissa käytetään apuna riskikarttaa. Riskikartta on kuvattu tämä dokumentin liitteessä 8.

Myös merkitykseltään ja vaikutuksiltaan pieneksi koettu riski tulee ottaa käsittelyyn, mikäli sillä on tunnistettu olevan tärkeä merkitys eduskunnan toiminnalle tai eduskunnan tietohallintotoimiston toiminnalle.

3.2.3 Riskien käsittely

Kaikki tietohallintotoimiston riskiarvioinneissa tunnistetut riskit kerätään riskisalkkuun. Riskien käsittely tapahtuu riskisalkkuun sisällytettyjen riskienhallintasuunnitelmien kautta.

Riskien käsittelyssä arvioidaan ja kirjataan

- merkityksen mukaan arvioidaan riskikohtaisesti, onko riski
    - vältettävissä eli riskialttiilta toiminnalta pidättäydytään
    - poistettavissa eli poistetaan riskiä aiheuttavat tekijät
    - pienennettävissä eli suunnitellaan ja toteutetaan toimet, joiden ansiosta riskin todennäköisyys ja/tai vaikutus pienenee
    - siirrettävissä eli määritellään esimerkiksi sopimuksilla vastuu riskistä toiselle osapuolelle tai sopimuskumppanille
    - siedettävissä eli hyväksytään riskin toteutumisen mahdollisuus ja seuraukset
- mahdollinen jäännösriski ja mikäli jäännösriski ei ole siedettävissä suoritetaan jäännösriskille riskiarviointi
- riskikohtaisesti riskienhallintasuunnitelmaan kirjataan:
    - riski ja sen suuruus

- syy riskiin / syy riskin olemassaoloon
- tavoitetila
- riskille tehtävät toimenpiteet riskienhallinnan periaatteiden mukaisesti tavoiteaikatauluineen
- riskin omistaja eli toimenpiteiden seurannasta vastaava henkilö
- riskin käsittelystä vastaava henkilö
- riskin status
- riskille tehtävien toimenpiteiden tarkastusaikataulu

4 Riskien hallinta, seuranta, katselmointi ja viestintä

4.1 Riskien seuranta ja katselmointi

Tietohallintotoimiston johtoryhmä seuraa riskejä riskisalkun avulla. Tietoturvapäällikkö ylläpitää riskisalkkua. Riskien seurantaa tehdään vuosikellon mukaisesti. Riskien omistajat seuraavat vastuullaan olevia riskejä riskienhallintasuunnitelmaan asetettujen tavoiteaikataulujen mukaan. Riskien seurannan tavoitteena ja tehtävänä on varmistaa, että riskeille suunnitellut toimenpiteet toteutuvat sovitulla tavalla.

Riskien katselmointi on vuosikellon mukainen tarkastelupiste, jolloin käydään läpi tunnistetut ja uudet riskit. Riskien katselmoinnissa riskeistä vastaavat tarkastavat tunnistetuille riskeille tehtyjen ja suunniteltujen toimenpiteiden toteutumisen. Riskien katselmoinnissa arvioidaan, onko tunnistettujen riskien suuruus muuttunut ja tarvitaanko uusi riskien arviointi. Uusien riskien osalta arvioidaan suuruus ja merkitys sekä suunnitellaan ja päätetään niille tehtävistä toimenpiteistä. Riskien katselmoinnissa arvioidaan myös mahdolliset muutokset jäännösriskeissä.

4.2 Riskejä koskeva viestintä ja tiedonvaihto

Kaikki tunnistetut riskit kirjataan eduskunnan tietoturvapäällikön ylläpitämään riskisalkkuun.

Riskiarviointien tulosten jakelusta päättää riskiarvioinnin kohteen omistaja, joka huolehtii tulosten jakelusta mm.

- sovelluspalveluiden tuottajille,
- käyttöpalveluiden tuottajille,
- tietoliikennepalveluiden tuottajille,
- sisällön omistajille ja
- palveluiden omistajille.

Riskiarviointien tulosten jakelussa tulee ottaa huomioon tietojen salassapidosta, luottamuksellisuudesta ja liikesalaisuuksista niin, että tietoa jaetaan vain niille, jotka sitä työtehtäviensä perusteella tarvitsevat.

5 Riskien hallinnan vuosikello ja riskienhallinnan toimenpiteet

Eduskunnan tietohallintotoimiston riskien hallinnan ja arvioinnin vuosikello sisältää riskienhallinnan kokonaisseurannan ja riskisalkun seurannan.

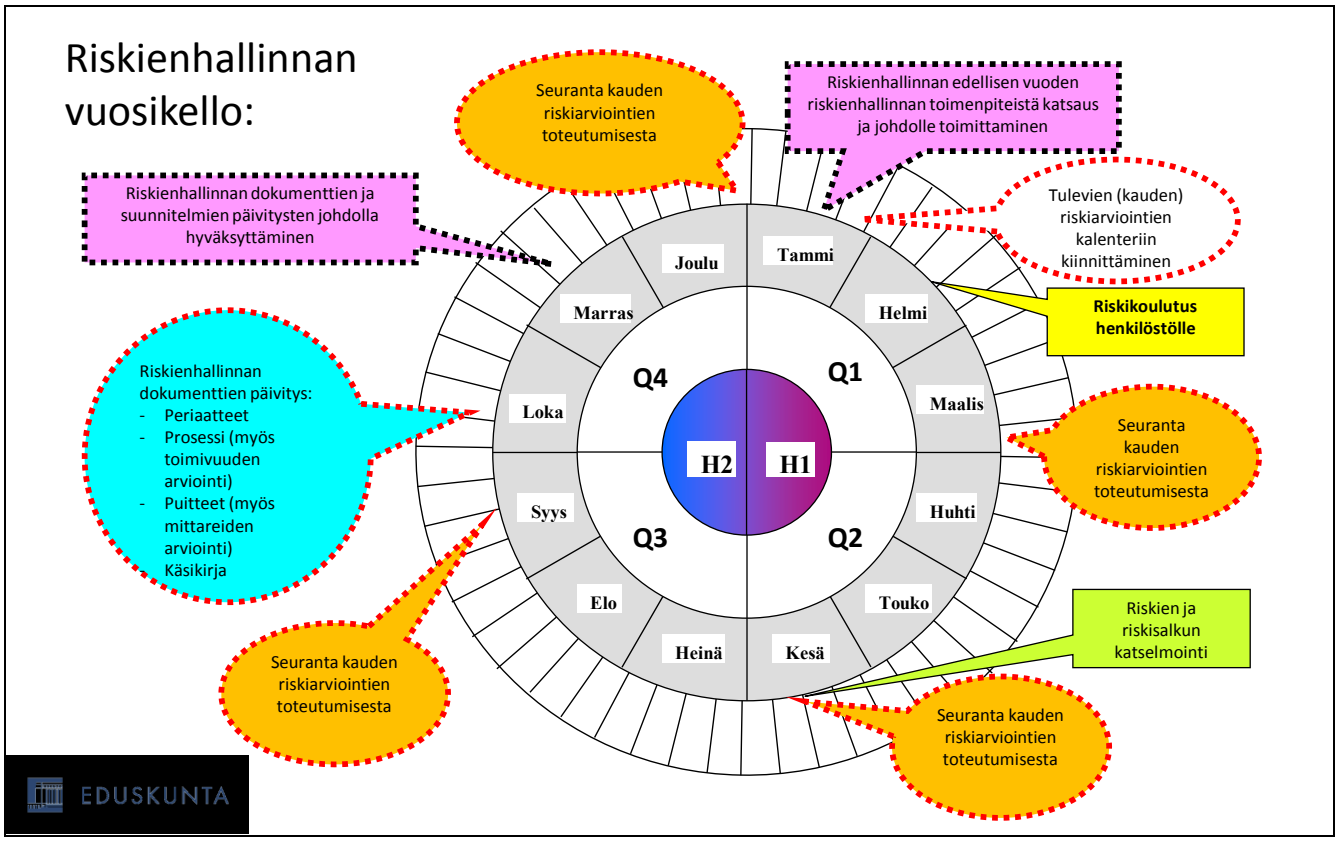
	Parittomina vuosina	Parillisina vuosina
Riskienhallinnan periaatteet - Muutostarpeiden arviointi - Muutosehdotusten laatiminen - Johdolla hyväksyttäminen	X	X
Riskienhallinnan periaatteet - Johdon/avainhenkilöiden haastattelut	X	
Riskienhallinnan puitteet - Prosessin toimivuus - Prosessin päivittäminen - Mittariston päivittäminen - Johdolla hyväksyttäminen	X	X
Riskienhallinnan käsikirja - Dokumentin ja vuosikellon päivittäminen - Esimerkkien arviointi ja päivittäminen - Johdolla hyväksyttäminen	X	X
Riskienhallinnan koulutus koko eduskunnan tietohallintotoimiston henkilöstölle		X
Riskienhallinnan tietoiskut henkilöstölle	X	
Riskiarviointien toteutus - Kohteiden valinta - Vuosikelloon päivittäminen - Seuranta ja katselmointi	X	X
Riskisalkun seuranta - Riskisalkun läpikäynti johtoryhmässä - Huom! Tämä tehdään neljännesvuosittain.	X	X

Yleiskuva vuosikellosta on tämän dokumentin liitteessä 2 riskienhallinnan vuosikello. Vuosittaiset riskienhallinnan toimenpiteet kuvataan tämän dokumentin liitteessä 3, johon kirjataan toimenpiteiden kohteet, toteuttajat sekä tavoite- ja seuranta-aikataulut.

