Enterprise Risk Management – Integrated Framework

(Kokonaisvaltainen ajatusmalli organisaation riskienhallintaan)

The Institute of Internal Auditors Finland 1956–2006

Yhteistyöllä tuloksiin

TIIVISTELMÄ

Syyskuu 2004

ESIPUHE

Toistakymmentä vuotta sitten Committee of Sponsoring Organizations of the Treadway Commission (COSO) tuotti julkaisun Internal Control – Integrated Framework (Sisäinen valvonta – kokonaisvaltainen ajatusmalli). Julkaisun tarkoituksena on auttaa yrityksiä ja muita yhteisöjä arvioimaan ja tehostamaan sisäisiä valvontajärjestelmiään. Siinä esitellystä mallista on sittemmin tullut osa strategioita, sääntöjä ja määräyksiä ja tuhannet organisaatiot soveltavat sitä pitääkseen toimintansa tavoitteidensa mukaisina.

Viime vuosina riskienhallintaan on kiinnitetty yhä enemmän huomiota ja samalla on käynyt yhä ilmeisemmäksi, että riskien tunnistamiseen, arviointiin ja hallintaan tarvitaan toimiva malli. Vuonna 2001 COSO käynnisti yhteistyössä PricewaterhouseCoopersin kanssa projektin luodakseen mallin, jolla johto voi helposti arvioida ja kehittää organisaationsa riskienhallintaa.

Samanaikaisesti mallin kehittämistyön kanssa eri maita ravisteli joukko näyttäviä yritysskandaaleja ja -romahduksia, joissa sijoittajat, yritysten henkilökunta ja muut sidosryhmät kärsivät huomattavia menetyksiä. Skandaalien seurauksena vaadittiin uusia lakeja, määräyksiä ja listausohjeita parantamaan yritysten johtamis- ja hallintojärjestelmää ja riskienhallintaa. Kävi yhä tarpeellisemmaksi saada aikaan riskienhallinnan malli, jossa määritellään toiminnan keskeiset käsitteet ja periaatteet, yhteinen kieli ja selkeät ohjeet. Enterprise Risk Management – Integrated Framework on mielestämme sellainen malli, ja uskomme julkaisun kuluvan niin yritysten, muiden yhteisöjen kuin sidosryhmienkin käsissä.

Yhdysvalloissa yritysskandaalit johtivat Sarbanes-Oxley-lain säätämiseen vuonna 2002, ja samantyyppisiä lakeja on jo voimassa tai valmisteilla myös muissa maissa. Laki laajentaa julkisten yhtiöiden jo pitkään voimassa ollutta velvollisuutta toteuttaa sisäistä valvontaa ja se edellyttää, että organisaation johto sertifioi ja riippumaton tarkastaja vahvistaa käytettävien järjestelmien toimivuuden. Edelleen käyttökelpoinen Internal Control – Integrated Framework on näiden raportointivaatimusten laajasti hyväksytty perusta.

Enterprise Risk Management – Intergrated Framework käsittelee sisäistä valvontaa entistä kattavammin ja keskittyy aikaisempaa selkeämmin ja perusteellisemmin organisaatioiden riskienhallintaan. Tarkoituksena ei ole syrjäyttää sisäisen valvonnan mallia vaan liittää se osaksi riskienhallintaa. Monet organisaatiot harkinnevat julkaisussa esiteltyä riskienhallinnan mallia parantaakseen omaa sisäistä valvontaansa ja kehittääkseen riskienhallintaprosessia nykyistä kokonaisvaltaisemmaksi.

Organisaation johdon vaikeimpia haasteita on päättää, missä määrin se on valmis sietämään riskejä pyrkiessään arvon luomiseen. Tämän raportin avulla organisaatiot voivat vastata haasteeseen entistä tehokkaammin.

John J. Flaherty
Puheenjohtaja, COSO

Tony Maki
Puheenjohtaja, COSOn neuvottelukunta

YHTEENVETO

Organisaatioiden riskienhallinnassa lähdetään siitä, että jokaisen organisaation tarkoituksena on tuottaa sidosryhmilleen arvoa. Kaikki organisaatiot joutuvat toimimaan epävarmuudessa ja johdon haasteena onkin päättää, kuinka paljon epävarmuutta siedetään pyrittäessä kasvattamaan sidosryhmäarvoa. Epävarmuus on sekä riski että mahdollisuus, koska se voi sekä vähentää että kasvattaa arvoa. Riskienhallinnan avulla organisaation johto voi tehokkaasti hallita epävarmuutta ja siihen liittyviä riskejä ja mahdollisuuksia, jolloin myös arvoa voidaan kasvattaa tehokkaammin.

