RISKIENHALLINTAPROSESSI JA OPERATIIVISTEN RISKIEN KVANTIFIOINTI

10. Turvallisuusjohdon koulutusohjelma
Teknillinen korkeakoulu
Koulutuskeskus Dipoli
Tutkielma 28.2.2010
Jyri Wesanko

SISÄLLYS

LYHENTEET

BIA	Business Impact Analysis
CBA	Cost / benefit analysis
COSO	Committee of Sponsoring Organizations of the Treadway Commission
ERM	Enterprise Risk Management
FERMA	Federation of European Risk Management Associations
FIVA	Finanssivalvonta
FTA	Fault tree analysis
HAZOP	Hazard and operability studies
HACCP	Hazard analysis and critical control point
IEC	The International Electrotechnical Commission
ISO	International Organisation for Standardization
NPV	Net Present Value
RCA	Root cause analysis
ROI	Return on Investment
SLA	Service Level Agreement
SOX	Sarbanes-Oxley Act

1 JOHDANTO

1.1 Tutkielman tausta

”*Without risk there is no advance*” ja ”*The higher the risk the greater the reward*” ovat pitkään liike-elämässä käytettyjä sanontoja, jotka kuvastavatkin varsin hyvin liike-elämän suhtautumista riskinottoon. Rahoitusmarkkinoilla käytettävä rahoitusteoria perustuu samankaltaiseen näkemykseen. Rahoitusteoriassa on kaksi keskenään vastakkaista tavoitetta: samanaikaisesti tulisi maksimoida tuotto ja minimoida riski[1]. Rahoitusteorian optimaalinen toteuttaminen perustuu siis sekin riskienhallintaan. Näistä liike-elämän periaatteiden ja rahoitusteorian kiteytyksistä on johdettavissa, että hyvä yritystoiminta on onnistunutta riskinottoa. Sen edellytyksenä on yritystoimintaan sisältyvien riskien onnistunut hallinta, mikä taas edellyttää, että riskit on oikein arvioitu. Tämä tutkielma käsitteleekin riskienhallintaa tästä lähtökohdasta: riskienhallinta on prosessi, jonka kuvaamisen lisäksi tarkastellaan erityisesti riskienhallintaprosessin sitä osaa, joka liittyy liike-elämän ehkä perinteisimpään menestymisen mittariin eli rahaan: riskien kvantifiointia.

Riskienhallintaprosessi on joukko organisaatiossa käytettäviä menetelmiä, joilla organisaatiolle asetettujen tavoitteiden saavuttaminen pyritään varmistamaan. Mikäli sitä toteutetaan oikein, on se kiinteä osa organisaation muita prosesseja. Riskienhallintaprosessi on kuitenkin tarpeen kuvata omana prosessinaan sen vaiheistuksen ja tavoitteiden ymmärtämiseksi, minkä jälkeen sitä voidaan toteuttaa osana liiketoimintaprosesseja. Tässä tutkielmassa esitetään riskienhallintaprosessin vaiheet, joita noudattamalla alussa esitetyt liike-elämän sanonnat saadaan toteutettua.

---

[1] Kuusela & Ollikainen 2005, s. 78.

Riskien kvantifioiminen on riskien arvojen määrittämistä. Käytännössä riskille määritellään ’hinta’, joka organisaation täytyy maksaa, jos riski toteutuu ennakoidun mukaisesti. Se ei ole erityisen monimutkaista niin sanottujen perinteisten ja nimenomaan vakuutettavien vahinkoriskien osalta. Esimerkiksi kiinteän omaisuuden jälleenhankinta-arvo on pääsääntöisesti melko tarkasti määriteltävissä. Yleisimpien vahinkoriskien, kuten palovahinkojen todennäköisyyskin on kattavien tilastojen ja riskin tuttuuden takia suhteellisen hyvin arvioitavissa. Jos näin ei olisi, ei omaisuuden palovakuuttaminenkaan olisi niin yleistä kuin se nyt on. Riskin kvantifiointi voi kuitenkin olla myös monimutkaista ja vaikeaakin etenkin yrityksen operatiiviseen toimintaan liittyvien riskien osalta: esimerkiksi tietojärjestelmän konfigurointivirheeseen tai asiakaslaskutuksen sisältämän tiedon oikeellisuuden vaarantumiseen liittyvän riskin kvantifiointi edellyttää perinteisiä vahinkoriskejä huomattavasti syvällisempää riskiarviointia ja usein myös monimutkaisempia kvantifioimismenetelmiä. Ne asettavat merkittäviä vaatimuksia myös koko riskienhallintaprosessille. Vaikeammin kvantifioitavissa olevat riskit edellyttävät yleensä myös monipuolisempia riskinhallintakeinoja kuin ’vain’ riskin vakuuttamista.

Tämän tutkielman aihevalinta perustuu edellä mainittujen lähtökohtien lisäksi tekijän omakohtaisiin havaintoihin riskienhallintaprosessin vaiheiden ymmärtämisen tärkeydestä sekä riskien kvantifioimisen haasteista erityisesti yrityksen operatiivisten riskien osalta. Aihevalinnan taustana ovat myös suomalaista finanssitoimialaa[2] koskevat vaatimukset operatiivisten riskien hallinnasta ja organisaation vakavaraisuudesta. Nämä vaatimukset on dokumentoitu Finanssivalvonnan asettamiin standardeihin, jotka määrittelevät varsin kattavasti Finanssivalvonnan valvomille organisaatioille, mitä niiden tulee tehdä. Se, miten vaatimukset toteutetaan, jää pääosin valvottavan organisaation päätettäväksi.

[2] Tässä tarkoitettuja Finanssialan toimijoita ovat Rahoitustarkastuksesta annetun lain (587/2003) 5 §:n tarkoittamat valvottavat, joihin kuuluu mm. luottolaitoksia, sijoituspalveluyrityksiä ja rahastoyhtiöitä.

Basel II:n[3] periaatteisiin perustuvien Finanssivalvonnan standardien noudattaminen edellyttää, että riskienhallintaa toteutetaan prosessina ja että operatiiviset riskit kyetään kvantifioimaan. Finanssivalvonnan standardi 4.1 'Sisäisen valvonta' asettaa vaatimukset kaikkien standardia koskevien organisaatioiden riskienhallinnalle:

> *"Riskienhallinnan on katettava kaikki olennaiset valvottavan liiketoimintaan liittyvät riskit: niin sisäiset kuin ulkoiset, niin mitattavissa olevat kuin ne, joita ei voi mitata, niin valvottavan omassa vaikutusvallassa olevat kuin ne, joihin valvottava ei voi itse suoraan vaikuttaa vaan joilta se voi vain suojautua. Valvottavan on määriteltävä mitattavissa oleville riskeille mittaamistavat, ja kehitettävä ei-mitattavissa olevien riskien hallintaan tarkoituksenmukaiset arviointimenetelmät."*

Perusteita näiden sitovien vaatimusten asettamiselle on vaikeaa kyseenalaistaa. Ne ovat luonteeltaan niin yleispäteviä, että niitä olisi hyvä soveltaa muuallakin kuin vain finanssitoimialalla: jokaisen yritystoimintaa harjoittavan organisaation tulisi toisaalta tunnistaa operatiiviseen toimintaansa liittyvät riskit ja niiden taloudellinen arvo sekä toisaalta varautua niihin toimintansa jatkuvuuden varmistamiseksi.

Operatiivinen riski voidaan määritellä sisältämään tappionvaaran lisäksi myös hyötymismahdollisuuden. Tässä tutkielmassa operatiivisen riskin määritelmä perustuu kuitenkin nimenomaan tappionvaaraan. Tämä Basel-komitean työhön perustuva määritelmä on valittu siksi, että se keskittyy operatiivisen riskin syihin ja niiden mittaamiseen.[4] Myös Finanssivalvonnan standardin 4.4b 'Operatiivisten riskien hallinta' sisältämä määritelmä operatiiviselle riskille vain tappionvaarana on oleellinen lähtökohta tutkielman ra-

---

[3] Baselin pankkivalvontakomitea (Basel Committee on Banking Supervision) on vuonna 1974 perustettu monikansallinen komitea, jonka tarkoituksena on valmistella yhteisesti sitovia säännöksiä pankkisektorille. Komitea kokoontuu yleensä Basel-kaupungissa. Komitean vuosia kestäneeseen työhön perustuvat pankkien vakavaraisuuslaskentaan liittyvät EU:n direktiivit astuivat voimaan kesäkuussa 2006 ja kansallisesti niihin perustuvat vaatimukset tulivat voimaan Suomessa vuoden 2007 alussa. Niiden keskeisenä tavoitteena on kannustaa pankkeja ja rahoituslaitoksia kehittämään riskienhallintajärjestelmiään.

[4] Basel Committee on Banking Supervision 2001, s. 2.

jausten kannalta. Operatiivisessa riskeissä toteutuu negatiivisia vaikutuksia harvemmin riskin positiivinen puoli (ns. ”upside” eli hyöty tai voiton mahdollisuus, kuten esim. FERMA:n riskin määritelmässä[5]). Toisaalta voiton mahdollisuutta arvioidessa korostuu pääoman tuottoasteen arviointi investoinnissa (ROI) eikä sitä ole tämän tutkielman laajuudessa mahdollisuutta käsitellä tarkemmin. Siksi tutkielmalle valittu operatiivisen riskien määritelmä perustuu vain tappionvaaraan. Huolimatta tästä rajauksesta tutkielman sisältö on pääosin hyödynnettävissä myös riskiin liittyvien hyötyjen kvantifioinnissa – periaatteet ja menetelmät ovat käytännössä samoja. Tarkastelun keskipisteenä eivät olekaan operatiivisen riskin vaikutukset vaan niiden arviointitavat.

Finanssitoimialan kansallinen ja kansainvälinenkin merkitys on johtanut siihen, että sille on asetettu säädösperustainen velvollisuus toteuttaa riskienhallintaa minimissään standardien edellyttämällä tasolla. Finanssivalvonnan standardien laajempi hyödyntäminen ja soveltaminen myös muilla toimialoilla, niiden erityispiirteet huomioiden, olisi monelta osin perusteltua.

Luvun alussa mainittujen sanontojen lisäksi myös suomalainen kansanperinne on vahvistanut operatiivisiin riskeihin varautumisen ja niiden hallinnan tarpeen, joskin hieman pessimistisemmästä näkökulmasta: ”*Ei vahinko huutele tullessansa*” ja tämän lisäksi vielä ”*Ei vahinko yksinään tule*”. Kansanperinteemme korostaa toisaalta myös varovaisuutta riskin toteutumisen välttämiseksi: *”Parempi virsta väärää kuin vaaksa vaaraa”* ja *”Parempi viikko vuntierata kuin päivä turhaa työtä”*. Vaikka pessimististä *”tämäkin vielä”* -asennoitumista on inhimillisistä syistä johtuen myös liike-elämän riskienhallinnassa, pyrkii tämä tutkielma lähestymään riskejä ja riskienhallintaa hyötymisen ja vaikutusmahdollisuuksien näkökulmasta. Se on toisaalta myös välttämätöntä: aiheena olevaa riskien kvantifiointia tehdään riskienhallintaprosessissa eli ennen riskien toteutumista. Mikäli ennakoitu tai ennakoima-

[5] FERMA 2003, 3.

ton riski on jo toteutunut – kävellään jo vaaran päällä – siirrytään vahinkojen kvantifiointiin.

2 TUTKIELMAN VIITEKEHYS JA TUTKIMUSMENETELMÄ

2.1 Viitekehys ja rajaukset

Riskienhallinnan teoreettinen kenttä on hyvin laaja ja siihen voidaan liittää huomattava määrä eri tieteenalojen teoreettisia kokonaisuuksia. Esimerkiksi kansantaloustieteen, johtamisen, rahoituksen ja laskentatoimen tieteenalat sisältävät riskienhallinnan teorioita ja määritelmiä. Tutkielman viitekehyksenä toimivat ne operatiivisten riskien hallintaan liittyvät käsitteet, jotka on tarkemmin määritelty luvussa 2.2. Keskeisimmät käsitteet ovat kokonaisvaltainen riskienhallinta, riskienhallintaprosessi ja sen osana sitä riskien arviointi sisältäen riskien kvantifioinnin sekä operatiivinen riski. Näistä elementeistä muodostuu tutkielman viitekehys.