KÄSIKIRJAN LIITE 1: RACI-taulukko

	Eduskunnan turvallisuus-johtaja	Eduskunnan hallintojohtaja	Tietohallinto-päällikkö	Eduskunnan tietohallinto-toimiston johtoryhmä	Tietoturva-päällikkö	ATK-päällikkö	Tietojärjestelmä-päällikkö	Projektipäälliköt, asiantuntijat ja suunnittelijat	Palveluntarjoajat
Eduskunnan tietohallintotoimiston riskienhallinnan periaatteet	I, C	I	A, C	I	R	C	C	I	I
Eduskunnan tietohallintotoimiston riskienhallinnan puitteet -dokumentti	I, C	I	A	I	R	C	C	I	
Puitteiden suunnittelu									
Riskienhallinnan toteuttaminen									
Puitteiden seuranta ja katselmointi									
Puitteiden jatkuva kehittäminen									
Eduskunnan tietohallintotoimiston riskisalkku	I	I	A	I	R	R	R	I	
Eduskunnan tietohallintotoimiston riskienhallinnan prosessin kuvaus	I, C	I	A	I	R	C	C	I	I
Eduskunnan tietohallintotoimiston riskienhallinnan käsikirja	I, C	I	A	I	R	C	C	I	I
Eduskunnan tietohallintotoimiston palveluiden riskienhallinnan prosessi käytännössä									
Toimintaympäristön määritteleminen					C	A	A	R	I, C
Riskienarviointiprosessi					C	A	A	R	R
Riskien tunnistaminen					C	A	A	R	R
Riskianalyysi					C	A	A	R	R
Riskien merkityksen arviointi					C	A	A	R	R
Riskien käsittely			I, C		C	A	A	R	I, C
Seuranta ja katselmointi			I		A	R	R	C	R
Viestintä ja tiedonvaihto			I		A	R	R	C	R
Eduskunnan tietohallintotoimiston organisaation riskienhallinnan prosessi käytännössä									
Toimintaympäristön määritteleminen			A		R	R	R	I	
Riskienarviointiprosessi			A		R	R	R	I	
Riskien tunnistaminen			A		R	R	R	I	
Riskianalyysi			A		R	R	R	I	
Riskien merkityksen arviointi			A		R	R	R	I	
Riskien käsittely			A		R	R	R	I	
Seuranta ja katselmointi			A		R	R	R	I	
Viestintä ja tiedonvaihto			A		R	R	R	I	

KÄSIKIRJAN LIITE 2: Riskienhallinnan vuosikello



KÄSIKIRJAN LIITE 3: Riskien hallinnan toimenpiteet

Riskien hallinnan toimenpiteet 2015

		Toteutuksesta vastaa	Toteutus-ajankohta	Toteutukseen osallistujat
Riskienhallinnan periaatteet - Muutostarpeiden arviointi - Muutosehdotusten laatiminen - Johdolla hyväksyttäminen				
Riskienhallinnan periaatteet - Johdon/avainhenkilöiden haastattelut				
Riskienhallinnan puitteet - Prosessin toimivuus - Prosessin päivittäminen - Mittariston päivittäminen - Johdolla hyväksyttäminen				
Riskienhallinnan käsikirja - Dokumentin ja vuosikellon päivittäminen - Esimerkkien arviointi ja päivittäminen - Johdolla hyväksyttäminen				
Riskienhallinnan koulutus koko eduskunnan tietohallintotoimiston henkilöstölle		Antti Laulajainen	08.06.2015 ja 24.06.2015	Tietohallintotoimiston koko henkilöstö
Riskienhallinnan tietoiskut henkilöstölle				
Riskiarviointien toteutus - Kohteiden valinta - Vuosikelloon päivittäminen - Seuranta ja katselmointi	**Arviointikohde:**			
	Active Directory (AD)	Antti Laulajainen	15.04.2015, 24.04.2015 ja 30.05.2015	Orvokki Halme Sari Wilenius Mika Halsvaha (toimittaja) Veli-Matti Ahlroth (toimittaja)
	Vaski	Sovittava	Sovittava	
	Tietohallintotoimisto organisaation riskit	Antti Laulajainen	Sovittava	
Riskisalkun seuranta - Riskisalkun läpikäynti johtoryhmässä - Huom! Tämä tehdään neljännesvuosittain.		Antti Laulajainen	Sovittava	

Riskien hallinnan toimenpiteet 2016

		Toteutuksesta vastaa	Toteutusajankohta	Toteutukseen osallistujat
Riskienhallinnan periaatteet - Muutostarpeiden arviointi - Muutosehdotusten laatiminen - Johdolla hyväksyttäminen				
Riskienhallinnan periaatteet - Johdon/avainhenkilöiden haastattelut				
Riskienhallinnan puitteet - Prosessin toimivuus - Prosessin päivittäminen - Mittariston päivittäminen - Johdolla hyväksyttäminen				
Riskienhallinnan käsikirja - Dokumentin ja vuosikellon päivittäminen - Esimerkkien arviointi ja päivittäminen - Johdolla hyväksyttäminen				
Riskienhallinnan koulutus koko eduskunnan tietohallintotoimiston henkilöstölle				
Riskienhallinnan tietoiskut henkilöstölle				
Riskiarviointien toteutus - Kohteiden valinta - Vuosikelloon päivittäminen - Seuranta ja katselmointi	**Arviointikohde:**			
Riskisalkun seuranta - Riskisalkun läpikäynti johtoryhmässä - Huom! Tämä tehdään neljännesvuosittain.				

KÄSIKIRJAN LIITE 4: Riskien käsittelyn esimerkkejä ja hyviä käytäntöjä

Tavoite:	**Riski (mikä voi mennä pieleen/mitä voi tapahtua):**	**Riskin tunnistaminen / huomaaminen:**	**Toimenpidesuositus riskeiltä suojautumiseen:**
Palvelut (tietojärjestelmillä tuotettavat palvelut) ovat käytettävissä sovitusti.	Palveluihin tulee **laaja käyttökatkos** esimerkiksi pääsynvalvonnasta ja käyttäjien tunnistamisesta vastaavaan järjestelmään.	Tunnista eri palveluiden (järjestelmien) riippuvuudet tai järjestelmän tärkeys toiminnalle (toiminnan laajuus).	Tunnistetaan riskit seuraavista näkökulmista: - luottamuksellisuus - eheys - erityisesti: saatavuus Tunnistetaan järjestelmien väliset riippuvuudet.
Uuden järjestelmän käyttöönottoprojekti pysyy aikataulussa ja tarvittavat yhteydet saadaan toimimaan.	**Aikataulu voi pettää** tehtävien viivästyessä, odottamattomien ongelmien ilmaantuessa, resurssien äkillisten poissaolojen vuoksi tai osaamisen puutteesta johtuen.	Tunnista ainakin seuraavat riskit: - ihmisiin liittyvät riskit - teknologiaan liittyvät riskit - projektin aikataulun liittyvät riskit	Riskien käsittelyssä suositeltavia asioita: - henkilöihin liittyvät riskit: o varahenkilöt o osaamisen varmistaminen - teknologiaan liittyvät riskit: o riippuvuuksien tunnistaminen o teknisten vaatimusten määrittely - projektinhallintaan liittyvät riskit: o realistinen aikataulutus o työmäärien ja tavoitteiden aktiivinen seuranta - muut riskit?
Tiedot ovat oikein ja tietoihin pystyy luottamaan.	**Tiedot vahingoittuvat, muuttuvat tai poistuvat** tahallisen tai tahattoman syyn vuoksi hallitsemattomasti.	Tunnistetaan tiedot ja tietoja sisältävät suojattavat kohteet.	Tarkastetaan esim. vuosittain: - tietojen käytettävyys - testataan pidemmän aikaa tallennettujen tietojen käsiteltävyys
Tietojärjestelmät toimivat muiden niihin liittyvien järjestelmien kanssa yhteen.	**Tietojärjestelmä vanhenee** ja/tai yhteensopivuus tai yhteentoimivuus menetetään, jolloin **tietoja ei pystytä käsittelemään**.	Elinkaarenhallinnan mukainen tarkastelu.	Tarkastetaan esim. vuosittain: - järjestelmän ajantasaisuus - tietojen käytettävyys Määräajoin järjestelmän elinkaarenhallinnan mukainen tarkastelu sekä riskien arviointi. testataan pidemmän aikaa tallennettujen tietojen käsiteltävyys
Asiakaspalvelu toimii moitteettomasti ja asiakaspalvelijat ovat tavoitettavissa. Tarvittavat asiantuntijat ovat riittävän nopeasti käytettävissä.	**Asiakaspalvelu ei ole käytettävissä. Henkilöt sairastuvat, vaihtavat työpaikkaa tai muutoin poistuvat työvahvuudesta. Henkilöiden osaaminen ei ole ajantasaista.**	Tunnistetaan riskit: - henkilöt - osaaminen - kuormitus	Tarkastetaan määräajoin: - vastuut ja varahenkilöt - henkilöiden osaaminen - tarjottavan palvelun riittävyys ja kattavuus sekä kapasiteetti - arvioidaan jäännösriskit ainakin kertaalleen
Tietoverkko on turvallinen käyttää ja haittaohjelmista vapaa.	**Tietojärjestelmään** ja/tai tietoliikenneverkkoon pääsee tai joutuu tai toimitetaan **haittaohjelma**. Järjestelmän koodiin jää tai pesiytyy haitallista ohjelmakoodia.	Suoritetaan arviointeina: - haittaohjelmaskannauksia - haavoittuvuusanalyysejä - ohjelmakoodin arviointeja	Arviointien jälkeen laaditaan toimenpidesuunnitelmat: - haittaohjelmien poistamiselle tai suojautumisen kehittämiselle - haavoittuvuusanalyysin tuloksille - koodin testaamiselle ja korjaamisille

