LAUREA AMMATTIKORKEAKOULU Uuden edellä

Hallinnon tietotekniikkakeskuksen kokonaisvaltaisen riskienhallinnan kehittämissuunnitelma

Marjamäki-Ruuskanen, Sonja

2013 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Hallinnon tietotekniikkakeskuksen kokonaisvaltaisen riskienhallinnan kehittämissuunnitelma

Sonja Marjamäki-Ruuskanen
Turvallisuusosaamisen koulutusohjelma
Opinnäytetyö
Maaliskuu, 2013

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea
Turvallisuusosaamisen YAMK

Sonja Marjamäki-Ruuskanen

Hallinnon tietotekniikkakeskuksen kokonaisvaltaisen riskienhallinnan kehittämissuunnitelma

Vuosi 2013 Sivumäärä 74

Riskienhallinnan tarkoitus on pyrkiä hallitsemaan organisaation toimintaan kohdistuvia riskejä. Mikäli organisaatiossa ei toteuteta riskienhallintaa, antaa se organisaation toiminnasta ja johtamisesta epävakaan kuvan – organisaatiosta, joka ei täytä sille asetettuja tietoturvavaatimuksia eikä turvaa sen strategisten eikä omistajilleen lupaamiensa tavoitteiden saavuttamista.

Valtionhallinnon virastoissa sovelletaan vuonna 2010 voimaan tullutta tietoturvallisuusasetusta (681/2010) Laissa säädetään viranomaisia koskevista yleisistä tietoturvavaatimuksista ja tietoturvallisuustasoista. Laissa otetaan huomioon myös tietoturvallisuusriskien kartoittaminen.

Tämän opinnäytetyön tarkoituksena oli kehittää Hallinnon tietotekniikkakeskuksen (HALTIK) kokonaisvaltaista riskienhallintaa. Opinnäytetyö suoritettiin konstruktiivisena tutkimuksena, jossa tutkimusongelmaksi asetettiin kokonaisvaltaisen riskienhallinnan vaikuttavuuden parantaminen.

Kehittämistehtävän teoreettinen osuus tapahtui 1.6 - 30.9.2012 välisenä aikana. Kehittämissuunnitelma valmistui loppuvuonna 2012 ja se esitettiin kohdeorganisaation johdolle joulukuussa 2012. Kehittämistyön toimeksiantajana oli Hallinnon tietotekniikkakeskus (HALTIK) ja kehittämistyön valvonnan kohdeorganisaatiossa toteutti kohdeorganisaation riskienhallintapäällikkö.

Opinnäytetyö jakaantuu konstruktiivisen tutkimuksen rakenteen mukaisesti kolmeen pääosaan - teoreettisen taustan hankintaan, käytännöllisen tutkimustiedon hankintaan sekä ratkaisujen laatimiseen. Teoreettisen taustan tarkoituksena oli hankkia tietoa riskienhallinnan toteuttamisesta sekä sen vaikuttavuuden parantamisesta. Tutkimustiedon hankinnassa selvitettiin riskienhallinnan kehittämiseen vaikuttavia asioita. Saadut tiedot mahdollistivat riskienhallinnan kehittämissuunnitelman luomisen.

Kehittämissuunnitelman avulla luotava standardiin pohjautuva kokonaisvaltainen riskienhallinta mahdollistaa kohdeorganisaation riskienhallinnan toteuttamisen yhteisesti hyväksyttyjen menetelmien ja käsitteiden mukaisesti. Tämä mahdollistaa jatkuvan ja toistettavan tavan toteuttaa riskienhallintaa. Kokonaisvaltainen riskienhallinta takaa sen, että kohdeorganisaation strategia, tavoitteet ja arvot ovat lähtökohtana kohdeorganisaation riskienhallinnalle ja että sitä toteutetaan kohdeorganisaation kaikissa prosesseissa. Standardiin pohjautuva kokonaisvaltainen riskienhallinta luo turvallisen ja varman perustan kohdeorganisaation toiminnalle ja takaa kohdeorganisaation johdolle luotettavan työkalun päätöstentekoon parantaen näin sen vaikuttavuutta.
Asiasanat: riski, kokonaisvaltainen riskienhallinta, riskienhallintapolitiikka, valtionhallinto

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Master's Programme in Security Management

Sonja Marjamäki-Ruuskanen

Developing an enterprise risk management plan for the ICT Agency HALTIK

Year 2013 Pages 74

The purpose of risk management is to manage the risks that an organization faces in its operations. If the organization does not execute risk management, it gives an unstable picture of the organization's operations and leadership – an organization that does not fulfill the security demands and secure the achievement of its strategic objective or promises given to the owners.

A government organization needs to apply the Decree on Information Security in Central Government law that was entered into force 2010. The law lays down provisions on general information security requirements and information security levels. The law also takes into account the assessment of the information security risks.

The purpose of this study was to develop the enterprise risk management of the ICT Agency HALTIK. The study was carried out as constructive research, where the research problem was set to improve the effectiveness of the target organization´s enterprise risk management.

The theoretical part of the development task was completed 1.6 - 9.30.2012. The development plan was completed in late 2012, and it was presented to the target organization's management in December 2012. The development process was sponsored by ICT Agency HALTIK and controlled by the risk manager of the target organization.

The study is divided by the constructive research structure into three major sections – the acquisition of theoretical background, the acquisition of practical research data and the establishment of solutions. The purpose of the theoretical background was to obtain information about the implementation of risk management, as well as improvement of its effectiveness. The acquisition of practical research data was to solve the issues affecting the development of the risk management. The data obtained allowed for the creation of the risk management development plan.

The development plan enables the creation of standard based enterprise risk management that allows for the implementation of enterprise risk management in the target organization using commonly accepted methods and concepts accordingly. This enables a continuous and repeatable method for risk management. Enterprise risk management ensures that the target organization's strategy, goals, and values are the basis for the target organization's risk management, and that it is carried out in all the processes of the target organization. Standard based enterprise risk management creates a safe and secure foundation for the target organization's operations and ensures to the target organization's management a reliable tool for decision-making, thereby improving its effectiveness.

Keywords: risk, enterprise risk management, risk management policy, government

Sisällys

1 Johdanto

Liiketoimintaan liittyy aina riski. Riskienhallinnan tavoite on tukea päätöksentekoa yrityksessä siten, että yrityksen johto voisi tehdä merkittävät liiketoimintapäätökset. (Ilmonen, Kallio, Koskinen & Rajamäki 2010, 12.) Toisaalta epävarmuus ja riskit kuuluvat arkipäiväämme. Arkielämässä riskienhallinnalla pyritään etukäteen parantamaan turvallisuutta sekä tulevaisuuden ennustettavuutta. (Kuusela & Ollikainen 2005, 13-15.)

Riskienhallinnan teoriassa tuodaan esille (kappale 2), että riskienhallinta tarjoaa työkalun organisaation strategiselle päätöksenteolle. Organisaatio voi riskienhallinnan avulla päättää minkä strategian valitsee sekä seurata sen toteutumisen mahdollistavia tai haittaavia tekijöitä. Riskienhallinnan avulla parannetaan projektien toimintaa niin aikataulussa pysymisessä kuin sille varatussa rahoituksessa.

Riskienhallinnan avulla organisaatioiden prosessit ja toiminnat kykenevät toimimaan tehokkaammin sekä arvioimaan mahdolliset toimintaan liittyvät häiriöt ja varautumaan niihin etukäteen. Ilman riskienhallintaa organisaatio ei pysty suunnittelemaan toimintansa jatkuvuutta. Ilmonen ym. toteavat, että riskienhallinnan tarkoituksena on lisätä ymmärrystä asioista päätösten ja toimenpiteiden tekemiseksi riskien osalta. Riskienhallinnan toimenpiteet voidaan jakaa mm. varautumiseen ja ennaltaehkäisyyn. Jatkuvuussuunnittelu normaaliolojen häiriötiloja varten on osa varautumista ja ennaltaehkäisyä. (2010, 156.)

Riskienhallintaa varten on kehitetty erilaisia standardeja, joiden tarkoituksena on tarjota riskien arviointiin, hallintaan sekä valvontaan prosessimaisia, hyväksi havaittuja (best practises) toimintatapoja:
"Standardien tarkoitus on hyödyttää koko yhteiskuntaa. Kaikilla aloilla teollisuudesta kauppaan ja tutkimukseen yhteisesti hyväksytyt käsitteet ja määritelmät nopeuttavat työtä, vähentävät virheitä ja auttavat saamaan entistä parempia käytännön tuloksia. Standardien ansiosta tuotteet, palvelut ja menetelmät sopivat siihen käyttöön ja niihin olosuhteisiin, joihin ne on tarkoitettu." (Suomen standardoimisliitto 2012.)

Tämän opinnäytetyön tarkoituksena oli kehittää Hallinnon tietotekniikkakeskuksen (HALTIK) kokonaisvaltaista riskienhallintaa. Tarve kehittämiselle tuli kohdeorganisaation riskienhallintapäälliköltä, jonka alaisuudessa työskentelin opintojeni aikana ja jonka yhtenä tehtävänä oli kehittää organisaation riskienhallintaprosessia.

Kehittämistehtävä toteutettiin tutkimusasettelun mukaisesti konstruktiivisena tutkimuksena. Riskienhallinnan kirjallisuuteen ja teoriaan tutustumisen jälkeen tutkimusongelmaa tarkasteltiin uudelleen ja todettiin, että kohdeorganisaation riskienhallintaa lähdetään kehittämään

riskienhallintastandardin toimiessa viitekehyksenä. Vertailtavina standardeina toimivat kaksi Euroopassa yleisimmin käytössä olevaa riskienhallintastandardia COSO ERM ja ISO 31000 (ks. 2.2) Standardien vertaileminen toteutettiin vertailevana analyysinä.

Kohdeorganisaation kehittämissuunnitelmaa varten toteutettiin GAP – puuteanalyysi valittua riskienhallintastandardia vasten. Vertailtavina dokumentteina toimivat riskienhallinnan perusasiakirjat - riskienhallintapolitiikka sekä – periaatteet. Tämän perusteella luotiin riskienhallinnan kehittämissuunnitelma, jossa hyödynnettiin osin Broadleaf Capital International PTY LTD – yrityksen luomaa dokumenttia How to bring your ERM framework into line with ISO 31000.

Kehittämissuunnitelman avulla kohdeorganisaatiolle luotiin prosessimainen toimintamalli, jossa otetaan huomioon riskienhallinnan kehittämisessä vaadittavat toimenpiteet mukaan lukien riskienhallinnan tärkeimpien asiakirjojen riskienhallintapolitiikan sekä – periaatteen päivittäminen viitekehyksenä käytettävän standardin mukaiseksi.

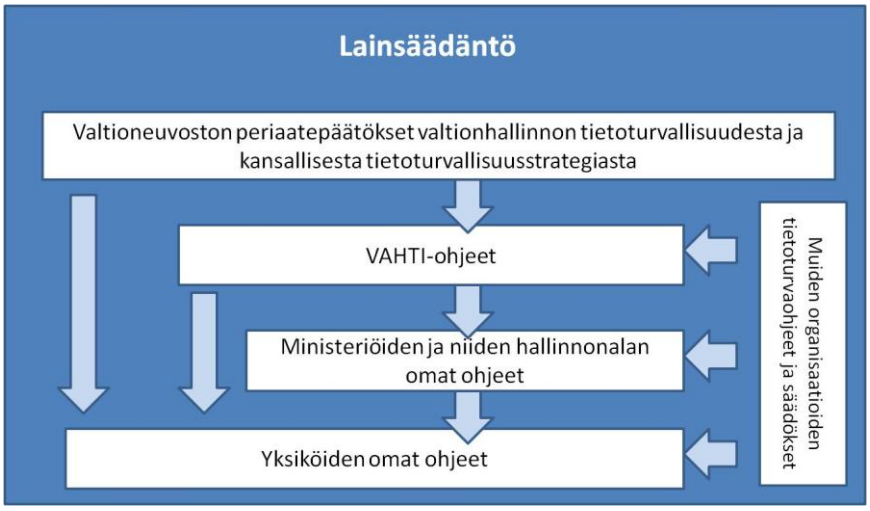
1.1 Kohdeorganisaation esittely

Hallinnon tietotekniikkakeskus (HALTIK) perustettiin vuonna 2008 Poliisin tietohallintokeskuksen pohjalta (PTHK) Kohdeorganisaation päätoimipaikka sijaitsee Rovaniemellä ja kohdeorganisaation palveluksessa on n. 420 henkilöä. Puolet henkilöstöstä työskentelee päätoimipaikassa, loput 29 eri paikkakunnalla suurimpina pääkaupunkiseutu, Kajaani ja Turku.

HALTIK tarjoaa tieto- ja viestintäteknisiä palveluja sekä yhteyspalveluja sisäasianministeriön hallinnonalan organisaatioille. Suurimpina asiakkaina ovat sisä-asianministeriö, poliisi, hätäkeskus, rajavartiolaitos sekä maahanmuuttokohdeorganisaatio. Kohdeorganisaation tehtävät on säädetty valtioneuvoston asetuksessa (810/2007) Tehtävinä ovat tieto- ja viestintätekniikan kehittämis-, asiantuntija-, tietoturva-, tuotanto-, hankinta-, raportointi-, koulutus-, puhelunvälitys-, ja tukipalvelujen tuottaminen sisäasianministeriölle ja hallinnonalan muille kohdeorganisaatioille ja laitoksille. Palveluja tuotetaan myös muille valtion virastoille ja laitoksille siten kuin palvelujen tuottamisesta on sovittu palvelusopimuksissa kyseessä olevien virastojen ja laitosten kanssa. Nettobudjetoitu kohdeorganisaatio toimii sisäasianministeriön alaisuudessa, sisäasianministeriön toimiessa kohdeorganisaation tulosohjaajana. (HALTIK 2011.)

Useat lait, asetukset, määräykset sekä ohjeistukset ohjaavat viranomaisten tietoturvallisuutta. Ensisijaisesti toimintaa ohjaa lainsäädäntö. Valtiovarainministeriön toimialaan kuuluu valtionhallinnon tietohallinnon ohjaus ja sen alaisuudessa toimii Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI. Seuraavana portaassa tulevat ministeriöt ja kyseisen ministeriön

hallinnonalan omat ohjeet. Tämän lisäksi virastoilla voi olla vielä omat tarkentavat ohjeistuksensa. Toiminnassa tulee ottaa huomioon myös sidosryhmien kuten mahdollisten muiden organisaatioiden tietoturvaohjeistukset (ks. kuvio 1)



Kuvio 1: Valtionhallinnon tietoturvallisuuden normisto

Valtioneuvoston tietoturvallisuutta koskevassa periaatepäätöksessä (VNp 11.11.1999) todetaan, että viranomaisilla tulee olla tietoturvallisuuden hallintaa ja ohjausta varten ajantasainen tiedonkäsittelyn turvaamissuunnitelma, vahinkojen varalta toipumissuunnitelma ja poikkeusolojen varalta tiedonkäsittelyn valmiussuunnitelma. Suunnitelmiin sisältyy organisaation tiedonkäsittelyriippuvuuden, tietotekniikan käyttöön liittyvien uhkatekijöiden ja riskien arviointi sekä niiden hallinnan edellyttämien turvaamis-, toipumis- ja varautumistoimenpiteiden määrittely ja toteuttamissuunnitelmat (VAHTI 7 2003, 9).

Tietoturvaa ohjaavista laista mainittakoon mm. laki viranomaisen toiminnan julkisuudesta (621/1999), asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999) Vuonna 2010 voimaan astuneessa Valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010) pykälässä 5 määrätään, että tietoturvallisuuden perustason toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava viranomaisen toimintaan liittyvien tietoturvallisuusriskien kartoittamisesta.

Näiden lisäksi asetus valtion talousarviosta (1243/1992) edellyttää johdon huolehtivan siitä, että kohdeorganisaatiossa toteutetaan sen talouden ja toiminnan laajuuteen ja sisältöön sekä niihin liittyviin riskeihin nähden asianmukaiset sisäisen valvonnan menettelyt. Nämä menettelyt varmistavat talouden ja toiminnan laillisuuden ja tuloksellisuuden, varojen ja omaisuuden turvaamisen sekä johtamisen ja ulkoisen ohjauksen edellyttämät oikeat ja riittävät tiedot kohdeorganisaation taloudesta ja toiminnasta (VAHTI 7 2003, 9).

Kohdeorganisaatiolla on käytössään riskienhallintapolitiikka, joka on tullut voimaan vuoden 2011 lopussa. Tätä tukee vuoden 2012 alussa voimaan tullut riskienhallinnan menettelyohjeistus. Politiikka sekä menettelyohjeistus noudattavat lähinnä valtiovarainministeriön VAHTI ohjeistusta riskienhallinnasta. Kohdeorganisaatiossa toteutettava riskienhallinta ei kohdistu yksittäiseen toimintoon tai prosessiin, vaan sitä noudatetaan kaikissa kohdeorganisaation toiminnoissa ollen näin kokonaisvaltaista riskienhallintaa.

1.2 Tutkimuksen tavoite ja tutkimusongelma

Tämän tutkimuksen tavoitteena on auttaa kohdeorganisaatiota kehittämään kokonaisvaltaisen riskienhallintansa vaikuttavuutta. Tutkimuksessa selvitetään ensin riskienhallinnan teoriaa riskienhallinnan kehittämisen taustaksi. Tämän jälkeen tutkimusongelmaa sekä tutkimuskysymystä tarkastellaan uudelleen opitun teorian valossa.

Kohdeorganisaatiolla on käytössään ISO 27001 standardin mukaisesti toteutettu tietoturvallisuuden hallintajärjestelmä, jota riskienhallinnan kehittämisessä tullaan hyödyntämään. Hallintajärjestelmän avulla kohdeorganisaation riskienhallintapäällikkö pystyy jalkauttamaan standardin perusteella rakennettua riskienhallintaa organisaation eri osiin ja prosesseihin tehokkaammin sekä varmistamaan sen jatkuva parantaminen ilman, että se olisi erillinen osa kohdeorganisaation tietoturvallisuuden hallintaa. Tämän lisäksi kohdeorganisaation johdon tavoitetilana on, että riskienhallinta on kokonaisvaltaista, ei kohdeorganisaation eri osastoissa ja toiminnoissa erillisesti toimiva tapahtuma.

Kohdeorganisaation tarpeet riskienhallinnalle tulevat kohdeorganisaatiolle asetetuista ulkoisista vaatimuksista (ks. luku 1.1) Tämän lisäksi kohdeorganisaation luoma, sertifioitu tietoturvallisuuden hallintajärjestelmä asettaa omat vaatimuksensa koskien riskienhallintaa.

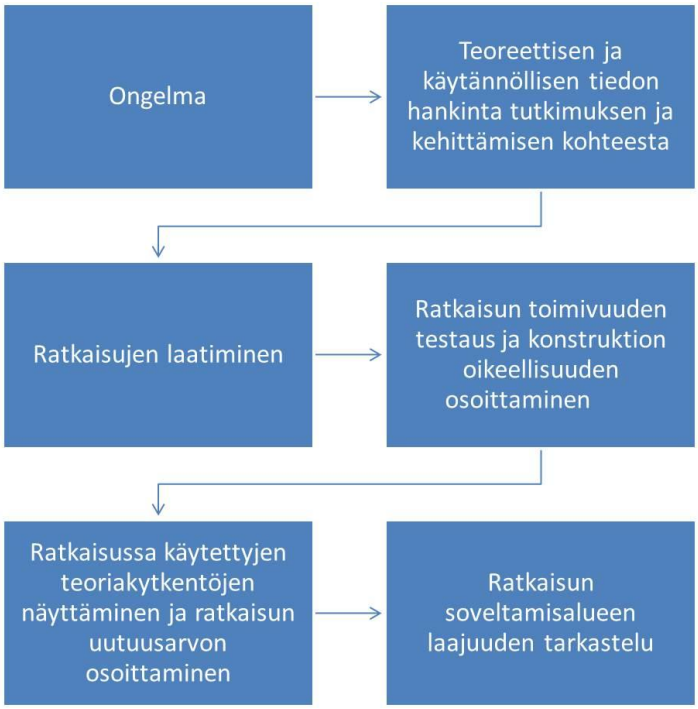
Riskienhallintapäällikön tahtotilana on parantaa olemassa olevan riskienhallintaprosessin vaikuttavuutta. Kehittämissuunnitelman pääkysymyksenä onkin kuinka saada kohdeorganisaation nykyisestä kokonaisvaltaisesta riskienhallinnasta vaikuttavampi huomioonottaen kaikki olennaiset riskienhallintaprosessiin liittyvät elementit mukaan lukien sen kokonaisvaltaisuus?

1.3 Konstruktiivinen tutkimus

Tutkimuskysymyksen asettelun perusteella tutkimus toteutettiin konstruktiivisena tutkimuksena. Konstruktiivisen tutkimuksen tavoitteena on käytännön ongelman ratkaisu luomalla uusi konkreettinen tuotos kuten esimerkiksi suunnitelma, malli tai menetelmä. Muutos kohdistuu johonkin konkreettiseen kohteeseen. (Ojasalo, Moilanen & Ritalahti 2009, 38.)

Uuden luomiseksi tarvitaan olemassa olevaa teoreettista tietoa ja käytännöstä kerättävää tietoa. Kehitystyön tuloksena syntyneitä tuotoksia arvioidaan niiden käytännön hyödyn perusteella. Konstruktiivisessa tutkimuksessa käytännön toimijat ovat aktiivisesti mukana ratkaisun laatimisessa ja tutkimus korostaakin sen hyödyntäjien ja toteuttajien välistä vuorovaikutusta ja kommunikaatiota. Toimeksiantajan on aina sitouduttava kehittämistyöhön. (Ojasalo ym. 2009, 65 – 66.)