Keskeisimmät rajaukset tutkielmalle muodostuvat erityisesti sen viitekehyksenä olevien käsitteiden tarkoista määrittelyistä. Vaikka riskienhallinnan klassinen terminologia onkin pysynyt varsin samansisältöisenä vuosikymmenien ajan[6], on riskienhallintaa käsittelevässä nykykirjallisuudessa useita toisistaan osittain ja merkittävästikin poikkeavia määritelmiä riskienhallinnan käsitteille. Lisäksi eri viranomaiset, riskienhallinnan asiantuntijaorganisaatiot, riskienhallintaan erikoistuneet järjestöt sekä luonnollisesti myös riskienhallintaa toteuttavat organisaatiot ovat laatineet omia määritelmiään riskienhallinnan käsitteille.

Kulloinkin vallitsevista trendeistä riskienhallinnan käsitteiden uusille määritelmille saa hyvän kuvan riskienhallinnan yleisissä keskustelufoorumeissa[7]. Raflaavimmat trendit vaikuttavat varsin paljon ainakin trendejä seuraaviin riskienhallintayhteisöihin. Yleensä trendit näkyvät myös riskienhallintapalve-

---

[6] Mm. Kuusela & Ollikainen 2005, s. 155.

[7] Erimerkiksi vuosittaiset RIMS-seminaarit Yhdysvalloissa (ks. tarkemmin www.rims.org) tai FERMA:n järjestämät seminaarit Euroopassa (www.ferma.eu).

luita ja -konsultointia tarjoavien tahojen toiminnassa. Näin ollen riskienhallintaan liittyvässä tieteellisessä kirjoittamisessa tulee kiinnittää erityistä huomiota käsitteiden määrittelyyn ja sitä kautta tutkimuskohteen rajauksiin. Luvussa 2.2 esitetään tässä tutkielmassa käytettyjen keskeisimpien käsitteiden määritelmät ja niiden rajaukset sekä tarvittaessa myös perusteluja sille, miksi kyseinen määritelmä on valittu. Määritelmät on valittu niiden lähteen, vakiintuneisuuden sekä viime kädessä myös niiden käytettävyyden perusteella tutkielman tekijän tulkintojen mukaisesti.

Vaikka tämän tutkielman viitekehykseksi onkin valittu finanssitoimialan vahvasti leimaamat riskienhallinnan käsitteet, on tarkoituksena käsitellä operatiivisten riskien kvantifioimista ja riskienhallintaprosessia yleisesti rajaamatta tarkastelua mihinkään toimialaan, organisaatiomalliin tai -tyyppiin.

2.2 Tutkielman keskeisimpien käsitteiden määrittely

Kokonaisvaltainen riskienhallinta eli Enterprise Risk Management (ERM) on prosessi, johon vaikuttavat organisaation ylin johto, toimiva johto sekä työntekijät. Sitä toteutetaan strategia- ja suunnitteluprosesseissa koko organisaation toimesta. Se on kehitetty tunnistamaan seikkoja, jotka voivat vaikuttaa organisaatioon sekä hallitsemaan riskejä määritellyn riskinottohalun piirissä, jotta organisaation tavoitteiden saavuttaminen olisi riittävän luotettavalla pohjalla. Se perustuu siihen, että organisaation tarkoituksena on tuottaa arvoa sen omistajille (tai muille sidosryhmille). Kokonaisvaltaisen riskienhallinnan avulla organisaation johto voi tehokkaasti hallita toimintaansa liittyvää epävarmuutta ja riskejä ja tätä kautta lisätä kykyään arvon kasvattamiseen.[8]

[8] COSO ERM 2004, 2.

Organisaatio on dynaaminen kokonaisuus, jossa organisaation resurssit (ihmiset, tekniikka, tieto, kumppanit, taloudelliset resurssit) tavoittelevat organisaatiolle asetettuja tavoitteita.[9]

Organisaation riskienhallinta on sen johdon ja muun henkilökunnan toteuttama prosessi, jota sovelletaan strategian laadinnassa ja koko organisaatiossa, ja jonka tarkoituksena on tunnistaa organisaatioon vaikuttavia potentiaalisia tapahtumia ja pitää riskit riskinottohalukkuuden rajoissa, jotta voidaan olla kohtuullisen varmoja organisaation tavoitteiden toteutumisesta.[10] COSO ERM:n alkuperäinen määritelmä organisaation riskienhallinnasta sisältää johdon ja muun henkilökunnan lisäksi hallituksen, koska määritelmä on ensisijaisesti laadittu yritysmaailman näkökulmasta[11]. Se ei sellaisenaan tue tässä tutkielmassa käytettävää organisaation käsitettä (mikäli organisaatiolla ei ole esim. hallitusta), joten määritelmää on muutettu vastaavasti. Määritelmien 'kokonaisvaltainen riskienhallinta' ja 'organisaation riskienhallinta' välinen ero on periaatteessa pieni, mutta organisaation riskienhallinta voi olla kokonaisvaltaista tai ei. Lisäksi kokonaisvaltainen riskienhallinta on käsitteenä huomattavan paljon vakiintuneempi johtuen siihen liittyvästä laajasta kirjallisuudesta.

Operatiivinen riski tarkoittaa tappionvaaraa, joka aiheutuu riittämättömistä tai epäonnistuneista sisäisistä prosesseista, henkilöstöstä, järjestelmistä, ulkoisista tekijöistä.[12] Tappiot voivat aiheutua välittömästi tai välillisesti.

---

[9] Condamin, Louisot, Naïm 2006, s. 3.

[10] COSO ERM 2004a, 3. Tätä COSO ERM:n määritelmää voidaan pitää poikkeuksellisen onnistuneena määritelmänä: "kohtuullinen varmuus" on tavoitetilana sellainen, johon jokaisen organisaation johdon pitäisi pystyä sitoutumaan ja joka toisaalta tuo esille riskienhallinnan perimmäisen ajatuksen: riskienhallinta on ennustamista ja epävarmojen asioiden käsittelyä.

[11] Vuonna 1985 COSO kuitenkin perustettiin erityisesti yksityisellä sektorilla toimineen National Commission of Fraudulent Financial Reporting -yhteisön toiminnan tukemiseksi. Rahoittajana olleet järjestöt, kuten Financial Executives International, toimivat myös pääosin yksityissektorilla.

[12] Finanssivalvonnan standardi 4.4b Operatiivisten riskien hallinta 2007, s. 12.

Riskien analysointi (risk analysis) tai ***riskianalyysi*** on osa riskienhallintaprosessia. Riskien analysointi on systemaattista tietojen käyttämistä riskien tunnistamiseksi ja niiden vaikutusten arvioimiseksi. Riskienhallintaprosessin yksi kokonaisuus on riskien arviointi (risk assessment), joka koostuu vaiheista *riskien analysointi* sekä sen perusteella laadittujen *riskiarvioiden evaluoinnista* (risk evaluation) etukäteen asetettuja kriteereitä vasten. Riskien analysointivaihe taas koostuu *riskien tunnistamisesta* (risk identification) sekä *riskihavaintojen arvioinnista* (risk estimation). Riskin kvantifiointi tehdään käytännössä riskihavaintojen arvioinnin yhteydessä, mutta sitä voidaan tehdä riskienhallintaprosessin soveltamistavoista riippuen myös erityisesti riskiarvioiden evaluointivaiheessa sekä riskin toteutustoimenpiteiden seuranta- ja arviointivaiheissa.[13]

Riskienhallintakonseptit ovat yleispäteviä riskienhallinnan viitekehyksiä tai standardeja, joiden tarkoitus on tukea organisaatioita riskienhallinnan kehittämisessä sekä riskeihin liittyvissä päätöksissä. Ne ovat yleensä riskienhallinnan asiantuntijoiden, organisaatioita valvovien ja ohjaavien elinten tai erilaisten yhdistysten ja komiteoiden laatimia. Tunnetuimpia riskienhallintakonsepteja ovat esimerkiksi COSO ERM[14], FERMA[15] (Risk Management Standard), AS/NZS 4360:2004[16], DeLoach EWRM[17] sekä ISO/IEC-standardit[18].

---

[13] IEC/ISO 27005:2008, s. 14 ja ISO 31000:2009, s. 5.

[14] Konseptin laatija COSO käynnisti PriceWaterhouseCoopersin kanssa vuonna 2001 projektin luodakseen mallin, jolla organisaation johto voi arvioida ja kehittää organisaationsa riskienhallintaa. Projektin tulos COSO ERM, kokonaisvaltainen ajatusmalli organisaation riskienhallintaan, julkaistiin vuonna 2004.

[15] FERMA on tällä hetkellä 18 maan kansallisen riskienhallintayhdistyksen yhdessä muodostama eurooppalainen riskienhallintajärjestö, joka perustettiin vuonna 1974. Siihen on liittynyt myös Suomen Riskienhallintayhdistys ry (FinnRiMa). FERMA:n 2002 ensimmäistä kertaa julkaisema A Risk Management Standard on kokonaisvaltainen kuvaus riskienhallinnan roolista organisaatiossa sekä itse riskienhallintaprosessista.

[16] Australia (AS) ja Uusi-Seelanti (NZS) ovat aktiivisia riskienhallinnan kehittäjämaita, jotka ovat yhdessä julkaisseet lukuisia standardeja ja ohjeita riskienhallintaan liittyen. AS/NZS 4360:2004 on Joint Standards Australia/ Standards New Zealand Committeen laatima kokonaisvaltaisen riskienhallinnan standardi, josta on johdettu myös tuorein AS/NZS-riskienhallintastandardi AS/NZS ISO 31000:2009.

[17] Deloachin EWRM (Enterprise-Wide Risk Management) on riskienhallinnan yleisteos, jonka laatija riskienhallintakonsultti James W. Deloach esittelee teoksessaan nk. Business Risk Model -mallin, jonka Deloach kehitti Arthur Andersen -yhteisölle. Nimensä mukaisesti se ja koko teos käsittelee erityisesti liiketoimintariskien hallintaa ja painottaa mahdollisuuksien (riskiin liittyvien hyötyjen) hallintaa osana yrityksen riskienhallintastrategiaa.

Riskienhallintaprosessi tarkoittaa riskienhallinnan käytännön systemaattista toteuttamista. Koska toisaalta 'kokonaisvaltainen riskienhallinta' on määritelmänsä mukaisesti prosessi, ovat määritelmät 'riskienhallinta' ja 'riskienhallintaprosessi' yleisesti hyvin lähellä toisiaan. Toisaalta käsitteellä 'riskienhallinta' tarkoitetaan useissa yhteyksissä 'riskien hallintaa' eli käytännössä niitä toimenpiteitä, joilla riskejä hallitaan.[19] Tämä puoltaa osaltaan käsitteen 'riskienhallintaprosessi' tarkempaa määrittelemistä.

Yksinkertaisimmillaan riskienhallintaprosessi koostuu neljästä vaiheesta: 1) riskien tunnistaminen, 2) riskien arviointi, 3) riskienhallintatoimenpiteiden suunnittelu ja toteutus sekä 4) riskienhallinnan (toteutettujen riskienhallintatoimenpiteiden) arviointi.[20] Se voidaan nähdä jopa vielä pelkistetymmin, kolmivaiheisena prosessina: 1) diagnosis of exposures 2) treatment of risk 3) audit of the risk management programmes.[21] Tämän tutkielman tavoitteiden kannalta on kuitenkin oleellista, että riskienhallintaprosessin määritelmä sisältää riskienhallintaprosessin yksityiskohtaisemman vaiheistuksen siten, että riskien arviointi ja sen osana riskien kvantifiointi ovat selkeästi oma kokonaisuutensa.

Yhtenä kehittyneimmistä riskienhallintaprosessien kuvauksista ovat ISO/IEC-standardien sisältämät riskienhallintaprosessin määritelmät. Standardi ISO 31000:2009 (Risk Management: Principles and guidelines) ja sitä tukeva standardi IEC/ISO 31010:2009 määrittelevät riskienhallintaprosessin seuraavasti:

---

[18] Erityisesti IEC/ISO 27005 (tietoturvariskien hallinta), ISO 31000 ja IEC/ISO 31010:2009 (riskienhallinnan yleisstandardi) sekä IEC/ISO 27001 (tietoturvallisuuden hallintajärjestelmä). Myös mm. standardi BS 25999 (jatkuvuuden hallinta) sisältää riskienhallinnan elementtejä.

[19] Sitra 2002, s. 11.

[20] Pöyry, 2008 s. 13.

[21] Condamin, Louisot, Naïm, 2006 s. 7.