Tavoite:	Riski (mikä voi mennä pieleen/mitä voi tapahtua):	Riskin tunnistaminen / huomaaminen:	Toimenpidesuositus riskeiltä suojautumiseen:
Projektin kustannukset pysyvät hallinnassa ja mahdolliset riskit tunnistetaan etukäteen ja muutoksiin varaudutaan etukäteen. Sovittujen riskeihin vaikuttamisen toimenpiteiden toteuttaminen ja toteuttamisen aktiivinen seuranta sekä säännölliset riskien katselmoinnit.	**Kustannukset kasvavat** hallitsemattomiksi projekteissa. *Projektin kustannuksiin liittyvien riskien arviointi jää tekemättä tai puutteelliseksi ja riskien arvioinnin yhteistä sovittua mallia ei noudateta tai kustannusten seuranta muutoin unohdetaan.*	Projektin riskit tunnistetaan: - projektisuunnitelmasta puuttuu riskien arviointi, käsittely ja toimenpidesuunnitelma - toimittajan raportointi ei vastaa sovittua - toimittaja ei raportoi tehtävien edistymisestä - ohjausryhmä ei kokoonnu sovitusti tai käsittele riskejä - projektipäällikkö ei raportoi projektin etenemisestä	Yhteinen malli hallintaan ja mallin kouluttaminen vastuuhenkilöille ja tarvittaessa koko henkilöstölle. Riskeiltä suojautumiseksi: - projektin riskit arvioidaan ennen projektin aloittamista - projektin ohjausryhmä tarkastaa projektisuunnitelman ja edellyttää riskien arviointia, käsittelyä ja toimenpidesuunnitelmaa - projektin riskit kirjataan projektisuunnitelmaan ja riskisalkkuun - käytetään projektin hallinnan mallia - projektin ohjausryhmä seuraa kustannusten kehittymistä - projektin riskeille tehdään arviointeja ja katselmointeja säännöllisesti - projektin edistymistä seurataan säännöllisesti
Palveluiden säännöllisesti toistuva riskiarviointi ja havaittujen riskien aktiivinen seuranta sekä vuosittainen katselmointi. Sovittujen riskeihin vaikuttamisen toimenpiteiden toteuttaminen ja toteuttamisen aktiivinen seuranta sekä säännölliset riskien katselmoinnit.	**Kustannukset kasvavat** hallitsemattomiksi palveluissa. *Palveluiden kehittämistä tehdään ilman riskien arviointia sekä kustannusten ja käytettävien työpanosten seurantaa.*	Palveluiden riskit tunnistetaan: - palveluihin liittyviä vaatimuksia ei ole asetettu eikä käsitelty - palvelusta tai siinä käytettävästä järjestelmästä ei ole elinkaarenhallintamallia - palvelun tai siinä käytettävän järjestelmän teknologian kehittymistä ei seurata - palveluun tai siinä käytettäviin järjestelmiin liittyviä riippuvuuksia ei ole tunnistettu	Yhteinen malli hallintaan ja mallin kouluttaminen vastuuhenkilöille ja tarvittaessa koko henkilöstölle. Toimenpiteinä: - palveluihin ja niissä käytettäviin järjestelmiin kohdistetaan riskien arviointeja - tunnistettuja riskejä seurataan - riskien katselmointia suoritetaan säännöllisesti
Riskienhallinnan periaatteiden, puitteiden ja prosessin säännöllisesti toistuva arviointi sekä vuosikellon mukainen toiminta.	Riskien hallinta (johtaminen) epäonnistuu ja tietoturvallisuus vaarantuu. *Puutteellisuudet mallissa tai johtamistoimien unohtaminen tai tarvittavan päätöksenteon (hyväksyntöjen) viivästyminen.*	Riskit tunnistetaan: - riskien arvioinnit ja katselmoinnit jäävät toteutumatta - vuosikelloon sovitut tehtävät jäävät tekemättä - dokumentit jäävät päivittämättä tai hyväksymättä	Johdon osallistuminen päätösten tekemiseen/aikaansaamiseen sekä selkeät nimetyt vastuuhenkilöt tarvittaville tehtäville. Toimenpiteinä: - palveluihin ja niissä käytettäviin järjestelmiin kohdistetaan riskien arviointeja - riskien katselmointia suoritetaan säännöllisesti ja tunnistettuja riskejä seurataan - dokumentteja päivitetään ja katselmoidaan säännöllisesti - johtoryhmä seuraa säännöllisesti riskiarviointien toteutumista
Riskienhallinnan periaatteiden, puitteiden ja prosessin säännöllisesti toistuva koulutus sekä vuosikellon mukaisten tavoitteiden aktiivinen seuranta.	Riskien hallinnan ohjeistusta ei noudateta ja tietoturvallisuus pettää. *Vastuuhenkilöiden ja/tai muun henkilöstön laiminlyönnit ohjeiden noudattamisessa tai koulutuksen puute.*	Riskit tunnistetaan: - riskeille sovitut toimenpiteet jäävät tekemättä - riskejä koskeva koulutus jää toteutumatta - riskien arvioinnit ja katselmoinnit jäävät toteutumatta - vuosikelloon sovitut tehtävät jäävät teke-	Toimenpiteinä: - riskeille sovittujen toimenpiteiden (riskienhallintasuunnitelmaan kirjatut) seuranta - riskejä koskeva koulutus toteutetaan säännöllisesti ja kattavasti - vuosikellon mukaista toimintaa edellytetään

Tavoite:	Riski (mikä voi mennä pieleen/mitä voi tapahtua):	Riskin tunnistaminen / huomaaminen:	Toimenpidesuositus riskeiltä suojautumiseen:
		mättä	
Projektien riskienhallinnassa riskienhallinnan mallin sekä riskienhallinnan käsikirjan ja muun riskienhallinnan ohjeistuksen noudattaminen. Sovittujen riskeihin vaikuttamisen toimenpiteiden toteuttaminen ja toteuttamisen aktiivinen seuranta sekä säännölliset riskien katselmoinnit.	Projektin laatu menetetään. *Projektissa ei noudateta yhteistä riskienhallinnan mallia tai projektin aikana syntyy odottamattomia muutoksia tai viivästyksiä. Projektin lopputulos ei vastaa sovittua.*	Riskit tunnistetaan: - laatu- ja hyväksymiskriteerit puuttuvat - testaamista ei ole suoritettu tai sovittu tehtäväksi - riskien seuranta ja raportointi puuttuu	Riskienhallinnan ohjeistuksen ja mallien noudattaminen, riskien etukäteen arviointi sekä riskien aktiivinen seuraaminen projektissa ja projektisuunnitelmassa. Toimenpiteinä: - projektin riskit arvioidaan ennen projektin aloittamista - projektin ohjausryhmä tarkastaa projektisuunnitelman ja edellyttää riskien arviointia, käsittelyä ja toimenpidesuunnitelmaa - projektin riskit kirjataan projektisuunnitelmaan ja riskisalkkuun - käytetään projektin hallinnan mallia - projektin riskeille tehdään arviointeja ja katselmointeja säännöllisesti - projektin edistymistä seurataan säännöllisesti - luodaan laatu- ja hyväksymiskriteerit - testaamiset suunnitellaan ja toteutetaan sovitusti
Riskien arvioinnit ja riskien kirjaaminen riskisalkkuun ja riskienhallintasuunnitelmien päivittäminen. Riskien säännöllinen ja kattava arviointi sekä riskien säännöllisesti toistuva katselmointi.	Palveluiden laatu menetetään. *Palveluiden tuottamisessa ei noudateta yhteisiä ohjeita tai palveluissa tehdään odottamattomia ja yllättäviä muutoksia.*	Riskit tunnistetaan: - odottamattomat käyttökatkokset - asiakkaan ja toimittajan välisissä tapaamisissa ei seurata palvelun laatua - muutoksia tehdään suunnittelematta	Muutostenhallinta ja odottamattomiin tilanteisiin varautuminen riskiarviointien perusteella sekä riittävän usein tapahtuva riskienhallinnan koulutus. Toimenpiteinä: - toimintamallista sopiminen ja sovitun mallin noudattaminen - asiakas-toimittaja –tapaamisten toteuttaminen säännöllisesti (laatu asialistalla) ja laatupoikkeamien käsittely - palvelutasosopimukset (*SLA, Service Level Agreement*) - palveluihin ja niissä käytettäviin järjestelmiin kohdistetaan riskien arviointeja - tunnistettuja riskejä seurataan - riskien katselmointia suoritetaan säännöllisesti
Aikatauluihin ja palveluaikoihin liittyvien riskien kartoittaminen sekä tunnistettujen riskien aktiivinen seuranta ja säännöllinen katselmointi. Sovittujen riskien käsittelytoimenpiteiden toteuttaminen ja toteuttamisen seuranta.	Projektin aikataulu pettää. *Projektinhallinnassa unohdetaan tehdä riskiarviointi ja/tai seurata projektisuunnitelman mukaisuuden toteutumista tai varahenkilöiden käytettävyydestä ja osaamiseen liittyvistä vaatimuksista ei ole sovittu etukäteen.*	Tunnistetaan: - ihmisiin liittyvät riskit, henkilöiden käytettävyyttä ei ole varmistettu ja/tai varahenkilöitä ei ole nimetty - teknologiaan liittyvät riskit, osaamisriski ja/tai vanhenemisriski - projektin aikatauluun liittyvät riskit, epärealistinen aikataulu - toimittajiin liittyvät riskit, henkilöitä ei ole nimetty - projektikokoukset jäävä pitämättä - projektin ohjausryhmä ei kokoonnu	Projektin riskien arviointi etukäteen myös aikataulujen sekä varahenkilöiden käytettävyyden osalta sekä aktiivinen projektin onnistumisen (aikataulussa pysymisen) seuranta. Toimenpiteinä: - henkilöihin liittyvät riskit: o varahenkilöt o osaamisen varmistaminen - teknologiaan liittyvät riskit: o riippuvuuksien tunnistaminen o teknisten vaatimusten määrittely - projektinhallintaan liittyvät riskit: o realistinen aikataulutus o työmäärien ja tavoitteiden aktiivinen seuranta