Konstruktiivinen tutkimus etenee alla olevan kuvan mukaisesti vaiheittain. Eri vaiheiden dokumentointi on tärkeää ja siinä käytettävät metodit tulee perustella huolellisesti.



Kuvio 2: Konstruktiivisen tutkimuksen prosessi

Konstruktiivisen tutkimuksen ratkaisun toimivuutta voidaan käytännössä arvioida myöhemminkin. Tämän takia tutkimuksen testaus saattaa puuttua erityisesti silloin, kun kyse on opinnäytetyöstä tai muusta työstä, joka on sidottu joltakin osin muun kuin kohdeorganisaation aikatauluihin. (Ojasalo ym. 2009, 68.) Tämän tutkimuksen ratkaisujen testausta ei opinnäytetyön aikatauluista johtuvista syistä suoritettu.

1.4 Riskienhallinnan keskeiset käsitteet

Kehittämissuunnitelman tarkoituksena on kehittää organisaation määrittelemää toimintaa haluttuun suuntaan. Kehittämissuunnitelman tarkoituksena on selvittää organisaation nykytila, hankkia tietoa kehitettävästä asiasta ja luomaan suunnitelman, jonka avulla organisaation tulisi päästä haluttuun tavoitteeseen.

Kokonaisvaltainen riskienhallinta tarkoittaa riskienhallintaa, jota toteutetaan läpi koko organisaation ja johon vaikuttavat yhtiön hallitus, johto ja työntekijät.

Riskienhallinta tarkoittaa tapaa, jolla organisaatio pyrkii hallitsemaan siihen kohdistuvia riskejä, riskin vaikuttaen organisaatioon negatiivisesti tai positiivisesti. Riskienhallinta on prosessi, jonka avulla toteutetaan riskienhallinnan toimenpiteitä (analysointi & arviointi), seurataan edistymistä ja tarkastellaan, mitä seuraavaksi pitäisi tehdä.

Standardi on yhteinen menettelytapa toistuvaan toimintaan. Se on standardisoinnista huolehtivan viranomaisen, järjestön tai muun tunnustetun elimen hyväksymä kirjallinen julkaisu. (SFS 2012.)

Vaikuttavuus määritellään ISO 9000 laatustandardin mukaan siten, missä määrin suunnitellut toimenpiteet toteutetaan ja tulokset saavutetaan. Tässä kehittämissuunnitelmassa käytettynä sanalla vaikuttavuus tarkoitetaan kehittämissuunnitelman avulla toteutettuja toimenpiteitä, joiden pyrkimyksenä on parantaa kohdeorganisaation kokonaisvaltaista riskienhallintaprosessia.

2 Riskienhallinnan teoreettinen tausta

Suunnitelman teoreettisen viitekehyksen muodostaa tässä luvussa esitelty riskienhallinnan teoria sekä kehittämissuunnitelmassa käytetty riskienhallintastandardi. Koska kyseessä on valtionhallinnon organisaatio, tulee yleensä yrityksien näkökulmasta tarkasteltua riskienhallintaa soveltaa valtionhallinnon kohdeorganisaatioon.

Riski määritellään eri teoksissa eri tavalla. Valtionhallinnon tietoturvasanasto määrittelee sanan riski seuraavanlaisesti (VAHTI 8 2008, 80):
1) todennäköisyys, että uhka toteutuu aiheuttaen tietyn menetyksen tai vahingon
2) uhkaan liittyvän vahingon rahallinen arvo tai odotusarvo (= arvo x todennäköisyys)

ISO 31000 riskienhallintastandardin määritelmän mukaan riski on sitä, että epävarmuus vaikuttaa asetettuihin tavoitteisiin. Vaikutus voidaan mieltää niin negatiivisesti kuin positiivisesti. COSO ERM standardi määrittelee riskin mahdollisuutena jossa tapahtuma ilmenee ja vaikuttaa haitallisesti tavoitteen saavuttamiseen. Riskiä voidaan ajatella myös arjessa, jolloin sanaa riski käytetään kuvaamaan onnettomuuden mahdollisuutta.

Riskejä voidaan jakaa eri kategorioihin. Hopkin jakaa kirjaan Fundamentals of Risk Management (2010) riskit kolmeen eri kategoriaan. Kategoriat voivat vaihdella riippuen siitä, mistä näkökulmasta riskejä tarkastellaan:

- hazard (or pure) risks - tilanne tai tapahtuma, joka aiheuttaa negatiivisen riskin. Esim. varkaus
- control (or uncertainty) risks - tapahtuman tulokseen vaikuttava negatiivinen riski (hallintaan liittyvä riski) Käytetään usein projektien hallinnassa
- opportunity (or speculative) risks - tahallisen riskin ottaminen esim. liiketoiminnassa tuoton parantamiseksi. Riskin ottamisella voi olla positiivinen tai negatiivinen tulos

Yllä olevan kategorian perusteella on hyvä huomioida, että riskillä voi olla myös positiivinen lopputulos. Riski mielletään yleensä aina negatiivisena asiana, mutta riskin ottaminen voi olla myös maineen tai talouden kannalta kannattava toimenpide.

Riskejä yritetään hallita, jotta ne eivät olisi enää pelottavia ja hallitsemattomia. Riskienhallinnan avulla organisaatio pyrkii varautumaan tunnistamiinsa riskeihin. Edellä esitetyn riskikategorian mukaan voidaan ajatella organisaation hallitsevan niitä riskejä, jotka voivat estää asetettujen tavoitteiden saavuttamisen (hazard risk), lisätä tavoitteiden saavuttamisen mahdollisuuksia (opportunity risk) tai luoda epävarmuutta niiden saavuttamisessa (control risk) (Hopkin 2010, 3).

Riskienhallinta on johdon työkalu, jonka avulla organisaation johto saa tarvittavaa ja tärkeää tietoa liiketoimintapäätöstensä tueksi. "Kun [organisaatio] pyrkii riskienhallinnallisin keinoin ymmärtämään sekä tulevia mahdollisuuksiaan että riskejään, erilaisten [organisaation] toimintakenttään ja markkinoihin liittyvien ilmiöiden ja trendien ymmärtäminen helpottuu huomattavasti. [Organisaation] johto kykenee tällöin ottamaan tehokkaammin huomioon alan ja toimintaympäristön muutospaineet osana johtamistaan. (Ilmonen ym. 2010, 18.)

Riskit voidaan jakaa riskilajeihin riskien kartoittamisen helpottamiseksi. Erään klassisien riskifilosofian Gahnin mukaan yrityksen riskejä voidaan tarkastella lähtemällä liikkeelle yrityksen toiminnoista kuvion 3 mukaisesti (Suominen 2003, 13). Suominen lisää, että liike- ja vahinkoriskit eivät ole erillisiä riskejä, vaan ne riippuvat toisistaan.

Kuvio 3: Riskilajit jaoteltuna Gahnin mallin mukaisesti

Toinen tapa luokitella riskit on jaotella ne neljään eri riskilajiin. Alla olevassa kuviossa näkyy Johda Riskejä- teoksen mukainen riskijaottelu (Ilmonen ym. 2010, 70–71).

Kuvio 4: Riskilajit Ilmonen ym. mallin mukaan

Riskien lajittelu riippuu yrityksen/organisaation luonteesta eikä täten voida antaa mitään yksiselitteistä luetteloa, joka pätisi kaikkiin organisaatioihin. Kuten Harri Koskenranta antamassaan haastattelussa teoksessa Heikoin lenkki (Flink, Reiman & Hiltunen 2007, 25) toteaa

"kaikki riskijaottelut ovat oikeita, mikäli jako on organisaation toiminnan kannalta tarkoituksenmukainen".

2.1.1 Riskienhallinnan prosessi

Perinteinen riskienhallinta noudattaa prosessia, jonka avulla riskienhallinta etenee suunnitelman mukaisena, vaiheittaisena prosessina. Yritystoiminnassa riskienhallintaprosessin avulla yritystä uhkaavia vaaroja voidaan torjua ja niistä aiheutuvia menetyksiä minimoida (Suominen 2003, 27). Riskienhallintaprosessin avulla toteutetaan riskienhallinnan toimenpiteitä, seurataan edistymistä ja tarkastellaan, mitä seuraavaksi pitäisi tehdä. Kuten kaikki prosessit, myös riskienhallintaprosessin tulisi noudattaa jatkuvan parantamisen- kaavaa.

Harringtonin ja Niehaus (2003, 8-9) esittävät riskienhallintaprosessin sisältävän viisi vaihetta. Samat periaatteet koskevat teoksen mukaan niin liiketoiminta- kuin yksittäisten riskien hallintaa:

- merkittävien riskien tunnistaminen
- vahinkojen todennäköisyyden ja vakavuuden arviointi
- riskienhallintamenetelmien kehittäminen ja sopivien valitseminen
- riskienhallintapäätökset
- toteutettujen riskienhallintaratkaisujen arviointi

Riskienhallinnan edetessä tietyssä suunnitellussa järjestyksessä, voidaan puhua riskianalyysistä, jonka tehtävänä on selvittää riskikohteet, riskien todennäköisyys, riskien vakavuus ja riskeistä aiheutuvat seurausvaikutukset (Suominen 2003, 35). Tässä suunnitelmassa tullaan käyttämään termiä riskienhallintaprosessi, mikä kuvaa parhaiten riskienhallinnan prosessimaista, jatkuvaa toimintatapaa.

Ensin tulee tunnistaa merkittävät riskit. Organisaation tulee havaita heihin kohdistuvia vaaratilanteita käyttäen eri menetelmiä. Vaaratilanteiden eri riskien tunnistamisen jälkeen arvioidaan niiden laajuutta ja seurauksien vaikutuksia. Tämän avulla riskit jaotellaan kriittisyyden mukaan.

Riskin todennäköisyyttä arvioidaan eri mallien mukaan. VAHTI 7/2003 luokittelee todennäköisyyden alla olevassa taulukossa esitetyn asteikon mukaisesti (2003):

Taulukko 1: VAHTIn mukainen esimerkki riskin todennäköisyyden arvioinnista

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 toteuttaminen on mahdollista tietyille käyttäjäryhmille (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 vain yksittäisille työntekijöille (asiantuntijat)
Ei merkitystä	• Todennäköisyys on tasan nolla. Tämä uhka ei voi toteutua missään olosuhteissa

Todennäköisyyttä voidaan myös luonnehtia asteikolla 1-5 äärimmäisen harvinaisesta riskistä erittäin todennäköiseen riskiin (Suominen 2003, 44).

Riskin laajuus voidaan arvioida joko sanallisessa muodossa kuten yllä tai esittämällä euromääräisiä vahinkolukuja. VAHTI esittää seurauksen arvioinnissa mm. seuraavia taulukon 2 mukaisia määritelmiä (VAHTI 7 2003, 42–43):

Taulukko 2: VAHTIn mukainen esimerkki riskin seurauksen arvioinnista

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 vaikutuksia 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 laajuutta voidaan sanallisesti kuvata myös sanoilla lievästi haitallinen, haitallinen ja erittäin haitallinen.

Kertomalla riskin todennäköisyyden arvo ja seurauksen arvo saadaan riskin merkittävyys tai suuruus, kuten joissakin kirjoissa sitä kutsutaan.
riskin merkittävyys = todennäköisyys x riskin laajuus/vakavuus

Näin riskit saadaan järjestettyä merkittävyytensä mukaan eri järjestykseen sekä priorisoitua niiden käsittelyjärjestys. Riskinhallinta keskittyy ensisijaisesti korkeimman prioriteetin omaaviin, kriittisiin riskeihin.

Riskienhallintatoimenpiteiden tarkoituksena on saattaa riski hyväksyttävälle tasolle. Riskienhallintakeinoina ovat riskin hyväksyminen, pienentäminen, poistaminen ja välttäminen sekä siirtäminen. (Ilmonen ym. 2010, 97.) Riskienhallintatoimenpiteiden jälkeen tulee arvioida riski uudelleen jolloin nähdään, ovatko tehdyt toimenpiteet vähentäneet riskien merkittävyyttä. Tällä saadaan myös selville, tarvitaanko mahdollisesti lisätoimia riskin vähentämiseksi vai onko riski saatu sellaiselle tasolle, että sen toteutuessa organisaatio pystyy sen käsittelemään. "Riskinkantokyky voi parhaimmillaan olla hyvinkin tarkka euromääräinen raja, mutta useissa tapauksissa se on määrittelemätön johdon yleinen käsitys asioiden tasosta ja siitä, kuinka paljon riskiä yritys voi perustellusti ottaa". (Ilmonen ym. 2010, 99.)

2.1.2 Kokonaisvaltainen riskienhallinta

Kehittämissuunnitelmassa painotetaan kohdeorganisaation kokonaisvaltaista riskienhallintaa, ei riskienhallintaa yksittäisenä toimintona. Kokonaisvaltaisen riskienhallinnan määritelmä on kuvattu teoksessa Riskit ja riskienhallinta (Leino M., Steiner M-L. & Wahlroos J. 2005, 126) seuraavanlaisesti:
"Kokonaisvaltainen riskienhallinta on prosessi, johon vaikuttavat yhtiön hallitus, johto ja työntekijät. Sitä toteutetaan strategia- ja suunnitteluprosessissa koko organisaatiossa. Se on kehitetty tunnistamaan seikkoja, jotka voivat vaikuttaa yhtiöön ja hallitsemaan riskejä määritellyn riskinottohalun piirissä, jotta yhtiön tavoitteiden saavuttaminen olisi riittävän luotettavalla pohjalla."

Yllä oleva määritelmä kuvaa mielestäni hyvin kokonaisvaltaisen riskienhallinnan idean. Se todellakin on prosessi, johon vaikuttavat kohdeorganisaation johto sekä työntekijät ja sitä toteutetaan koko organisaatiossa. Juuri tämän takia myös kehittämissuunnitelman kohteena oleva kohdeorganisaatio on valinnut kokonaisvaltaisen riskienhallinnan. Suominen on osuvasti teoksessaan todennut, että riskienhallinta ei toimi riittävän tehokkaasti jos se jätetään pelkästään riskienhallinnan ammattilaisten hoidettavaksi (Suominen 2003, 30). Hän lisää myös, että ollakseen tehokas, riskienhallinnan tulee toimia kaikilla organisaation tasoilla.

Teoksessa Johda riskejä kuvataan kokonaisvaltainen riskienhallinta systemaattisena prosessina, jolla yrityksen tavoitteita, prosesseja ja kilpailuetuja uhkaavat merkittävimmät riskit kerätään, arvioidaan, hallitaan, raportoidaan sekä koko prosessia seurataan ja kehitetään. Ilmonen ym. jatkavat, että kokonaisvaltaisen riskienhallinnan tavoitteena on sen integroituminen osaksi liiketoimintaa. (2010, 93–94.)

2.1.3 Riskienhallintapolitiikka ja riskienhallintaperiaatteet

Riskienhallinnan kehittämisen lähtökohtana ovat riskienhallinnan tavoitteet ja periaatteet organisaatiotasolla. Riskienhallintaan liittyvä ohjeistus pitää yleensä sisällään seuraavat asiakirjat: riskienhallintapolitiikka, - periaatteet ja toimintaohjeet. Riskienhallintapolitiikka on organisaation johdon hyväksymä dokumentti, jossa kuvataan riskienhallinnan periaatteet, tavoitteet, kattavuus ja mitä riskillä tarkoitetaan. Riskienhallintapolitiikan avulla organisaatio omaksuu yhteisen riskienhallintatermistön. Riskienhallintapolitiikassa kuvataan yleensä myös riskienhallinnan osapuolten roolit ja tehtävät. Politiikka on yleensä lyhyt, muutaman sivun pituinen asiakirja ja sitä tulee arvioida säännöllisesti. (Leino ym. 2010, 128).

Leino ym. mukaan riskienhallinnan periaatteet dokumentaatio sisältää yleensä seuraavat kuvaukset (2010, 128):

- riskienhallinnan strategiat ja tavoitteet
- riskienhallintaprosessi
- merkittävimmät riskialueet
- yksityiskohtaisemmat organisatoriset vastuut
- menetelmät joilla riskienhallinnan onnistumista mitataan
- miten johto varmistuu riskienhallinnan prosessien ja toimenpiteiden tehokkuudesta ja riittävyydestä

Riskienhallinnan toimintapolitiikat voidaan laatia erillisinä ohjeina ja kuvauksina, jotta eri alueiden vastuuhenkilöt saavat tarkemman käsityksen oman alueensa toiminnasta ja menetelmistä riskienhallinnassa. Tämän avulla voidaan eriyttää yhteiset osat, riskienhallinnan periaatteet -asiakirjasta ja toimintapolitiikat pienemmille ryhmille sopiviksi. (Leino ym. 2010, 129.)

2.2 Riskienhallintastandardit

Riskienhallintastandardit kattavat laajasti koko riskienhallinnan ja siihen liittyvät osa-alueet. Perinteinen riskienhallinta on yksittäistä operatiivisen tason vakuuttamiseen liittyvää riskienarviointia. Kokonaisvaltainen riskienhallinta tarkoittaa taasen johdon työkalua, jossa lähdetään yrityksen arvoista ja strategiasta, jotka luovat perustan ja suunnan riskienhallinnalle. (Ilmonen ym. 2010, 46–47.)

Ensimmäinen riskienhallintastandardi julkaistiin Australiassa vuonna 1995. Tämän jälkeen niitä julkaistiin niin Kanadassa, Japanissa kuin Yhdysvalloissa. Standardeja kehittävät kansainväliset standardiorganisaatiot sekä valtioiden laitokset ympäri maailmaa. (Hopkin 2010, 53.)

Suomessa standardisoinnin keskusjärjestönä toimii Suomen Standardoimisliitto SFS ry, jonka päätehtäviä on standardien laadinta ja julkaiseminen. Suomen standardoimisliiton mukaan standardien avulla lisätään turvallisuutta ja järkeistetään toimintaa. Niiden avulla tuotteet, palvelut ja menetelmät sopivat siihen käyttöön joihin ne on tarkoitettu. SFS:n mukaan standardien avulla parannetaan toiminnan vaikuttavuutta ja tehokkuutta. (SFS 2012.)

FERMAn (Federation of European Risk Management Associations) toteutti vuonna 2012 riskienhallinnan tutkimuksen (Keys to Understanding the Diversity of Risk Management in a Riskier World) Tutkimukseen vastasi 809 eurooppalaista yksityisen ja julkisen sektorin edustajaa (3 % vastaajista edusti Suomea). FERMAn toteaa, että tutkimuksen (taulukko 3) perusteella riskienhallintastandardien käyttö ei vielä ole hallitseva tapa toteuttaa riskienhallintaa. Riskienhallinnassa tukeudutaan pääasiassa sisäisiin, organisaation omiin viitekehyksiin. Riskienhallintastandardien käyttö on kuitenkin kasvamassa edelliseen, vuonna 2010 tekemään tutkimukseen verrattuna. Vielä ei kuitenkaan ole havaittavissa johtavaa standardia, jota eurooppalaiset organisaatiot riskienhallintaprosessissaan toteuttaisivat. (FERMA 2012.) Huomattavaa kuitenkin on ISO 31000 standardin nousu vuoden 2010 tutkimukseen verrattuna.

Taulukko 3: FERMAn toteuttaman European Risk Management Benchmarking Survey 2012 tulokset koskien riskienhallintastandardin käyttöä

Riskienhallintastandardi	Organisaatiolla käytössä oleva standardi (vastaajia 809 kpl)	Vuoden 2010 tutkimukseen verrattuna (vastaajia 782 kpl)
Organisaation sisäinen viitekehys	37 %	-
COSO ERM	29 %	30 %
ISO 31000	25 %	13 %
Ei käytössä olevaa riskienhallintastandardia	23 %	47 %
Kansalliset riskienhallintastandardit	13 %	23 %

Seuraavissa kappaleissa tutustumme FERMAn 2012 teettämän tutkimuksen perusteella kahteen yleisimmin käytössä olevaan riskienhallintastandardiin ja niiden perusteisiin.

2.2.1 COSO ERM

Committee of Sponsoring Organizations of the Treadway Commission (COSO) julkaisi vuonna 1992 viitekehyksen sisäinen valvonta – kokonaisvaltaisen ajatusmalli (Internal Control – Integrated Framework). Julkaisun tarkoituksena oli amerikkalaisten yritysten sisäisen valvonnan

ongelmien korjaaminen, joita ilmeni varsinkin 70- luvulla runsaasti. Tuolloin monissa yrityksissä annettiin virheellisiä, positiivisen tuloksen omaavia kirjanpitotietoja juuri ennen yrityksen kaatumista. Tämän seurauksena Yhdysvaltain kongressi sääti lain, jonka mukaan edellä kuvatun kaltaiset tapaukset tulee estää. Lakia ei kuitenkaan koskaan allekirjoitettu, mutta tämän seurauksena ryhmä yksityisen sektorin ammattilaisia päätti aloittaa asian tutkimisen ja kehittämisen. Ryhmää tuki viisi amerikkalaista kaupallisen alan organisaatiota ja ryhmän nimeksi tuli lyhennelmä COSO.

Sisäinen valvonta -viitekehyksen julkaisun jälkeen tuli esiin tarve myös toisenlaiselle standardille. Tuolloin riskienhallinta ymmärrettiin pääasiassa vakuutusalalle liittyvänä toimintona jota toteutettiin eri aloilla erilaisin tavoin. Riskienhallinnan prosesseja ei myöskään ollut kuvattuna. Tämän lisäksi riskienhallintaan saatettiin toteuttaa yrityksen eri osissa, ilman että niiden tuloksia tai prosesseja olisi millään lailla yhdistetty.