> *”Risk management process is a systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.”*

Tässä tutkielmassa käytettävä riskienhallintaprosessin määritelmä perustuu ISO 31000:2009 - ja ISO/IEC 27005:2008 -standardeihin. Niiden mukaisesti riskienhallintaprosessi sisältää *riskin analysoinnin*, jonka määritelmä on kuvattu tässä luvussa erikseen. Standardien ISO 31000:2009, IEC/ISO 31010:2009 sekä ISO/IEC 27005:2008:n määritelmät ovat muutoinkin keskeisiä tämän tutkielman kannalta. Perusteluna sille ovat kyseisten standardien laaja-alainen soveltamismahdollisuus, laaja valmisteluun osallistunut taustayhteisö sekä niiden tuoreet julkaisuajankohdat. Riskienhallintaprosessia käsitellään vielä tarkemmin luvussa 4 tämän *riskienhallintaprosessi*-määrittelyn täydentämiseksi.

Riskien tunnistaminen (risk identification) on osa *riskien analysointivaihetta* ja siinä riskejä kartoitetaan, tunnistetaan ja kuvataan. Riskien tunnistamiseen sisältyvät riskeihin vaikuttavien tekijöiden (risk source), tapahtumien (event), niihin liittyvien syiden (cause) ja vaikutusten tai seurausten (consequence) kartoittaminen, tunnistaminen ja kuvaaminen.[22] Lisäksi riskien tunnistamisvaiheessa kartoitetaan ja kuvataan olemassa olevat riskiin liittyvät kontrollit eli riskiä pienentävät hallintatoimenpiteet. Riskin tunnistamisvaiheen tuloksena muodostuu tunnistettu riski eli riskihavainto.

Riskihavaintojen arviointi (risk estimation) on toinen osa riskien analyysivaihetta ja tarkoittaa arvojen määrittämistä riskihavaintojen vaikutuksille ja todennäköisyydelle. Riskihavaintojen arviointi on keskeinen osa riskien kvantifioimista.[23]

---

[22] ISO 31000:2009, s.4.

[23] IEC/ISO 27005:2008, s. 2 ja 14. Käsitettä *risk estimation* on kuvattu hieman eri tavoin eri standardeissa (mm. ISO 31000:2009 kuvaa sen olevan vain osa riskianalysointia ja ISO 27001:2006 ei määrittele sitä lainkaan). *Risk estimation* -käsitteen suomenkielinen käännös *riskihavaintojen arviointi* on tutkielman laatijan oma ja perustuu

Riskinottohalukkuus (risk appetite) on se riskin taso, jonka organisaatio on valmis ottamaan pyrkiessään tavoitteisiinsa. Riskinottohalukkuus heijastelee organisaation riskienhallintastrategiaa ja vaikuttaa tällä tavoin laajasti organisaation toimintatapaan. Riskinottohalukkuus määritellään organisaation strategian määrittelyn yhteydessä, jolloin strategiasta johdetun toivotun lopputuloksen tulee olla yhdensuuntainen organisaation riskinottohalukkuuden kanssa.[24] Finanssivalvonnan standardi 4.2 Valvottavan vakavaraisuuden hallinta velvoittaa valvottavien organisaatioiden ylimmän johdon riskinottohalukkuuden vahvistamisesta:

> *”Ylin johto vahvistaa strategian ja liiketoimintasuunnitelmien perusteella valvottavan riskinottotason ja riskinottohalukkuuden sekä hyväksyy suunnitelman riskinottotasoon suhteutetun vakavaraisuuden ylläpitämisestä.”*[25]

Riskinottohalukkuuden vahva linkitys organisaation vakavaraisuuden hallintaan on seurausta erityisesti finanssialalle tyypillisistä markkina- ja luottoriskeistä. Riippumatta operatiivisen riskin vähimmäisvakavaraisuuden laskennassa sovellettavasta laskentavaihtoehdosta valvottavilla tulee olla käytössään tarkoituksenmukaiset toimintapolitiikat ja -tavat operatiivisen riskin arvioimiseksi ja hallitsemiseksi.

2.3 Tutkimusmenetelmä

Tutkielma on luonteeltaan menetelmäselvitys riskienhallintajohtamista varten ja se tehdään TKK Dipolin Turvallisuusjohdon Koulutusohjelmassa annetun ohjeistuksen mukaisesti.

---

hyvien suomenkielisten vastineiden puuttumiseen termeille *estimation, evaluation* ja *assessment* sekä tautologian välttämiseen riskienhallintaprosessin vaiheiden nimeämisessä. Riskienhallintakonsepteissa ei ole vakiintunutta suomenkielistä termistöä näille määritelmille.

[24] COSO ERM 2004, s. 124.

[25] FIVA 4.2 2007, s. 19.

Tutkielmassa havainnollistetaan riskien kvantifioimista osana riskienhallinta-prosessia sekä esitetään erilaisia kvantifioimismenetelmiä operatiivisille riskeille. Tutkielmassa tarkastellaan kvantifioimista kiinteänä osana yrityksen riskienhallintaprosessia. Tämän takia tutkielmassa tarkastellaan ja esitetään myös riskienhallintaprosessin periaatteita ja toteutustapoja.

Tutkimusmenetelmä on tutkimuskohteiden (valittu kirjallisuus ja riskienhallintakonseptit, kuten COSO ERM, FERMA ja riskienhallinnan ISO/IEC-standardit) eksplisiittisen ja implisiittisen riskienhallintainformaation tarkastelu, joka on tyypillinen kvalitatiivisen tutkimustavan menetelmä.

3 TUTKIELMAN TAVOITTEET

Riskienhallinnan kirjallisuudessa ja riskienhallintakonsepteissa on useita toisistaan poikkeavia määritelmiä riskienhallinnan tavoitteille. Näin ollen seuraavassa hieman tarkemmin riskienhallinnan yleisistä tavoitteista, joista tämän tutkielman tavoitteet on johdettu.

3.1 Riskienhallinnan tavoitteista

Riskienhallinnan tavoitteet määritellään jollekin tietylle kohteelle. Vaikka riskienhallintaa voidaankin toteuttaa mille kohteelle tahansa sukupolvesta yksityishenkilöön, rajataan tässä tutkielmassa kohteeksi organisaatio. Organisaatio on määritelmänsä mukaisesti organisoitu toimimaan yhteisten tavoitteiden saavuttamiseksi.[26] Organisaation yhteisten tavoitteiden määrittely onkin keskeisessä asemassa kaikille niistä johdettaville tavoitteille, mukaan lukien riskienhallinnan tavoitteet. Tässä tutkielmassa käytetään oletuksena sitä, että organisaatiolla on nykyaikaisen liberaalin talousjärjestelmän mukaisesti aina tavoitteena toimintansa taloudellinen tehokkuus eli organisaation tavoitteiden saavuttaminen mahdollisimman pienellä määrällä resursseja.

Edellä mainitun toiminnan tehokkuusvaatimuksen seurauksena on selvää, että organisaation toimintaan liittyy aina riski tietylle toiminnan osalle kohdistettujen resurssien riittävyydestä tai saatavuudesta. Ehkä tämä riski voidaan nähdä organisaatiolle jopa sen toiminnan lähtökohtana – organisaation tavoitteethan saavutetaan täysin vain, jos ne saavutetaan minimiresurssein. Muutoin toteutuu riski tehokkuusvaatimuksen epäonnistumisesta. Edelleen tämä riski resurssien riittävyydestä tai saatavuudesta sisältää mahdollisuuden odottamattomista tapahtumista, kuten resursointia kohtaavista vahin-

[26] Condamin, Louisot, Naïm 2006, s. 8. Organisaation resurssien määritelmä: ks. luku 2.2.

goista. Tämä vaikuttaa suoraan riskienhallinnan tavoitteiden asettamiseen: senkin tulee täyttää tehokkuusvaatimus.

Riskienhallinnan tehokkuusvaatimus on sisällytetty myös Finanssivalvonnan riskienhallintaa koskevaan standardiin 4.2 Valvottavan vakavaraisuuden hallinta:

”Finanssivalvonta edellyttää, että valvottava suhteuttaa riskien mittaamiseen ja arviointiin käyttämänsä menetelmät oman toimintansa vaativuuden ja erityispiirteiden mukaisesti.”[27]

Vaikka kyseinen riskiperustaisen pääomatarpeen arviointiin liittyvä vaatimus on ensisijaisesti tarkoitettu varmistamaan nimenomaan vaatimuksen vähimmäistaso, sisältää se myös vaatimuksen riskiperustaisen pääomatarpeen arvioinnin tehokkuudesta. Valvottavan tulee siis suhteuttaa myös operatiivisen riskin kvantifiointimenetelmänsä toimintansa vaativuuden ja erityispiirteiden mukaisesti. Liian järeitäkään menetelmiä ei tule käyttää.

Organisaation riskienhallinnan tavoitteet ovat viimeisen muutaman vuosikymmenen aikana olleet jatkuvana tarkastelun kohteena, kun riskienhallinnan teorioita ja käytäntöjä on aktiivisesti kehitetty etenkin riskienhallinnan kokonaisvaltaisuuteen perustuvan ERM-lähestymistavan[28] yleistyttyä. Organisaatioiden riskienhallintaan on muutoinkin kohdistettu aiempaa merkittävästi enemmän resursseja joko pakollisten riskienhallintavaatimusten, kuten SOX[29]-, Basel- tai Solvency-vaatimusten tai organisaatioiden omien valintojen, kuten riskienhallinnan ISO-standardien noudattamisen kautta. Tämä on

---

[27] FIVA 4.2 2007, s. 37.

[28] Kokonaisvaltaisesta riskienhallinnasta tarkemmin luvussa 1.2.

[29] Yhdysvalloissa presidentti George W. Bushin hallinnon laatima Sarbanes-Oxley Act. Se perustuu etenkin viime vuosituhannen vaihteessa tapahtuneeseen ja aikanaan Yhdysvaltain taloushistorian suurimpaan konkurssiin, kun energiayhtiö Enronin johto paranteli yhtiön tunnuslukuja ja johti sijoittajia harhaan aiheuttaen lopulta yrityksen konkurssin.

ollut ainakin osittain syynä riskienhallinnan tavoitteiden määrittelyn yleistymiselle ja määrittelyjen moninaisuudelle.

Organisaation riskienhallinnan tavoitteita ja tarkoitusta on määritelty muun muassa riskienhallintakonsepteissa, joita käsitellään osittain luvussa 2.2. Organisaation riskienhallinnan tavoitteiksi on esitetty myös seuraavia:

> *- ”Riskienhallinnan ensisijainen tavoite on katastrofien välttäminen ja siten liiketoiminnan jatkuvuuden varmistaminen kaikissa olosuhteissa. Toinen tavoite on riskikustannusten optimointi ja liiketoimintamahdollisuuksien hyödyntäminen.”*[30]
>
> *- ”Riskienhallinnan tavoitteeksi voidaan määritellä resurssien saatavuus kaikissa olosuhteissa sillä tasolla, mikä on organisaation perimmäisten tavoitteiden suhteen yhteensopiva.”*[31]
>
> *- ”Risk management is a process with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.”*[32]

Organisaation riskienhallinnan tavoitteena voi olla myös yksinkertaisesti lisäarvon tuottaminen organisaatiolle tai sen organisaation tavoitteiden saavuttamisen varmistaminen. Riskienhallinnan voidaan määritellä olevan myös hyvien päätösten tekemistä: siten, että päätökseen mahdollisesti liittyvät riskitkin hyväksytään tietoisesti. Sitä kautta organisaation riskienhallinnan tavoitteena voi olla yksinkertaisesti ’oikeiden päätösten tekeminen’.

3.2 Tutkielman tavoitteet

Edellä kuvatut riskienhallinnan yleiset tavoitteet huomioiden tämän tutkielman tavoiteasetanta perustuu oletukseen siitä, että organisaation riskienhallinnan tulee tuottaa suurin mahdollinen arvo pienimmin mahdollisin resurs-

---

[30] Juvonen – Korhonen – Ojala – Salonen – Vuori 2005, s. 20.

[31] Condamin, Louisot, Naïm 2006, s. 8. Tämä määritelmä on johdettu siitä olettamasta, että organisaation tulee saavuttaa sille asetetut yleiset tavoitteet mahdollisimman pienillä resursseilla.

[32] FERMA 2003, s. 3.

sein. Näin ollen operatiivisten riskien kvantifiointikin tulee toteuttaa vastaavalla tavalla. Koska riskienhallinnan tehokkuusvaatimus ohjaa organisaatiota käyttämään ’vain’ riittäviä menetelmiä ja resursseja operatiivisten riskien kvantifioimisessa, tavoittelee tämä tutkielma kyseisen lähtökohdan – joka on samalla tutkielman tutkimusongelma – asettamiin haasteisiin vastaamista.