Tavoite:	Riski (mikä voi mennä pieleen/mitä voi tapahtua):	Riskin tunnistaminen / huomaaminen:	Toimenpidesuositus riskeiltä suojautumiseen:
		- projektia koskevat päätökset jäävät tekemättä - muutoksenhallinta projekteissa tapahtuu odottamatta tai ilman suunnittelua ja vaikutusten arviointia	

KÄSIKIRJAN LIITE 5: Uhkaluokat

Riskien tunnistamisessa käytetään apuna seuraavia uhkaluokkia

riskiluokka	**sisältö**
operatiivinen johtaminen ja prosessit	• strategia ja päätöksenteko • toimintaprosessi • projektinhallinta • tiedonkulku • lakien, määräysten ja sopimusten mukaisuus
henkilöt	• henkilöstö (määrä, osaaminen, motivaatio) • etiikka • virka- ja työsuhteiden hallinta
järjestelmät	• toimitilat, fyysinen turvallisuus • tietojärjestelmät • toiminnan infrastruktuuri • tietoturvallisuus
ulkoiset tekijät	• rikollisuus • luonnonilmiöt

KÄSIKIRJAN LIITE 6: Riskien vaikutusluokat

Vaikutusten arvioinnissa käytetään seuraavaa taulukkoa apuna

Asteikko	**Euroa**		**Järjestelmiin tai tiloihin kohdistuva[1]**		**Maineen menetys, joka**		**Tavoitteiden saavuttamisen ja perustehtävien kannalta kysymyksessä on riski, joka toteutuessaan olisi vaikutuksiltaan**
5 – Vakava	> 1 milj.	ja/tai	huomattava tuho tai onnettomuus, josta seuraavalla toimintakyvyn menetyksellä on merkittävä vaikutus myös eduskunnan (kanslian) sidosryhmiin.	ja/tai	voisi johtaa vakavaan ja pysyvään (> 3 vuotta) maineen menetykseen keskeisten sidosryhmien ja suuren yleisön keskuudessa.	ja/tai	pysäyttävä.
4 – Merkittävä	100.000 - 1 milj.	ja/tai	vahinko tai onnettomuus, jolla on pitkäkestoinen vaikutus kanslian useisiin toimintoihin.	ja/tai	voisi johtaa rajattuun, pitkäkestoiseen (1–3 vuotta) maineen menetykseen.	ja/tai	kriittinen/merkittävä.
3 – Huomattava	10.000 - 100.000	ja/tai	vahinko tai laitevika, joka aiheuttaa rajatun toimintakyvyn menetyksen huomattavaksi ajaksi.	ja/tai	voisi johtaa rajattuun ja kestoltaan enintään kohtalaiseen (< 1vuosi) maineen menetykseen, rajoittuu esimerkiksi tiettyihin sidosryhmiin.	ja/tai	huomattava.

2 – Kohtalainen	1.000 - 10.000	ja/tai	laitevika tai muu häiriö, joka vaikeuttaa joitakin toimintoja lyhytkestoisesti.	ja/tai	olisi vaikutuksiltaan vähäinen.	ja/tai	kohtalainen.
1 – Vähäinen	Kattaa kaikki muut tapaukset, jotka eivät täytä yllä mainittuja kriteerejä						

KÄSIKIRJAN LIITE 7: Todennäköisyyksien luokitus

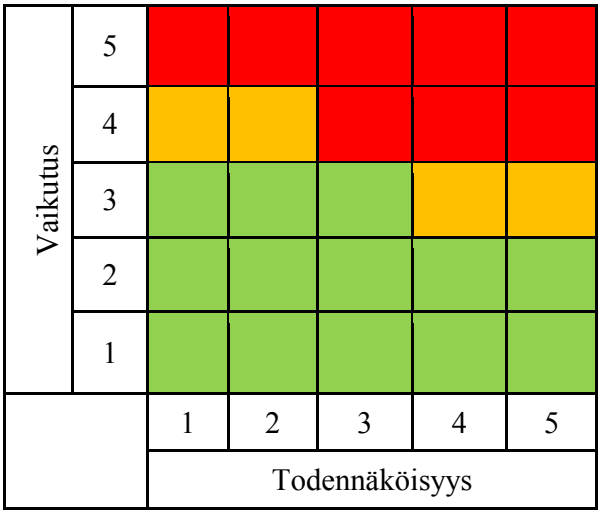
Todennäköisyyksien arvioinnissa käytetään seuraavaa taulukkoa arvioinnin apuna

Riskin arvioitu toteutumistiheys ottaen huomioon nykyiset hallintatoimet	**Kuvaus**
5 – Toteutuu seuraavan 1 vuoden aikana.	Vastaava riski on toteutunut 12 viime kuukauden aikana ja/tai sen odotetaan tapahtuvan vuosittain, ja/tai sisäisessä ja ulkoisessa toimintaympäristössä on tapahtunut erittäin merkittäviä muutoksia. Kontrollit, joilla riskiä voisi hallita, eivät ole käytössä.
4 – Toteutuu seuraavan 2 vuoden aikana.	Vastaava riski on toteutunut 12 viime kuukauden aikana ja/tai sen odotetaan tapahtuvan seuraavien vuosien aikana, ja/tai sisäisessä ja ulkoisessa toimintaympäristössä on tapahtunut merkittäviä muutoksia. Kontrollit, joilla riskiä voisi hallita, ovat vanhentuneet eivätkä vastaa muuttunutta tilannetta.
3 – Toteutuu seuraavan 5 vuoden aikana.	Vastaava riski on toteutunut parin viime vuoden aikana, ja seuraavan odotetaan toteutuvan 5 vuoden kuluessa, ja/tai sisäisessä ja ulkoisessa toimintaympäristössä on tapahtunut muutoksia. Kontrollit, joilla riskiä voisi hallita, ovat vain osittain käytössä.
2 – Toteutuu seuraavan 10 vuoden aikana.	Toiminnalliset prosessit ovat melko vakaita, ja käytössä olevien kontrollien odotetaan kattavan odotettavissa olevat riskit. Näköpiirissä on muutoksia organisaation tai toiminnon rakenteessa, miehityksessä, johtamisessa, järjestelmissä ja prosesseissa. Muutokset ovat valmisteilla, käynnissä ja/tai toimintaan liittyvät riski-indikaattorit ovat varoittavia.

	Kontrollijärjestelmä ei ole kattava.
1 – Toteutuu seuraavan 20 vuoden aikana.	Toiminnalliset prosessit ovat hyvin vakaita, ja kontrollien uskotaan kattavan odotettavissa olevat riskit.

KÄSIKIRJAN LIITE 8: Riskikartta

Riskien suuruuden ja merkityksen arvioinnissa käytetään seuraavaa karttaa apuna. Riskin suuruus määräytyy vaikutuksen ja todennäköisyyden suuruksien kautta. Riskienhallinnan periaatteissa on määritelty tietohallintotoimiston riskienottokyky.



Korkea riski = **punainen**

Kohtalainen riski= **oranssi**

Alhainen riski= **vihreä**

KÄSIKIRJAN LIITE 9: Riskisalkku

Riskisalkku on erillinen excel-taulukko, jonka ylläpidosta vastaa tietoturvapäällikkö.

KÄSIKIRJAN LIITE 10: Riskien arviointityökalu

Riskien arviointityökalu on erillinen excel-taulukko, jonka ylläpidosta vastaa tietoturvapäällikkö.

KÄSIKIRJAN LIITE 11: Riskienhallinnan koulutusmateriaali

Riskienhallinnan koulutusmateriaali on erillinen ppt-esitys, jonka ylläpidosta vastaa tietoturvapäällikkö.