Tämän tarpeen seurauksena COSO päätti kehittää kokonaisvaltaisen riskienhallinnan standardin, jonka avulla saatiin yhtenäinen määritelmä sanalle riskienhallinta sekä kuvattua sen käyttö koko organisaation kattavana, yhteisenä toimintona. COSO ERM (Enterprise Risk Management) julkaistiin vuonna 2004 ja siitä lähtien se on ollut yksi tunnetuimmista riskienhallintastandardeista.

COSO ERM on amerikkalaisena riskienhallintastandardina saanut runsaasti käyttäjiä juurikin amerikkalaisista sekä Amerikassa toimivista yrityksistä. Tämä johtuu myös siitä, että vuonna 2002 säädettiin Sarbanes-Oxley laki, jonka tarkoituksena on mm. asettaa organisaation johtajille henkilökohtaiseen vastuuseen organisaationsa dokumentaatiosta, niiden tarkastamisesta sekä organisaation sisäisistä valvontakeinoista. Laki määrää, että organisaation tulee toteuttaa toiminnassaan COSOn sisäisen valvonnan ajatusmallia (Internal Control – Integrated) Vaikka laki julkaistiin ennen COSO ERM standardia, on se otettu organisaatioissa käyttöön COSOn sisäisen valvonnan ajatusmallin kautta. (Moeller ja Wiley John & Sons 2007, 239.)

Kuten edellä on jo todettu, ovat COSO kokonaisvaltainen riskienhallinta ja COSO sisäinen ajatusmalli kaksi eri asiaa. Tämä on hyvä tarkentaa selvennyksen vuoksi. COSO ERM viitekehystä ei ole saatavilla suomenkielisenä.

COSO ERM määrittelee kokonaisvaltaisen riskienhallinnan seuraavanlaisesti:
"Organisaation riskienhallinta on sen hallituksen, johdon ja muun henkilökunnan toteuttama prosessi, jota sovelletaan strategian laadinnassa ja koko organisaatiossa. Tarkoituksena sillä on tunnistaa organisaatioon vaikuttavia potentiaalisia tapahtumia ja pitää riskit riskinottohalukkuuden rajoissa, jotta voidaan olla kohtuullisen varmoja organisaation tavoitteiden toteutumisesta". (Committee of Sponsoring Organizations of the Treadway Commission 2004, 4.)

COSO ERM voidaan kiteyttää seuraaviin pääperiaatteisiin (Committee of Sponsoring Organizations of the Treadway Commission 2004, 4):
Johto punnitsee organisaationsa riskinottohalukkuutta arvioidessaan strategisia vaihtoehtoja, asettaessaan niihin liittyviä tavoitteita ja kehittäessään mekanismeja niihin liittyvien riskien hallintaan.

Vastataan riskeihin tehokkaammin. Organisaation riskienhallinta pakottaa määrittämään, kuinka riskeihin vastataan ja valitsemaan eri vaihtoehtojen välillä. Riskit voidaan välttää, hyväksyä tai jakaa tai niitä voidaan vähentää.

Vähennetään toiminnallisia yllätyksiä ja tappioita. Organisaatiot kykenevät tunnistamaan potentiaalisia tapahtumia ja vastaamaan niihin paremmin. Näin yllättävät tilanteet ja niistä aiheutuvat kustannukset ja tappiot vähenevät.

Tunnistetaan ja hallitaan monitahoisia ja koko organisaatiota koskevia riskejä. Jokaisella organisaatiolla on valtava määrä erilaisia riskejä, jotka vaikuttavat organisaation eri osiin. Riskienhallinnan avulla johto voi tehokkaammin reagoida ristikkäisiin vaikutuksiin ja reagoida kokonaisvaltaisesti monitahoisiin riskeihin.

Tartutaan tilaisuuksiin. Otetaan huomioon kaikki potentiaaliset tapahtumat organisaation johto kykenee tunnistamaan niihin sisältyvät mahdollisuudet ja hyödyntämään niitä ennakoivasti

Käytetään pääomaa tehokkaammin. Yksiselitteinen riskitieto auttaa johtoa arvioimaan tehokkaasti pääoman kokonaistarvetta ja kohdentamaan pääoman käytön entistä paremmin.

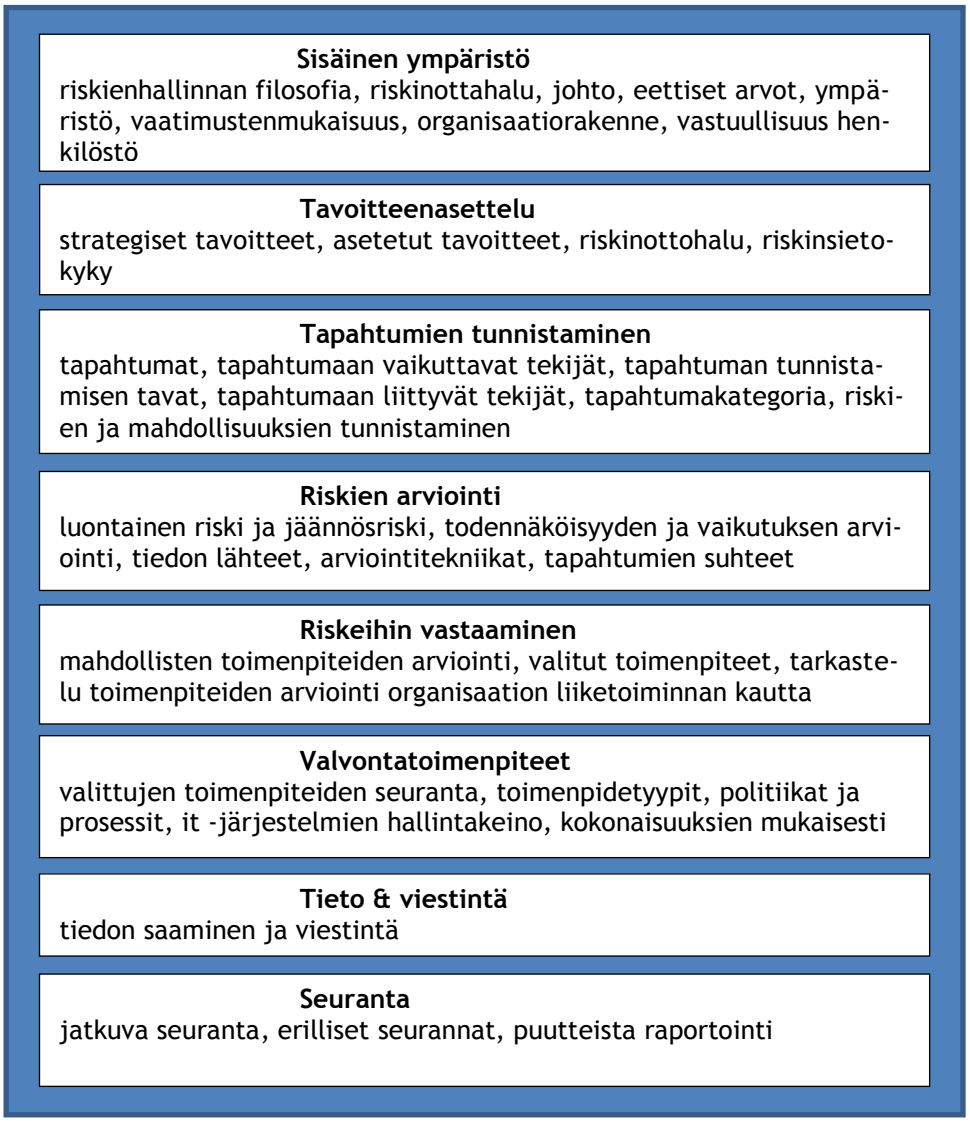
COSO ERM dokumentaatio jakautuu kahteen osaan, jossa ensimmäisessä osassa viitekehys (framework) määrittelee organisaation riskienhallinnan kuvaten ne periaatteet ja käsitteet joiden avulla organisaation johto voi arvioida ja kehittää riskienhallintaa. Toisessa osassa kuvataan menetelmiä (application techniques), joista on hyötyä mallin osa-alueita sovellettaessa (Ilmonen ym. 2010, 32).

COSO ERM on ehkä tullut suurimmalle osalle tunnetuimmaksi sen kuutiomaisesta viitekehysmallistaan (kuvio 5)

Kuvio 5: COSO ERM viitekehyksen kuutiomalli

Kuutiossa neljä pystysuoraa pylvästä esittävät yrityksen tavoitteita joita ovat strategia, toiminta, raportointi sekä vaatimustenmukaisuus. Kahdeksan vaakariviä kuvaa riskikomponentteja, jotka ovat osa johtamisjärjestelmää. Kuution kolmantena ulottuvuutena ovat organisaation yksiköt, joiden kaikkien tulee toteuttaa ja joiden läpi kokonaisvaltaista riskienhallintaa toteutetaan.

COSO ERM määrittelee riskienarviointoprosessin termillä kokonaisvaltainen riskienhallinta. Tämä muodostuu alla esitetyn kuvion mukaisista kahdeksasta, toisistaan riippuvaisesta avainkomponentista, jotka ovat peräisin siitä kuinka organisaation johto johtaa liiketoimintaa ja kuinka ne ovat yhdistyneitä hallintaprosessiin.



Kuvio 6: COSO ERM menetelmät

Alla on avattuna COSOn eri komponenttien käsitteet määritelmiin (Committee of Sponsoring Organizations of the Treadway Commission 2004, 5):

> *Sisäinen ympäristö* käsittää organisaation ilmapiirin ja henkilökunta tarkastelee ja käsittelee riskejä sen pohjalta. Henkilökunnan toimintaan vaikuttavat organisaation riskienhallintafilosofia, riskinottohalukkuus, rehellisyys, eettiset arvot sekä ympäristö, jossa arvoja sovelletaan
>
> *Tavoitteenasettelu* on laadittava, ennen kuin organisaation johto voi tunnistaa niiden toteutumiseen vaikuttavat potentiaaliset tapahtumat. Riskienhallinnalla varmistetaan, että johdolla on käytössään prosessi tavoitteenasetteluun, että valitut tavoitteet ovat organisaation toiminta-ajatusta tukevia ja sen mukaisia ja että ne ovat sopusoinnussa organisaation riskinottohalukkuuden kanssa

Tapahtumat tulee tunnistaa. Organisaation tavoitteiden toteutumiseen vaikuttavat sisäiset sekä ulkoiset tapahtumat on tunnistettava ja samalla on tehtävä ero riskien ja mahdollisuuksien välillä. Mahdollisuudet kanavoidaan takaisin johdon strategian ja tavoitteenasetteluun

Riskit tulee arvioida. Riskit arvioidaan ottamalla huomioon niiden todennäköisyys ja vaikutukset, minkä pohjalta päätetään, kuinka ne on hallittava. Riskit arvioidaan bruttoriskeinä ja jäännösriskeinä

Riskeihin tulee vastata. Organisaation johto päättää, kuinka riskeihin vastataan. Riskit vältetään, hyväksytään tai jaetaan tai niitä vähennetään. Johto laatii keinot riskien sopeuttamiseksi organisaation sietokykyyn ja riskinottohalukkuuteen

Valvontatoimenpiteiden osalta laaditaan ja toteutetaan toimintalinjat sekä menettelytavat, joita käyttämällä riskeihin kyetään vastaamaan tehokkaasti

Tarvittava *tieto* tunnistetaan, poimitaan ja *viestitään* sellaisessa muodossa ja niin pian, että henkilökunta voi hoitaa tehtävänsä. Tehokasta viestintää tapahtuu organisaatiossa tätä laajemmin sekä vertikaalisesti että horisontaalisesti.

Organisaation koko riskienhallintaa *seurataan* ja muutoksia tehdään tarpeen mukaan. Seuranta toteutetaan johdon jatkuvan toiminnan ja/tai erillisten arviointien avulla.

Kesällä 2010 COSO (The Committee of Sponsoring Organizations of the Treadway Commission) tilasi Pohjois-Carolinan osa-valtion yliopiston tutkimaan COSOn jäsenorganisaatioissa, COSOn viitekehykseen perustuvaa kokonaisvaltaisen riskienhallinnan käyttöä tai sen käyttöönoton harkintaa (COSO's 2010 report on ERM - Current state of Enterprise Risk Oversight and Market Perceptions of COSO's ERM framework). Tutkimukseen osallistui yhteensä 460 henkilöä, jotka työskentelivät COSOn jäsenorganisaatioissa. Kyselyssä esitettiin vastaajien riskienhallintatehtäviin liittyviä kysymyksiä sekä vastaajien käsityksiä koskien COSO ERM viitekehyksen vahvuuksia ja heikkouksia.

Kyselyyn osallistuneista organisaatioissa oltiin tyytyväisiä useisiin COSO ERM viitekehykseen ominaisuuksiin (taulukko 4). Vastaajien mielestä se tarjoaa teoreettisesti päteviä, kokonaisvaltaisen riskienhallinnan periaatteita sekä opastusta (66,6 % vastaajista) sekä tarjoaa organisaatioille sekä osakkeenomistajille yleisesti käytetyn riskienhallinnan termistön (46,4 % vastaajista) Tämän lisäksi siinä kuvataan selvästi vakaan riskienhallintaprosessien tärkeimmät elementit (45,8 %).

Taulukko 4: COSO ERM -viitekehyksessä havaitut positiiviset ominaisuudet

COSOn riskienhallintakykyyn liittyvät positiiviset kommentit	Prosentit %		
	Ei yhtään tai vähän	Kohtuullisesti	Merkittävästi tai hyvin paljon
Tarjoaa teoreettisesti päteviä kokonaisvaltaisen riskienhallinnan periaatteita ja opastusta	8,4	25,0	66,6
Tarjoaa organisaatioille sekä osakkeenomistajille yleisesti käytetyn riskienhallinnan termistön	20,2	33,4	46,4
Kuvaa selvästi vakaan riskienhallintaprosessien tärkeimmät elementit	17,8	36,4	45,8
Osoittaa, että kokonaisvaltainen riskienhallinta voi tuoda organisaatiolle lisäarvoa	29,5	32,5	38,0
Mahdollistaa johdon paremman arviointikyvyn organisaation riskiensietokyvylle suhteessa organisaatiolle asetettuun tavoitteeseen	26,8	37,0	36,2
Tarjoaa selvän ja käytännöllisen suunnan ja ohjeistuksen kokonaisvaltaisen riskienhallinnan käyttöönotolle	35,8	39,5	24,7

Negatiivisia asioita kysyttäessä vastauksissa oli havaittavissa suurta hajontaa, joista voidaan tutkimuksen mukaan päätellä, että viitekehys ei olekaan kaikille vastaajille tuttu tai se ei ole niin paljon käytössä kuin aikaisemmista vastauksista voisi saada kuvan (taulukko 5). Viitekehys tarjosi osalle vastaajista liian määräävän (ohjaavan) viitekehyksen (27,4) kun taas osalle ei yhtään tai vähän ohjaavan (38,6).

Taulukko 5: COSO ERM -viitekehyksessä havaitut negatiiviset ominaisuudet

COSOn riskienhallintakykyyn liittyvät negatiiviset kommentit	Prosentit %		
	Ei yhtään tai vähän	Kohtuullisesti	Merkittävästi tai hyvin paljon
Tarjoaa liian teoreettisen lähestymisen riskienhallintaan	23, 5	31,9	44,6
Tarjoaa liian määräävän(ohjaavan) riskienhallinnan viitekehyksen	38,6	34,0	27,4
Sisältää liian epämääräistä opastusta	43,1	30,4	26,5
Kuvaa kokonaisvaltai-	58,7	25,0	16,3

sen riskienhallinnan niin epäselvästi minkä takia standardi ei ole yleisesti käytössä

COSOn yleisesti tunnettu ”kuutio” antoi vastaajien mielestä hyvä käsityksen riskienhallintaan kuuluvien osa-alueiden keskinäisistä suhteista (41 %) 29,5 % vastaajista piti kuutiota monimutkaisena aivan kuten COSO ERM viitekehystäkin ja 26,4 % vastaajista piti sitä turhankin monimutkaisena lisäten negatiivisia reaktioita viitekehystä kohtaan. Monien vastaajien mielestä kuution selittäminen johdolle ja henkilöille, jotka eivät ole riskienhallinnan kanssa tekemisissä, on liian vaikeaa. Vastaajien mielestä COSO ERM- viitekehyksen kuution monimutkaisuuden takia viitekehys ei ole saanut valta-asemaa viitekehysten maailmassa.

2.2.2 ISO 31000

ISO 31000 standardi juontaa juurensa Australiaan ja Uuteen-Seelantiin, jossa se on toiminut nimellä AS/NZ 4360:2004 jo useita vuosia. AS/NZ 4360:2004 -standardin kehittivät Australian ja Uuden-Seelannin yhteisten standardien tekninen komitea. Se kehitettiin tarpeeseen aivan kuten COSO ERM ja sen tarkoituksena oli kehittää riskienhallinnan käytännön ohjeistus niin julkiselle kuin yksityisellekin sektorille. Virallinen julkaistu versio ilmestyi vuonna 2004.

Vuonna 2009 International Organization for standardization (ISO) julkaisi ISO 31000 standardin, jonka pohjana toimii AS/NZ 4360:2004 standardi ja ISO standardia voidaankin pitää sen kehitetymmäksi versioksi. ISO 31000 standardi on viitekehykseltään laajempi kuin sen pohjalla olevan standardin ja sitä on kehitetty AS/NZ standardissa havaittujen puutteiden perusteella. Tämän lisäksi sen käyttöä on laajennettu koskemaan mitä tahansa organisaatiota ja sektoria. Standardin tarkoituksena on tarjota käytännön tavat kehittää, toteuttaa ja parantaa organisaation tapaa hallita riskejä. Standardia ovat olleet kehittämässä muun muassa henkilöt, jotka ovat kehittäneet AS/NZ 4360:2004 standardin.

ISO 31000 standardi on suomennettu Suomen standardoimisliiton toimesta vuonna 2011. Suomen standardoimisliiton Internet -sivuston mukaan valmisteilla on riskienhallinnan soveltamisopas ISO 31004: Guidelines for the application of ISO 31000. Tarkempaa julkaisuajankohtaa ei kehittämissuunnitelman tekohetkellä ollut soveltamisoppaasta mainittu. Vaikka kyseessä on ISO standardi, tulee huomioida, että kehittämissuunnitelman kirjoittamisen hetkellä standardia ei ole tarkoitettu käytettäväksi sertifioinnin perustana (SFS-ISO 31000, 12).

ISO 31000 standardi perustuu periaatteesta, puitteista ja prosessista, jotka ovat kaikki toisiinsa kytköksissä. Riskienhallinnan periaatteet määrittelevät sen, miten organisaatio ja sen työntekijät tulisivat suhtautuvat riskienhallintaan. Organisaation tulee määritellä tietoturvallisuu-

delle periaatteet ja yleisen suunnan. Sama koskee riskienhallintaa. Riskienhallinnan periaatteet kuvataan yleensä riskienhallintapolitiikassa. Standardin mukaan organisaation tulisi noudattaa tiettyjä periaatteita kaikilla tasoilla, jotta riskienhallinta olisi toimivaa (SFS-ISO 31000 2011, 22). Alla on kuvattuna ISO 31000 standardin periaatteet määritelmineen. Periaatteita on yhteensä yksitoista ja ne ovat suorassa yhteydessä standardin puitteiden valtuuksiin ja sitoutumiseen:

Organisaation periaatteena tulee olla, että riskienhallinta luo lisäarvoa ja säilyttää sen. Riskienhallinta edesauttaa tavoitteiden saavuttamista ja toiminnan tason havaittavaa kehittymistä esimerkiksi ihmisten terveyden, turvallisuuden, lakien ja viranomaisten vaatimusten noudattamisen, yleisen hyväksynnän saavuttamisen, ympäristönsuojelun, tuotteiden laadun, projektinhallinnan, toimintojen ja hallintotavan tehokkuuden sekä maineen osalta.

Riskienhallinta on olennainen osa kaikkia organisaation prosesseja. Riskienhallinta ei ole organisaation muista toiminnoista ja prosesseista erillinen toiminto. Riskienhallinta on osa johdon vastuualuetta ja olennainen osa kaikkia organisaation prosesseja, kuten strategisen suunnittelun prosesseja ja kaikkien projektien ja muutoksenhallinnan prosesseja.

Riskienhallinnan on osa päätöksentekoa. Riskienhallinta auttaa päätöksentekijöitä tekemään tietoisia valintoja, asettamaan toimintoja tärkeysjärjestykseen ja erottamaan vaihtoehtoiset toimintatavat.

Riskienhallinnan lähtökohtana on epävarmuuden huomioon ottaminen. Riskienhallinnassa otetaan huomioon epävarmuus, sen luonne ja käsittelymahdollisuudet. *Riskienhallinta on järjestelmällistä, jäsenneltyä ja ajantasaista*. Järjestelmällinen, ajantasainen ja jäsennelty riskienhallinnan toimintamalli lisää tehokkuutta ja tekee tuloksista yhdenmukaisempia, luotettavampia ja helpommin vertailtavia.

Riskienhallinta perustuu parhaaseen saatavilla olevaan tietoon. Riskienhallintaprosessin lähtötiedot perustuvat tietolähteisiin, joita ovat esimerkiksi historiatiedot, kokemus, sidosryhmien antama palaute, havainnot, ennusteet ja asiantuntijoiden näkemykset. Päätöksentekijöiden olisi kuitenkin otettava selvää tietoihin tai malleihin liittyvistä rajoituksista ja toisistaan poikkeavista asiantuntijoiden näkemyksistä ja otettava ne huomioon.