Tämän tutkielman ensisijaisena tavoitteena on esitellä riskienhallintaprosessia sekä yleisesti käytössä olevia ja tehokkaan riskienhallinnan käyttöön soveltuvia operatiivisten riskien kvantifioimismenetelmiä. Menetelmät voivat olla olemassa olevia malleja, niiden yhdistelmiä tai niistä laadittuja soveltamistapoja.

Tutkielman tavoitteena on myös kuvata riskien kvantifioimista osana organisaation riskienhallintaprosessia. Tällä pyritään vastaamaan kysymykseen ”milloin riskin arvo määritellään”. Tämän myötä tutkielmassa painottuu riskienhallintaprosessin kuvaaminen ja siihen liittyvien käsitteiden määrittely. Vaikka riskien kvantifioinnin osuus kohdistuu erityisesti operatiivisiin riskeihin, on tutkimuksen tavoitteena esitellä kvantifioimismenetelmiä siten, että niitä voidaan soveltaa myös muihin riskilajeihin.

Olemassa olevista riskien kvantifiointimenetelmistä jätetään tarkastelun ulkopuolelle tai vain maininnan asteelle erityisesti vakuutusyhtiöiden soveltamat laajaan tilastolliseen aineistoon ja analyysiin perustuvat riskien kvantifiointimallit. Niiden menestyksellinen hyödyntäminen on luonnollisesti oleellinen osa vakuutusyhtiön liiketoimintaa. Vastaavanlaisten menetelmien soveltaminen organisaation omien operatiivisten riskien *tehokkaassa* hallinnassa ei kuitenkaan ole tarkoituksenmukaista.

4 RISKIENHALLINTAPROSESSI

Tämän tutkielman keskeisenä viitekehyksenä oleva riskienhallintaprosessin määritelmä toimii myös operatiivisten riskien kvantifioinnin teoriataustana. Prosessin kuvaus osoittaa myös riskien kvantifioinnin osana prosessia. Vaiheittainen toteutustapa on edellytys riskienhallintaprosessin tehokkaalle toiminnalle ja sille, että riski voidaan kvantifioida mahdollisimman oikein. Tästä johtuen riskienhallintaprosessin sisältöä avataan tässä luvussa tarkemmin. Riskienhallintaprosessin kuvaus perustuu riskienhallintakonsepteista erityisesti standardeihin ISO/IEC 27005:2008, FERMA: A Risk Management Standard 2003 ja IEC/ISO 31010:2009.

4.1 Riskienhallintaprosessin yleiskuvaus

Luvussa 2.2 olevan määritelmän mukaisesti riskienhallintaprosessi sisältää seuraavat vaiheet[33].

- Viitekehyksen / taustatietojen määrittäminen
- Riskien tunnistaminen
- Riskien analysointi
- Riskiarvioiden evaluointi

Riskien arviointivaihe

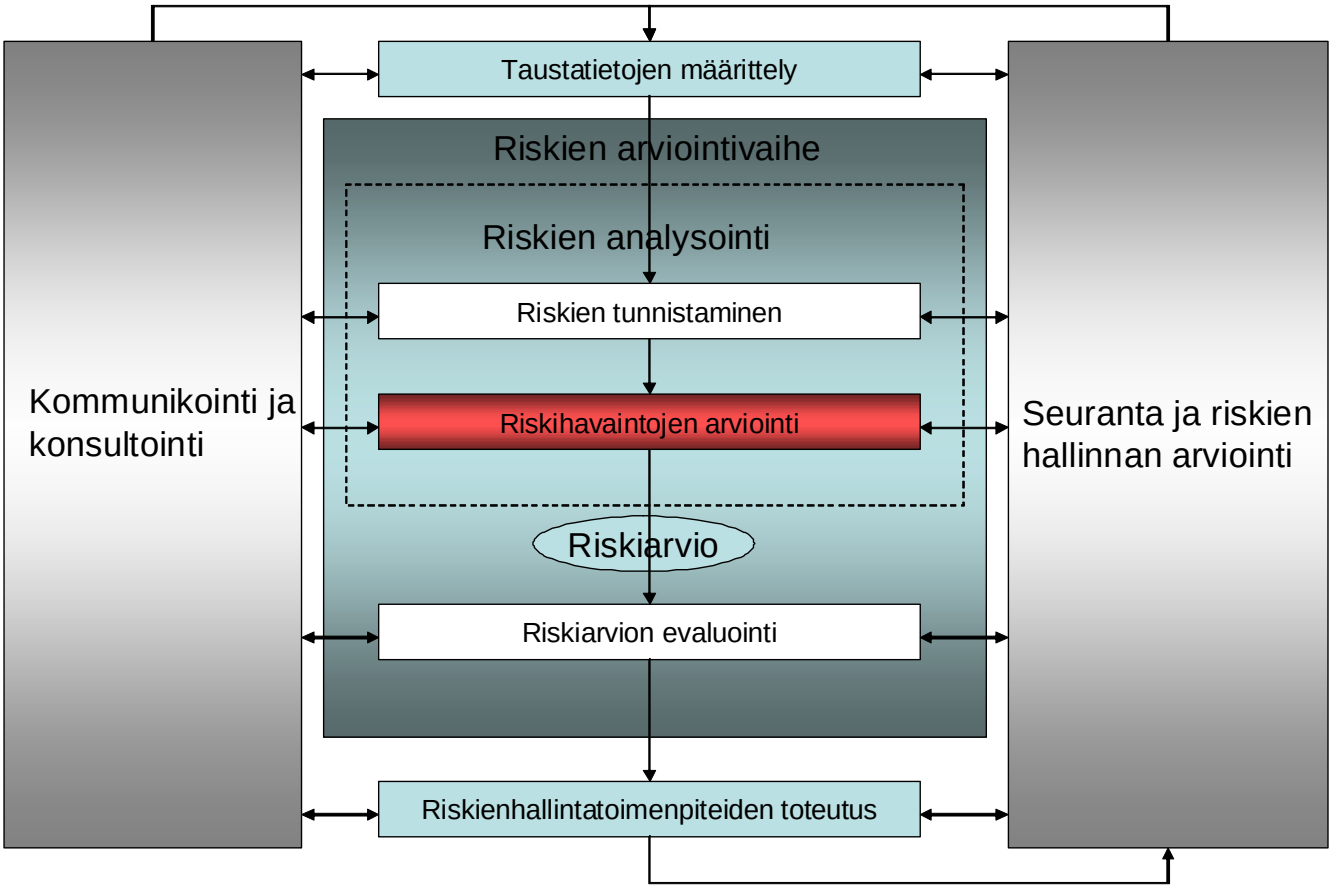
- Riskienhallintatoimenpiteiden toteuttaminen
- Seuranta
- Riskin hallinnan arviointi

Prosessin kaikkiin vaiheisiin sisältyy tarvittavien ulkoisten ja sisäisten sidosryhmien kommunikointi ja konsultointi.

Riskienhallintaprosessia noudatetaan kronologisessa järjestyksessä ja se aloitetaan uudelleen, mikäli johonkin vaiheeseen liittyvä informaatio muut-

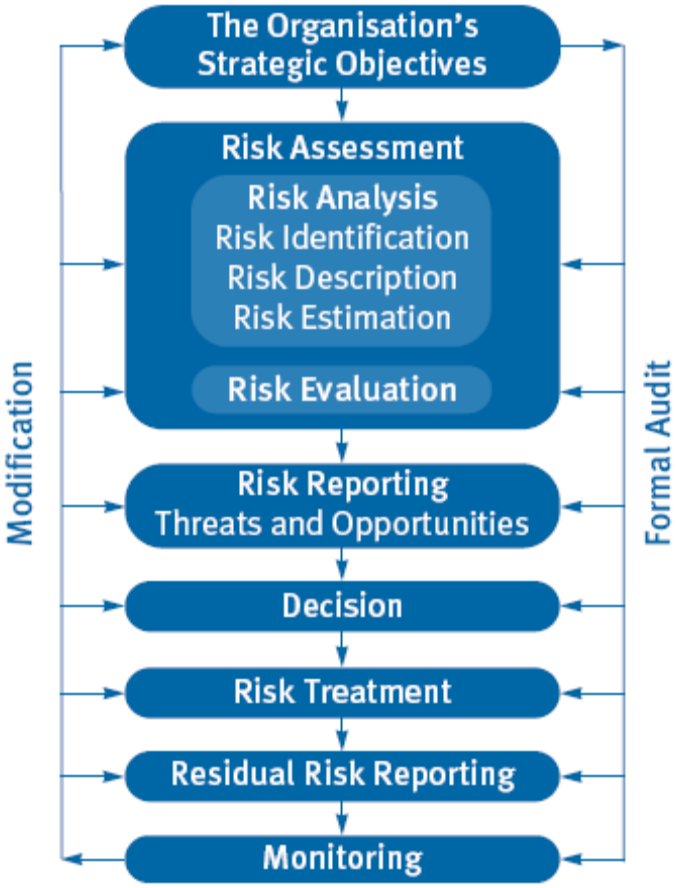
[33] IEC/ISO 31000:2009, s. 14.

tuu. Vaiheiden sisältöä on määritelty luvussa 2.2. Seuraavassa on kuvattu riskienhallintaprosessi kaaviona.



Kuva 1: Riskienhallintaprosessi (johdettu standardeista ISO/IEC 31000:2009 ja ISO/IEC 27005:2008)

Kuvassa olevan prosessin vaiheistus on kuvattu standardissa ISO/IEC 31000:2009 kattavasti ja siten, että prosessia voi soveltaa käytännössä minkä tahansa riskilajin osalta. Kyseisen standardin kuvaus on kuitenkin visuaalisesti vajavainen, koska siitä ei selvästi käy ilmi aiemmin mainittua organisaation riskienhallinnan ’yksinkertaisinta tavoitetta’ eli päätösten tekemistä. FERMA:n A Risk Management Standard sisältää tämän elementin, vaikka ei muutoin ole riskienhallintaprosessin kuvauksena aivan samaa tasoa tuoreemman standardin ISO/IEC 31000:2009:n kanssa:



Kuva 2: Riskienhallintaprosessi (FERMA 2003)

FERMA:n kuvaus riskienhallintaprosessista sisältää kohdan 'Riskienhallinta-päätös' (Decision). Kyseinen elementti ei toki kokonaan puutu em. ISO-standardien riskienhallintaprosessien määritelmistä, mutta sen merkitystä on syytä korostaa, kun riskienhallintaprosessin kulkua kuvataan. Toinen oleellinen ero FERMA:n riskienhallintaprosessin kuvauksessa on jäännösriskin raportointi (Residual Risk Reporting), joka tarkoittaa käytännössä samaa kuin kuvan 1 riskienhallintaprosessin "kommunikointi". Seuraavassa kuvataan tarkemmin riskienhallintaprosessin kulkua perustuen kuvaan 1 ja korostaen sitä, että ennen riskienhallintatoimenpiteiden toteuttamista tehdään päätös riskin hyväksymisestä.

4.2 Taustatietojen määrittely

Riskienhallintaprosessi alkaa siis taustatietojen määrittelyllä. Siinä määritellään organisaatiokohtaiset tiedot, jotka vaikuttavat riskienhallintaprosessin toteuttamiseen. Taustatietojen avulla pystytään määrittelemään organisaation tavoitetila valitulle kohteelle valitussa laajuudessa toteuttavalle riskienhallintaprosessille. Niiden avulla prosessi kyetään ylipäätänsä suorittamaan tehokkaasti ja oikein.

Operatiivisten riskien hallinnan osalta keskeisiä määriteltäviä taustatietoja ovat toteutettavan operatiivisen riskien hallinnan:

- tarkoitus (esimerkiksi organisaation tavoitteiden saavuttamisen varmistaminen, vaatimustenmukaisuus tai jatkuvuussuunnittelu)
- tarkastelun laajuus (kaikki organisaation operatiiviset riskit tai jonkin organisaatioyksikön riskit, kaikki riskiluokat vai vain rajattu joukko operatiivisen riskin riskiluokkia)
- kohteen lähtötiedot eli esimerkiksi suojattavien kohteiden, prosessien tai tietojärjestelmien kriittisyys, niihin liittyvät keskeiset vaatimukset, niiden arvo, tiedossa olevat keskeytyksestä aiheutuvat (esim. palvelutaso-) seuraukset sekä tietojen luokittelu niiden luottamuksellisuuden mukaisesti
- tarkasteltavaan kohteeseen liittyvät ulkoisen ja sisäisen ympäristön taustatiedot (esimerkiksi teknologia, kulttuuri, sidosryhmien odotukset, kohteiden keskinäiset riippuvuussuhteet, sisäiset periaatteet ja muut vaatimukset)
- riskiarvioiden laatimisen yleiset kriteerit (Miten riskin todennäköisyys määritellään? Mikä on arvioinneissa käytettävä aikajakso? Miten riskin arvo määritellään?)
- riskiarvioiden evaluointikriteerit (millainen riskiarvio on hyväksyttävissä)
- riskien hyväksymiskriteerit (mitkä riskit ovat ylipäätänsä hyväksyttäviä ja mikä on päätöksentekomekanismi eritasoisille riskeille)

Taustatietojen määrittely on siis samalla suunnitelma riskienhallintaprosessin toteuttamistavasta. Asettamalla selkeä toimintamalli, yhteiset arviointikriteerit ja lähtötiedot kaikille riskienhallintaprosessin osallistuville mahdollistetaan prosessin lopputuloksena syntyvien riskienhallintapäätösten ja -toimenpiteiden oikeellisuus, oikea-aikaisuus ja riittävyys.