Liite 8. Riskienarvioinnin työkalu

Esitiedot

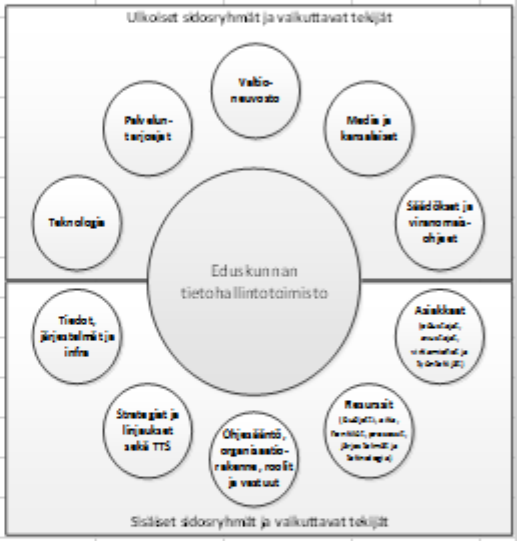
Arvioinnin kohde, omistaja ja arviointiajankohta		Muut vastuuhenkilöt ja asiantuntijat
Kohteen tyyppi:	6 Organisaatio	[henkilön nimi, rooli]
Kuvaus:		[henkilön nimi, rooli]
		[henkilön nimi, rooli]
Kohteen nimi:		
Nimilyhenne:		
Omistaja:	[henkilön nimi, rooli]	
Arviointipäivä:		

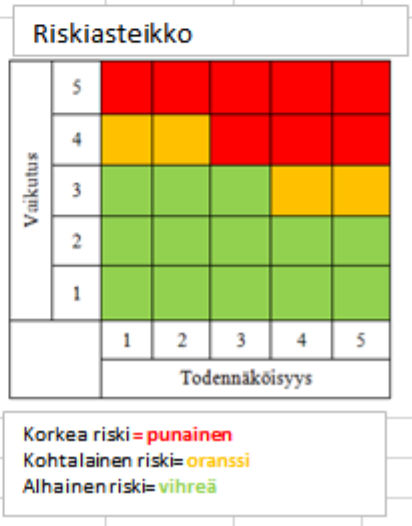
Kuvaus toimintaympäristöstä	
	[sanallinen kuvaus toimintaympäristöstä tai tieto siitä, missä ja miten toimintaympäristö on kuvattu]

Riippuvuudet (tärkeimmät riippuvuudet)	
Kohde on riippuvainen:	[katso oheinen kuva tai yllä kuvattu toimintaympäristö ja kerro 2-3 kriittisintä riippuvuutta]
Kohteesta ovat riippuvaisia:	[katso oheinen kuva tai yllä kuvattu toimintaympäristö ja kerro 2-3 kriittisintä riippuvuutta]

Kohteen kriittisyys eduskunnan toiminnalle	
	[sanallinen kuvaus kriittisyydestä ja esim. häiriön vaikutuksista]

Arviointikriteeristön (asteikon) sovellettavuus	
	[sanallinen kuvaus asteikon sovellettavuudesta arvioinnissa]





Aktiiviset riskit

	Arvioinnin kohde		Arviointi pvm													
		0	0.1.1900													
		"Mitä voi tapahtua?	"Miksi ei toimita oikein?"						"Miten tulisi toimia?	Mitä pitäisi korjata?						
	ID	Riski-tunniste	Riski	Syy riskiin	Toden-näköisyys (1-5)	Vakavuus (1-5)	Kriittisyys (TN*V)	Riskin suuruus	Tavoite	Toimenpide-ehdotus	Vastuu-henkilö	Tavoite-aikataulu	Tarkis-tettu	Täytä 1-4	Status	Uhka-luokka
0	1	01	[Riski]		1	5	5	Korkea riski			[Henkilö]	p.kk.vvvv	p.kk.vvvv	4	Aloitamatta!	Operatiivinen johtaminen ja prosessit
0	2	02	[Riski]		2	4	8	Kohtalainen riski			[Henkilö]	p.kk.vvvv	p.kk.vvvv	3	Kesken, ei etene.	Henkilöt
0	3	03	[Riski]		3	3	9	Matala riski			[Henkilö]	p.kk.vvvv	p.kk.vvvv	2	Kesken, etenee.	Järjestelmät
0	4	04	[Riski]		4	2	8	Matala riski			[Henkilö]	p.kk.vvvv	p.kk.vvvv	1	Kunnossa, ok.	Ulkoiset tekijät
0	5	05	[Riski]		5	1	5	Matala riski			[Henkilö]	p.kk.vvvv	p.kk.vvvv	4	Aloitamatta!	Operatiivinen johtaminen ja prosessit
0	6	06	[Riski]		1	5	5	Korkea riski			[Henkilö]	p.kk.vvvv	p.kk.vvvv	3	Kesken, ei etene.	Henkilöt
0	7	07	[Riski]		2	4	8	Kohtalainen riski			[Henkilö]	p.kk.vvvv	p.kk.vvvv	2	Kesken, etenee.	Järjestelmät
0	8	08	[Riski]		3	3	9	Matala riski			[Henkilö]	p.kk.vvvv	p.kk.vvvv	1	Kunnossa, ok.	Ulkoiset tekijät
0	9	09	[Riski]		4	2	8	Matala riski			[Henkilö]	p.kk.vvvv	p.kk.vvvv	4	Aloitamatta!	Operatiivinen johtaminen ja prosessit
0	10	010	[Riski]		5	1	5	Matala riski			[Henkilö]	p.kk.vvvv	p.kk.vvvv	3	Kesken, ei etene.	Henkilöt
0	11	011	[Riski]		1	5	5	Korkea riski			[Henkilö]	p.kk.vvvv	p.kk.vvvv	2	Kesken, etenee.	Järjestelmät
0	12	012	[Riski]		2	4	8	Kohtalainen riski			[Henkilö]	p.kk.vvvv	p.kk.vvvv	1	Kunnossa, ok.	Ulkoiset tekijät
0	13	013	[Riski]		3	3	9	Matala riski			[Henkilö]	p.kk.vvvv	p.kk.vvvv	4	Aloitamatta!	Operatiivinen johtaminen ja prosessit
0	14	014	[Riski]		4	2	8	Matala riski			[Henkilö]	p.kk.vvvv	p.kk.vvvv	3	Kesken, ei etene.	Henkilöt
0	15	015	[Riski]		5	1	5	Matala riski			[Henkilö]	p.kk.vvvv	p.kk.vvvv	2	Kesken, etenee.	Järjestelmät

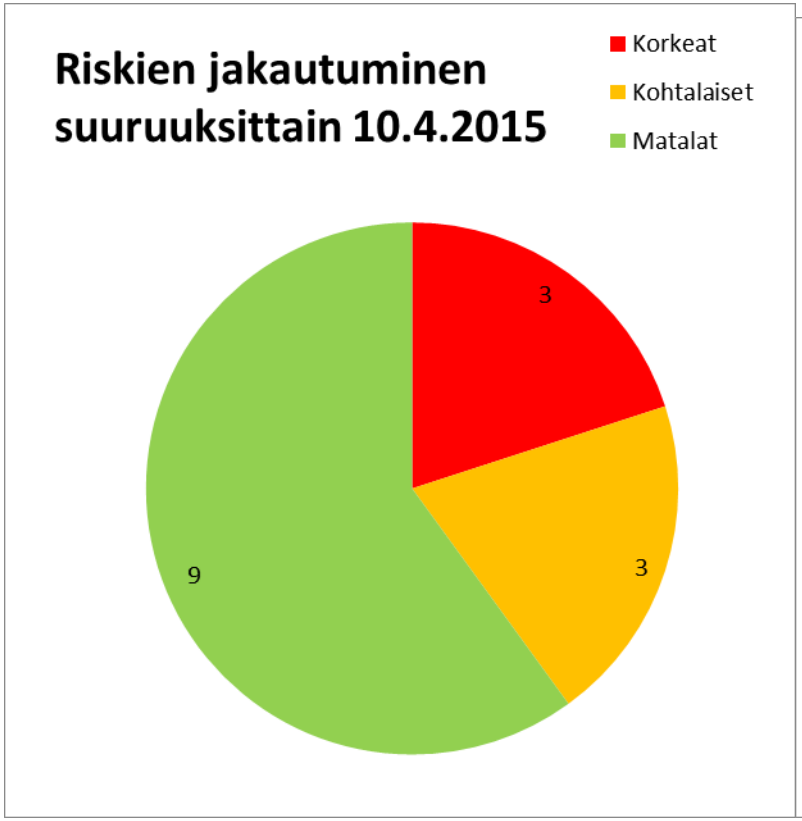
Historiatiedot 1

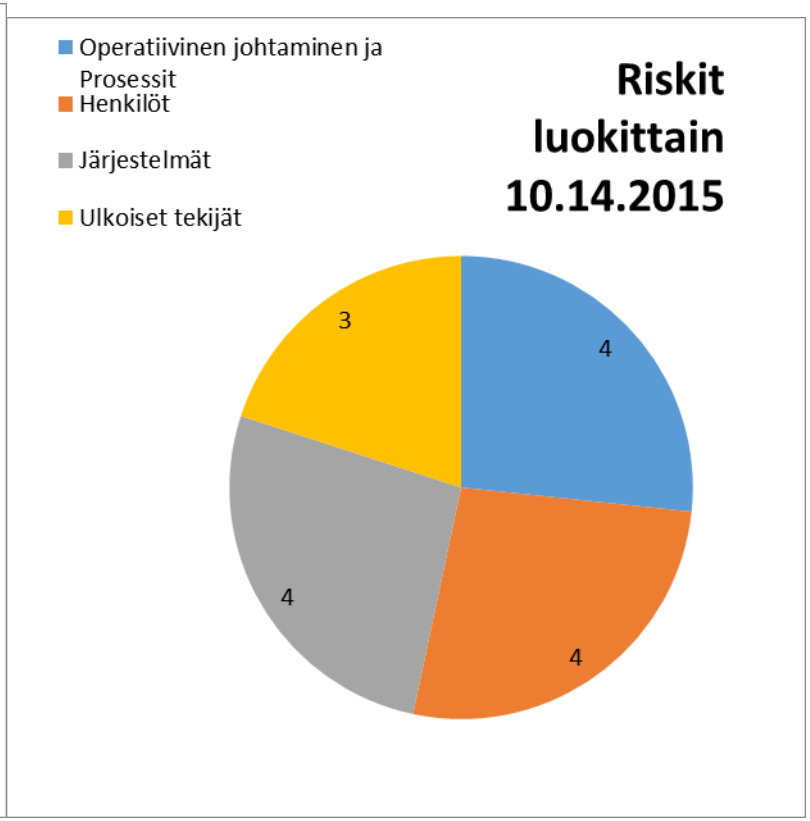
Arvioinnin kohde										
0										
Riski-tunniste	Arviointi	Toden-näköisyys	Vaikutus	Kriittisyys	Riskien suuruudet	Riskiluokka	Riskiluokat ja suuruudet yhteensä			
							Operatiivinen johtaminen ja Prosessit	Henkilöt	Järjestelmät	Ulkoiset tekijät
01	10.4.2015	1	5	5	Korkea riski	Operatiivinen johtaminen ja prosessit	4	4	4	3
02	10.4.2015	2	4	8	Kohtalainen riski	Henkilöt	Korkeat	Kohtalaiset	Matalat	
03	10.4.2015	3	3	9	Matala riski	Järjestelmät	3	3	9	
04	10.4.2015	4	2	8	Matala riski	Ulkoiset tekijät				
05	10.4.2015	5	1	5	Matala riski	Operatiivinen johtaminen ja prosessit				
06	10.4.2015	1	5	5	Korkea riski	Henkilöt				
07	10.4.2015	2	4	8	Kohtalainen riski	Järjestelmät				
08	10.4.2015	3	3	9	Matala riski	Ulkoiset tekijät				
09	10.4.2015	4	2	8	Matala riski	Operatiivinen johtaminen ja prosessit				
010	10.4.2015	5	1	5	Matala riski	Henkilöt				
011	10.4.2015	1	5	5	Korkea riski	Järjestelmät				
012	10.4.2015	2	4	8	Kohtalainen riski	Ulkoiset tekijät				
013	10.4.2015	3	3	9	Matala riski	Operatiivinen johtaminen ja prosessit				
014	10.4.2015	4	2	8	Matala riski	Henkilöt				
015	10.4.2015	5	1	5	Matala riski	Järjestelmät				