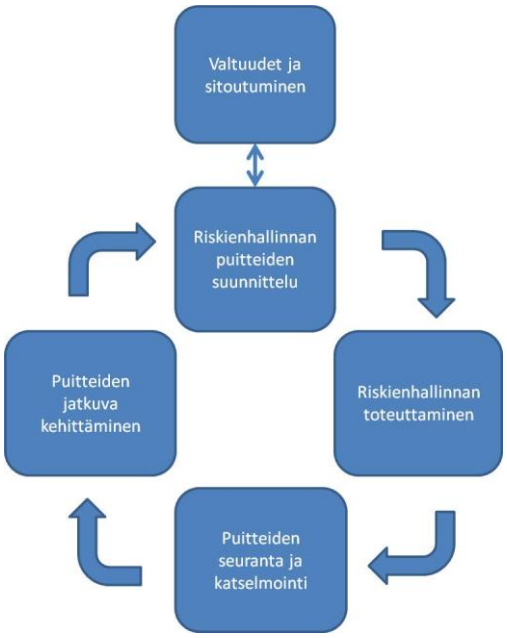
Riskienhallinta toteutetaan organisaation tarpeiden mukaan. Riskienhallinta on sovitettu yhteen organisaation ulkoisen ja sisäisen toimintaympäristön ja riskiprofiilin kanssa. *Riskienhallinta ottaa inhimilliset ja kulttuuriset tekijät huomioon*. Riskienhallinnalla tunnistetaan organisaation omien ja ulkopuolisten henkilöiden kyvyt, näkemykset ja aikomukset, jotka voivat auttaa tai haitata organisaation tavoitteiden saavuttamista.

Riskienhallinta on avointa ja kattavaa. Sidosryhmien ja erityisesti organisaation eri tasoilla olevien päätöksentekijöiden ottaminen sopivalla tavalla ja oikeaan aikaan mukaan riskienhallintaan takaa, että riskienhallinta pysyy tarkoituksenmukaisena ja ajantasaisena. Sidosryhmien osallistuminen mahdollistaa sen, että sidosryhmät ovat kunnolla edustettuina ja että heidän näkemyksensä otetaan huomioon riskikriteerien määrittelyssä.

Riskienhallinta on dynaamista, toistuvaa ja muutoksiin reagoivaa. Riskienhallinnan avulla muutokset havaitaan ja niihin reagoidaan viipymättä. Ulkoisten ja sisäisten tapahtumien myötä toimintaympäristö ja tietämys muuttuvat, riskejä seurataan ja katselmoidaan, ilmaantuu uusia riskejä, osa riskeistä muuttuu ja osa katoaa.

Riskienhallinta tukee organisaation jatkuvaa kehittämistä. Organisaatioiden olisi kehitettävä ja toteutettava strategioita, joilla niiden riskienhallintaa kehitetään muiden organisaation osa-alueiden ohella

Riskienhallinnan puitteet luovat riskienhallinnalle perustan, syyn miksi riskienhallintaa tulisi toteuttaa. Riskienhallinnan puitteiden (kuvio 7) avulla varmistetaan, että riskienhallintaprosessissa saatu tieto raportoidaan oikein ja että sitä käytetään organisaatiossa päätöksenteon apuna sekä vastuiden perustana. Riskienhallinnan puitteet ovat ISO 31000 standardissa yhtä kuin riskienhallinnan viitekehys (framework)

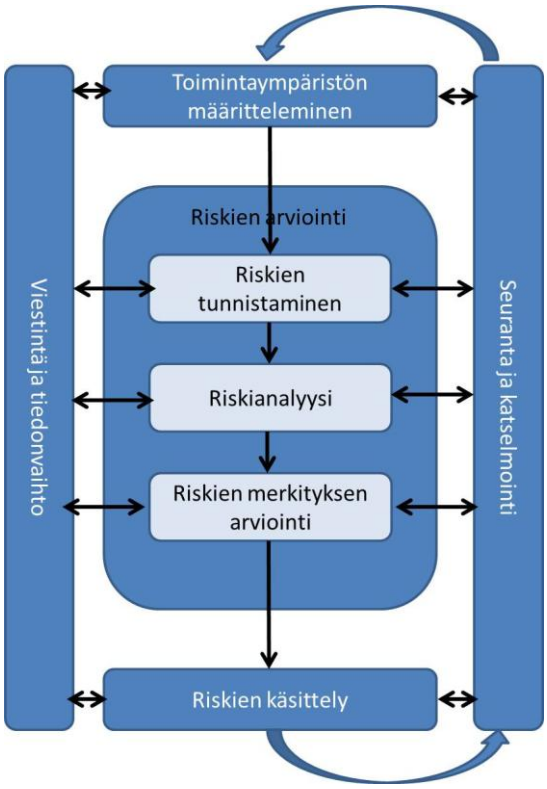


Kuvio 7: ISO 31000 riskien hallinnan puitteet noudattavat Demingin laatuympyrän PDCA- mallia (Plan-Do-Check-Act)

Standardissa kehotetaan huomioimaan, että organisaation olisi muutettava puitteiden osia tarpeitaan vastaavaksi, mikäli organisaatiolla on jo olemassa yleinen johtamisjärjestelmä.

Riskienhallinnan puitteet antavat pohjan organisaation riskienhallinnalle. Organisaatiossa voidaan jo toteuttaa riskienhallintaa, mutta mikäli sen puitteita ei ole suunniteltu ja määritelty, ei riskienhallinta ole hallittua eikä riskien tieto saavuta välttämättä kaikkia tarvittavia tahoja.

Riskienhallinnan prosessi kattaa alla olevassa kuviossa (kuvio 8) nähtävät toiminnot. Prosessin olisi oltava yhtenäinen osa johtamista, sisällytetty organisaation kulttuuriin ja käytäntöihin sekä mukautettu organisaation liiketoimintaprosesseihin sopivaksi (SFS-ISO 31000 2011, 34).



Kuvio 8: ISO 31000 standardin mukaiset prosessit

ISO 31000 standardin käytöstä ja sen kokemuksista ei suunnitelman tekohetkellä ollut olemassa virallisia tutkimuksia. Tutkimuksia toki löytyy, mikäli etsii standardin pohjalla olevasta AS/NZ 4360:2004 tehtyjä tutkimuksia. Tämä ei anna kuitenkaan kokonaiskuvaa siitä, mitkä ovat ISO standardin kokemukset ja käyttöasteet. Syy tutkimusten vähyyteen on ISO standardin ikä. Standardihan on julkaistu vasta vuonna 2009, suomenkielisenä vuonna 2011.

2.3 Riskienhallinta valtion organisaatioissa

Valtiovarainministeriön (VM) tehtävänä on ohjata ja yhteen sovittaa julkishallinnon ja varsinkin valtionhallinnon tietoturvallisuuden kehittämistä. Tätä varten VM on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. (VAHTI 2012, 7.) VM on asettanut VAHTIn tavoitteeksi parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista (VAHTI 2012, 23). VAHTI on mitannut valtionhallinnon ministeriöiden sekä virastojen tietoturvallisuuden tilaa vuodesta 2008 lähtien.

VAHTIn vuoden 2011 toimintakertomuksen mukaan kyseisenä vuonna suoritettuun kyselyyn vastasi kaikki ministeriöt sekä suuri osa virastoista. Seuranta osoitti, että kokonaisuutena valtion tietoturvallisuuden tilanne on monilta osin parantunut vuonna 2011. Toimintakertomuksen mukaan tähän on vaikuttanut Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä sekä sen pohjalta VAHTIn vuonna 2010 (VAHTI 2/2010) julkaisema ohjeistus asetus asetuksen täytäntöönpanosta (VAHTI 2012, 29).

Valtionhallinnon organisaatioissa arvioidaan riskienhallintaa myös johdon sisäisen tarkastajan toimesta. Valtioneuvoston asettaman sisäisen valvonnan ja riskienhallinnan neuvottelukunnan sisäisen valvonnan luoma arviointikehikko (2005) tarjoaa työkalun myös riskienhallinnan arvioimiselle. Arviointikehikko on tarkoitettu pääasiassa valtionhallinnon johdon työvälineeksi sisäisen valvonnan ja riskienhallinnan arviointiin. Arviointikehikko perustuu löyhästi COSO ERM- viitekehykseen ja sitä on muokattu valtionhallinnon toimintaympäristöön ja tarpeisiin sopivaksi. (Herrainsilta J. 2006, 49.)

Vuoden 2011 seurannassa havaittiin, että riskienhallintapolitiikka oli käytössä 46 % organisaatioista. Edellisvuoteen verrattuna tulos oli noussut 7 prosenttia. Säännöllistä tietoturvariskien arviointia toteutettiin 57 % organisaatioissa, vuonna 2010 tuloksen ollessa 60 %. Kuitenkin ydintoimintojen riskienarviointia ja dokumentointia toteutettiin 53 % organisaatioista (vuonna 2010 39 %) Suurin muutos vuoteen 2010 verrattuna oli johdon sisäisen valvonnan ja riskienhallinnan arviointi- ja vahvistuslausuman riskienkäsittely, josta ei aikaisemmin ollut tulosta mutta vuonna 2011 sellainen löytyi 49 % organisaatioiden lausumasta.

Taulukko 6: Riskienhallinnan tila valtionhallinnossa VAHTIn suorittaman selvityksen perusteella

Tietoturvallisuuden hallinta ja johtaminen	V. 2011 tulokset (%)	Vuoden 2010 tulokset (%)
Riskienhallintapolitiikka	46	39
Säännöllinen tietoturvariskien arviointi	57	60

Ydintoimintojen riskien arviointi ja dokumentointi	53	39
Johdon sisäisen valvonnan ja riskienhallinnan arviointi- ja vahvistuslausumassa käsitellään tietoturvariskejä	49	-

2.4 Tutkimusongelman tarkastelu teorian perusteella

Tämän tutkimuksen tavoitteena oli pyrkiä parantamaan kohdeorganisaation nykyisen, kokonaisvaltaisen riskienhallinnan vaikuttavuutta. Riskienhallinnan teorian ja kirjallisuuden mukaan riskienhallinnan keskeisiä osa-alueita ovat riskienhallintaprosessi (ks. 2.1.1), jonka mukaan riskienhallinta etenee vaiheittaisena prosessina. Riskienhallinnan kehittämisen lähtökohtana tulee luvun 2.1.3 mukaan olla riskienhallinnan tavoitteet ja periaatteet organisaatiotasolla. Nämä kuvataan riskienhallintapolitiikassa sekä – periaatteissa.

Riskienhallintastandardit kattavat laajasti koko riskienhallinnan ja siihen liittyvät osa-alueet käsittäen näin ollen niin prosessin kuin yleisellä tasolla riskienhallinnan tavoitteet ja periaatteet (ks. 2.2). Teorian perusteella riskienhallintastandardit parantavat toiminnan tehokkuutta ja vaikuttavuutta. Ilmosen ym. mukaan riskienhallintastandardien suurin hyöty on siinä, että ne luovat yhteisen riskienhallintasanaston sekä tavan, mikä mahdollistaa jatkuvan ja toistettavan tavan riskienhallintaan (2010, 30).

Riskienhallinnan teorian perusteella voidaan siis olettaa, että riskienhallintastandardit ottavat huomioon riskienhallinnan kaikki osa-alueet, luovat yhteisen kielen sekä tavan toteuttaa riskienhallintaa parantaen näin sen vaikuttavuutta. Näin ollen riskienhallinnan kehittäminen organisaatiossa, joka käyttää omaa sisäistä riskienhallinnan viitekehystä ja jonka ei koeta tuottavan tulosta, tulisi saadun teorian perusteella aloittaa kehittäminen riskienhallintastandardiin perustuen.

Keskustelin asiasta kohdeorganisaation riskienhallintapäällikön kanssa ja päädyimme teorian perusteella siihen johtopäätökseen, että organisaation tulisi ottaa käyttöönsä riskienhallinnan viitekehykseksi riskienhallintastandardin. Keskustelussa totesimme, että oman sisäisen riskienhallintastandardin kehittämisen sijaan tukeutuisimme jo kansainvälisesti hyväksyttyyn, riskienhallinnan osa-alueet huomioon ottavaan standardiin.

Kappaleen 2.3 perusteella teimme päätöksen, että valitsemme Euroopassa käytössä olevista riskienhallintastandardeista kaksi yleisimmin käytettyä standardia. Osana tutkimusta verrataan näiden kahden standardin eroavaisuuksia keskenään. Saadun tuloksen perusteella päätetään standardin, jonka mukaan kohdeorganisaation riskienhallintaa lähdetään kehittämään. FERMAn (ks. 2.2) tekemän tutkimuksen perusteella vertailtaviksi standardeiksi valikoituivat COSO ERM sekä ISO 31000 riskienhallintastandardit. Standardin lisäksi kehittämisen lähtökohdiksi otimme teorian mukaan riskienhallinnan rungon luovat asiakirjat eli riskienhallinnan politiikan ja – periaatteet. Kehittämissuunnitelma tulee keskittymään riskienhallintapolitiikan ja sekä – menettelyohjeistuksen kehittämiseen standardin mukaiseksi.

3 Tutkimustiedon hankinta

Tutkimuksessa tarvittavan tutkimustiedon hankinta toteutettiin 1.6 - 30.9.2012 välisenä aikana. Konstruktiivisen tutkimuksen tiedon kerääminen toteutettiin standardien vertailevana analyysinä sekä GAP -analyysinä. Saadun tiedon avulla pystyin luomaan kohdeorganisaatiolle riskienhallinnan kehittämissuunnitelman.

Vertailevalla analyysilla hahmotetaan valittujen tapauksien välisiä yhtäläisyyksiä ja eroja. Vertailun kohteena voivat olla esimerkiksi erilaiset tapaukset, prosessit tai vaikkapa maantieteellisesti rajautuneet yksiköt, jotka on todettu jollain tavoin yhteismitallisiksi ja sen vuoksi vertailukelpoisiksi. Vertaileva analyysisi voi perustua sekä määrällisiin aineistoihin ja tilastollisiin analyysimenetelmiin että laadullisten aineistojen ja analyysimenetelmien käyttöön. (Jyväskylän Yliopisto 2013).

Vertailevaa analyysia suunniteltaessa tulee miettiä mitä vertailulla halutaan saada esille (Saukkonen 2013). Tutkimuksen vertailevan analyysin tarkoituksena on selvittää, mitkä ovat valittujen riskienhallintastandardien erot, jotta kohdeorganisaatio voi näistä kahdesta valita itselleen sopivimman? Koska kyseessä on kaksi standardia, toimii tutkimusaineistona kyseiset standardit materiaaleineen. Standardien eroavaisuuksia verrataan riskienhallinnan teoriassa saatuihin pääteemoihin, joita ovat riskienhallinnan käsitteet sekä riskienhallintaprosessi (luku 2).

GAP- analyysi eli puuteanalyysi on menetelmä, jolla voidaan verrata ja kuvata nykytilan ja tavoitetilan välisiä eroja (JHS 171, 2009. 4). Puuteanalyysin kautta saadut erot otetaan huomioon kehittämistoimenpiteissä. GAP -analyysiä käytetään tässä tutkimuksessa analysoimaan kohdeorganisaatiolla olemassa olevaa riskienhallintaprosessin eroavaisuuksia valittuun riskienhallintastandardin prosessiin. Näin saadaan selville mitä tulee riskienhallinnan kehittämisessä ottaa huomioon - mitä on jo olemassa, mitä tulee luoda uutta ja mitä kehittää.

3.1 Standardien vertaileva analyysi

Riskienhallintastandardien vertailevan analyysin tarkoituksena on antaa tukea niin kehittämissuunnitelmalle kuin kohdeorganisaation riskienhallintapäällikön päätöksentekoon valittavan standardin osalta sekä perustelut, miksi riskienhallintaa kannattaisi kyseisen standardin mukaan kehittää. Vertaileva analyysi suoritettiin kesällä 2012.

Vertailevassa analyysissä selvitetään valittujen standardien eli COSO ERMin sekä ISO 31000 eroavaisuuksia. Teorian perusteella eroavaisuuksia etsitään riskienhallinnan käsitteistä, jotka teorian mukaan tuleva muodostamaan kohdeorganisaation riskienhallinnassa käytetyn termistön. Tämän lisäksi riskienhallintaprosessi esittää teorian mukaan merkittävää osaa riskienhallinnassa. Näin ollen vertailevassa analyysissä selvitetään myös prosessin eroavaisuutta eri standardien kesken.

3.1.1 Vertailtavien standardien rakenne

Siinä missä COSO ERMin viitekehys muodostuu kuution kahdeksasta vaakarivistä, on ISO 31000 standardi erotellut viitekehyksen riskienhallinnan puitteisiin. COSO ERMin viitekehyksen sisäinen ympäristö määritellään ISO 31000 standardissa periaatteissa ja puitteissa. ISOn riskienhallintaprosessi käsittelee asioita, joita käsitellään COSOn viitekehyksen tapahtumien tunnistamisessa, riskien arvioinnissa, riskeihin vastaamisessa ja valvontatoimenpiteissä. COSOn viitekehyksen toiminnan ja parantamisen seurantaa sekä tiedon levittämistä ja viestintää toteutetaan ISOn puitteissa (taulukko 7).

Taulukko 7: Miten ISOn viitekehys ja prosessi ovat suhteessa COSO ERMin viitekehykseen

ISO 31000	COSO ERM (käsittää kokonaisuudessaan viitekehyksen)
Periaatteet ja puitteet (viitekehys)	Sisäinen ympäristö (viitekehys)
Puitteet (viitekehys)	Tavoitteenasettelu (viitekehys)
Riskienhallintaprosessi (prosessi)	Tapahtumien tunnistaminen (viitekehys)
Riskienhallintaprosessi (prosessi)	Riskien arviointi (viitekehys)
Riskienhallintaprosessi (prosessi)	Riskeihin vastaaminen (viitekehys)
Riskienhallintaprosessi (prosessi)	Valvontatoimenpiteet (viitekehys)
Puitteet (viitekehys) & riskienhallintaprosessi (prosessi)	Tieto ja viestintä (viitekehys)
Puitteet (viitekehys) & riskienhallintaprosessi (prosessi)	Seuranta (viitekehys)

Menemättä sen tarkemmin sisälle eri osa-alueisiin ja niissä suoritettaviin tehtäviin, voidaan todeta että kummatkin standardit käsittelevät samoja asioita vaan eri tavalla esitettynä. Suurin ero standardien eri osa-alueiden välillä on se, että COSO ERM yhdistää viitekehyksen ja prosessin samaan pakettiin kun ISO 31000 erottelee nämä toisistaan. ISO 31000 standardissa on kohtia, joita on kuvattu niin puitteissa kun periaatteissa.

3.1.2 Käsitteiden erovaisuudet

Taulukkoon 6 on koottuna ISO 31000 ja COSO ERM standardien käsitteitä. COSO ERM käsittelee riskienhallintaprosessia kokonaisvaltaisena riskienhallinta, jota siis toteutetaan organisaation eri yksiköissä. ISO 31000 ei ota kantaa siihen toteutetaanko riskienhallintaa organisaatiossa kokonaisvaltaisesti vai vain esim. yksittäisiin tehtäviin, vaan jokaisella toimialalla tai riskienhallinnan soveltamiskohteella on omat tarpeensa, kohdeyleisönsä, näkemyksensä ja kriteerinsä (SFS-ISO 31000 2011, 6).

ISO 31000 standardi määrittelee sanan riski epävarmuuden vaikutuksena tavoitteisiin. Tällä voi olla niin negatiivinen kuin positiivinenkin vaikutus. Riski on sama kuin jokin tapahtuma ja sen seuraus tai niiden yhdistelmä. ISO -standardin termien määrittelyssä viitataan riskillä myös siihen, että riski ilmaistaan usein tapahtuman seurausten (myös olosuhteiden muutosten) ja riskin toteutumisen todennäköisyyden yhdistelmänä (SFS-ISO 31000 2011, 12). COSO kuvaa riskin tapahtuman ilmenemisellä ja sen haitallisena vaikutuksena tavoitteen saavuttamisessa. Tapahtuma merkitsee ISO 31000 maailmassa tiettyjen olosuhteiden tapahtumista tai muuttumista, kun taasen COSO ERM määrittelee sen ulkoisista tai sisäisistä lähteistä aiheutuvaksi poikkeamaksi tai tapahtumaksi, mikä vaikuttaa tavoitteiden saavuttamiseen.