Arvo maksimoidaan, kun organisaation johto strategiansa ja tavoitteidensa avulla luo optimaalisen tasapainon kasvun, tuottotavoitteiden ja niihin liittyvien riskien välillä ja kykenee tehokkaasti käyttämään voimavaroja organisaation tavoitteiden toteuttamiseksi. Organisaation riskienhallinta on:

- Riskinottohalukkuuden ja strategian yhdenmukaistamista – Johto punnitsee organisaationsa riskinottohalukkuutta arvioidessaan strategisia vaihtoehtoja, asettaessaan niihin liittyviä tavoitteita ja kehittäessään mekanismeja niihin liittyvien riskien hallintaan.
- Tehokkaampaa riskeihin vastaamista - Organisaation riskienhallinta pakottaa määrittämään, kuinka riskeihin vastataan ja valitsemaan eri vaihtoehtojen välillä. Riskit voidaan välttää, hyväksyä tai jakaa tai niitä voidaan vähentää.
- Toiminnallisten yllätysten ja tappioiden vähentämistä – Organisaatiot kykenevät tunnistamaan potentiaalisia tapahtumia ja vastaamaan niihin paremmin. Näin yllättävät tilanteet ja niistä aiheutuvat kustannukset ja tappiot vähenevät.
- Monitahoisten ja koko organisaatiota koskevien riskien tunnistamista ja hallintaa – 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.
- Tilaisuuksiin tarttumista – Ottamalla huomioon kaikki potentiaaliset tapahtumat organisaation johto kykenee tunnistamaan niihin sisältyvät mahdollisuudet ja hyödyntämään niitä ennakoivasti .
- Tehokkaampaa pääoman käyttöä –Yksiselitteinen riskitieto auttaa johtoa arvioimaan tehokkaasti pääoman kokonaistarvetta ja kohdentamaan pääoman käytön entistä paremmin.

Näiden riskienhallinnan luontaisten ominaisuuksien avulla organisaation johto kykenee saavuttamaan tulos- ja kannattavuustavoitteensa ja estämään voimavarojen menetykset. Riskienhallinta auttaa myös varmistamaan tehokkaan raportoinnin sekä lakien ja määräysten noudattamisen. Sen avulla myös vältetään organisaation maineen vahingoittuminen seurauksineen. Kaiken kaikkiaan riskienhallinta auttaa organisaatiota etenemään päämääräänsä ja välttämään sudenkuopat ja yllättävät tilanteet tavoitteita kohti kuljettaessa.

Tapahtumat – riskit ja mahdollisuudet

Tapahtumilla voi olla kielteisiä ja/tai myönteisiä vaikutuksia. Kielteisesti vaikuttavat tapahtumat ovat riskejä, jotka voivat estää arvon muodostumisen tai rapauttaa jo luotua arvoa. Myönteisesti vaikuttavat tapahtumat voivat kumota kielteisiä vaikutuksia tai tarjota mahdollisuuksia. Mahdollisuudessa tapahtumasta voi tulla tosi ja se voi edistää tavoitteiden toteutumista ja tukea arvon muodostumista tai säilymistä. Organisaation johto kanavoi mahdollisuudet takaisin strategiaansa tai tavoitteenasetteluunsa ja laatii suunnitelmat tilaisuuksiin tarttumisesta.

Organisaation riskienhallinnan määritelmä

Organisaation riskienhallinnassa käsitellään arvon muodostumiseen ja säilymiseen vaikuttavia riskejä ja mahdollisuuksia ja se määritellään seuraavasti:

Organisaation riskienhallinta on sen hallituksen, 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.

Määritelmän mukaisesti:

- riskienhallinta on koko organisaation kattava jatkuva prosessi
- riskienhallintaa toteutetaan organisaation kaikilla tasoilla
- riskienhallintaa sovelletaan strategian laadinnassa
- riskienhallintaa sovelletaan koko organisaatiossa, kaikilla tasoilla ja kaikissa yksiköissä ja siinä organisaatiota tarkastellaan kokonaisuutena
- riskienhallinnan tarkoituksena on tunnistaa potentiaalisia tapahtumia, jotka toteutuessaan vaikuttavat organisaatioon, ja hallita riskiä organisaation riskinottohalukkuuden mukaisesti
- riskienhallinnan avulla johto ja hallitus voivat saavuttaa kohtuullisen varmuuden organisaation tavoitteiden toteutumisesta
- riskienhallinta on kehitetty toteuttamaan tavoitteita, jotka on ryhmitelty erillisiin, mutta osittain päällekkäisiin luokkiin.