4.3 Riskien arviointivaihe

Riskien arviointivaihe sisältää riskien analysoinnin ja riskiarvioiden evaluoinnin. Analysointi koostuu riskien tunnistamisesta sekä riskihavaintojen arvioinnista. Riskihavaintojen arvioinnin tuloksena syntyvä riskiarviointi evaluoidaan asetettuja taustatietoja vasten. Tämän ja koko riskien arviointivaiheen lopputuloksena on riskiarvio, joka on laadullisesti ja sisällöllisesti hyväksytty; riskistä ei kuitenkaan vielä ole tehty riskienhallintapäätöstä. Operatiivisten riskien osalta yleinen riskin esitystapa sisältää seuraavat tiedot riskistä:

- yleiskuvaus (riskin nimeäminen)
- riskin luokittelu (esim. henkilö- tai tietoriski)
- vaikutukset toteutumisesta (tappiot, joita riskin toteutumisesta seuraa; erityisesti taloudelliset seuraukset eli riskin kvantifioinnin kautta saatu lukuarvo)
- syyt toteutumiselle (miksi riski toteutuu ja mitä muuttujia niihin liittyy)
- tämänhetkiset riskienhallintatoimenpiteet (kontrollit) kustannuksineen (esim. vakuutusmaksu)
- toteutumisen todennäköisyys valitulla tarkastelujaksolla
- riskin merkittävyys (johdettuna vaikutuksista ja todennäköisyydestä)
- tarvittavat uudet riskienhallintatoimenpiteet kustannuksineen
- vaikutukset (tappionvaara) uusien riskienhallintatoimenpiteiden toteuttamisen jälkeen
- toteutumisen todennäköisyys uusien riskienhallintatoimenpiteiden toteuttamisen jälkeen

- riskin merkittävyys uusien riskienhallintamekanismien toteuttamisen jälkeen
- riskin riippuvuussuhteet muista riskeistä
- riskin historia (jos ei ole uusi riskihavainto)
- riskin omistaja
- riskin käsittelyvaiheiden kuvaus ja mahdolliset asiantuntijalausunnot

Riskien arviointivaiheen jälkeen tehdään organisaation johtamis- ja riskienhallintajärjestelmien mukaisesti riskienhallintapäätös, jonka jälkeen käynnistetään riskienhallintatoimenpiteet.

4.4 Riskien analysointi

Riskienhallintaprosessin yleensä työläin vaihe, ainakin riskin kvantifioinnin kannalta, on riskien analysointivaihe. Siinä riskit tunnistetaan ja tehdään niihin liittyvä riskihavaintojen arviointi. Käytännössä riskien analysointi tarkoittaa riskin ymmärtämisen 'rakennusvaihetta'[34]. Analyysin tuloksena syntyy riskiarvio, joka hyväksytyn evaluoinnin jälkeen siirtyy päätöksentekovaiheeseen.

Riskianalyysivaiheen jälkimmäisessä osassa, riskihavaintojen arvioinnissa, määritellään riskille vaikutukset ja toteutumistodennäköisyys. Myös riskin syyt ja riskin toteutumiseen vaikuttavat tekijät (muuttujat) tunnistetaan ja arvioidaan riskianalyysin aikana. Luonnollisesti nämä myös dokumentoidaan – kärjistäen riskienhallinta on tosiasiassa olemassa vain silloin, kun se on dokumentoitua. Tämä periaate on sama riskienhallintaprosessin kaikissa vaiheissa.[35]

---

[34] IEC/ISO 31000:2009, s. 18.

[35] Klassinen vitsi riskienhallinnan tuomasta 'läpinäkyvyyden parantumisesta' siinä yhteydessä, kun tarvittavia riskienhallinnan dokumentteja ei löydy, ei välttämättä kevennä tilannetta esimerkiksi tilintarkastajan haastattelussa.

Riskin analysointivaihe perustuu taustatietoihin, joita riskienhallintaprosessin alussa on määritelty. Riskihavaintojen vaikutuksia ja todennäköisyyttä arvioidaan suhteuttaen ne taustatiedoista ilmenevään tavoitetilaan (riskinkantokyky ja -halukkuus) taustatiedoissa määritellyllä tavalla. Analysointivaiheen lopputuloksena syntyvä riskiarvio hallintamekanismeineen kuvataan niin kuin se taustatiedoissa on määritelty.

4.4.1 Riskien tunnistaminen

Riskienhallinnan standardi IEC/ISO 31010:2009 kiteyttää riskien tunnistamisvaiheen seuraavasti:

> *"The purpose of risk identification is to identify what might happen or what situations might exist that might affect the achievement of the objectives of the system or organization. Once a risk is identified, the organization should identify any existing controls such as design features, people, processes and systems.*[36]

Luvussa 2.2 esitetyn riskien tunnistamisen määritelmän tukena oheinen kuvaus havainnollistaa riskien tunnistamisvaiheen luonteen: tarkoitus on tunnistaa, mitä *voi* tapahtua tai mitä tilanteita *voi* ilmetä, joilla *voi* olla vaikutusta organisaation tavoitteiden saavuttamiseen. Riskien tunnistamisvaiheen kattavuus ja onnistuminen onkin koko riskienhallintaprosessin kriittisimpiä kohtia. Riskiarviointeja varten määritellyillä taustatiedoilla tai tunnistettujen riskien arvioinnilla eivät korvaa sitä, jos riskit tunnistetaan puutteellisesti tai ei lainkaan. Riskien tunnistamiselle on kehitetty erilaisia menetelmiä vastaamaan tähän haasteeseen. Seuraavassa on esitetty näitä tunnistamismenetelmiä tarkemmin.

1) Tarkistuslistoihin ja toteutuneisiin riskeihin perustuva tunnistamismenetelmä

---

[36] ISO/IEC 31010:2009, s. 12.

Check-list -tyyppinen riskien tunnistaminen on yksi yleisimmistä käytössä olevista menetelmistä. Operatiivisten riskien tunnistamiseen on lukuisa joukko kattavia tarkistuslistoja, joista yhtenä erinomaisena esimerkkinä on standardin ISO/IEC 27005:2008 liitemateriaali[37] tietoturvariskien tunnistamisen tarkistuslistaksi. Toteutuneista operatiivisista riskeistä koottu vahinkotilasto on myös hyvänä apuvälineenä riskien tunnistamisvaiheessa, joskaan se ei välttämättä tue uusien, vielä toteutumatta olevien riskien tunnistamista.

2) Ryhmätyönä tehtävä riskien tunnistaminen, jossa joukko asiantuntijoita tunnistaa kohteen riskejä hyödyntäen systemaattista prosessia, jota tukee huolellisesti määritelty kysymyslista asiantuntijoille tarkasteltavaan aiheeseen liittyen. Keskustelun järjestäjä (”fasilitoija”) varmistaa, että tunnistetut riskit dokumentoidaan ja että niihin liittyvät syyt ja seuraukset sekä hallintamekanismit tulevat myös tunnistetuksi.

3) Induktiiviset päättelymenetelmät

Induktiivinen päättely johdattelee yksittäisestä havaintojoukosta yleistyksen. Se toimii operatiivisten riskien tunnistamisessa erityisesti HAZOP-menetelmän osalta. HAZOP on strukturoitu ja systemaattinen tunnistamismenetelmä, jossa tutkitaan olemassa olevaa tai suunnitteilla olevaa kohdetta (esim. prosessi, menetelmä tai järjestelmä) HAZOP-menetelmään perehtyneen ryhmän toimesta. HAZOP on alkujaan kehitetty arviointimenetelmäksi kemiakaaleja käsittelevien prosessien ja järjestelmien arvioimiseksi, mutta sitä voidaan soveltaa mihin tahansa ihmisiin, laitteisiin, ympäristöön tai organisaation tavoitteisiin liittyvien riskien tunnistamiseen. Se on kvalitatiivinen ja strukturoitu menetelmä, joka perustuu tarkasteltavan kohteen toiminnan tai tarkasteltavan suunnitelman onnistumisen kyseenalaistamiseen

[37] Erityisesti liitteet C ja D, joissa on kattava listaus tietoturvariskien tunnistamisen avuksi.

niiden eri vaiheissa. Sen avulla tunnistetaan riskejä prosessien, järjestelmien tai menetelmien virheistä sekä niiden syistä ja seurauksista, joten menetelmä kattaa koko riskien analysointivaiheen tehtävät.[38]

Lisäksi operatiivisten riskien tunnistamisessa voidaan käyttää muita, edellä mainittuja menetelmiä tukevia tunnistamistapoja. Yleisesti käytetty menetelmä on ’brainstorming’, joka operatiivisten riskien tunnistamisessa perustuu laajakatseiseen ja ennakkoluulottomaan keskusteluun asiantuntijoista koostuvassa ryhmässä ja heidän synnyttämäänsä ’ajatusvirtaan’. Ryhmää pyritään stimuloimaan uusien riskien, niistä aiheutuvien vahinkojen, riskienhallintatoimenpiteiden ja ylipäätänsä vaihtoehtoisten toimintatapojen tunnistamiseksi.

Brainstorming-menetelmässä, jota käytetäänkin terminä varsin laveasti ja alkuperäisestä tarkoituksestaan poiketen, on tärkeää huolehtia keskustelun tehokkaasta fasilitoinnista: oikeanlainen keskustelun avaaminen, ryhmän johdatteleminen keskustelun aikana tarvittaviin suuntiin ja esille nousseiden havaintojen systemaattinen poimiminen ovat edellytyksiä brainstorming-keskustelun hyödyllisyydelle.[39]

Operatiivisten riskien tunnistamisen tukena voidaan hyödyntää myös Delphi-menetelmää. Sen tarkoituksena on muodostaa luotettava konsensus asiantuntijaryhmän mielipiteestä – eli riskien tunnistamisvaiheessa erityisesti siitä, onko tunnistettu riski relevantti vai ei. Sen keskeisenä erityispiirteenä on asiantuntijoiden mielipiteiden kerääminen ensin yksityisesti ja anonyyminä, jonka jälkeen asiantuntijat tutustuvat muiden tekemiin arvioihin samasta asiasta. Asiantuntijat vastaavat ensin asiaan liittyvään kyselyyn, jonka jälkeen sen tulokset toimitetaan koko ryhmälle anonyymisti kommentoitavaksi. Tällä tavoitellaan (tarvittavien iteraatiokierrosten jälkeen) konsensuksen muodostumista asiantuntijoiden keskuudessa. Esimerkiksi jonkin tietojärjes-

[38] ISO/IEC 31010:2009, s. 32.

[39] ISO/IEC 31010:2009, s. 27.

telmän kompleksisen virhetilanteen syiden arviointi voi ratketa Delphi-menetelmällä, joka saattaa paljastaa – inhimillisistä syistä johtuen – esimerkiksi sen suunnittelussa olevan virheen, jota ei asiantuntijoiden keskinäisessä vuorovaikutuksessa samalla tavalla saataisi selvitettyä[40]. Anonyymi työskentelytapa saattaa siis mahdollistaa 'ei-toivottujen' mielipiteiden asiallisen käsittelyn ja toisaalta Delphi-menetelmällä asiantuntijoiden lausunnot käsitellään kaikki tasa-arvoisina ilman organisaatiossa mahdollisesti ilmeneviä sosiaalisia ristiriitatilanteita.

4.4.2 Riskihavaintojen arviointi

Riskienhallintaprosessissa riskihavaintojen arviointi on riskin kvantifioimisen kannalta merkittävin vaihe. Kvantifioiminen edellyttää toki aiempien vaiheiden asianmukaista suorittamista ja erityisesti käytettävissä olevan informaation oikeellisuutta, mutta prosessin vaiheena se on kriittisin operatiivisen riskin kvantifioinnin kannalta.