Taulukko 8: Standardien keskeiset käsitteet ja niiden eroavaisuudet (COSO ERMistä vapaasti suomennettu)

Määritelmä	ISO 31000	COSO ERM
Standardin soveltamisala	Kaikki julkiset ja yksityiset yritykset, yhteisöyritykset, järjestöt, ryhmät tai yksityiset henkilöt. Ei siten koske erityisesti mitään toimialaa tai sektoria.	Kokonaisvaltainen riskienhallinta ottaa huomioon kaikki organisaation eri tasojen toiminnot.
Riskienhallintaprosessi	Hallintaperiaatteiden, -menettelyjen, ja -käytäntöjen järjestelmällinen soveltaminen viestintään ja tiedonvaihtoon sidosryhmien kanssa ja toimintaympäristön määrittelemiseen liittyviin toimintoihin sekä riskien tunnistamiseen, analysointiin, arviointiin, käsittelyyn, seurantaan ja katselmointiin	Synonyymi kokonaisvaltaiselle riskienhallinnalle, jota kohteessa toteutetaan
Kokonaisvaltainen ris-	Ei määritelty	Muodostuu kahdeksasta toisiinsa liittyvis-

kienhallinta		tä komponenteista: • sisäinen ympäristö • tavoitteenasettelu • tapahtumien tunnistaminen • riskien arviointi • riskeihin vastaaminen • valvontatoimenpiteet • tieto & viestintä • seuranta
Riski	Epävarmuuden vaikutus tavoitteisiin. Vaikutus on poikkeama odotetusta, niin myönteisessä kuin kielteisessäkin mielessä. Tavoitteilla voi olla eri näkökohtia ja niitä voidaan soveltaa eri tasoihin. Riskiä kuvataan usein viittaamalla mahdollisiin tapahtumiin ja seurauksiin tai niiden yhdistelmään. Riski ilmaistaan usein tapahtuman seurausten (myös olosuhteiden muutosten) ja riskin toteutumisen todennäköisyyden yhdistelmänä. Epävarmuus on tila, johon liittyy osittain tai täydellinen tapahtuma, sen seurauksia tai todennäköisyyttä koskevan käsityksen tai tiedon puute.	Mahdollisuus, että tapahtuma ilmenee ja vaikuttaa haitallisesti tavoitteen saavuttamiseen
Riskin omistaja	Henkilö tai taho, jolla on vastuu ja valtuudet hallita riskiä	Jokaisella organisaatiossa on jokin vastuu kokonaisvaltaisesta riskienhallinnasta. Toimitusjohtajalla on lopullinen vastuu ja omistajuus
Riskinottohalu	Standardi ei varsinaisesti käytä termiä riskinottohalu. Standardissa käytetään sanoja "organisaation asenne riskiin"	Se riskin määrä/taso, jonka organisaatio on valmis hyväksymään tehtävän/tavoitteen saavuttamisessa
Riskin sietotoleranssi	Päätöksenteossa riski olisi otettava huomioon laaja-alaisesti ja harkittava sellaisten riskien sietotoleranssi, jotka kohdistuvat muihin osapuoliin kuin siihen organisaatioon, joka riskistä hyötyy.	Hyväksyttävät riskin arvon vaihtelut tavoitteen saavuttamiseksi. Riskinsietotoleranssia voidaan mitata ja parhaiten se toteutuu käyttämällä samoja arvoja kuin siihen liittyvä kohde

Riskin arviointi	Kokonaisprosessi, joka kattaa riskien tunnistamisen, riskianalyysin ja riskin merkityksen arvioinnin.	Riskin arvioinnilla tarkastellaan missä määrin mahdolliset tapahtumat vaikuttavat tavoitteiden saavuttamisessa.
Tapahtuma	Tiettyjen olosuhteiden tapahtuminen tai muuttuminen	Ulkoisista tai sisäisistä lähteistä aiheutuva poikkeama tai tapahtuma, mikä vaikuttaa tavoitteiden saavuttamiseen.
Jäännösriski	Riskin käsittelyn jälkeen jäljellä oleva riski. Jäännösriskistä saatetaan myös käyttää termiä säilytetty riski	Johdon toimien jälkeen jäljelle jäänyt riski.

3.1.3 Eroavaisuudet riskienhallintaprosessissa

Riskienhallinnan pidetään sisältävän neljä perusprosessia, kuten jo aikaisemmin luvussa riskienhallinnan viitekehys esiteltiin. Moeller on teoksessaan määritellyt samat asiat hieman eri sanoilla kuvaten (Moeller 2007, 22):

1. riskien tunnistaminen
2. tunnistettujen riskien kvantitatiivinen tai kvalitatiivinen arviointi
3. riskin priorisointi ja niiden käsittely
4. riskin seuranta

Karkeasti kuvattuna riskit tulee siis ensin tunnistaa, sen jälkeen niiden toteutumisen vakavuudesta suoritetaan arviointi todennäköisyyden ja seurauksen perusteella. Vakavuuden arvioinnin jälkeen ne priorisoidaan ja niille valitaan organisaation mukaiset käsittelykeinot. Tämän jälkeen riskien tilan muuttumista seurataan.

Seuraavissa taulukoissa on pyritty tunnistamaan standardien tärkeimmät määrittelyt koskien edellä esitettyjä perusprosesseja. COSO ERM standardin kohdat on otettu kyseisen kappaleen tiivistelmästä, ISO standardista on pyritty tiivistämään pääperiaatteet.

Riskien tunnistaminen (taulukko 7) mahtuu ISO 31000 standardissa yhteen vajaan puolen sivun kappaleeseen. COSO ERMissä sitä kuvataan 7 sivun verran. ISO -standardin kuvaus riskien tunnistamisesta kertoo, mitä tulee tehdä. COSO ERM ottaa asiaan laajemmin kantaa kuvaten viitekehyksessään myös eri tapoja toteuttaa tunnistamista. Suurin, mielestäni tekstistä havaittavissa olevasta erosta on se, että ISO ei ota kantaa siihen, kuka sitä tekee vaan siinä olisi oltava mukana tarvittavat tiedot omaavat henkilöt. COSO ERMin tiivistelmän mukaan johdon tulee tunnistaa tapahtumat. Viitekehystä lukemalla selviää, että tapahtumia tulee tunnistaa myös "aktiivisella tasolla" organisaation liiketoimintayksiköissä ja prosesseissa.

Taulukko 9: Standardien määritelmät koskien riskien tunnistamista (COSO ERM vapaasti suomennettu)

Riskien tunnistaminen	
ISO 31000	Organisaation olisi tunnistettava riskin lähteet, vaikutusalueet, tapahtumat (mukaan lukien olosuhteiden muutokset) ja niiden syyt sekä mahdolliset seuraukset. Riskien tunnistamisen olisi katettava kaikki riskit riippumatta siitä, onko niiden lähde organisaation hallinnassa, vaikka riskin lähde tai syy ei olisikaan selvillä. 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. Sen olisi soveltuvin osin sisällettävä myös taustatiedot, jos niitä on saatavilla. Riskien tunnistamisessa olisi oltava mukana henkilöitä, joilla on tarvittava tietämys.
COSO ERM	Johto tunnistaa mahdolliset tapahtumat, jotka ilmetessään vaikuttavat organisaatioon sekä päättävät, muodostavatko ne organisaatiolle positiivisen mahdollisuuden vai vaikuttavatko ne haitallisesti organisaation kykyyn toteuttaa menestyksekkäästi sille asetettuja tavoitteita ja strategiaa. Tapahtumat, joilla on negatiivinen vaikutus, ilmenevät riskeinä jotka tarvitsevat johdon arviointia ja päätöksiä. Tapahtumat, joilla on positiivinen vaikutus, ilmenevät mahdollisuuksina jotka johto kanavoi takaisin strategiaan sekä tavoitteita toteuttaviin prosesseihin. Kun tapahtumia tunnistetaan, johto arvioi monipuolisesti eri sisäisiä ja ulkoisia tekijöitä, jotka voivat aiheuttaa riskejä ja mahdollisuuksia organisaation kokonaisuuden näkökulmasta katsottuna.

Riskin arviointi ei eroa standardien suhteen kuten taulukon 8 perusteella voidaan nähdä. COSO ERM puhuu jälleen muodossa johto, ISO ei määrittele kenen toimia arviointi on. COSO käsittelee asiaa laajemmassa mittakaavassa, ISO lyhyemmin. Periaatteet riskien arvioinnissa ovat kummassakin standardissa lähtökohtaisesti samat. COSO ERM mainitsee riskien luontaisuuden sekä jäännösriskin. ISO- standardissa asiaa ei käsitellä niillä termeillä vaan todetaan, että on tärkeää ottaa huomioon käytettävissä olevat hallintakeinot ja niiden vaikuttavuus ja tehokkuus.

Taulukko 10: Standardien määritelmät koskien riskien arviointia (COSO ERM vapaasti suomennettu

Tunnistettujen riskien kvantitatiivinen tai kvalitatiivinen arviointi	
ISO 31000	Riskianalyysi on lähtökohta riskin merkityksen arvioinnille ja päätöksille siitä, tarvitseeko riskejä käsitellä ja mitkä ovat sopivimmat riskienkäsittelystrategiat ja -menetelmät. 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. Tapa, jolla seuraukset ja todennäköisyydet ilmaistaan ja jolla ne yhdistetään riskitason määrittämiseksi, olisi valittava sen mukaan, minkä tyyppinen riski on kyseessä, millaista tietoa on saatavilla ja mihin tarkoitukseen riskin arvioinnin tuloksia aiotaan käyttää. Kaikkien näiden olisi oltava yhdenmukaisia riskikriteerien kanssa. On myös tärkeää ottaa huomioon eri riskien ja niiden lähteiden keskinäiset riippuvuudet.
COSO ERM	Riskin arviointi mahdollistaa organisaatiota arvioimaan missä määrin mahdollisilla tapahtumilla on vaikutusta tavoitteiden saavuttamisessa. Johto arvioi tapahtumia kahdesta eri näkökulmasta - todennäköisyys ja vaikutus- sekä käyttävät yleensä kvalitatiivisia ja kvantitatiivisia tapoja. Tapahtumien positiiviset ja negatiiviset vaikutukset tulee tarkistaa joko yksittäin tai luokittain läpi organisaation. Riskejä arvioidaan niin luontaisina kuin jäännösriskeinä.

Taulukossa 9 nähdään, että ISO 31000 mainitsee riskien käsittelyn olevan toistuva prosessi. COSO ERM ei riskien käsittelytavassa ja valvontatoimenpiteissä mainitse niiden prosessimaisuudesta. Tämä ehkä sen takia, että viitekehyksen alussa COSO mainitsee kokonaisvaltaisen riskienhallinnan olevan prosessi. ISO- standardi pitää prosessin ja viitekehyksen erillään sekä painottaa standardi kummankin osa-alueen prosessimaisen kehittämisen.

Taulukko 11: Standardien määritelmät riskien priorisoinnin ja käsittelyn osalta (COSO ERM vapaasti suomennettu)

Riskin priorisointi ja niiden käsittely

ISO 31000	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. Riskien käsittely on toistuva prosessi, johon kuuluvat seuraavat vaiheet: — riskien käsittelyn arviointi — päätös siitä, onko jäännösriskien taso siedettävä — jos jäännösriskien tasoa ei pidetä siedettävänä, uuden riskien käsittelyn aloittaminen — riskien käsittelyn vaikuttavuuden arvioiminen
COSO ERM	Arvioituaan merkitykselliset riskit, johto päättää niiden käsittelytavoista. Käsittelytavat sisältävät riskin välttämisen, vähentämisen, jakamisen ja hyväksymisen. Käsittelytapaa harkitessaan johto arvioi tapahtuman todennäköisyyttä ja vaikutusta, sekä kuluja ja hyötyjä, joilla saadaan jäännösriski halutulle riskinsietotasolle.

Riskien seurannan suhteen (taulukko 10) ISO 31000 standardi käsittelee asiaa laajemmin ottaen huomioon prosessien parantamisen. COSO ottaa seuranta- luvussa huomioon osa-alueiden tehokkuuden. COSO painottaa enemmän riskin seurannassa niiden valvontatoimenpiteiden määrittelemiseen sekä tarkasteluun.

Taulukko 12: Standardien määritelmät koskien riskin seurantaa (COSO ERM vapaasti suomennettu)

Riskin seuranta	
ISO 31000	Organisaation seuranta- ja katselmointiprosessien olisi katettava kaikki riskienhallintaprosessien osa-alueet, jotta — voidaan varmistaa, että hallintakeinot ovat vaikuttavia ja tehokkaita sekä rakenteeltaan että toiminnaltaan — saadaan lisätietoa ja voidaan parantaa riskin arviointia — voidaan analysoida tapahtumia (kuten läheltä piti -tilanteita), muutoksia, kehityssuuntia, onnistumisia ja epäonnistumisia ja oppia niistä — havaitaan ulkoisen ja sisäisen toimintaympäristön muutokset, myös riskikriteerien ja itse riskin muuttuminen, mikä voi

COSO ERM	edellyttää riskin käsittelyn ja tärkeysjärjestyksen uudelleentarkastelua — uudet riskit tunnistetaan. Valvontatoimenpiteet ovat politiikkoja sekä prosesseja, jotka auttavat varmistamaan sen, että johdon valitsemat riskien käsittelytavat tullaan toteuttamaan. Valvontatoimenpiteitä toteutetaan koko organisaatiossa, jokaisella tasolla ja joka toiminnassa.

3.1.4 Standardien eroavaisuuksien yhteenveto

Alla olevaan taulukkoon on koottu perustietoja edellä vertailluista standardeista. Taulukon avulla saadaan nopeasti selville standardien taustojen, soveltamisalueiden, tekijöiden ja saatavuuden erot.

Taulukko 13: Standardien perustietoja

	ISO 31000	**COSO ERM**
Tausta	Suhteellisen uusi standardi. Toki sen on ollut jo käytössä monia vuosia AS/AZ 4360:2004 nimellä, ennen kuin se vuonna 2009 julkaistuun ISOn toimesta parannettuna versiona ISO 31000. Suomessa sen julkaisi suomennettuna versiona Suomen standardoimisliitto vuonna 2011, minkä seurauksena se on vasta nyt ottamassa jalansijaa myös meillä.	Tullut tutuksi yritysten sisäisille tarkastajille COSOn Internal Control – Integrated Framework, sisäisen valvonnan viitekehysmallin kautta. Sisäisen tarkastajan yhtenä tehtävänä kun on myös huomioida, miten organisaatiossa toteutetaan mm. riskienhallintaa.
Soveltamisalue	Voidaan toteuttaa koko organisaatioon, sen eri osiin, yksittäisiin prosesseihin, projekteihin tai tehtäviin.	Kokonaisvaltainen viitekehys, jota olisi tarkoitus toteuttaa koko organisaatiossa.
Tekijät	Riskienhallinnan ammattilaiset	Kirjapitäjät, sisäiset tarkastajat
Saatavuus	Suomenkielisenä, 31 sivua	Englanninkielisenä, 230 sivua

Vertailevan tutkimuksen perusteella voidaan todeta, että suurimmat erot näiden kahden standardin pohjalta ovat riskin sekä viitekehyksen määritelmät (ks. luku 3.2.2). ISO standardille riski on epävarmuuden vaikutus tavoitteisiin. COSO ERM määrittelee sen ilmenevänä tapahtumana, joka mahdollisesti vaikuttaa haitallisesti tavoitteiden saavuttamiseen. COSOn

viitekehys ovat kaikki kahdeksan osa-aluetta, ISOn puitteet muodostavat viitekehyksen, riskienhallintaprosessi itse prosessin.

ISO määrittelee riskin omistajuuden tahona tai henkilönä jolla on vastuu ja valtuudet hallita riskiä. COSO ERM toteaa, että lopullinen vastuu on organisaation johtajalla. COSO ERMiä tulee toteuttaa kokonaisvaltaisesti koko organisaatiossa, ISO 31000 standardia organisaation haluamissa osissa tai koko organisaatiossa. Muutoin standardien eroavaisuudet ovat vähäisiä ja ehkä enemmänkin nyanssi kuin todellisia riskienhallinnan toimintaan vaikuttavia asioita.

COSO ERM on laaja ja sen ovat tehneet sisäiset tarkastajat, joiden vastuulla on organisaation sisäisten kontrollien tehokkuuden ja toimivuuden varmistaminen. ISO 31000 standardi on tehty riskienhallinnan ammattilaisten toimesta, tarkoituksena avustaa mitä tahansa organisaatio tai yhteisöä toteuttamaan tehokasta riskienhallintaa. COSO ERM on rakennettu amerikkalaisille yhtiöille, jotka noudattavat toiminnassaan Sarbanes-Oxley lakia. ISO 31000 pohjalla olevan standardin tarkoituksena oli yhtenäistää käytettävät termistöt ja tavat toteuttaa riskienhallintaa.

Standardin valinta on näin ollen siis riippuvainen siitä, mitä vaatimuksia organisaatiolla on standardistaan. Standardin valinta ei pois sulje toisen standardin hyödyntämistä sen rinnalla. Toinen standardi voi toisaalta antaa apuja, mikäli toinen standardi ei ole kehittäjien mielestä ottanut kaikkia asioita huomioon.

Kumpikaan standardi ei tällä hetkellä tarjoa ohjeistusta siitä, miten asioita pitäisi tehdä vaan niissä mainitaan mitä tulee ottaa huomioon. Tämä on yleinen piirre standardien maailmassa - organisaation kun itse pitää kehittää organisaation mukaiset toimintatavat ottaen kuitenkin huomioon standardin asettamat vaatimukset siitä, mitä tulee huomioida. ISO standardista on tulossa soveltamisopas, joka toivottavasti antaa organisaatioille apua ISO standardin soveltamisessa. COSO on keskittynyt tällä hetkellä sisäisen valvonnan viitekehyksen päivittämiseen (julkaisuajankohta 2013), mutta on todennäköistä, että myös riskienhallintaa tullaan jossain vaiheessa päivittämään.

3.1.5 Vertailevan tutkimuksen johtopäätökset

Hankitun tutkimustiedon perusteella tulin siihen tulokseen, että HALTIKin riskienhallinnan kehittämisen kannalta olisi ISO 31000 standardi parempi vaihtoehto kohdeorganisaation kokonaisvaltaisen riskienhallinnan kehittämiseen. Perusteluni ovat seuraavanlaiset:

1. kehitettävällä organisaatiolla on käytössään ISO 27001 tietoturvallisuuden hallintajärjestelmä, jonka ISO 31000 ottaa mielestäni hyvin huomioon saaden toinen toisistaan

"synenergiaa". Standardi toteaa, että sen puitteiden tarkoitus ei ole määrätä johtamisjärjestelmän rakennetta, vaan auttaa organisaatiota sisällyttämään riskienhallinta sen yleiseen johtamisjärjestelmään (SFS-ISO 31000 2011, 26).

2. organisaatiolla ei ole käytössä riskienhallintaa joka perustuisi varsinaisesti mihinkään standardiin. Mikäli käytössä olisi COSO ERM, ei ISO standardin vaihtaminen olisi välttämättä järkevää, mutta sieltä voisi ottaa jotain kohtia täydentämään COSO ERM viitekehystä.
3. COSO ERM on monimutkainen. Jo aikaisemmin esittelemässäni tutkimuksessa on havaittu, että sen kuutiomainen tapa esittää viitekehys on vaikea hahmottaa sekä sitä on vaikea selittää organisaation johdolle. Tämän lisäksi viitekehys ja menetelmäkuvaus ovat todella laajoja.
4. ISO 31000 on selkeä kuvaten erillisinä osina viitekehyksen sekä prosessin. Se toteuttaa samaa ajatusmaailmaa kuin ISO 27001 ja on yksinkertaisempi sekä helpompi ymmärtää.
5. ISOn periaatteet antavat hyvän ja selkeän raamin organisaation riskienhallintapolitiikalle periaatteidensa muodossa. Periaatteet on helppo sisäistää ja johdon hyväksyä sekä noudattaa.
6. ISO käsittää riskin epävarmuuden vaikutuksena tavoitteisiin, COSO ERM tapahtumana, joka ilmenee ja vaikuttaa haitallisesti tavoitteen saavuttamiseen. ISOn riski saattaa olla myös organisaatiossa tapahtuvat hitaat muutokset. Näin ollen koen, että ISOn riskimääritelmä on osuvampi kuin COSOn antaen myös organisaation henkilöstölle paremman käsityksen siitä, mitä riski voi olla.
7. ISO määrittelee riskin omistajuuden tahona tai henkilönä jolla on vastuu ja valtuudet hallita riskiä. COSOlla lopullinen vastuu on aina organisaation johdolla. Tämä ISOn määritelmä toimii mielestäni paremmin valtionhallinnon organisaatiossa, jossa painotetaan omistajan vastuuta asioissa, myös riskeissä.
8. valtionhallinnon muissa kohdeorganisaatioissa kuten valtiokonttorissa on suunnitteilla ISO 31000 standardin käyttöönotto.

Tutkimuksen päätteeksi esitin kohdeorganisaation riskienhallintapäällikölle standardien vertailutulokset sekä omat käsitykseni sopivammasta standardista. Tämän sekä vallitsevien olosuhteiden perusteella valitsimme kohdeorganisaatiolle sopivammaksi standardiksi ISO 31000.

Kohdeorganisaation riskienhallintapäällikkö esitti organisaation johdolle suosituksensa riskienhallintaa kehittävästä standardista alkutalvesta 2012. Johto hyväksyi valitun standardin saaden näin johdon hyväksynnän analyysin perusteella ehdotetulle standardille.

3.2 GAP-analyysi

Riskienhallinnan teorian mukaan riskienhallinnan kehittämisen lähtökohtana ovat riskienhallinnan tavoitteet ja -periaatteet organisaatiotasolla. Teoriassa mainittiin, että riskienhallintaan liittyvä ohjeistus pitää yleensä sisällään riskienhallintapolitiikan sekä – periaatteet. Jotta kohdeorganisaation riskienhallintaa pystytään kehittämään valitun standardin mukaisesti, tulee ensin saada selville mitkä ovat nykyisen riskienhallintaprosessin eroavaisuudet valittuun standardiin. Tässä hyödynnetään GAP- analyysiä.

GAP -analyysissä verrattiin kyseistä standardia ja olemassa olevaa riskienhallintapolitiikkaa sekä - menettelyohjeistusta keskenään. Tämän avulla saatiin selville mitä eroja käytössä olevalla riskienhallintaprosessilla oli valittuun ISO 31000 standardiin nähden. Näin myös selvitettiin mitkä asiat oli jo otettu huomioon ja mitä tuli lisätä/parantaa olemassa olevaan. Tämän lisäksi olisi tullut suorittaa kypsyysanalyysi, jonka avulla olisi saatu selville jo olemassa olevan toiminnon kypsyystaso.

3.2.1 Riskienhallintapolitiikka

Riskienhallintapolitiikka on osa ISO standardin puitteiden suunnittelua. ISO 31000 standardissa todetaan, että jotta riskienhallinta olisi vaikuttavaa, organisaation olisi noudatettava standardin esittämiä periaatteita kaikilla tasoilla (2011, 22). Riskienhallintapolitiikka luo organisaatiolle riskienhallinnan rungon, viitekehyksen joka tukee riskienhallintaprosessia. Riskienhallintapolitiikan ollessa tärkeässä roolissa riskienhallinnan kehittämisessä, verrattiin olemassa olevaa politiikkaa ISO standardin periaatteisiin sekä puitteisiin. Periaatteet ja puitteet auttavat hallitsemaan riskejä vaikuttavasti (SFS-ISO 31000 2011, 26) ja luovat riskienhallinnalle viitekehyksen.