Historiatiedot 2

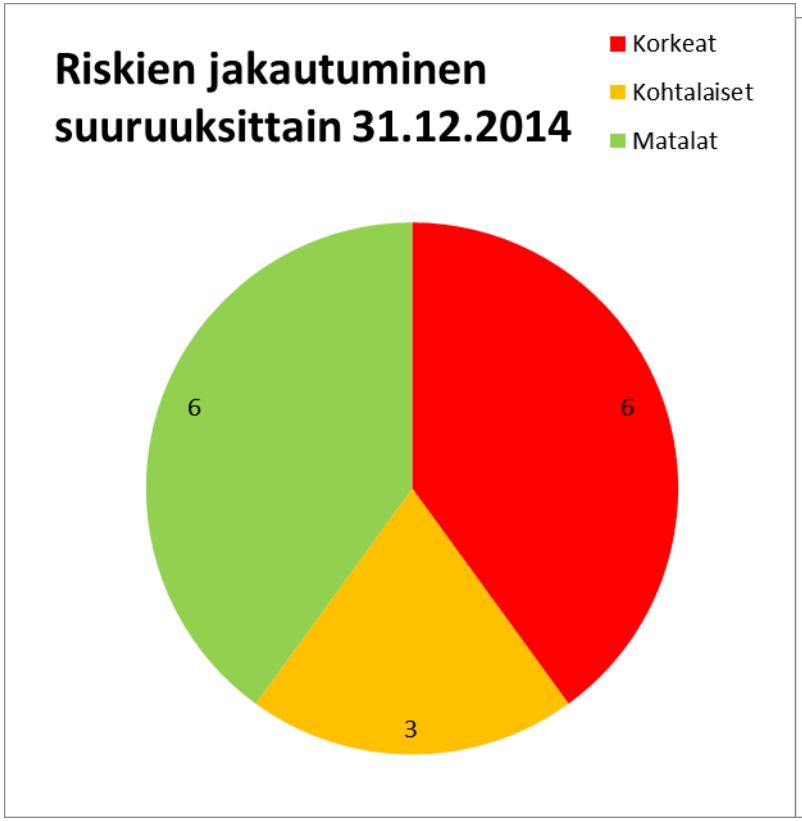
Riski-tunniste	Arviointi	Toden-näköisyys	Vaikutus	Kriittisyys	Riskien suuruudet	Riskiluokka	Riskiluokat ja suuruudet yhteensä			
							Operatiivinen johtaminen ja Prosessit	Henkilöt	Järjestelmät	Ulkoiset tekijät
01	31.12.2014	5	2	10	Matala riski	Operatiivinen johtaminen ja prosessit	4	4	4	3
02	31.12.2014	4	3	12	Kohtalainen riski	Henkilöt	Korkeat	Kohtalaiset	Matalat	
03	31.12.2014	3	4	12	Korkea riski	Järjestelmät	6	3	6	
04	31.12.2014	2	5	10	Korkea riski	Ulkoiset tekijät				
05	31.12.2014	1	1	1	Matala riski	Operatiivinen johtaminen ja prosessit				
06	31.12.2014	5	2	10	Matala riski	Henkilöt				
07	31.12.2014	4	3	12	Kohtalainen riski	Järjestelmät				
08	31.12.2014	3	4	12	Korkea riski	Ulkoiset tekijät				
09	31.12.2014	2	5	10	Korkea riski	Operatiivinen johtaminen ja prosessit				
010	31.12.2014	1	1	1	Matala riski	Henkilöt				
011	31.12.2014	5	2	10	Matala riski	Järjestelmät				
012	31.12.2014	4	3	12	Kohtalainen riski	Ulkoiset tekijät				
013	31.12.2014	3	4	12	Korkea riski	Operatiivinen johtaminen ja prosessit				
014	31.12.2014	2	5	10	Korkea riski	Henkilöt				
015	31.12.2014	1	1	1	Matala riski	Järjestelmät				