Tunnistetun operatiivisen riskihavainnon arviointi voidaan toteuttaa riskin luonteesta riippuen monilla eri tavoilla ja riskiin liittyvien omaisuuserien, suojattavien kohteiden tai muiden riskin objektien kriittisyydestä riippuen monella eri tasolla. Arviointitapa voi olla kvalitatiivinen tai kvantitatiivinen tai näiden yhdistelmä.

Kvalitatiivisessa riskien vaikutusarvioinnissa pyritään arvioimaan tunnistetut riskit niin, että ne voidaan sijoittaa taustatietojen määrittelyvaiheessa asetetulle asteikolle. Riskille annetaan esimerkiksi sen vaikutusten osalta numeraalinen arvo asteikolla 1–5, jossa pienin numero kuvaa pientä, lähinnä haittaavaa ja suurin numero esimerkiksi tuhoisaa vaikutusta. Vastaavalla tavalla riskin toteutumistodennäköisyys voidaan arvioida annetun asteikon mukai-

[40] ISO/IEC 31010:2009, s. 29.

sesti joko hyvin epätodennäköisesti tarkastelujakson aikana toteutuvaksi riskiksi tai varmasti toteutuvaksi riskiksi.

Riskien kvalitatiivisen vaikutusarvioinnin etuna on se, että se on yleensä helposti ymmärrettävissä kaikkien riskien arviointiin osallistuvien henkilöiden keskuudessa. Toisaalta sen haittana ovat usein epämääräiset ja subjektiiviset riskiarviot, jotka annetuista arviointiohjeista ja -asteikoista huolimatta aina jättävät mahdollisuuden sille, että asteikkoa tulkitaan eri tavalla eri henkilöiden toimesta tai että vaikutuksia ali- tai yliarvioidaan. Myös asetettu asteikko on voitu asettaa väärin. Toisaalta myöskään kvantitatiivinen riskianalyysi on aina arvio: riskienhallinnan laadulla ja määrällä voidaan vain pienentää riskeihin liittyvää epävarmuutta, ei poistaa sitä kokonaan.

Kvalitatiivisen riskiarvioinnin asteikkona käytetään usein riskimatriisia. Tästä on olemassa useita esitysmuotoja, joista kuitenkin perinteisin ja yksinkertaisin malli on riskien esittäminen matriisissa huomioiden niiden vaikutusten ja todennäköisyyden suhde - esimerkiksi vaikutusten ja todennäköisyyden tulona[41] tai kaavalla vaikutus² x todennäköisyys[42].

Riskihavainnon kvantitatiivisessa arvioinnissa riskin vaikutuksia ja todennäköisyyttä arvioidaan käytännönläheisinä lukuarvoina. Analyysi tuottaa arvion niiden muodostamasta riskitasosta esittäen sen niissä yksiköissä, mitä taustatietojen asettamisvaiheessa on määritelty. Kvantitatiivisia analyysimenetelmiä esitetään tarkemmin luvussa 5.

---

[41] Tämä menetelmä on mainittu mm. Finanssivalvonnan standardissa 4.4b Operatiivisten riskien hallinta 2007, s. 14.

[42] Riskiarvon tai riskin odotusarvon määritelmä on perinteisesti esitetty riskin todennäköisyyden ja vaikutusten tulona. Tämä ei kuitenkaan tue riskienhallinnan tavoitetta saada riskit keskenään vertailukelpoisiksi. Organisaation kannalta tuhoisa riski, joka toteutuu hyvin epätodennäköisesti, on kyseisellä laskukaavalla samanarvoinen kuin merkityksetön riski, joka toteutuu varmuudella (kerran tai useammin). Mikäli riskienhallintapolitiikka perustuu tähän riskiarvon määritelmään, saattavat riskienhallintakeinot olla väärin mitoitettuja erityisesti tuhoisten, mutta epätodennäköisten riskien osalta. Riskiarvon laskeminen painottamalla vaikutusta (vaikutus² x todennäköisyys) korjaa tämän epäkohdan. Mm. Juvonen – Korhonen – Ojala – Salonen – Vuori 2005, s. 10.

4.5 Riskiarvioiden evaluointi

Riskiarvioiden evaluoinnissa riskien tunnistamisen ja riskihavaintojen arvioinnin kautta muodostunutta riskiarviota evaluoidaan niitä kriteerejä vasten, joita taustatietojen määrittelyvaiheessa on asetettu. Evaluoinnin tarkoituksena on vahvistaa riskin merkittävyys ja sen riskiluokittelu. Evaluoinnissa riskiarviota tarkastellaan myös esimerkiksi juridisesta, eettisestä tai taloudellisesta näkökulmasta. Näihin liittyvät havainnot voivat edellyttää riskiarvioon muutoksia, jotka toteutetaan ennen riskiarvion hyväksymistä. Evaluoinnissa päätetään erityisesti riskienhallintatoimenpiteistä (risk treatment):

- riskin hallintatoimenpiteiden tarve, tunnistettujen hallintatoimenpiteiden riittävyys, oikeellisuus sekä toteutusmahdollisuudet
- hallintatoimenpiteiden keskinäinen priorisointi
- mitä ’reittiä’ riskiä ryhdytään hallitsemaan; vältetäänkö se kokonaan esimerkiksi muuttamalla prosessia tai lopettamalla kyseinen liiketoiminta, siirretäänkö riski tai yritetäänkö sitä pienentää?

Riskin evaluointivaiheessa tulee siis olla käytettävissä sekä riskien arvioinnille asetetut taustatiedot että riskiarvioinnin kautta saatava tieto riskienhallintatoimenpiteiden kustannuksista. Ne tulee siis olla arvioituna riskihavainnon arviointivaiheen aikana, jotta riskihavainto voidaan evaluoida kattavasti.

4.6 Riskienhallintatoimenpiteiden toteuttaminen, seuranta ja riskien hallinnan arviointi

Kun riskiarvioiden evaluointi on valmis ja riskistä on tehty riskienhallintapäätös, käynnistetään (uusien) riskienhallintatoimenpiteiden toteuttaminen. Toimenpiteet voivat operatiivisten riskien osalta olla esimerkiksi prosessimuutoksia, tietojärjestelmän konfigurointia tai henkilöiden toimenkuvien muutoksia. Toimenpiteiden toteuttamiselle on tärkeää nimetä vastuussa oleva henkilö, jotta myös toimenpiteiden seuranta on mahdollista tehdä.

Riskienhallintapäätöksen oleellinen osa on sen mukaisten toimenpiteiden toteuttamisen seuranta. Niistä raportoidaan riskienhallintajärjestelmän vaatimusten mukaisesti tarvittaville sidosryhmille. Seuranta voi kestää operatiivistenkin riskien osalta jopa vuosia, mikäli toimenpidesuunnitelma edellyttää pitkäkestoisia toimenpiteitä. Näin ollen myös seuranta edellyttää selkeää vastuuttamista. Seurannan avulla voidaan tarvittavin väliajoin arvioida riskienhallintapäätöstä uudelleen. Riskin hallintaa voidaan siis uudelleenarvioinnin kautta muuttaa toimintaympäristön muutoksia tai muita arviointikriteereitä vasten. Oleellista on pitää riski seurannassa – ’avoimena’ – niin kauan, kunnes se on saavuttanut riskienhallintapäätöksen edellyttämän riskitason eli hallintatoimenpiteet saadaan toteutettua tai riski muutoin saavuttaa sille riskienhallintapäätöksessä asetetun tavoitetason.

Riskien seuranta ja niiden hallinnan arviointi on kiinteä osa riskienhallintaprosessia. Operatiivisten riskien raportointi korostuu etenkin organisaatiossa, jonka riskienhallintajärjestelmä edellyttää pääoman varaamista operatiivisille riskeille.

5 OPERATIIVISTEN RISKIEN KVANTIFIOIMINEN

Riskin kvantifioinnille on riskienhallinnan teorioille tyypillisesti lukuisia erilaisia määritelmiä ja toteutustapoja. Se on väistämätöntä johtuen jo siitäkin, että riskin määritelmät poikkeavat toisistaan. Lisäksi on riskilajikohtaisia eroja kvantifioimistavoissa. Tässä luvussa esitetään erityisesti operatiivisten riskien kvantifioimiseen soveltuvia menetelmiä. Lisäksi luvussa on lyhyt katsaus riskien kvantifioimisen historiaan.

5.1 Katsaus riskien kvantifioimisen historiaan

Riskien kvantifioimisen voidaan katsoa alkaneen jo reilut 500 vuotta sitten. Italialaisen matemaatikon Pacciolin vuonna ilmestyneessä 1494 teoksessa Summa käsitellään uhkapelaamisen osalta kysymystä siitä, miten pelipanokset jaetaan pelaajien kesken, kun peli jostain syystä keskeytyy. Tämän teoksen on tulkittu olevan alku kirjallisuudessa tapahtuvaan pohdintaan ja teoretisointiin todennäköisyyksien systemaattisesta mittaamisesta ja sitä kautta riskien määrällisestä mittaamisesta eli kvantifioimisesta.[43]

Varsinaisen todennäköisyyslaskennan katsotaan saaneen alkunsa ranskalaisten Blaise Pascalin ja kirjeenvaihdosta Pierre de Fermantin sekä kreivi de Meren välisestä kirjeenvaihdosta vuonna 1654. Tämä kirjeenvaihtokin käsitteli todennäköisyyslaskentaa uhkapelaamisen kannalta. Kirjeenvaihdon perusteella kehitetty todennäköisyysteoria antoi pohjan tulevien tapahtumien todennäköisyyksien systemaattiselle analysoinnille. Tätä teoriaa voidaankin pitää kulmakivenä nykyaikaisille riskiarviointimenetelmille.[44]

---

[43] Kuusela & Ollikainen 2005, s. 20 ja Bernstein 1996. s. 29.

[44] Kuusela & Ollikainen 2005, s. 74.

5.2 Operatiivisten riskien kvantifioimismenetelmiä

Operatiivisen riskin matemaattisen arvon yleinen määritelmä on riskin odotusarvon (expected value), käytännössä nimenomaan tappion odotusarvon määrittäminen kertomalla keskenään riskille arvioidut vaikutukset (odotetut tappiot) ja riskin toteutumistodennäköisyys[45]. Tämä ei kuitenkaan ole riskien kvantitatiivista vaan kvalitatiivista analysointia. Riskin kvantifiointi tarkoittaa nimenomaan riskin vaikutusten ja todennäköisyyden kvantitatiivista arviointia, ei niiden keskinäistä suhdetta.

5.2.1 Operatiivisen riskin vaikutusten kvantifiointi

Operatiivisen riskin vaikutusten kvantifiointi toteutetaan riskienhallintaprosessin vaiheessa ’riskien analysointi’. Kun riski ja sen vaikutukset on tunnistettu, arvioidaan ne tarkemmin riskihavainnon arviointivaiheessa. Riskin vaikutukset eli operatiivisen riskin osalta tappiot, joita riskin toteutuminen aiheuttaa, kvantifioidaan tässä vaiheessa riskienhallintaprosessia.

Operatiivinen riski voi aiheuttaa välittömiä ja välillisiä vahinkoja. Tavanomaisia välittömiä vahinkoja operatiivisille riskeille ovat omaisuus- ja henkilövahingot, vahingon rajoittamisen, selvittämisen ja korjaamisen aiheuttamat kulut sekä välittömät taloudelliset seuraamukset riskin toteutumisesta (esimerkiksi sopimussakko). Välittömien vahinkojen arviointi on yleensä varsin suoraviivaista, mikäli riskin vaikutukset on kattavasti tunnistettu ja niiden arvioimiseksi on käytettävissä riittävästi taustatietoja. Niitä ovat muun muassa omaisuuserien arvot, vakuutusmäärät ja omavastuut sekä arvio vahingon edellyttämistä rajoittamis-, korjaus-, ja selvittämistyömääristä mahdollisine sopimushintoineen. Näiden kvantifioinnin suoraviivaisuus edellyttää, että luvussa 4 kuvattua riskienhallintaprosessia on noudatettu: riskienhallin-

[45] Näin esimerkiksi Suominen 2003, s. 10.

taprosessi alkaa kattavalla taustatietojen määrittelyllä. Omaisuuserien arvot ja liiketoimintaprosessien katkosta aiheutuvat vahingot ovat tietoja, joita riskienhallintaprosessin kvantifiointivaiheessa *haetaan* taustatiedosta. Niitä ei siis ryhdytä määrittelemään siinä vaiheessa, kun esimerkiksi olemassa olevan prosessin tai järjestelmän käyttökatkoriskiä käsitellään. Kvantifiointi on siis yksinkertaisimmillaan vain tietojen yhdistämistä: esimerkiksi tunnistetun käyttökatkoriskin ajallinen pituus kerrotaan taustatiedoissa olevalla saamatta jääneen katteen tai SLA-sakkojen määrällä.