GAP -analyysi (liite 1) osoitti, että organisaatiolla käytössä oleva riskienhallintapolitiikka kattaa jo merkittävin osin standardin vaatimukset koskien riskienhallintapolitiikkaa. Kohdeorganisaation riskienhallintapäällikön mukaan politiikka ei ole täysin jalkautunut organisaatioon. Tämä ei tullut yllätyksenä riskienhallintapolitiikan nuoren iän takia. Kohdeorganisaation tietoturvallisuuden hallintajärjestelmää noudattavat kohteet toteuttavat riskienhallintaa säännöllisesti, mutta muut organisaation osat eivät ole sitä vielä ottaneet täysin mukaan prosesseihinsa.

Standardissa kohdassa 4.3.2 mainitaan tyypillisen riskienhallintapolitiikan sisältö (SFS-ISO 31000, 28). Standardissa todetaan, että riskienhallintapolitiikan olisi ilmaistava selkeästi organisaation tavoitteet riskienhallinnalle sekä sitoutuminen siihen (2011,28) Alla olevassa taulukossa on kuvattuna standardin riskienhallintapolitiikan vaatimukset sekä kohdeorganisaatiolla olemassa olevan politiikan rakenne.

Taulukko 14: ISO 31000 standardin vaatimus koskien riskienhallintapolitiikan sisältöä verrattuna organisaation tämän hetkiseen riskienhallintapolitiikkaan

ISO 31000 riskienhallintapolitiikan sisältö	Kohdeorganisaation tämän hetkisen riskienhallintapolitiikan rakenne
• **organisaation riskienhallinnan perusteet** • **organisaation tavoitteiden ja toimintaperiaatteiden ja riskienhallintapolitiikan väliset yhteydet** • **riskienhallintaan liittyvät vastuut ja velvollisuudet** • **eturistiriitojen käsittelytapa** • **sitoutuminen tarvittavien resurssien varaamiseen riskienhallinnasta vastaavien tahojen käyttöön** • **riskienhallinnan tason mittaus- ja raportointikeinot** • **sitoutuminen riskienhallintapolitiikan ja puitteiden katselmointiin ja kehittämiseen sekä säännöllisin väliajoin että reaktiona tapahtumiin tai olosuhteiden muuttumiseen**	1. Riskienhallinnan periaatteet 2. Jatkuvuudenhallinnan ja riskien arvioinnin säädöspohja 3. Roolit ja vastuut 4. Menettelyt ja toimintatavat 5. Valvonta ja raportointi 6. Riskienhallintapolitiikan vahvistaminen ja tarkastaminen

3.2.2 Riskienhallinnan periaatteet

Standardin puitteissa havaittiin GAP -analyysin avulla kohtia, jotka kuuluvat selvästi kohdeorganisaation riskienhallinnan menettelyohjeeseen. Jotta riskienhallintapolitiikasta ei tulisi asiakirjana liian pitkää, on kohdeorganisaatiossa käytössä riskienhallinnan menettelyohjeet, joissa kuvataan mm. riskienhallintaprosessi. Kohdeorganisaation tavoitteena on pitää politiikat lyhyinä ja ytimekkäinä, menettelyohjeiden ollen sitten tarkemmin prosessia kuvaavia ohjeistuksia. Standardi on erotellut viitekehyksen sekä prosessin ja tätä mallia haluttiin myös jatkossa noudattaa erottamalla politiikalla periaatteet ja puitteet, menetelmäkuvauksella prosessi.

Kohdeorganisaation riskienhallinnan menettelyohjeistus on rakenteeltaan seuraavanlainen:

1. riskien arviointi
    - kohteen rajaus ja arvioinnin suunnitteleminen
    - uhkien tunnistaminen

    - riskin luokittelu
    - riskin vaikutusaika
    - riskin todennäköisyyden määrittäminen
    - riskin seurauksen määrittäminen
    - turvamekanismien valinta
2. riskien käsittely ja raportointi
    - osastot
    - projektit
    - riskienhallintapäällikkö
    - kohdeorganisaation johto
3. riskienhallinnan valvonta
4. riskienhallinnan kehittäminen
5. toimintaohje uuden työjärjestyksen osalta
6. liitteet
    - sanastoa
    - riskienhallinnan vuosikello

GAP -analyysin perusteella huomattiin, että prosessi noudatti periaatteessa samaa kaavaa kuin ISO -standardin, mutta riskienarviointiprosessissa oli enemmän vaiheita kuin standardin.

4 Riskienhallinnan kehittämissuunnitelma

Kohdeorganisaatiolle luodussa kehittämissuunnitelmassa on otettu huomioon riskienhallinnan teoria sekä tutkimustiedon hankinnassa saadut tulokset. Tämän lisäksi käytännön tietoa riskienhallintaprosessin toteutuksesta on saatu kohdeorganisaation riskienhallintapäälliköltä keskustelujen muodossa. Erillisiä haastattelutilanteita ei tiedon saamiseksi tarvittu. Kehittämisessä hyödynnettiin myös kohdeorganisaation sisäisen tarkastajan vuonna 2011 tekemää tietoturvallisuuden hallintajärjestelmän tarkastusraporttia, jonka osana oli myös riskienhallintapolitiikka sekä menettelyohjeistus. Lisäksi kehittämisessä otetaan huomioon ISO 27001 standardin vaatimukset koskien tietoturvallisuuden hallintajärjestelmän riskien hallintaa.

Kehittämissuunnitelma pohjautuu riskienhallinnan kehittämiseen kohdeorganisaation valitsemaan ISO 31000 standardiin. Kehittämisessä hyödynnetään osin Broadleaf Capital International PTY LTD organisaation tuottamaa dokumenttia How to bring your ERM framework into line with ISO 31000 (Purdy 2008) muokaten sitä kyseiseen tilanteeseen ja organisaatioon sopivaksi. Dokumentin tuottanut Broadleaf Capital International on Australialainen konsulttiyritys, jonka yhtenä toimialana on riskienhallinnan konsultointi. Edellä mainitun dokumentin kirjoittajalla Grant Purdyllä on riskienhallinnasta yli 35 vuoden kokemus ja hän toimii myös Australian riskienhallintakomitean puheenjohtajan, komitean joka kehitti australialaisen riskienhal-

lintastandardin AS/NZS 4360. (Broadleaf Capital 2013.) Tähän samaiseen standardiin pohjautuu vuonna 2009 julkaistu ISO 31000 riskienhallintastandardi. Näiden perusteella kohdeorganisaation riskienhallintapäällikkö hyväksyi Purdyn prosessimallin käyttämistä riskienhallinnan kehittämisessä.

Riskienhallinnan jalkauttaminen tulee Purdyn (2008) mukaan toteuttaa ensin mukauttamalla organisaatiossa käytettävä riskin ja riskienhallinnan "kieli" yhteiseksi. Kielellä tarkoitetaan riskienhallinnassa käytettävää termistöä ja niiden määrityksiä. Mikäli toteuttamisessa käytetään mm. riskienhallintastandardia, tulisi organisaation riskienhallinnassa käyttää standardin termistöä. Yhteisen kielen määrittelemistä suosittelevat myös Ilmonen ym. (2010, 42), jotka teoksessaan tuovat esille että keskeiset käsitteet tulee olla määriteltynä ja että kaikkien tulee käyttää niitä samalla tavalla.

Purdyn prosessin mukaisesti seuraavaksi arvioidaan olemassa olevan riskienhallinnan politiikat sekä ohjeistukset, jotta selviää onko niissä standardin mukaiset elementit. Tämän jälkeen olemassa olevan riskienhallinnan kypsyys tulee arvioida ja kartoittaa. Analyysien avulla nähdään mitä muutoksia ja parannuksia tulee tehdä, jonka jälkeen luodaan suunnitelma muutoksille sekä varmistetaan riskienhallinnan tehokkuuden ylläpitäminen.

Konstruktiivisen tutkimuksen mukaisesti kohdeorganisaatiolle on suoritettu tarvittavan tiedon saamiseksi GAP -analyysi, jossa selvitettiin olemassa olevan riskienhallinnan ero verrattuna valittuun riskienhallintastandardiin. Kypsyystason arviointia ei tässä tutkimuksessa suoritettu, olemassa olevan riskienhallintaprosessin nuoren iän takia. Kehittämissuunnitelma luotiin Purdyn mallista muokaten seuraavan, taulukossa 13 esitetyn prosessin mukaiseksi:

Taulukko 15: Kehittämissuunnitelmassa käytettävän riskienhallinnan kehittämisen prosessi

1. Johdon tuki	Johdon tuki ja hyväksyntä standardin asettamille periaatteellisille vaatimuksille. Riskienhallinnan periaatteiden noudattaminen tulee aloittaa ylhäältä alaspäin.
2. Aikataulutus	Luodaan aikataulu suunnitelman avulla riskienhallinnan kehittämiselle.
3. Resurssit ja rahoitus	Kartoitetaan olemassa olevat resurssit, lisäkoulutuksen tarve sekä mahdollisen konsultin käytön selvittäminen. Mahdollisille lisäkustannuksille tulee saada johdon hyväksyntä.
4. Käyttöönottoon valmistautuminen	Johdon hyväksyntä uudelle riskienhallintapo-

	litiikalle sekä menettelyohjeistukselle
	Uuden riskienhallinnan käyttöönottoon valmistautuminen suunnitellen käyttöönottoaikataulu sekä jalkauttaminen organisaation eri osiin
5. Riskienhallinnan jatkuva parantaminen	Riskienhallinnan ylläpitäminen PDCA- mallin (plan, do, check, act) mukaisesti sekä suorituskyvyn mittaus. Mittauksien, palautteiden ja käyttökokemuksien avulla parannetaan riskienhallintaprosessia.

4.1 Johdon tuki

Kohdeorganisaation riskienhallintapolitiikka on johdon hyväksymä asiakirja. Kokonaisvaltaisen riskienhallinnan kehittäminen perustuen ISO -standardiin vaatii aikaa ja mikäli siihen käytetään ulkopuolista konsulttia, niin myös rahaa. Tässä tapauksessa ulkopuolista konsulttia ei tulla kehittämisessä käyttämään, mutta mikäli tällainen olisi käytettävissä, tulisi kohdeorganisaation varautua konsultin mahdollisiin kustannuksiin.

Kohdeorganisaation johdon tulee antaa riskienhallintapäällikölle tuki riskienhallintapolitiikan sekä menettelyohjeen päivittämiselle standardin mukaiseksi sekä niiden jalkauttamiselle. Tätä varten riskienhallintapäällikön tulee esittää edellä kuvatun vaiheen tuloksia siitä, mitä mahdollista hyötyä standardin käyttöönotolle on, mikä on tämän hetkinen riskienhallinnan kypsyystaso sekä GAP -analyysin tulokset. Johdon tulee olla tietoinen riskienhallinnalle asetetuista ulkoisista vaatimuksista.

Kohdeorganisaation johdon tulee ymmärtää ja hyväksyä ISO 31000 perustuvan riskin käsitteen, sen periaatteet sekä heillä tulee olla tahtotila ja halu parantaa olemassa olevaa riskienhallintaa standardin mukaiseksi. Kohdeorganisaation johdon tulee ymmärtää riskienhallinnan antama lisäarvo niin sille asetettujen tavoitteiden saavuttamisessa kuin toiminnan jatkuvuuden varmistamisessa. Riskienhallinta perustuu laadukkaaseen johtamiseen, eikä sitä voi näin ollen kehittää ilman organisaation ylimmän johdon sitoutumista ja tukea (Ilmonen ym. 2010, 41).

Kohdeorganisaation johdolle esitettiin riskienhallinnan kehittämissuunnitelma aikatauluineen joulukuussa 2012. Organisaation johto esitti tukensa riskienhallinnan kehittämiselle sekä koki sen viraston toiminnan kannalta tärkeäksi prosessiksi. Johtoryhmä esitti johdon riskienkäsitte-

lyn toteutettavaksi jokaisessa johtoryhmän kuukausittaisessa kokouksessa nykyisen prosessin sijaan. Tämä tullaan huomioimaan riskienhallinnan menettelyohjetta luotaessa.

4.2 Aikataulutus

Organisaation tulisi varata aikaa riskienhallinnan kehittämiselle. Kehittäminen sisältää niin tarvittavien asiakirjojen valmistelun kuin koulutusmateriaalin luomisen. Riskienhallinnan kehittäminen on aikaa vaativa prosessi ja kiinteästi sidoksissa organisaation johtamisen kypsyyteen (Ilmonen ym. 2010, 46).

Kohdeorganisaation riskienhallintapäällikkö on asettanut riskienhallinnan kehittämissuunnitelman tavoiteaikatauluksi vuoden 2012 loppuun mennessä. Kehittämissuunnitelma esitettiin kohdeorganisaation johdolle joulukuussa 2012 tavoiteaikatauluineen. Johdolta saadun hyväksynnän mukaan kohdeorganisaation ISO 31000 mukaisen riskienhallintapolitiikka sekä – menettelyohjeistus tulee hyväksyttää organisaation johdolla viimeistään maaliskuussa 2013. Riskienhallinnan jalkauttaminen aloitetaan riskienhallintapolitiikan ja -menettelyohjeistuksen hyväksynnän jälkeen. Jalkautus tullaan toteuttamaan huhti- ja syyskuun aikana käyttöönottoon valmistautumisen mukaisesti. Jalkauttamiseen halutaan varata aikaa, jotta se saadaan toteutettua perusteellisesti aloittaen kohteista jotka jo toteuttavat prosessin mukaista riskienhallintaa.

4.3 Resurssi ja rahoitus

Kohdeorganisaation riskienhallinnan kehittäminen toteutetaan organisaation sisäisin voimavaroin oman työn ohella. Näin ollen kohdeorganisaation ei tarvitse käyttää kehittämiseen ulkopuolista konsultointia eikä lisätyövoimaa, vaan kehittäminen tapahtuu siitä vastuussa olevan yksikön voimin. Resursseina kehittämisessä sekä jalkauttamisessa tullaan käyttämään kyseisen kohde-organisaation tietoturva-asiantuntijoita sekä tietenkin kohdeorganisaation riskienhallintapäällikköä. Jalkauttaminen tulee tapahtumaan myös kohdeorganisaatiossa toimivan tietoturvallisuustyöryhmän avulla kohdeorganisaation muihin osastoihin ja yksiköihin. Kehittäminen ei siis vaadi erillistä rahallista budjetointia vaan jalkauttaminen tapahtuu normaalin tietoturvatyön ohella.

4.4 Käyttöönottoon valmistautuminen

Kohdeorganisaation tulee varata tarpeeksi aikaa ISO 31000 mukaisen riskienhallinnan käyttöönotolle. Kohdeorganisaatiolle luodaan päivitetty riskienhallintapolitiikka sekä menettelyohjeistus sovitun aikataulun mukaisesti (luku 4.2) Tämän lisäksi tulee ottaa huomioon mahdol-

listen riskityökalujen, koulutusaineiston sekä riskienhallintaan käytettävän sähköisen portaalin päivittäminen.

Päivitetyn riskienhallinnan jalkauttamista mietittäessä tulee kohdeorganisaation panostaa ensin ns. "valmiisiin" kohteisiin ja prosesseihin ja sen jälkeen edetä haastavampiin. Näin jalkauttamisesta saatuja kokemuksia voidaan hyödyntää tehokkaammin haastavampien kohteiden aikana.

4.4.1 Riskienhallintapolitiikan kehittäminen

Organisaation riskienhallintapolitiikkaa tulee muokata vastaamaan ISO 31000 standardin mukaista sisältöä sekä vaatimuksia soveltuvin osin. Tämän avulla kohdeorganisaatioon jalkautetaan standardin mukaiset riskienhallinnan periaatteet sekä käsitteet ja luodaan sen puitteet. Riskienhallintapolitiikka on johdon lausunto siitä, kuinka riskienhallintaa kohdeorganisaatiossa toteutetaan.

Esityksessä kohdeorganisaation uudeksi riskienhallintapolitiikan rungoksi on otettu huomioon standardissa mainitut vaatimukset riskienhallintapolitiikalle sekä ne standardin kohdat, jotka antavat kyseiseen kohtaan sisältöä sekä vaatimuksia. Standardin kohdat on tunnistettu tutustumalla standardiin ja päättelemällä kohtien otsikoiden ja sisältöjen perusteella mihin politiikan kohtaan ne kuuluisivat. Politiikan sisältöä luotaessa tulee hyödyntää soveltuvin osin standardin tekstejä sekä tarvittaessa avata tekstit organisaatiolle ymmärrettävään muotoon.

Riskienhallintapolitiikaksi esitetyn uuden rungon otsikoiden nimien on tarkoitus olla mahdollisimman kuvaavia, mutta samalla yksinkertaisia ja standardissa määritellyn termistön mukaisia. Päälinjauksena voidaan pitää sitä, että standardin johdanto ja puitteet sekä osin toteuttaminen, ovat avattuina politiikassa (taulukko 14)

Taulukko 16: Esitys kohdeorganisaation uuden riskienhallintapolitiikan rungoksi

Vastaa ISO standardin riskienhallintapolitiikan sisällön kohtaa	Kohdeorganisaation uuden riskienhallintapolitiikan runko	Sisältäen standardin kohdat
Organisaation riskienhallinnan perusteet	1. Riskienhallintapolitiikan tarkoitus ja tavoitteet 2. Riskienhallinnan termit ja määritelmät 3. Riskienhallinnan periaatteet	johdanto kohta 2 kohta 3
Riskienhallintaan liittyvät vastuut ja velvollisuudet **Sitoutuminen tarvittavien re-**	4. Riskienhallinnan roolit, vastuut ja resurssit	kohta 4.2 kohta 4.3.3 kohta 4.3.5

surssien varaamiseen riskienhallinnasta vastaavien tahojen käyttöön		
Organisaation tavoitteiden ja toimintaperiaatteiden ja riskienhallintapolitiikan väliset yhteydet	5. Riskienhallinnan puitteet	kohta 4.3.1 kohta 4.3.4
Riskienhallinnan tason mittaus- ja raportointikeinot.	6. Riskienhallinnan raportointi ja viestintä	kohta 4.3.6 kohta 4.3.7
Sitoutuminen riskienhallintapolitiikan ja puitteiden katselmointiin ja kehittämiseen sekä säännöllisin väliajoin että reaktiona tapahtumiin tai olosuhteiden muuttumiseen	7. Riskienhallintapuitteiden seuranta, katselmointi ja jatkuva kehittäminen	kohta 4.4.1 kohta 4.5 kohta 4.6

Yhtenä kehittämisen tarpeena havaittiin myös riskilajit. Kohdeorganisaation sisäinen tarkastus suoritti riskienhallinnalle tarkastuksen vuonna 2011 osana tietoturvallisuuden hallintajärjestelmän tarkastusta ja havaittuina kehittämisasioina oli paremman liiketoimintanäkökulman huomioon ottaminen kohdeorganisaation riskienhallinnassa sekä tulosten tulisi olla vertailukelpoisia (Sisäinen tarkastus HALTIK, 2011).

Riskien luokittelun avulla riskejä voidaan paremmin vertailla keskenään. Kuten riskienhallinnan teoreettisessa viitekehyksessä todetaan, on yleisin tapa luokitella riskit neljään lajiin: strategisiin ts. liiketaloudellisiin, taloudellisiin, operatiivisiin riskeihin sekä vahinkoriskeihin. Tällöin riskit jaotellaan niiden lähteen sekä niiden tyypin mukaan. Riskin lähteellä tarkoitetaan niitä tekijöitä, joiden vaikutuksesta riski toteutuu. Tekijöitä voi olla useita. Kaikissa näissä riskilajeissa voi olla riskejä, joiden lähde on joko sisäinen, organisaation sisäisiin toimintoihin, tapahtumiin ja valintoihin liittyvä tai ulkoinen, esimerkiksi asiakkaaseen, markkinoihin tai lainsäädäntöön liittyvä. (Ilmonen ym. 2010, 70.)

Riskienhallintapolitiikkaa kehitettäessä tulee pohtia, onko riskilajit arvioitu tarpeeksi kattavasti. Niiden sisällöt tulee menettelyohjeessa kuvata tarpeeksi selväksi, jotta voidaan varmistaa että kaikki riskilajit on käyty läpi riskienarvioinnissa. Kuten aikaisemmin luvussa 2.3 todettiin, tulee riskien lajin eli kategorian olla organisaation mukainen.

4.4.2 Riskienhallinnan menettelyohjeen kehittäminen

Tämä tulee yhtenäistää standardin mukaiseksi. Tämän lisäksi valittujen riskienhallintastrategioiden kuvaaminen tulee olla tarkempaa. Menettelyohjeessa oleva prosessi eroaa politiikassa mainitusta prosessista, joten tämä tulee tarkistaa. Ohjeessa ei mainita ulkoisen toimintaympäristön huomioon ottamista. Ohjeen sanasto tulee siirtää politiikkaan, päivittäen se standardin mukaiseksi. Riskienhallinnan vuosikello tulee siirtää riskienhallinnan portaaliin mainiten menettelyohjeessa sen olemassa olo. Näin ollen sen päivittäminen on helpompaa.