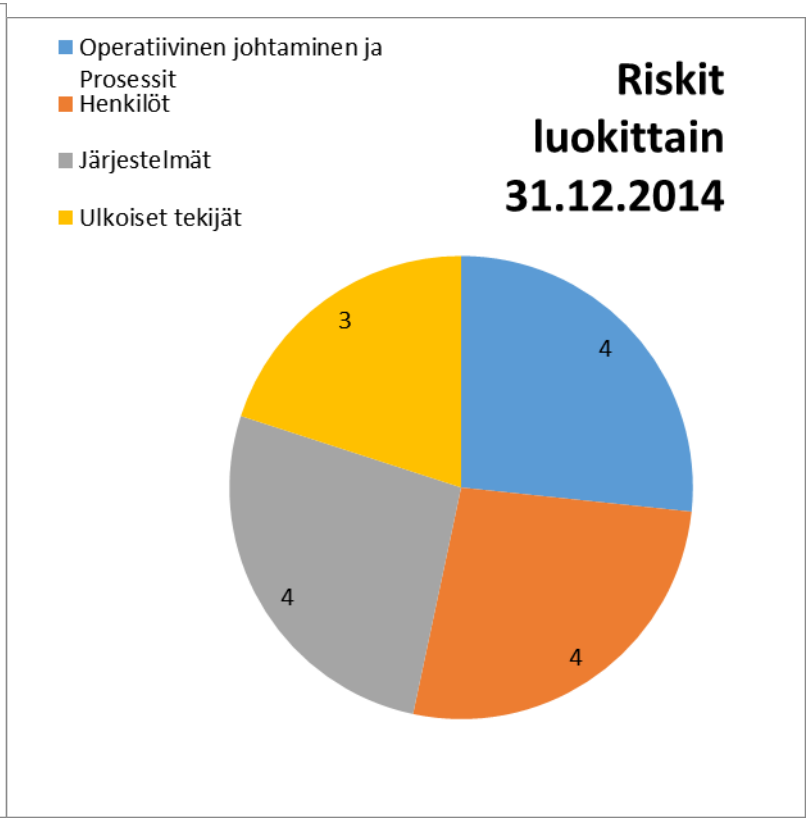
Historiatiedot 3 seurantataulukot



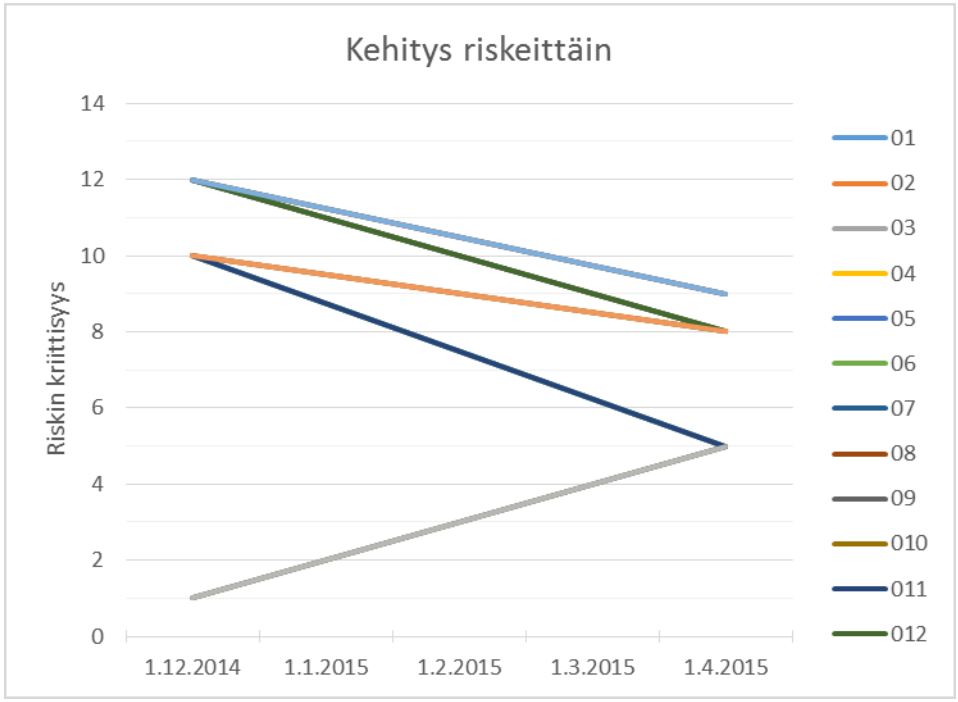


Historiatiedot 4 seurantataulukot





Historiatiedot 5 seurantataulukot



Liite 9. Riskisalkku

Arvioinnin kohde		Arviointi pvm

Riski-tunniste	Riski	Toden-näköisyys (1-5)	Vaikutus (1-5)	Kriittisyys (TN*V)	Riskin suuruus	Vastuu-henkilö	Tavoite-aikataulu	Täytä 1-4	Status	Uhka-luokka
[Tunniste]	[Riski]	1	5	5	Korkea riski	[Henkilö]	p.kk.vvvv	4	Aloitamatta!	Operatiivinen johtaminen ja prosessit
[Tunniste]	[Riski]	2	4	8	Kohtalainen riski	[Henkilö]	p.kk.vvvv	3	Kesken, ei etene.	Henkilöt
[Tunniste]	[Riski]	3	3	9	Matala riski	[Henkilö]	p.kk.vvvv	2	Kesken, etenee.	Järjestelmät
[Tunniste]	[Riski]	4	2	8	Matala riski	[Henkilö]	p.kk.vvvv	1	Kunnossa, ok.	Ulkoiset tekijät
[Tunniste]	[Riski]	5	1	5	Matala riski	[Henkilö]	p.kk.vvvv	4	Aloitamatta!	Operatiivinen johtaminen ja prosessit
[Tunniste]	[Riski]	1	5	5	Korkea riski	[Henkilö]	p.kk.vvvv	3	Kesken, ei etene.	Henkilöt
[Tunniste]	[Riski]	2	4	8	Kohtalainen riski	[Henkilö]	p.kk.vvvv	2	Kesken, etenee.	Järjestelmät
[Tunniste]	[Riski]	3	3	9	Matala riski	[Henkilö]	p.kk.vvvv	1	Kunnossa, ok.	Ulkoiset tekijät
[Tunniste]	[Riski]	4	2	8	Matala riski	[Henkilö]	p.kk.vvvv	4	Aloitamatta!	Operatiivinen johtaminen ja prosessit
[Tunniste]	[Riski]	5	1	5	Matala riski	[Henkilö]	p.kk.vvvv	3	Kesken, ei etene.	Henkilöt
[Tunniste]	[Riski]	1	5	5	Korkea riski	[Henkilö]	p.kk.vvvv	2	Kesken, etenee.	Järjestelmät
[Tunniste]	[Riski]	2	4	8	Kohtalainen riski	[Henkilö]	p.kk.vvvv	1	Kunnossa, ok.	Ulkoiset tekijät
[Tunniste]	[Riski]	3	3	9	Matala riski	[Henkilö]	p.kk.vvvv	4	Aloitamatta!	Operatiivinen johtaminen ja prosessit
[Tunniste]	[Riski]	4	2	8	Matala riski	[Henkilö]	p.kk.vvvv	3	Kesken, ei etene.	Henkilöt
[Tunniste]	[Riski]	5	1	5	Matala riski	[Henkilö]	p.kk.vvvv	2	Kesken, etenee.	Järjestelmät

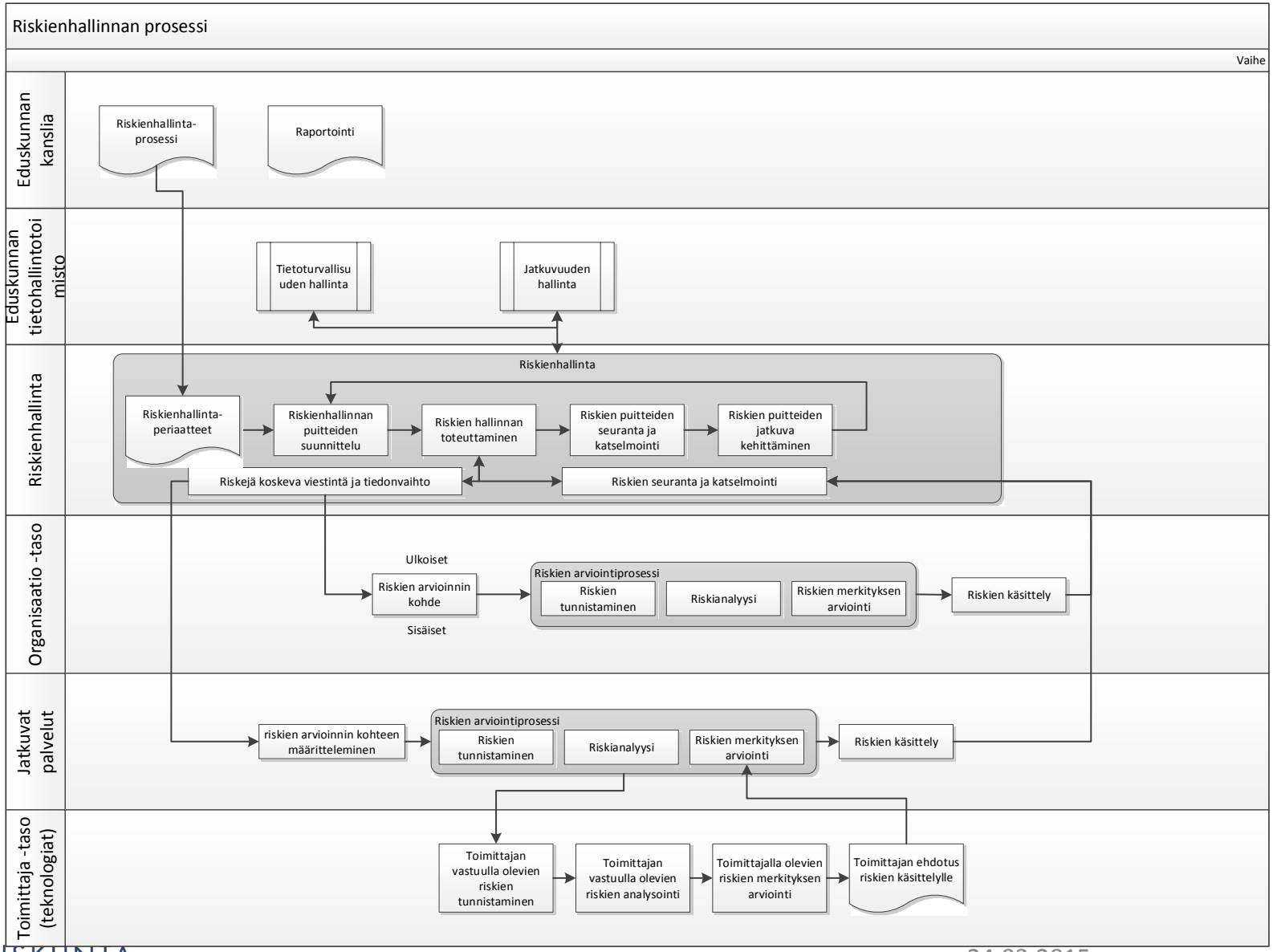
Eduskunnan tietohallintotoimiston riskienhallinnan prosessikuva