Jos tunnistettu riski on esimerkiksi elektroniikkalaitteita valmistavan tuotantolaitoksen varastossa tapahtuva vesivahinko ja tunnistetut välittömät vaikutukset siitä olisivat 30 % varastossa olevien laitteiden kastuminen ja rikkoontuminen, vahingon korjaamiseen liittyvät veden poistaminen, putkiliittimien uusinta, tilan tyhjentäminen sekä kuivatus sekä tapahtuman selvittämiseen liittyvät kulut, saadaan välittömät vaikutukset laskemalla edellä mainitut yksinkertaisesti yhteen. Tämä olisi siis riskin vaikutusten kvantifiointia, joka edellyttää, että riskienhallintaprosessissa on taustatiedot asetettu oikein.

Välillisten vahinkojen kvantifiointi voi olla huomattavasti monimutkaisempaa. Kuvatussa vesivahinkoriskissä välillisiä vahinkoja voisivat olla muun muassa laitetilausten viivästyminen asiakkaille ja sitä kautta aiheutuva asiakastyytymättömyys, tilapäisen varastotilan järjestämisestä aiheutuvat kulut ja siitä aiheutuva logistiikkakulujen lisääntyminen sekä tuotantolinjaston tehokkuuden hetkellinen laskeminen johtuen logistiikkaketjun muuttumisesta. Edelleen riskin vaikutusten kvantifiointi on periaatteessa vain riskienhallintaprosessin taustatietojen hyödyntämistä ja sitä kautta tunnistettujen vaikutusten arvon laskemista yhteen. Käytännössä tässä vaiheessa on kuitenkin syytä kiinnittää huomiota siihen, minkälaista *arviointimenetelmää* käytetään, jotta tunnistettujen vaikutusten kvantifiointi olisi mahdollista.

Operatiivisten riskien vaikutusten arviointimenetelmistä aiemmin mainittu HAZOP soveltuu hyvin operatiivisten riskien vaikutusten arviointiin. Sen lisäksi käyttökelpoisia menetelmiä ovat erityisesti:

- HACCP
- business impact -analyysi
- juurisyyanalyysi sekä
- kustannus- / hyötyanalyysi.

Seuraavassa niiden esittely tarkemmin.

HACCP (Hazard analysis and critical control point) on operatiivisten riskien vaikutusten arviointia tukeva riskiarviointimenetelmä, joka kehitettiin alkujaan Yhdysvaltain avaruushallinnon NASA:n tarpeisiin astronauttien ruokatarvikkeiden laadun varmistamiseksi. Sen käyttö on myöhemmin laajentunut eri toimialoille. Sen perusperiaate on riskin arvioiminen siitä näkökulmasta, mitkä muuttujat voivat vaikuttaa riskin toteutumiseen ja määritellä niiden osalta ne kontrollipisteet, joissa kyseisiä muuttujia voidaan seurata ja joissa niihin tulee eri kontrollein vaikuttaa. HACCP tavoittelee enemmän kaikkien relevanttien riskien minimoimista luomalla niille kontrollit kuin varsinaisen riskin kohteen (esim. tuote tai prosessi) tarkempaa analysointia ja sen muutostarpeiden tunnistamista. HACCP soveltuu siis erityisesti sellaisten operatiivisten riskien arviointiin, joissa riski kohdistuu ’vakioituun’ kohteeseen, jota ei haluta tai voida muuttaa tunnistettujen riskien takia.[46]

Business impact -analyysi (”BIA”) on menetelmä, jolla erityisesti keskeytysriskin vaikutuksia voidaan arvioida organisaation toimintaan liittyen. Sen avulla voidaan tunnistaa organisaation kriittiset prosessit, toiminnot ja niihin liittyvät resurssit sekä näiden väliset riippuvuudet. Lisäksi BIA:n avulla voidaan tunnistaa keskeytysriskin vaikutukset organisaation tavoitteiden saa-

[46] ISO/IEC 31010:2009, s. 35.

vuttamiseen sekä keskeytysriskien hallitsemisen ja keskeytymisestä toipumisen edellyttämät kyvykkyydet ja resurssit. BIA:n arviointimenetelmässä kuvataan myös koko toimitusketju (supply chain), jotta kaikki operatiiviset riskit niin omassa kuin kumppaninkin verkossa voitaisiin tunnistaa ja arvioida. BIA soveltuukin hyvin operatiivisiin riskeihin kuuluvan liiketoiminnan jatkuvuus -osa-alueen riskiarviointimenetelmäksi.[47]

Juurisyyanalyysi (root cause analysis, ”RCA”) on erityisesti omaisuusvahinkojen arviointiin soveltuva menetelmä, joka perustuu vahingon perimmäisen syyn selvittämiseen. Sitä käytetään yleisimmin suurten omaisuusvahinkoriskien arvioimiseen, mutta siitä on olemassa useita erityyppisiä versioita: muun muassa prosessi-, turvallisuus-, tuotanto- ja järjestelmälähtökohtainen analyysi.[48] Vaikka juurisyyanalyysiä käytetäänkin usein jo toteutuneiden riskien vaikutusten selvittämiselle, on se erittäin käyttökelpoinen mille tahansa operatiiviselle riskille, jonka syy ei ole ilmeinen. Yhdistämällä juurisyyanalyysin ja HACCP:n pystyy hyödyntämään molempien menetelmien parhaat puolet eli tunnistetun riskin todellisen syyn paikallistamisen ja toisaalta juurisyyarvioinnin aikana havaittujen muiden kontrollitarpeiden ja -pisteiden tunnistamisen. Yhdistetty menetelmä on kuitenkin riskienhallinnan tehokkuuden kannalta raskas ja näin ollen käyttökelpoinen vain organisaation merkittävimpien eli avainriskien arvioinnissa.

Kustannus/hyötyanalyysi (cost / benefit analysis, ”CBA”) on yleensä kvantitatiivinen arviointimenetelmä, jossa riskin toteutumisen kokonaisvaikutuksia verrataan hyötyihin, joita riskin ottaminen mahdollistaa. Operatiivisten riskien osalta (joissa riskikäsite rajautuu tappionvaaraan) kustannus/hyötyanalyysi ei ole ensisijainen arviointimenetelmä, mutta se on kuitenkin sovellettavissa myös operatiivisten riskien hallintaan erityisesti tilanteissa, joissa muiden menetelmien käyttö on jättänyt riskille keskenään samanarvoisia vaihtoehtoja tai tilanteeseen, jossa riskienhallintatoimenpiteen

[47] ISO/IEC 31010:2009, s. 43.

[48] SO/IEC 31010:2009, s. 44.

hyväksyminen tai hylkääminen edellyttää lisäinformaatiota. CBA:ssa tunnistetaan kaikki välittömät ja välilliset kustannukset ja hyödyt, joita tarkasteltavaan kohteeseen kuuluu. Tarkasteltavasta ajankohdasta riippuen hyödyt, jotka usein realisoituvat pidemmällä aikavälillä kuin kustannukset, diskontataan nykyarvoonsa. NPV-laskelmia (net present value) käyttämällä kustannus/hyötyanalyysi tuottaa informaation siitä, mikä vaihtoehto on kannattavin.

5.2.2 Operatiivisen riskin todennäköisyyden arviointi

Riskin kvantifioiminen edellyttää sen vaikutusten kvantifioimisen lisäksi todennäköisyyden kvantifioimista. Operatiivisen riskin kvalitatiivinen todennäköisyyden arviointi toteutetaan subjektiivisella arviolla annettua todennäköisyysasteikkoa vastaan. Operatiivisen riskin todennäköisyyden kvantitatiivinen arviointi voidaan toteuttaa käytännössä kolmella eri tavalla:

1) Käyttämällä relevanttia historiallista informaatiota avuksi, jotta tunnistetaan tapahtumat ja tilanteet, joissa arvioitava riski on toteutunut ja sitä kautta tehdään päätelmä riskin toteutumisesta tulevaisuudessa. Tämä on luotettavin arviointitapa silloin, kun kyseessä on usein toistunut tapahtuma, jonka toteutumisesta on kerätty pitkään ja kattavasti tietoja organisaation vahinkotilastoihin tai niitä saadaan muistakin samankaltaisista organisaatioista. Esimerkkejä tällaisista tapahtumista:

- tietojärjestelmän käyttökatkojen lukumäärä, ajankohdat, kesto ja juurisyy
- vähittäistavarakaupan hävikin keskiarvoinen määrä, kohde ja tapausten selvittämisprosentti
- maksukortteihin liittyvä väärinkäytön lukumäärä keskiarvona ja suhteutettuna kokonaiskorttivaihtoon, korttityyppikohtainen jakauma ja maakohtaiset tilastot

Vahinkotilastoista saa joka tapauksessa ainakin sen tiedon, että riskiä ei ole aikaisemmin toteutunut (mikäli se olisi dokumentoitu). Näin ollen niiden hyödyntäminen on aina suotavaa. Todennäköisyys tarkasteltavalle riskille lasketaan kyseessä olevan tarkastelujakson (esim. vuosineljännes, projektin kesto, prosessin läpimenoaika, yksi vuosi) suhteen. Mikäli se toteutuu varmasti vähintään kerran, on todennäköisyys yksi (tai 100 %). Mikäli historiatietojen lisäksi ei ole muuta arviointiin vaikuttavaa tietoa, suhteutetaan historiatietojen toteuma riskille valitut hallintamekanismien vaikutus huomioiden tarkasteltavaan ajanjaksoon.

2) Todennäköisyyslaskennan hyödyntäminen siten, että laaditaan ennustemalleja esimerkiksi Fault tree -analyysiä käyttämällä. Kun historiatietoa ei ole riittävästi tai se ei ole luotettavaa, tulee todennäköisyys päätellä analysoimalla riskiin vaikuttavia objekteja ja muuttujia. Numeraalinen informaatio esimerkiksi ihmisten, laitteiden, järjestelmien ja organisaatioiden lukumäärästä voidaan yhdistää ja sitä kautta muodostaa arvio riskin toteutumisen todennäköisyydestä.

3) Asiantuntija-arvion käyttäminen strukturoidulla ja systemaattisella päättelyprosessilla riskin toteutumisen todennäköisyyden päättelemiseksi. Asiantuntijalle luovutetaan kaikki relevantti historia- ja muu tieto ja käyttämällä määriteltyä päättelyprosessia saadaan arvio esimerkiksi Delphi-menetelmää käyttämällä tehtyä.[49]

Todennäköisyyden arvioinnissa käytettäviä kvantifioimismenetelmiä ovat aiemmin jo esitellyn Delphi-menetelmän lisäksi Fault tree -analyysi sekä Bayesin teoria, jotka esitellään seuraavassa:

Fault tree -analyysi ”FTA” on menetelmä, jolla pyritään tunnistamaan ja analysoimaan muuttujat, jotka voivat vaikuttaa riskin toteutumiseen. Muut-

[49] ISO/IEC 31010:2009, s. 14.

tujien kautta tunnustetaan syyt, jotka voivat johtaa riskin toteutumiseen. Syyt päätellään deduktiivisella tavalla (yleisestä yksityiseen), järjestetään ne loogiseksi kokonaisuudeksi ja sen jälkeen esitetään ne puuna, jossa tekijöiden suhde riskiin (joka on puun 'ylimmässä latvassa') havainnollistetaan. Menetelmää käytetään kvalitatiivisesti siihen, että riskiin johtavat tapahtumat ja niiden syyt tunnistetaan ja kuvataan. Kvantitatiivisesti sitä käytetään riskin toteutumistodennäköisyyden arviointiin siten, että riskin toteutumiseen tunnistettujen tapahtumien ja syiden todennäköisyys arvioidaan osana päättelyketjua. Kun tunnistettujen riskin toteutumiseen vaikuttavien tapahtumien todennäköisyys on saatu määriteltyä, voidaan koko fault tree -kuvan perusteella arvioida riskin toteutumistodennäköisyys. Tapahtumien todennäköisyysarviointia varten tarvitaan niihin liittyvää tilasto- tai muuta tietoa.[50] Fault tree -menetelmä on erittäin käyttökelpoinen menetelmä operatiivisten riskien todennäköisyyden arvioinnissa silloin, kun riski voi toteutua useiden eri muuttujien vaikutuksesta eikä sen toteutumisesta ole aiempaa historiatietoa.