Riskienhallintapäällikön kanssa menettelyohjeesta keskusteltaessa tuli ilmi, että riskienhallinnan raportointiosuutta johdolle tulisi tehokkuuden lisäämiseksi muuttaa. Tällä hetkellä johdolle raportoidaan neljän kuukauden välein kohdeorganisaation osastojen avainriskit. Johtoryhmän, jossa riskit esitellään ja johon osallistuu myös henkilöstön edustaja, kokouksia järjestetään kerran kuussa ja näin ollen niihin kertyy paljon muutakin käsiteltävää asiaa. Jotta riskienhallintaa saataisiin paremmin jalkautettua sekä sen vaikuttavuutta parannettua, olisi toivottavaa että riskejä käsiteltäisiin johdon edustajien keskuudessa useammin. Tämä on myös tavoitetila, jonka johto antoi palautteena riskienhallinnan kehittämissuunnitelmalle joulukuussa 2012. Näin ollen riskienhallinnan päivitettävässä menettelyohjeessa tulisi esittää riskien käsittelyä kuukauden välein, neljän sijaan.

Riskienhallinnan menettelyohjeen runko on luotu samoilla periaatteilla kuin esitetyn uuden riskienhallintapolitiikankin. Toisin kuin politiikassa, menettelyohje keskittyy standardin kohtiin prosessi, jossa siis kuvataan miten asiat käytännössä toteutetaan politiikassa luotujen puitteiden avulla (taulukko 15)

Taulukko 17: uuden riskienhallintamenettelyohjeen runko ISO 31000 standardin kohtien mukaan

Kohdeorganisaation uuden riskienhallinta-menettelyohjeen runko	**Sisältäen standardin kohdat**
Riskienhallintaprosessi	kohta 5.1
Riskienhallintaprosessin raportointi ja viestintä	kohta 5.2
Riskienhallintaprosessin toimintaympäristön määritteleminen	kohta 5.3
Riskin arviointi • **riskien tunnistaminen** • **riskin analyysi** • **riskin merkityksen arviointi**	kohta 5.4
Riskin käsittely	kohta 5.5
Riskien seuranta ja katselmointi	kohta 4.4.2 kohta 5.6
Riskienhallintaprosessin tallenteet	kohta 5.7

Riskienhallinnan menettelyohjeessa tulee myös huomioida johdon politiikassa määrittelemät ja mahdollisesti uudelleen arvioidut riskilajit. Riskienhallinnan menettelyohjeessa tulee avata riskilajeihin liittyvät osa-alueet ja luoda menettelyohjeessa tarkastuslista, joiden avulla voidaan varmistaa, että kaikki riskilajit on käyty läpi ja kattavasti pyritty tunnistamaan kaikki riskit (Ilmonen ym. 2010, 70).

4.5 Riskienhallinnan jatkuva parantaminen

Riskienhallinnan jalkauttamisen jälkeen tulee kohdeorganisaation yhä jatkaa riskienhallinnan seuraamista, sen kehittämistä sekä parantamista Demingin PDCA- mallin mukaisesti (kuvio 7) Riskienhallinta ei saa jäädä hetkittäiseksi kehittämiseksi johon johto antaa sen hetkisen tukensa. Kohdeorganisaation tulee suunnitella miten aiotaan ylläpitää, parantaa, kehittää ja jalkauttaa riskienhallintaa jatkossa. Jotta riskienhallinta saadaan pysymään tehokkaana ja toimivana, tulee kohdeorganisaation sisällyttää se kaikkiin sen tärkeisiin prosesseihin. Tämän lisäksi riskienhallinnan suorituskyvyn mittaaminen tulee sisällyttää niin kohdeorganisaatio - kuin henkilökohtaiselle tasolle saaden näin myös esimiehet ja tiimiesimiehet vastuuseen omistamistaan riskilistoista ohjeistuksien vaatimalla tasolla. Riskienhallinnan kehitys yleensä pysähtyy silloin, kun riskienhallinnan perusprosessit on saatu jalkautettua ja riskien säännöllinen raportointi on käynnissä (Ilmonen ym. 2010, 46).

Riskienhallinnan kehittäminen otetaan mukaan osaksi kohdeorganisaation ISO 27001 tietoturvallisuuden hallintajärjestelmää. Hallintajärjestelmä noudattaa standardin mukaista PDCA-mallia. Kyseiseen hallintajärjestelmään kohdistetaan tietoturvallisuuden arviointeja mm. vuosittaisia sisäisen tarkastajan tarkastuksia sekä sertifiointiarvioijan auditointeja. Näin ollen myös riskienhallintaa arvioidaan itsenäisen tahon toimesta vuosittain sekä sen toteutumista mitataan hallintajärjestelmän kehittämisen ja raportoinnin avulla. Tällöin riskienhallinta on osa kohdeorganisaation tietoturvallisuuden hallintajärjestelmää, kuten ISO 31000 standardissa kehotetaan huomioimaan.

5 Yhteenveto

Tutkimuksen tavoitteena oli kehittää kohdeorganisaation riskienhallinnan vaikuttavuutta ottaen huomioon sen kokonaisvaltaisuus. Riskienhallinnan vaikuttavuuden parantamisen tarpeet asetti kohdeorganisaation riskienhallintapäällikkö. Tämän lisäksi kehittämisessä hyödynnettiin kohdeorganisaation sisäisen tarkastajan riskienhallinnasta kirjoittamaa raporttia.

Tutkimuskysymyksen asettelun perusteella tutkimusmenetelmäksi valittiin kehittämistyön menetelmät – teoksen mukaisesti konstruktiivinen tutkimus. Konstruktiivisen tutkimuksen tarkoituksena on muuttaa ja parantaa olemassa olevaa toimintaprosessia. Konstruktiivista tutkimusta käytetään kun ongelmanratkaisuun tarvitaan teoreettista tietämystä (Ojasalo 2009, 66).

Tutkimukseen tarvittavan teoriatiedon hankinnassa keskityttiin riskienhallinnan teoriaan, sen käsitteisiin, prosessiin sekä tärkeimpiin asiakirjoihin. Tämän lisäksi selvitettiin kokonaisvaltaisen riskienhallinnan määritelmää. Teoriassa hankittiin myös tutkimustietoa riskienhallinta-

standardeista sekä niiden käyttötilastoista. Tämän lisäksi selvitettiin valtionhallinnon organisaatioista tehtyä tietoturvallisuuden tutkimusta keskittyen riskienhallinnan osuuteen.

Tutkimukseen tarvittavan teoriatiedon perusteella tarkennettiin tutkimuskysymystä. Teorian avulla saatiin tietoa siitä, miten kehittämisen kanssa tulisi edetä ja mitä asioita tulisi ottaa huomioon. Teoriassa saadun tiedon perusteella kohdeorganisaatio päätti lähteä kehittämään riskienhallintaansa yleisesti hyväksi havaitun riskienhallintastandardin perusteella. Tämän avulla kohdeorganisaation voisi luottaa siihen, että kaikki tarvittavat riskienhallinnan osa-alueet tulisi huomioiduksi. Tämän lisäksi päätettiin keskittyä riskienhallinnan perusasiakirjojen kehittämiseen valitun standardin mukaiseksi. Leinon ym. mukaan (2005, 128) mukaan riskienhallintapolitiikka sekä – periaatteet luovat riskienhallinnan perustan, toisin sanoen kertovat kohdeorganisaation riskienhallinnan tavoitteet, vastuut sekä prosessin.

Kehittämissuunnitelmaan tarvittava riskienhallintastandardi päätettiin kohdeorganisaation riskienhallintapäällikön kanssa valita FERMAn tekemän tutkimuksen perusteella. Tutkimuksessa tuli esille kaksi yleisimmin Euroopassa käytettyä riskienhallintastandardia – COSO ERM ja ISO 31000. Tutkimustiedon hankkimiseksi sekä riskienhallintastandardin valinnan tueksi suoritettiin näiden kahden standardin eroavaisuuksien vertaileminen vertailevaa analyysiä käyttäen. Vertailevalla analyysilla hahmotetaan valittujen tapauksien tai sosiaalisten yksiköiden välisiä yhtäläisyyksiä ja eroja. Vertailevassa analyysissä huomioitiin teoriassa saatujen riskienhallinnan tärkeimmät osa-alueet kuten riskienhallinnan käsitteistö (yhteinen termistö) sekä riskienhallintaprosessi. Päätöksenteossa huomioitiin myös kohdeorganisaation ympäristö.

Vertailevassa analyysissa tulee ottaa huomioon, ettei olemassa yhtä ja ainoaa tapaa tehdä vertailevaa analyysia, saati että olisi olemassa erityinen vertaileva tapa, jota kaikki voisivat käyttää (Kekkonen 2008, 33). Kekkonen toteaa, että onnistunut vertailu vaatii aina syvällistä vertailtavien kohteiden tuntemusta (2008,34). Luvussa 2.2 esitellyt riskienhallintastandardit sekä niiden kuvaukset auttoivat vertailevan analyysin suorittamisessa, standardien eroten toisistaan varsinkin viitekehyksen ja – prosessin osalta.

Kehittämissuunnitelman rakentamiseksi tuli kohdeorganisaation riskienhallinnan asiakirjoja verrata valitun standardin vaatimuksiin. Tämä suoritettiin GAP – puuteanalyysin muodossa, jonka tarkoituksena on verrata ja kuvata nykytilan sekä tavoitetilan välisiä eroja. Analyysin avulla saatiin tietoa siitä, missä tilassa kohdeorganisaation riskienhallintapolitiikka sekä – menettelyohjeistus olivat – mitä tulisi asiakirjojen päivittämisessä ottaa huomioon.

Kehittämissuunnitelman viitekehyksenä käytettiin kohdeorganisaation valitsemaa ISO 31000 riskienhallintastandardia. Kehittämissuunnitelmassa otettiin huomioon riskienhallinnan ammattilaisen Grant Purdyn ISO 31000 standardin mukainen riskienhallinnan kehittämisprosessi.

Purdyn käytännön ohjeistukset antoivat kehittämissuunnitelmalle perustellun kehittämisprosessin rungon.

Kehittämissuunnitelman kehittämisprosessissa otettiin Purdyn mallista muokaten huomioon kehittämiseen tarvittava johdon tuki, kehittämisen aikataulu, resurssi ja rahoitus, käyttöönottoon valmistautuminen sekä riskienhallinnan jatkuva parantaminen. Käyttöönottoon valmistautumisessa huomioitiin tarvittavat päivitykset niin riskienhallintapolitiikkaan kuin – menettelyohjeistukseen. Kehittämissuunnitelman avulla kohdeorganisaatio pystyi kehittämään riskienhallintaansa teoriassa hyväksi havaittuun riskienhallintastandardiin pohjautuen, ottaen samalla huomioon tarvittavat kehittämisen prosessin vaiheet.

5.1 Tutkimuksen tarkastelu

Tutkimustyö perustui riskienhallinnan kirjalliseen teoriaan sekä riskienhallinnasta saatuihin tutkimustietoihin. Päätös riskienhallinnan kehittämisestä standardia vahvistui riskienhallinnan kirjallisuuteen tutustuttaessa. Kuten Ilmonen tuo teoksessa Johda Riskejä esille, on standardien suurin hyöty siinä, että ne luovat yhteisen riskienhallintasanaston ja metodin, joka mahdollistaa jatkuvan ja toistettavan lähestymistavan riskienhallintaan (Ilmonen ym. 2010, 30).

Kehittämissuunnitelma olisi voitu toteuttaa päättämällä mitä riskienhallintaa kohdeorganisaatio alkaa viitekehyksenään käyttää ilman, että asiasta olisi tehty minkäänlaista tutkimusta valinnan pohjaksi. Tämä olisi kuitenkin vaatinut kohdeorganisaatiolta pohjatietoa siitä, mitä standardeja on olemassa ja kuinka yleisessä käytössä ne ovat. Valinta ilman tutkimusta ei olisi antanut perusteltua tietoa siitä miksi kyseinen standardi tulisi valita ja olisiko toinen standardeista kenties tarjonnut kohdeorganisaatiolle sille sopivamman tavan toteuttaa riskienhallintaa.

Uskon löytäneeni tutkimustuloksen pohjalta standardien välillä keskeiset erot ja pystyneeni perustelemaan ehdottamani standardin valinnan syyt. Mielestäni tutkimukseni tuloksia pystyvät hyödyntämään myös muut organisaatiot ja etenkin valtionhallinnon kohdeorganisaatiot. Tutkimus antaa kootun kuvan siitä, miten standardit käsittelevät ja kuvaavat eri määritelmiä sekä miten niiden perusrakenne eroaa toisistaan.

Edellisen lisäksi kehittämissuunnitelman rakennetta voidaan käyttää myös muiden organisaatioiden kehittäessään riskienhallintaansa valitsemansa standardin mukaan. Mikäli organisaatio on valinnut ISO 31000 standardin käytettäväksi riskienhallintastandardiksi, auttaa tämä kehittämissuunnitelma organisaatioita luomaan standardin rakenteen mukaisen politiikan ja -periaatteet. Sisältö on tietenkin organisaatiokohtainen.

Mielestäni tutkimus ja sen pohjalta luotu kehittämissuunnitelma pohjautuu vankasti riskienhallinnan teoriaan ja siinä esitettyihin tärkeisiin osa-alueisiin. Kuten teoriassa tuli esille noudattaa riskienhallinta prosessia, jonka avulla se etenee suunnitelman mukaisesti. Riskienhallintastandardit tarjoavat hyväksi havaitun tavan toteuttaa riskienhallintaa, ottaen huomioon kaikki tärkeät riskienhallinnan osa-alueet. Näin ollen kohdeorganisaation kannalta oli hyvä ratkaisu kehittää organisaation riskienhallintaa valmiiseen standardiin pohjautuen. Toisena vaihtoehtona olisi ollut kehittää organisaation omaa, sisäistä riskienhallinnan viitekehystä. Standardin avulla riskienhallinnasta saadaan kuitenkin luotettavampi, koska sen ovat luoneet kansainväliset organisaatiot ja näin ollen se on laajasti tarkasteltu ja hyväksytty tapa toteuttaa riskienhallintaa.

Lähteet

Beasley, Mark S., Branson, Bruce C, Hancock, Bonnie V. 2010. COSO's 2010 report on ERM - Current state of Enterprise Risk Oversight and Market Perceptions of COSO's ERM framework.

Flink, A., Reiman, T., & Hiltunen, M. (toim.) 2007. Heikoin lenkki? Riskienhallinnan inhimilliset tekijät. Helsinki: Edita.

Harrington, S., Niehaus. G. 2003. Risk Management and Insurance. 2. painos. New York: McGraw - Hill Education.

Hirsjärvi, S., Remes, P. & Saajavaara, P. 2003. Tutki ja kirjoita. 6.-9. painos. Vantaa:Dark

Hopkin, P. 2010. Fundamentals of Risk Management: understanding, evaluating, and implementing effective risk management. India: The Institute of Risk Management

Ilmonen, I., Kallio, J., Koskinen, J., Rajala M. 2010. Johda riskejä – käytännön opas yrityksen riskienhallintaan. Helsinki: Kustannusosakeyhtiö Tammi.

Kekkonen, J. 2008. Vertailevan tutkimuksen haasteita. Tieteessä tapahtuu 3-4/2008. 32 - 37.

Kuusela, H. & Ollikainen, R. (toim.) 2005. Riskit ja riskienhallinta. Tampere: Tampereen yliopistopaino.

Leino M., Steiner M-L. & Wahlroos J. 2005. Corporate Governance ja riskienhallinta. Teoksessa Kuusela, H. & Ollikainen, R. (toim.) 2005. Riskit ja riskienhallinta. Tampere: Tampereen yliopistopaino.

Moeller, R. COSO Enterprise Risk Management 2007, Understanding the New Intergrated ERM Framework, Robert , Inc.: Hoboken New Jersey.

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

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

SFS-ISO 27001. 2006. Informaatioteknologia, Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Suomen standardoimisliitto.

Suominen, A. 2003. Riskienhallinta. 3. painos. Vantaa: Dark.

Suominen, A. 1994. Yritysten riskienhallintakäyttäytyminen ja vakuutuspolitiikka liikkeenjohdon toiminnan osana. Turku: Åbo Akademis Tryckeri.

Uusitalo, H. 1997. Tiede, tutkimus ja tutkielma. Johdatus tutkielman maailmaan. Juva: WSOY.

VAHTI 7 2003. Ohje riskien arvoinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Valtiovarainministeriö. Helsinki: Edita prima.

VAHTI 8 2008. Valtionhallinnon tietoturvasanasto. Valtiovarainministeriö. Helsinki: Edita prima.

VAHTI 1 2012. VAHTIn toimintakertomus vuodelta 2011. Valtiovarainministeriö.

Valtioneuvoston asetus Hallinnon tietotekniikkakeskuksesta 810/2007

Valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa 681/2010

Valtion talousarvio 1243/1992

Valtioneuvoston tietoturvallisuutta koskeva periaatepäätös 11.11.1999

Sähköiset lähteet:

Broadleaf Capital International. 2008. How to bring your erm framework into line with ISO 31000. Viitattu 10.2.2012.
http://www.broadleaf.co.nz/pdfs/articles/lexisnexis_paper_jun08_ver0.pdf. Luettu 18.7.2012

Broadleaf Capital International. 2013. Grant Purdy. Viitattu 18.7.2012.
http://www.broadleaf.com.au/purdy/index.html

Committee of Sponsoring Organizations of the Treadway Commission COSO. 2004. Enterprise Risk Management – Integrated Framework (Kokonaisvaltainen ajatusmalli organisaation riskienhallintaan.) Viitattu 13.8.2012.
http://www.coso.org/documents/coso_erm_executivesummary_finnish.pdf

Federation of European Risk Management Associations FERMA. 2012. Keys to Understanding the Diversity of Risk Management in a Riskier World. Viitattu 6.1.2013
http://www.ferma.eu/2012/10/ferma-risk-management-benchmarking-survey-2012-the-results/

Hallinnon tietotekniikkakeskus. 2011. Viitattu 24.8.2012
HALTIK. http://www.haltik.fi/

Herrainsilta, J. 2006. Riskienhallinta valtionhallinnossa ja valtiokonttorin riskienhallintamenetelmän käyttöönotto. Tampereen yliopisto. Oikeustieteiden laitos. Pro gradu-tutkielma. Viitattu 28.12.2012. http://www.valtiokonttori.fi/download/noname/%7BA05E0B82-2F5A-4017-A38C-5756ECED9E0B%7D/69427

JUHTA- julkisen hallinnon tietohallinnon neuvottelukunta. 2009. JHS 171 ICT-palvelujen kehittäminen: Kehittämiskohteiden tunnistaminen. Viitattu 24.9.2012. http://www.jhs-suositukset.fi/suomi/jhs171

Jyväskylän yliopisto – KOPPA. 2013. Vertaileva tutkimus. Viitattu 24.9.2012.
https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/vertaileva-tutkimus

Saukkonen, P. 2013. Tutkielmanteon tukisivut. Viitattu 21.9.2012.
http://www.mv.helsinki.fi/home/psaukkon/tutkielma/Tutkimusasetelma%202.html

Suomen standardoimisliitto SFS Oy 2012. ISO 31000 Riskienhallinta. Viitattu 12.8.2012.
http://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_31000_riskienhallinta/

Suomen standardoimisliitto SFS Oy 2012. Mihin standardeja tarvitaan? Viitattu 10.9.2012.
http://www.sfs.fi/julkaisut_ja_palvelut/standardi_tutuksi/mihin_standardeja_tarvitaan/

Suomen standardoimisliitto SFS Oy 2012. Standardien laadinta. Viitattu 21.9.2012.
http://www.sfs.fi/standardien_laadinta

Suomen standardoimisliitto SFS Oy 2012. Riskit aiheena standardisoinnin vuositapahtumassa. Viitattu 28.12.2012.

http://www.sfs.fi/ajankohtaista/uutiset/riskit_aiheena_standardisoinnin_vuositapahtumassa.1295.news

Suomen standardoimisliitto SFS Oy 26.10.2012. Turvallisuus on kilpailuetu liiketoiminnassa. Viitattu 12.11.2012.
http://www.sfs.fi/ajankohtaista/tuoteuutiset/turvallisuus_on_kilpailuetu_liiketoiminnassa.1307.news

Suomen standardoimisliitto SFS Oy 2012. Usein kysyttyä. Viitattu 13.1.2013.
http://www.sfs.fi/julkaisut_ja_palvelut/usein_kysyttya#Mikonstandardi

Julkaisemattomat lähteet:

HALTIK. Sisäinen tarkastus 2011. Tietoturvallisuuden hallintajärjestelmän sisäinen auditointi 2011. Viitattu 14.9.2012

HALTIK. Strategisen johdon pöytäkirja 19.12.2012.