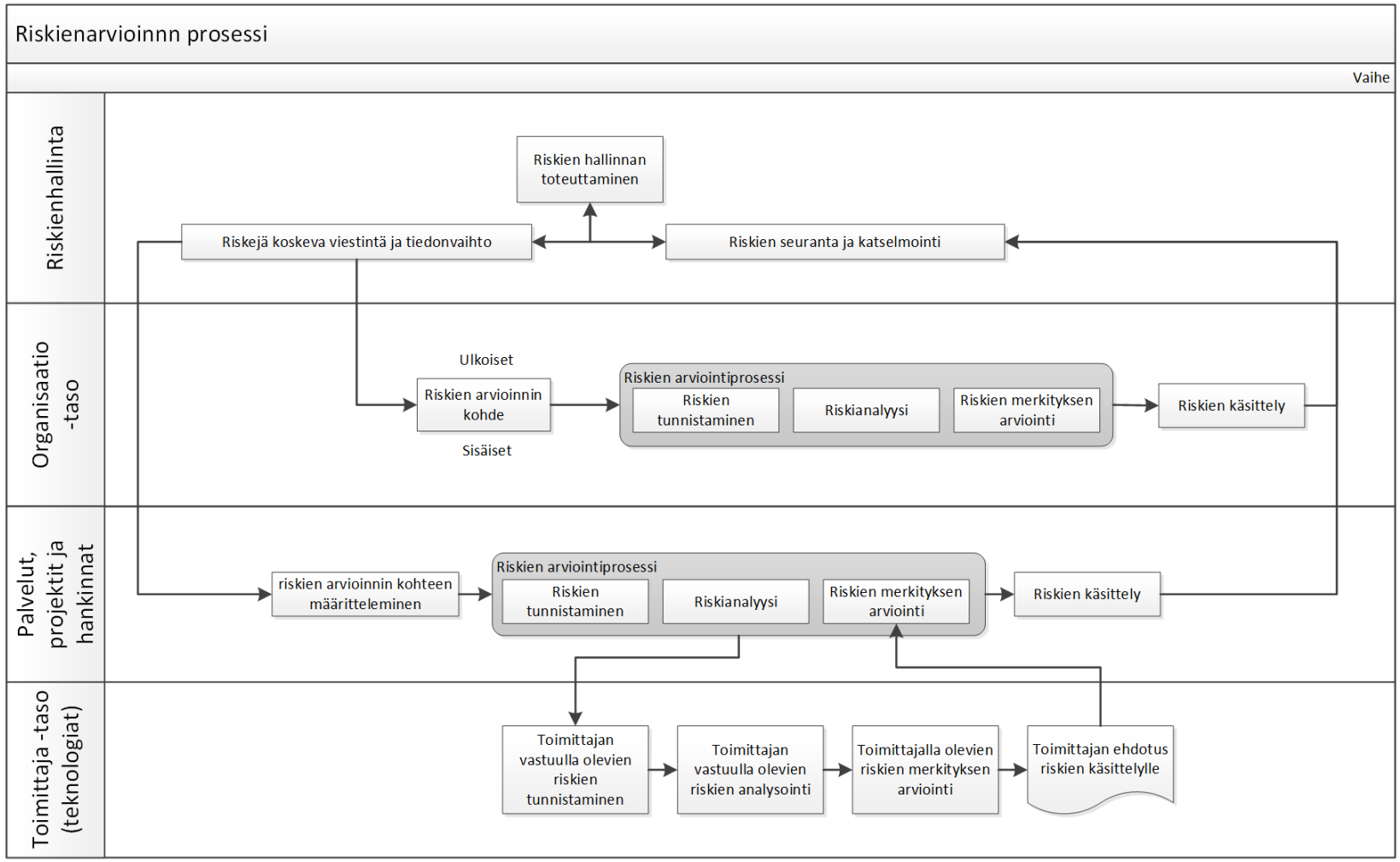
Antti Laulajainen, tietoturvapäällikkö

Versio 1.0 24.03.2015

EDUSKUNTA

Päivämäärä	Versio	Muuttaja	Muutos/Toimenpide	Tila
27.2.2015	0.9	Antti Laulajainen	Dokumentin valmistelu hyväksyttäväksi	luonnos
24.3.2015	1.0	Antti Laulajainen	Tietohallintotoimiston johtoryhmän hyväksyntä	hyväksytty


Riskienhallinnan prosessi
Vaihe
Eduskunnan kanslia
Riskienhallinta-prosessi
Raportointi
Eduskunnan tietohallintotoimisto
Tietoturvallisuuden hallinta
Jatkuvuuden hallinta
Riskienhallinta
Riskienhallinta
Riskienhallinta-periaatteet
Riskienhallinnan puitteiden suunnittelu
Riskien hallinnan toteuttaminen
Riskien puitteiden seuranta ja katselmointi
Riskien puitteiden jatkuva kehittäminen
Riskejä koskeva viestintä ja tiedonvaihto
Riskien seuranta ja katselmointi
Organisaatio -taso
Ulkoiset
Riskien arvioinnin kohde
Sisäiset
Riskien arviointiprosessi
Riskien tunnistaminen
Riskianalyysi
Riskien merkityksen arviointi
Riskien käsittely
Jatkuvat palvelut
riskien arvioinnin kohteen määritteleminen
Riskien arviointiprosessi
Riskien tunnistaminen
Riskianalyysi
Riskien merkityksen arviointi
Riskien käsittely
Toimittaja -taso (teknologiat)
Toimittajan vastuulla olevien riskien tunnistaminen
Toimittajan vastuulla olevien riskien analysointi
Toimittajalla olevien riskien merkityksen arviointi
Toimittajan ehdotus riskien käsittelylle


Riskienarvioinnn prosessi
Vaihe
Riskienhallinta
Organisaatio -taso
Palvelut, projektit ja hankinnat
Toimittaja -taso (teknologiat)
Riskien hallinnan toteuttaminen
Riskejä koskeva viestintä ja tiedonvaihto
Riskien seuranta ja katselmointi
Ulkoiset
Riskien arvioinnin kohde
Sisäiset
Riskien arviointiprosessi
Riskien tunnistaminen
Riskianalyysi
Riskien merkityksen arviointi
Riskien käsittely
riskien arvioinnin kohteen määritteleminen
Riskien arviointiprosessi
Riskien tunnistaminen
Riskianalyysi
Riskien merkityksen arviointi
Riskien käsittely
Toimittajan vastuulla olevien riskien tunnistaminen
Toimittajan vastuulla olevien riskien analysointi
Toimittajalla olevien riskien merkityksen arviointi
Toimittajan ehdotus riskien käsittelylle

Eduskunnan tietohallintotoimiston riskienhallinnan vuosikello

Antti Laulajainen, tietoturvapäällikkö

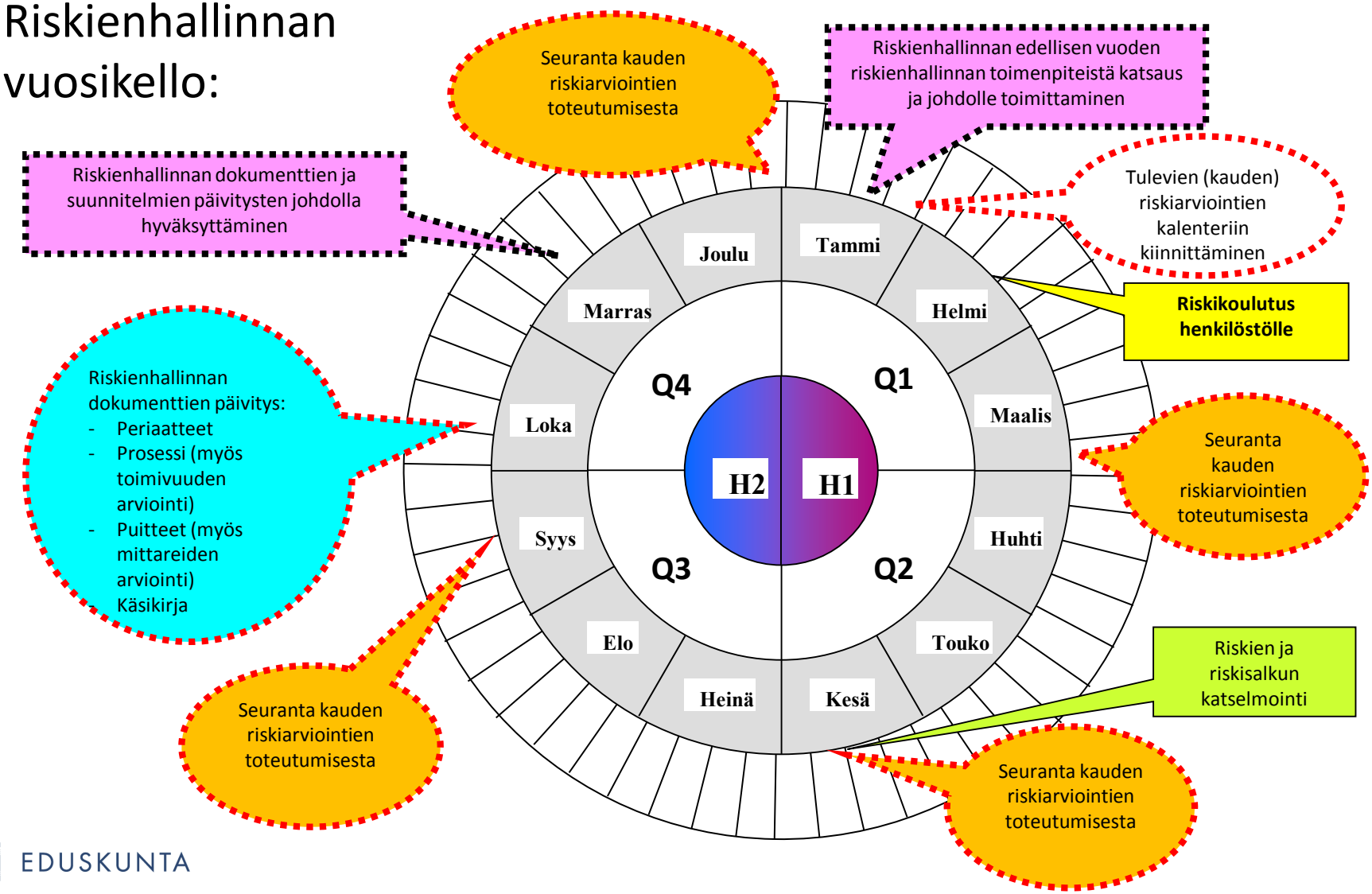
Versio 1.0

7.4.2015

EDUSKUNTA

Päivämäärä	Versio	Muuttaja	Muutos/Toimenpide	Tila
1.4.2015	0.9	Antti Laulajainen	Dokumentin valmistelu hyväksyttäväksi	luonnos
7.4.2015	1.0	Antti Laulajainen	Tietohallintotoimiston johtoryhmän hyväksyntä	hyväksytty

Riskienhallinnan vuosikello:



EDUSKUNTA

Luottamukselliset liitteet

Liite 12. Riskienhallinnan nykymalli

Liite on erillisessä tiedostossa Liite 12.pdf

Liite 13. Tietohallintotoimiston nykyiset riskit

Liite on erillisessä tiedostossa Liite 13.pdf

Liite 14. Tietohallintotoimiston käsitellyt riskit

Liite on erillisessä tiedostossa Liite 14.pdf

Liite 15. Active Directory riskit

Liite on erillisessä tiedostossa Liite 15.pdf

Liite 16. Tietohallintotoimiston riskisalkku

Liite on erillisessä tiedostossa Liite 16.pdf.