Bayesiläinen teoria / tilastotiede perustuu Bayesin kaavaan, jonka avulla korjataan aiemmin määriteltyä todennäköisyyttä käyttäen tarkasteltavaa riskiä koskevaa lisätietoa. Siinä alkuperäisen todennäköisyysarvion ja lisätietoina saadun todennäköisyyden yhdistämisellä saadaan korjattu todennäköisyys riskin toteutumiselle. Tässä tutkielmassa ei esitetä Bayesin kaavaa tai sen soveltamistapoja tarkemmin.[51] Operatiivisten riskien hallinnassa se on kuitenkin käyttökelpoinen erityisesti silloin, kun siihen pohjautuvia todennäköisyyslaskennan ohjelmistoja käytetään hyödyksi riskienhallintaprosessin suorittamisessa.

---

[50] ISO/IEC 31010:2009, s. 50.

[51] Tarkemmin Bayesin teoreemaa esittelee mm. Condamin – Louisot – Naïm 2006, s. 76–87 .

6 JOHTOPÄÄTÖKSET

Tutkielmassa esitettiin riskienhallintaprosessia kokonaisuutena ja tarkemmin sen eri vaiheita erityisesti riskien kvantifioinnin osalta. Riskienhallinnan prosessimaisuus korostaa sen alkuvaiheessa tehtävää taustatietojen määrittelyä eli riskien tunnistamista, arviointia ja evaluointia varten tarvittavien tietojen määrittelemistä. Taustatietojen tulee olla oikea-aikaisesti saatavissa ja sisällöltään oikeita. **Vastuu riskienhallintaprosessin taustatietojen määrittämisestä jakautuu koko organisaatiolle.** Riskienhallintamenetelmien ja asteikkojen kuvaaminen on riskienhallintajärjestelmästä vastaavan tahon vastuulla ja esimerkiksi liiketoimintaprosessin mittareiden ja historiatietojen kuvaaminen on prosessista vastaavan tahon vastuulla. **Näin ollen vastuu riskin kvantifioinnin lopputuloksesta ei ole vain riskihavainnon arvioijalla vaan vain osittain: ensisijaisesti riskin kvantifioimisen lopputulos riippuu kyseisen riskihavaintoon liittyvien taustatietojen määrittäjästä.** Tämä korostaa riskienhallinnan kokonaisvaltaisuutta.

Lukujen 4 ja 5 perusteella on pääteltävissä, että riskien arvioimiseen liittyy helposti riski tehokkuusvaatimuksen laiminlyömisestä. Kattava kvantitatiivinen riskiarviointi vie aikaa erityisesti riippuvuusriskien osalta, kun kaikki riskiin liittyvät tekijät, esimerkiksi alihankkijoiden alihankkijat tai asiakkaiden asiakkaat huomioidaan riskiarviossa. **Näin ollen on suositeltavaa, että operatiiviselle riskille tehdään aina ensin kvalitatiivinen riskiarviointi, koska sen avulla voidaan tunnistaa suurimmat riskit sekä arvioida riskin vaikutukset yleisellä tasolla.** Kvantitatiivinen riskien arvioiminen on yleensä tarpeen tehdä vasta myöhemmässä vaiheessa, kun kohteen riskikartta alkaa olla muodostunut. Kvantitatiivinen riskihavainnon arviointi on aina monimutkaisempaa ja käyttää enemmän resursseja kuin kvalitatiivinen riskiarviointi.

Esimerkiksi vakuutusta hakevan teollisuusyrityksen kiinteistön palovahinkoriskin kvantifioiminen kattavasti on ehdoton edellytys vahinkovakuutusyhtiön

liiketoiminnan kannalta. Kvantifioinnissa ja vakuutuksen hinnanmäärityksessä vakuutusyhtiö hyödyntää paitsi yleisiä riskin arviointimenetelmiä ja riskikartoituksia niin myös tilastoanalyysiä, jossa riskin todennäköisyyttä ja vaikutuksia arvioidaan historiatietojen avulla esimerkiksi toimialakohtaisten painotusten avulla. Yrityksellä, joka palovakuutusta hakee, ei vastaavanlaisia vahinkotilastoja ole käytössään eikä yleensä myös kvantifioimisen edellyttämiä henkilö- ja tietopääomaresursseja. Sille saattaa riittää, että se tunnistaa riskin kiinteistönsä palamiselle, arvioi seurausten olevan joka tapauksessa kestämättömiä omalle liiketoiminnalleen ja vertaa niitä saamaansa tarjoukseen esimerkiksi kiinteistön täysarvovakuutuksesta. Tällaisessa tapauksessa vakuutusmaksu on yleensä helpommin hyväksyttävissä kuin riskin kantaminen itse – eikä syvällisempi kvantifioiminen ole edes kannattavaa.

Milloin riskin kvantifioimiseen kannattaa panostaa? Miksi operatiivisia riskejä kvantifioidaan? Onko riskin kvantifiointi tarpeen, jos sen hallintamekanismien tiedetään olevan joka tapauksessa riittäviä riskin toteutumistodennäköisyyden pienentämiseksi? Kuinka paljon kvantifiointiin kannattaa käyttää resursseja, jos se on pois jostain muusta osasta riskienhallintaprosessia? Tai voiko kvantifioinnin korvata jollain muulla osalla riskienhallintaprosessia? Näitä kysymyksiä operatiivisten riskien kvantifioinnista helposti esitetään, kun riskienhallinnan ja organisaation tehokkuusvaatimukset asettavat paineita riskienhallintaprosessin suorittajille.

Vastauksia on kuitenkin olemassa erityisesti finanssitoimialalla, jolla viranomaisvaatimukset asettavat organisaation operatiivisten riskien hallinnan ja kvantifioinnin minimitavoitteet.

Basel II -sääntelyn pohjalta laadittu Finanssivalvonnan standardi 4.2 Vakavaraisuuden hallinta asettaa operatiivisen riskien kvantifioinnille seuraavan vaatimuksen:

> *”Valvottavan tulee huolehtia sekä määrällisten (mitattavissa olevien) että laadullisten (ei mitattavissa olevien) riskien tunnistamisesta ja arvioinnista.”*

> *”Määrällisillä riskeillä tarkoitetaan riskejä, joihin liittyvä odottamaton tappio voidaan arvioida tilastomatemaattisin menetelmin tai stressitestein. Laadullisia riskejä ovat esimerkiksi strateginen riski, maineriski, oikeudellinen riski, sääntely- ja valvontaympäristöstä aiheutuvat riskit sekä riskit, jotka aiheutuvat hallinnon, sisäisen valvonnan tai riskienhallinnan puutteista. Useat rahoitustoiminnan riskeistä ovat mitattavissa olevia riskejä.*
>
> *Määrällisille riskeille valvottavien on kehitettävä ja otettava käyttöön tehokkaan riskienhallinnan mahdollistavat, riittävät mittausmenetelmät.”*[52]

Tämä Finanssivalvonnan sitova standardi antaa paljon vastauksia valvottavan operatiivisten riskien hallinnalle[53]. Standardi siis määrittelee osan operatiivisista riskeistä määrälliseksi (kvantifioitavissa olevaksi) ja osan laadulliseksi (ei voi kvantifioida). Laadullisen riskin määritelmään sisältyy lukuisa joukko operatiiviseksi luokiteltavia riskejä: oikeudellinen riski (jollainen voi olla esimerkiksi sopimusriski, joka ainakin sanktioiden tai vahingonkorvausvelvollisuuden osalta on usein kvantifioitavissa), vaatimustenmukaisuusriski (jollainen voi olla esimerkiksi viranomaisen tai muun sidosryhmän asettama sakko vaatimustenmukaisuuspoikkeamasta) sekä tarkemmin nimeämätön joukko ”sisäisen valvonnan tai riskienhallinnan puutteista johtuvista” riskeistä. Johtopäätöksenä voi todeta, että **kaikkia operatiivisia riskejä ei standardin väittämän mukaan voi kvantifioida.**

Koska Finanssivalvonnan standardit asettavat sitä koskeville organisaatioille vain minimivaatimukset, niin luonnollisesti organisaatio voi toteuttaa edellä mainitun vakavaraisuusvaatimuksen osalta standardia laajemmin riskien kvantifioimista. Standardin määritelmät ovat kuitenkin tämän tutkielman tarkastelukohteen kannalta merkittäviä. Ne vastaavat osittain – ainakin finanssialan osalta – kysymyksiin siitä, missä laajuudessa ja milloin operatiivisten riskien kvantifiointi on tarpeen. Edellä esitetty ote standardista 4.2

---

[52] FIVA 4.2 2007, s. 23.

[53] Myös standardi FIVA 4.2:n liite 2 antaa yhden vastauksen kysymykseen ”Miksi operatiivisia riskejä kvantifioidaan” – siksi, että operatiivisille riskeille voidaan allokoida riittävä pääoma vakavaraisuuden takaamiseksi.

sisältää myös viimeisessä virkkeessä vaatimukset riskienhallinnan keinojen tehokkuudesta ja riittävyydestä. Kuten aiemmin kolmannessa luvussa on todettu, niin nämä vaatimukset voi tulkita molemmista suunnista: menetelmät eivät saa olla tehottomia eli liikaa organisaation resursseja käyttäviä ja niiden tulee olla riittäviä eli ali-, mutta ei myöskään ylimitoitettuja. **Johtopäätöksenä riskienhallinnan tulee tukea organisaation tavoitteita siten, että sekin täyttää yleisen tehokkuusvaatimuksen.** Se vaikuttaa myös riskien kvantifioinnissa käytettävien menetelmien valintaan.

Tässä tutkielmassa esitetyistä riskienhallinnan standardien, käsitteiden ja tavoitteiden moninaisuudesta ja tulkinnanvaraisuudesta johtuen sekä yllä kuvattujen johtopäätösten perusteella on johdettavissa yksi varma asia riskienhallinnan tulevaisuudelle: organisaatioiden riskienhallintajärjestelmät ja riskienhallintaprosessien toteuttamistavat tulevat jatkossakin olemaan jatkuvassa muutoksessa. Toisaalta kokonaisvaltaisen riskienhallinnan periaatteiden mukaisesti niiden pitäisikin muuttua aina, kun organisaation johtamisjärjestelmää tai organisaatiorakennetta muutetaan. Riskienhallintaprosessin muuttaminen kehittyneemmäksi ja paremmin organisaation tavoitteita vastaavaksi onkin oikea suunta. Samalla se kuitenkin tarkoittaa organisaation riskienhallintajohdolle jatkuvaa haastetta saada organisaatio ymmärtämään riskienhallintaprosessin sekä toimimaan sen mukaisesti.

LÄHTEET

A Risk Management Standard 2003. Federation of European Risk Management Associations.

Basel Committee on Banking Supervision 2001.

Bernstein, P.L. 1996. Against the Gods: The Remarkable Story of Risk. New York: John Wiley & Sons, Inc.

Condamin Laurent, Louisot Jean-Paul & Naim Patrick 2006. Risk quantification: Management, Diagnosis and Hedging. Chippenham, Wiltshire: Antony Rowe Ltd.

COSO 2004b. Enterprise Risk Management Framework. Committee of Sponsoring Organizations of the Treadway Commission.

Finanssivalvonnan standardit:

4.1 Sisäisen valvonnan järjestäminen (2008)
4.2 Valvottavan vakavaraisuuden hallinta (2007)
4.4b Operatiivisten riskien hallinta (2007)

ISO/IEC-standardit:

ISO/IEC 27001:2006. Information technology. Security techniques. Information security management systems.
ISO/IEC 27005:2008. Information technology — Security techniques — Information security risk management.
ISO 31000:2009. Risk management — Principles and guidelines
ISO/IEC 31010:2009. Risk management – Risk assessment techniques.

Juvonen Marko, Korhonen Heikki, Ojala Veli Matti, Salonen Tero & Vuori Heli 2005. Yrityksen riskienhallinta. Helsinki: Yliopistopaino.

Kuusela Hannu & Ollikainen Reijo (toim.) 2005. Riskit ja riskienhallinta. Tampere: Tampereen yliopistopaino-Juvenes Print Oy.

Pöyry Olli 2008. KOKONAISVALTAINEN RISKIENHALLINTA (ERM) – Jalkauttamisen avaintekijät ja haasteet. Pro gradu -tutkielma. Tampereen yliopisto, oikeustieteiden laitos.

Riskien hallinta Suomessa 2002. Suomen itsenäisyyden juhlarahasto Sitra. Helsinki: Edita Prima Oy.

Suominen Arto 2003. Riskienhallinta. Vantaa: Dark Oy.