Määritelmä on tietoisesti tehty kattavaksi. Se sisältää avainkäsitteet, joiden avulla yritykset ja muut organisaatiot hallitsevat riskejään ja sitä voidaan soveltaa kaikilla organisaatioiden, teollisuuden ja eri toimialojen alueilla. Sen pääpaino on organisaation asettamien tavoitteiden toteuttamisessa, ja niiden toteutumien avulla voidaan määritellä riskienhallinnan tehokkuus.

Tavoitteiden toteutuminen

Johto laatii strategiset tavoitteet, valitsee strategian ja määrittelee sen mukaiset, koko organisaatiota koskevat päämäärät organisaation toiminta-ajatuksen tai tavoitetilan mukaisesti. Organisaation riskienhallinnan mallin avulla pyritään toteuttamaan nämä tavoitteet, jotka on ryhmitelty neljään luokkaan:

- strategiset – korkean tason tavoitteet, jotka ovat organisaation toiminta-ajatuksen mukaisia ja sitä tukevia
- toiminnalliset – organisaation voimavarojen tehokas ja taloudellinen käyttö
- raportointia koskevat – raportoinnin luotettavuus
- vaatimustenmukaisuutta koskevat – sovellettavien lakien ja määräysten noudattaminen.

Tämän tavoiteluokittelun avulla organisaatio voi keskittyä riskienhallintansa osa-alueisiin. Nämä neljä luokkaa ovat erillisiä mutta osittain päällekkäisiä (tavoite voi sisältyä useaan luokkaan), soveltuvat organisaatioiden erityyppisiin tarpeisiin ja voivat olla eri johtajien vastuulla. Luokittelun avulla voidaan myös tehdä ero yksittäisiin luokkiin kohdistuvien odotusten välillä. Jotkin organisaatiot käyttävät lisäksi kategoriaa 'Voimavarojen turvaaminen '.

Koska raportoinnin luotettavuutta ja lakien ja määräysten noudattamista koskevien tavoitteiden saavuttaminen on organisaation päätösvallassa, on kohtuullista olettaa että riskienhallinta varmistaa niiden toteutumisen. Strategisten ja toiminnallisten tavoitteiden toteutuminen riippuu kuitenkin ulkoisista tapahtumista, jotka ovat usein organisaatiosta riippumattomia. Riskienhallinnan avulla voidaan saada kohtuullinen varmuus siitä, että johto ja valvojana toimiva hallitus saavat ajoissa tiedon näiden tavoitteiden toteutumisvauhdista.

Organisaation riskienhallinnan osa-alueet

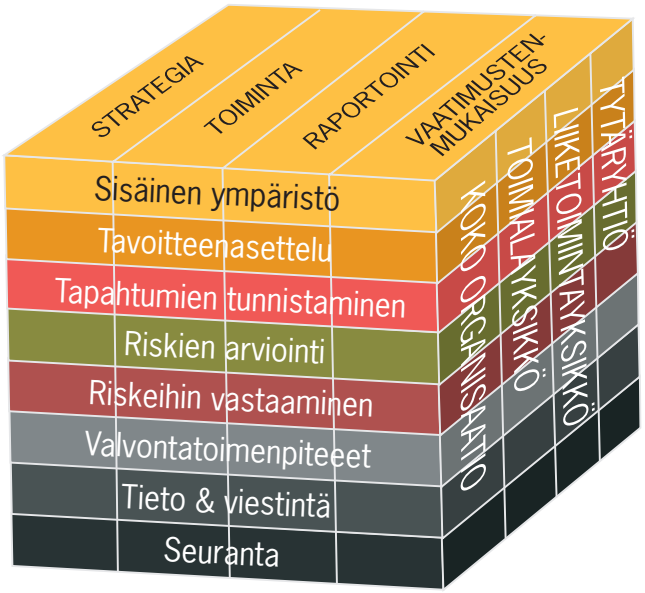
Organisaation riskienhallinta koostuu kahdeksasta toisiinsa liittyvästä osa-alueesta. Ne ovat kiinteä osa johtamisprosessia ja perustuvat siihen, kuinka organisaatiota johdetaan. Osa-alueet ovat:

- Sisäinen valvontaympäristö – 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 – Tavoitteet 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.
- Tapahtumien tunnistaminen – Organisaation tavoitteiden toteutumiseen vaikuttavat sisäiset ja ulkoiset tapahtumat on tunnistettava, ja samalla on tehtävä ero riskien ja mahdollisuuksien välillä. Mahdollisuudet kanavoidaan takaisin johdon strategian- ja tavoitteenasetteluun.
- Riskien arviointi – Riskit arvioidaan ottamalla huomioon niiden todennäköisyys ja vaikutukset, minkä pohjalta päätetään, kuinka ne on hallittava. Riskit arvioidaan bruttoriskeinä ja jäännösriskeinä.
- Riskeihin vastaaminen – Organisaation johto päättää, kuinka riskeihin vastataan. Riskit vältetään, hyväksytään tai jaetaan tai niitä vähennetään. Johto laatii keinot riskien sopeuttamiseksi organisaation sietokykyyn ja riskinottohalukkuuteen.
- Valvontatoimenpiteet – Laaditaan ja toteutetaan toimintalinjat ja menettelytavat, joita käyttämällä riskeihin kyetään vastaamaan tehokkaasti.
- Tieto ja viestintä – 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.
- Seuranta – Organisaation koko riskienhallintaa seurataan ja muutoksia tehdään tarpeen mukaan. Seuranta toteutetaan johdon jatkuvan toiminnan ja/tai erillisten arviointien avulla.

Organisaation riskienhallinta ei tiukasti ottaen ole tapahtumaketju, jossa yksi osa-alue vaikuttaa ainoastaan seuraavaan. Se on monisuuntainen ja toistuva prosessi, jossa lähes kaikki osa-alueet vaikuttavat tai ainakin voivat vaikuttaa toisiinsa.

Tavoitteiden ja osa-alueiden suhde

Tavoitteet (se, mihin organisaatio pyrkii) ja organisaation riskienhallinnan osa-alueet (se, mitä tarvitaan tavoitteiden toteuttamiseksi) ovat suorassa suhteessa toisiinsa. Suhdetta voidaan kuvata kolmiulotteisena kuutiomatriisina (kts. seuraava sivu), jossa neljä tavoitekategoriaa (strategiset, toiminnalliset, raportointia koskevat ja vaatimustenmukaisuutta koskevat tavoitteet) on kuvattu pylväinä, kahdeksan osa-aluetta vaakariveinä ja organisaation yksiköt kolmantena ulottuvuutena. Malli kuvaa organisaation valmiutta keskittyä riskienhallinnan kokonaisuuteen tai sen kykyä tarkastella sitä yksittäisten tavoiteluokkien, osa-alueiden tai yksiköiden tai niiden osien pohjalta.



Tehokkuus

Organisaation riskienhallinnan tehokkuuden määrittely perustuu kahdeksan osa-alueen käytettävyyden ja toimivuuden arviointiin. Siten osa-alueet ovat myös riskienhallinnan tehokkuuden kriteeri. Jotta osa-alueet olisivat käytettävissä ja toimivia, niissä ei saa olla merkittäviä heikkouksia ja riski on suhteutettava organisaation riskinottohalukkuuteen.

Riskienhallinnan toteaminen tehokkaaksi jokaisessa neljässä tavoiteluokassa antaa organisaation hallitukselle ja johdolle kohtuullisen varmuuden siitä, että he tietävät kuinka hyvin organisaation strategiset ja toiminnalliset tavoitteet ovat toteutumassa, että organisaatio raportoi luotettavasti ja että asiaankuuluvia lakeja ja määräyksiä noudatetaan.

Kahdeksan osa-aluetta eivät toimi samalla tavoin kaikissa organisaatioissa. PK-yrityksissä niiden soveltaminen voi olla epävirallisemmalla ja joustavammalla pohjalla kuin suuryrityksissä. Pienissä organisaatioissa riskienhallinta voi silti olla tehokasta, kunhan jokainen osa-alue on käytettävissä ja toimiva.