Kuviot

Taulukot

Liitteet

Liite 1 GAP- analyysi

ISO 31000 - periaatteet	Riskienhallintapolitiikka	Havainnot	Tullaan lisämään ohjeistukseen
Riskienhallinta luo lisäarvoa ja säilyttää sen. Riskienhallinta edesauttaa tavoitteiden saavuttamista ja toiminnan tason havaittavaa kehittymistä esimerkiksi ihmisten terveyden, turvallisuuden, lakien ja viranomaisten vaatimusten noudattamisen, yleisen hyväksynnän saavuttamisen, ympäristönsuojelun, tuotteiden laadun, projektinhallinnan, toimintojen ja hallintotavan tehokkuuden sekä maineen osalta	Riskienhallintapolitiikan tarkoituksena on on selkeyttää riskienhallinnan tavoitteita, periaatteita, vastuita ja toimintatapoja. Kohdeorganisaation riskienhallinnan tarkoituksena on varmistaa HALTIKin ydintoiminnan jatkuvuus ja tavoitteiden saavuttaminen.	Lisätään standardin teksti tämä politiikan periaatteisiin	Riskienhallintapolitiikka - periaatteet
Riskienhallinta on olennainen osa kaikkia organisaation prosesseja. Riskienhallinta ei ole organisaation muista toiminnoista ja prosesseista erillinen toiminto. Riskienhallinta on osa johdon vastuualueetta ja olennainen osa kaikkia organisaation prosesseja, kuten strategisen suunnittelun prosesseja ja kaikkien projektien ja muutoksenhallinnan prosesseja	Riskienhallintapolitiikka on HALTIKin johdon kokonaisvaltainen näkemys HALTIKissa toteutettavasta riskien hallinnasta. Riskienhallintapolitiikka on käsitelty ja hyväksytty johtoryhmän kokouksessa.	Lisätään standardin teksti tämä politiikan periaatteisiin	Riskienhallintapolitiikka - periaatteet
Riskienhallinta on osa päätöksentekoa. Riskienhallinta auttaa päätöksentekijöitä tekemään tietoisia valintoja, asettamaan toimintoja tärkeysjärjestykseen ja erottamaan vaihtoehtoiset toimintatavat.	Politiikassa mainitaan riskienhallinnan olevan osa päätöksentekoa.	Lisätään standardin teksti tämä politiikan periaatteisiin	Riskienhallintapolitiikka - periaatteet
Riskienhallinnan lähtökohtana on epävarmuuden huomioon ottaminen. Riskienhallinnassa otetaan huomioon epävarmuus, sen luonne ja käsittelymahdollisuu-	Politiikassa mainitaan tavoitteiden saavuttamista estävät uhkaavat riskit.	Lisätään standardin teksti tämä politiikan periaatteisiin	Riskienhallintapolitiikka - periaatteet

ISO 31000 - periaatteet	Riskienhallintapolitiikka	Havainnot	Tullaan lisämään ohjeistukseen
det.			
Riskienhallinta on järjestelmällistä, jäsenneltyä ja ajantasaista. Järjestelmällinen, ajantasainen ja jäsennelty riskienhallinnan toimintamalli lisää tehokkuutta ja tekee tuloksista yhdenmukaisempia, luotettavampia ja helpommin vertailtavia.	Riskienhallintapolitiikka tarkastetaan vuosittain sen varmistamiseksi, että se vastaa vallitsevia oloja ja liiketoimintaympäristössä tapahtuneita muutoksia	Lisätään standardin teksti tämä politiikan periaatteisiin	Riskienhallintapolitiikka - periaatteet
Riskienhallinta perustuu parhaaseen saatavilla olevaan tietoon. Riskienhallintaprosessin lähtötiedot perustuvat tietolähteisiin, joita ovat esimerkiksi historiatiedot, kokemus, sidosryhmien antama palaute, havainnot, ennusteet ja asiantuntijoiden näkemykset. Päätöksentekijöiden olisi kuitenkin otettava selvää tietoihin tai malleihin liittyvistä rajoituksista ja toisistaan poikkeavista asiantuntijoiden näkemyksistä ja otettava ne huomioon.	Politiikassa on huomioitu järjestelmälliset ja yhtenäiset menetelmät arvioida sekä hallita mahdollisia riskejä	Lisätään standardin teksti tämä politiikan periaatteisiin	Riskienhallintapolitiikka - periaatteet
Riskienhallinta toteutetaan organisaation tarpeiden mukaan. Riskienhallinta on sovitettu yhteen organisaation ulkoisen ja sisäisen toimintaympäristön ja riskiprofiilin kanssa.		Lisätään standardin teksti tämä politiikan periaatteisiin	Riskienhallintapolitiikka - periaatteet
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.		Lisätään standardin teksti tämä politiikan periaatteisiin	Riskienhallintapolitiikka - periaatteet
Riskienhallinta on avointa ja kattavaa. Sidosryhmien ja erityisesti organisaation eri ta-		Lisätään standardin teksti tämä politiikan	Riskienhallintapolitiikka - periaatteet

ISO 31000 - periaatteet	Riskienhallintapolitiikka	Havainnot	Tullaan lisämään ohjeistukseen
soilla olevien päätöksentekijöiden ottaminen sopivalla tavalla ja oikeaan aikaan mukaan riskienhallintaan takaa, että riskienhallinta pysyy tarkoituksenmukaisena ja ajantasaisena. Sidosryhmien osallistuminen mahdollistaa sen, että sidosryhmät ovat kunnolla edustettuina ja että heidän näkemyksensä otetaan huomioon riskikriteerien määrittelyssä.		periaatteisiin	
Riskienhallinta on dynaamista, toistuvaa ja muutoksiin reagoivaa. Riskienhallinnan avulla muutokset havaitaan ja niihin reagoidaan viipymättä. Ulkoisten ja sisäisten tapahtumien myötä toimintaympäristö ja tietämys muuttuvat, riskejä seurataan ja katselmoidaan, ilmaantuu uusia riskejä, osa riskeistä muuttuu ja osa katoaa.		Lisätään standardin teksti tämä politiikan periaatteisiin	Riskienhallintapolitiikka - periaatteet
Riskienhallinta tukee organisaation jatkuvaa kehittämistä. Organisaatioiden olisi kehitettävä ja toteutettava strategioita, joilla niiden riskienhallintaa kehitetään muiden organisaation osa-alueiden ohella.		Lisätään standardin teksti tämä politiikan periaatteisiin	Riskienhallintapolitiikka - periaatteet

ISO 31000 Puitteet	Riskienhallintapolitiikka	Havainnot	Tullaan lisämään ohjeistukseen
4.2 Valtuudet ja sitoutuminen	Riskienhallintapolitiikassa on mainittu roolit ja niiden vastuut.	Johdon roolia tulee korostaa standardin mukaan	Riskienhallintapolitiikka- vastuut ja velvollisuudet
4.3.1 Organisaation ja sen toimintaympäristön ymmärtäminen	Kohdeorganisaation riskienhallintapolitiikka ottaa kantaa sille asetettuihin vaatimuksiin sekä kohdeorganisaation strategiaan.	Näitä tulee vielä avata standardin mukaisesti.	Riskienhallintapolitiikka - puitteet
4.3.2 Riskienhallintapolitiikan määritteleminen Riskienhallintapolitiikan olisi ilmaistava selkeästi organisaation tavoitteet riskienhallinnalle sekä sitoutuminen siihen. Riskienhallintapolitiikka kattaa tyypillisesti seuraavat kohdat: — organisaation riskienhallinnan perusteet — organisaation tavoitteiden ja toimintaperiaatteiden ja riskienhallintapolitiikan väliset yhteydet — riskienhallintaan liittyvät vastuut ja velvollisuudet — eturistiriitojen käsittelytapa — sitoutuminen tarvittavien resurssien varaamiseen riskienhallinnasta vastaavien tahojen käyttöön — riskienhallinnan tason mittaus- ja raportointikeinot — sitoutuminen riskienhallintapolitiikan ja puitteiden katselmointiin ja kehittämiseen sekä säännöllisin väliajoin että reaktiona tapahtumiin tai olosuhteiden muuttumiseen. Riskienhallintapolitiikasta olisi viestittävä asianmukaisesti.	Riskienhallintapolitiikka antaa perusteet riskienhallinnalle sekä esittää tavoitteet miksi sitä toteutetaan. Politiikassa ei mainita riskienhallinnan menettelyohjeistusta, mutta prosessi kyllä. Prosessi on ristiriidassa menettelyohjeen prosessin kanssa. Politiikka ei ota kantaa eturistiriitojen käsittelytavalla. Politiikassa on kuvattu velvollisuudet ja vastuut sekä raportointi sisäiselle tarkastajalle. Resurssien varaamisesta ei ole mainittu. Mittauksesta ei mainita. Politiikassa mainitaan sen tarkastaminen vuosittain sekä kehittäminen. Kohdeorganisaation riskienhallintapäällikön mukaan riskienhallintapolitiikka viestittiin organisaation Intranetissä sekä erikseen hallintajärjestelmää noudattavissa kohteissa, mutta viestintää tulee vielä parantaa	Riskienhallintapolitiikkaa tulee viestittää tehokkaammin. Politiikan tulee kattaa standardin kohdat. Prosessi tulee yhtenäistää menettelyohjeen prosessin mukaisesti sitten kun sen on päivitetty	Riskienhallintapolitiikka
4.3.3 Vastuut ja velvollisuudet Organisaation olisi var-	Vastuut ja velvollisuudet on määritelty.		Riskienhallintapolitiikka- vastuut ja velvollisuudet

ISO 31000 Puitteet	Riskienhallintapolitiikka	Havainnot	Tullaan lisämään ohjeistukseen
mistettava, että organisaatiossa on määritellyt vastuut ja velvollisuudet, valtuudet sekä riittävä osaaminen riskienhallintaan, kuten riskienhallintaprosessin toteuttamiseen ja ylläpitämiseen sekä mahdollisten hallintakeinojen riittävyyden, vaikuttavuuden ja tehokkuuden varmistamiseen.			
4.3.4 Sisällyttäminen organisaation prosesseihin **Riskienhallinta olisi sisällytettävä kaikkiin organisaation käytäntöihin ja prosesseihin tarkoituksenmukaisella, vaikuttavalla ja tehokkaalla tavalla. Riskienhallintaprosessia ei saisi pitää erillisenä prosessina, vaan se olisi liitettävä osaksi organisaation prosesseja. Riskienhallinnan olisi oltava osa etenkin toimintaperiaatteiden kehittämistä, liiketoimintasuunnittelua, strategista suunnittelua, katselmuksia ja muutoksenhallintaprosesseja.** **Organisaatiolla olisi oltava koko organisaation kattava riskienhallintasuunnitelma, jolla varmistetaan, että riskienhallintapolitiikka toteutetaan ja sisällytetään kaikkiin organisaation käytäntöihin ja prosesseihin. Riskienhallintasuunnitelma voidaan liittää osaksi muita organisaation suunnitelmia, kuten strategista suunnitelmaa.**	Politiikassa otetaan huonosti kantaa organisaation prosesseista ja niihin riskienhallinnan sisällyttämisestä. Vastuissa ja velvollisuuksissa mainitaan prosessien omistajat ja heidän vastuunsa sisällyttää prosesseihin riskienhallintaa.	Prosessit otettava huomioon politiikassa paremmin	Riskienhallintapolitiikka - puitteet
4.3.5 Resurssit **Organisaation olisi kohdennettava tarvittavat resurssit riskienhallin-**	Vastuut ja velvollisuudet kohdassa on listattu kattavasti kaikkien roolit ris-		Riskienhallintapolitiikka- vastuut ja velvollisuudet

ISO 31000 Puitteet	Riskienhallintapolitiikka	Havainnot	Tullaan lisämään ohjeistukseen
taan.	kienhallinnassa. Organisaatiolla on riskienhallintapäällikkö ja hänen apunaan riskienhallinnan kehittämisessä toimivat kohdeorganisaation tietoturva-asiantuntijat.		
4.3.6 Sisäisten viestintä- ja raportointimallien laatiminen **Organisaation olisi luotava sisäisen viestinnän ja raportoinnin mallit, joilla vahvistetaan vastuuta ja riskien omistajuutta.**	Viestintä ja raportointi on ohjeistettu riskienhallinnan menettelyohjeessa.	Tulee tarkentaa standardin mukaan sekä ottaa huomioon organisaation tietoturvallisuuden hallintajärjestelmän asiakirjojen ohjauksen.	Riskienhallintapolitiikka
4.3.7 Ulkoisten viestintä- ja raportointimallien laatiminen **Organisaation olisi laadittava suunnitelma siitä, kuinka se aikoo viestiä ulkoisten sidosryhmien kanssa, ja toteutettava se.**	Organisaation viestinnästä ja raportoinnista mainittu riskienhallinnan menettelyohjeessa.	Tulee tarkentaa standardin mukaan.	Riskienhallintapolitiikka
4.4 Riskienhallinnan toteuttaminen **4.4.1 Riskienhallinnan puitteiden toteuttaminen** **Riskienhallinnan puitteita toteuttaessaan organisaation olisi** **— 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 riskienhallintaprosessien tulosten kanssa** **— järjestettävä tiedo-**	Riskienhallinnan puitteiden toteuttamista otetaan huomioon riskienhallinnan menettelyohjeessa.	Menettelyohje tulee tarkentaa standardin mukaisesti.	Riskienhallinnan menettelyohje

ISO 31000 Puitteet	Riskienhallintapolitiikka	Havainnot	Tullaan lisämään ohjeistukseen
tus- ja koulutustilaisuuksia — viestittävä ja vaihdettava tietoa sidosryhmien kanssa varmistaakseen, että sen riskienhallinnan puitteet ovat edelleen tarkoituksenmukaisia.			
4.4.2 Riskienhallintaprosessin toteuttaminen Riskienhallinta olisi toteutettava varmistamalla, että standardin kohdassa 5 kuvattua riskienhallintaprosessia sovelletaan riskienhallintasuunnitelman mukaisesti kaikilla kyseeseen tulevilla organisaation tasoilla ja tehtäväalueilla osana sen käytäntöjä ja prosesseja.		Ei jalkauttamisohjeita	Tullaan huomioimaan hallintajärjestelmän avulla
4.5 Puitteiden seuranta ja katselmointi Jotta organisaatio voi varmistaa, että sen riskienhallinta on vaikuttavaa ja tukee jatkuvasti organisaation suorituskykyä, sen olisi — 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 ris-	Riskienhallinta noudattaa tietoturvallisuuden hallintajärjestelmää, jota kautta sitä tullaan jatkuvasti parantamaan.	Riskienhallintaa ei organisaatiossa mitata. Tämä tulee lisätä riskienhallinnan menettelyohjeeseen sekä politiikkaan	Riskienhallintapolitiikka - puitteet

ISO 31000 Puitteet	Riskienhallintapoli-tiikka	Havainnot	Tullaan lisämään ohjeistukseen
kienhallintapolitiikkaa noudatetaan — katselmoitava ris-kienhallinnan puittei-den vaikuttavuutta.			
4.6 Puitteiden jatkuva kehittäminen Seurannan ja katsel-mointien tulosten pe-rusteella olisi päätettä-vä, kuinka riskienhal-linnan puitteita, ris-kienhallintapolitiikkaa ja -suunnitelmaa voi-daan kehittää. Näiden päätösten olisi johdet-tava organisaation ris-kienhallinnan ja sen riskienhallintakulttuurin kehitykseen.	Riskienhallintapro-sessin arviointi löy-tyy politiikasta. Tä-män lisäksi on mai-nittu, että sitä tar-kastellaan vuosittain että se vastaa vallit-sevia olosuhteista.		Riskienhallintapoli-tiikka - puitteet

ISO 3100 riskienhallintaprosessi	Riskienhallinnan menettelyohje	Havainnot	
5.1 Yleistä **Riskienhallintaprosessin olisi oltava** **— olennainen osa johtamista** **— sisällytetty organisaation kulttuuriin ja käytäntöihin** **— mukautettu organisaation liiketoimintaprosesseihin sopivaksi.**	Riskienhallintapolitiikassa mainitaan riskienhallintaprosessi. Riskienhallinnan menettelyohjeessa huomioidaan organisaation kulttuuri ja käytännöt. Tullaan huomioimaan päivitettävässä menettelyohjeessa		Riskienhallinnan menettelyohje
5.2 Viestintä ja tiedonvaihto **Ulkoisten ja sisäisten sidosryhmien kanssa olisi viestittävä ja vaihdettava tietoa kaikkien riskienhallintaprosessin vaiheiden aikana.**	Riskienhallinnasta viestitään sisäisille sidosryhmille prosessin aikana. Ulkoiset sidosryhmät tulee huomioida paremmin viestinnässä.		Riskienhallinnan menettelyohje

5.3 Toimintaympäristön määritteleminen **5.3.1 Yleistä** **Määrittelemällä toimintaympäristön organisaatio ilmaisee selkeästi sen tavoitteet, määrittelee ulkoiset ja sisäiset muuttujat, jotka on otettava huomioon riskien hallinnassa, sekä jäljellä olevan prosessin laajuuden ja riskikriteerit.** **5.3.2 Ulkoisen toimintaympäristön määritteleminen** **Ulkoinen toimintaympäristö on se ulkoinen ympäristö, jossa organisaatio pyrkii saavuttamaan tavoitteensa. Se perustuu koko organisaation laajuiseen toimintaympäristöön mutta sisältää lakien ja viranomaisten vaatimusten yksityiskohdat, sidosryhmien näkemykset ja muut riskienhallintaprosessin soveltamisalaan liittyvien riskien näkökohdat.** **5.3.3 Sisäisen toimintaympäristön määritteleminen** **Sisäinen toimintaympäristö on se sisäinen ympäristö, jossa organisaatio pyrkii saavuttamaan tavoitteensa. Sisäinen toimintaympäristö kattaa kaikki organisaation sisäiset tekijät, jotka voivat vaikuttaa tapaan, jolla organisaatio hallitsee riskejä.** **5.3.4 Riskienhallintaprosessin toimintaympäristön määritteleminen** **Organisaation, tai riskienhallintaprosessien kattamien organisaation osien, toimintojen tavoitteet, strategiat, laajuus ja** **muuttujat olisi määriteltävä. Organisaation riskien hallinnassa olisi otettava huomioon tarve perustella siihen käytettävät** **resurssit. Tarvittavat resurssit, vastuut, valtuudet ja tallenteet olisi määriteltävä.**	Ohjeen mukaan tulee tunnistaa suojattavat kohteet. Ulkoista toimintaympäristöä otettu huomioon heikommin.	Riskienhallinnan menettelyohje
5.3.5 Riskikriteerien määrit-	Kriteerit määritelty	

teleminen **Organisaation olisi määriteltävä kriteerit, joita käytetään riskien merkityksen arvioinnissa.**		
5.4 Riskin arviointi **5.4.1 Yleistä** **Riskin arviointi on kokonaisvaltainen prosessi, joka kattaa riskien tunnistamisen, riskianalyysin ja riskin merkityksen arvioinnin.**	Riskienarviointi toteutetaan prosessina. Prosessi kattaa riskien tunnistamisen, analyysin sekä riskin merkityksen arvioinnin. Arviointiprosessi tulee tarkastaa yhtenäiseksi politiikassa mainitun prosessin mukaisesti	Riskienhallinnan menettelyohje
5.4.2 Riskien tunnistaminen **Organisaation olisi tunnistettava riskin lähteet, vaikutusalueet, tapahtumat (mukaan lukien olosuhteiden muutokset) ja niiden syyt sekä mahdolliset seuraukset**	Riskejä tunnistetaan mm. POA-menetelmän avulla turvallisuuden keskeisimmiltä osa-alueilta. Osa-alueet tulee tarkistaa päivityksen yhteydessä.	Riskienhallinnan menettelyohje
5.4.3 Riskianalyysi **Riskianalyysiin kuuluu käsityksen muodostaminen riskistä.**	Ohjeessa riskianalyysin muodostavat riskin luokittelu, riskin vaikutusaika, riskin todennäköisyys sekä riskin merkittävyys. Näiden prosessien osan avulla toteutetaan riskianalyysi, jonka perusteella voidaan toteuttaa riskin merkityksen arviointi. Tämä tulee yhtenäistää standardin mukaiseksi	Riskienhallinnan menettelyohje
5.4.4 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 arviointia voidaan verrata menettelyohjeen riskien merkittävyyden selvittämiseen. Tällä selvitetään riskien merkittävyys jonka mukaan päätetään riskin taso. Tulee yhtenäistää standardin mukaiseksi	Riskienhallinnan menettelyohje
5.5 Riskien käsittely **5.5.1 Yleistä** **Riskien käsittelyyn sisältyy yhden tai useamman riskinkäsittelytavan valitseminen ja valittujen vaihtoehtojen toteuttaminen.** **Riskinkäsittelytavat luovat tai muuttavat hallintakeinoja.**	Ohjeen prosessi turvamekanismien valinta on osa riskin käsittelyä. Riskin eri käsittelytavat on kuvattu turvamekanismien valinnassa.	Riskienhallinnan menettelyohje
5.5.2 Riskinkäsittelytavan valinta **Kun riskinkäsittelytavoista valitaan sopivinta, niiden to-**	Riskien käsittelytavan valinnasta ei ole tarkempia kuvauksia. On kuvattu eri tavat ja lyhyesti mitä ne	Riskienhallinnan menettelyohje

teuttamisen vaatimia kustannuksia ja työmäärää verrataan niistä saataviin hyötyihin ottaen huomioon lakien ja viranomaisten vaatimukset sekä muut vaatimukset, kuten yhteiskuntavastuu ja ympäristönsuojelu	tarkoittavat. Tulee tarkentaa standardin mukaiseksi	
5.5.3 Riskinkäsittelysuunnitelman laatiminen ja toteuttaminen Riskinkäsittelysuunnitelmien tarkoituksena on dokumentoida, kuinka valitut käsittelyvaihtoehdot toteutetaan	Riskit listataan riskilistalle johon myös kirjataan ehdotetut käsittelytavat. Erillisiä suunnitelmia ei ole. Kuvauksien tulee olla tarkempia	Riskienhallinnan menettelyohje
5.6 Seuranta ja katselmointi Sekä seurannan että katselmoinnin olisi oltava suunniteltu osa riskienhallintaprosessia, ja niihin olisi kuulluttava säännöllisiä tarkastuksia tai valvontaa.	Riskienhallintapäällikkö valvoo ja seuraa riskilistojen ylläpitoa sekä varmistaa, että ajan tasalla olevat listat on sisäisen tarkastajan saatavilla. Riskienhallintaa tarkastellaan myös tietoturvallisuuden hallintajärjestelmän kautta. Tulee lisätä menettelyohjeeseen	Riskienhallinnan menettelyohje
5.7 Riskienhallintaprosessin tallenteet Riskienhallintatoimintojen olisi oltava jäljitettäviä. Riskienhallintaprosessin tallenteet ovat menetelmien ja työkalujen sekä koko prosessin kehittämisen lähtökohta.	Tallenteet toteutetaan riskienhallinnan portaaliin	Riskienhallinnan menettelyohje