Rajoitukset

Organisaation riskienhallinnalla on omat tärkeät etunsa, mutta myös rajoituksensa. Edellä esitettyjen tekijöiden lisäksi rajoituksiin ovat syynä ihmisen päätöksentekokyvyn puutteet, tarve ottaa huomioon suhteelliset kustannukset ja hyödyt päätettäessä valvontatoimenpiteistä ja riskeihin vastaamisesta, inhimillisten kömmähdysten (jokapäiväiset erehdykset ja virheet) aiheuttamat häiriöt, mahdollisuus kiertää valvontaa kahden tai useamman ihmisen yhteisvoimin ja organisaation johdon valta kumota riskienhallintaa koskevat päätökset. Nämä rajoitukset estävät hallitusta ja johtoa saamasta täyttä varmuutta organisaation tavoitteiden saavuttamisesta.

Sisäinen valvonta

Sisäinen valvonta on organisaation riskienhallinnan olennainen osa. Tässä esiteltävä riskienhallinnan ajatusmalli käsittää sisäisen valvonnan, selkeämmän käsitteenmuodostuksen ja organisaation johdon välineet. Sisäinen valvonta määritellään ja kuvataan julkaisussa Internal Control – Integrated Framework. Koska julkaisussa kuvattu malli on osoittautunut toimivaksi ja muodostaa pohjan nykyisille säännöille, määräyksille ja laeille, se on edelleen sisäisen valvonnan perusmääritelmä ja -malli. Koska tässä esiteltävässä riskienhallinnan mallissa on lainattu julkaisua Internal Control – Integrated Framework vain osittain, julkaisussa esitelty ajatusmalli sisältyy viittausten kautta kokonaisuudessaan tässä esiteltävään malliin.

Roolit ja vastuut

Jokainen työntekijä on jossain määrin vastuussa organisaation riskienhallinnasta. Ylin vastuu on toimitusjohtajalla, jonka tulisi olla myös riskienhallinnan omistaja. Muut johtajat tukevat organisaation riskienhallintafilosofiaa, kannustavat riskinottohalukkuudessa pitäytymiseen ja hallitsevat riskejä omilla vastuualueillaan riskinsietokyvyn mukaisesti. Esimerkiksi riskivastaavalla, talousvastaavalla ja sisäisellä tarkastajalla on tavallisesti tärkeitä tukivastuita. Organisaation muun henkilökunnan vastuulla on riskienhallinnan toteuttaminen ohjeiden ja sääntöjen mukaisesti. Hallitus valvoo riskienhallintaa, sekä tietää ja hyväksyy organisaation riskinottohalukkuuden. Ulkoiset osapuolet, kuten asiakkaat, myyjät, liikekumppanit, ulkoiset tarkastajat, viranomaiset ja rahoitusanalyytikot antavat usein tietoa, joka on hyödyksi riskienhallinnan toteuttamisessa. He eivät kuitenkaan ole sen osa eivätkä vastuussa sen tehokkuudesta.

Raportin rakenne

Tämä raportti on kaksiosainen. Ensimmäinen osa käsittää ajatusmallin (Framework) sekä tämän yhteenvedon (Executive Summary). Framework määrittelee organisaation riskienhallinnan ja siinä kuvataan ne periaatteet ja käsitteet, joiden avulla yritysten ja muiden organisaatioiden eri tasojen johto voi arvioida ja kehittää riskienhallintaa. Executive Summary on korkean tason yleiskatsaus, joka on tarkoitettu toimitusjohtajille, muulle ylimmälle johdolle, hallitusten jäsenille ja sääntelijöille. Toisessa osassa (Application Techniques) kuvataan menetelmiä, joista on hyötyä mallin osa-alueita sovellettaessa.

Raportin käyttö

Raportin pohjalta käynnistettävät toimet riippuvat osapuolten asemasta ja roolista:

- Organisaation hallitus – Hallituksen olisi keskusteltava organisaation riskienhallinnan tilasta ylimmän johdon kanssa ja valvottava toimintaa tarpeen mukaan. Hallituksen olisi oltava selvillä tärkeimmistä riskeistä, johdon toimista ja siitä, kuinka johto varmistaa riskienhallinnan tehokkuuden. Hallituksen olisi myös harkittava sisäisten ja ulkoisten tarkastajien sekä muiden osapuolten käyttöä.
- Ylin johto – Toimitusjohtajan olisi arvioitava organisaationsa riskienhallintakyky. Hän voi esimerkiksi harkita riskienhallintakyvyn ja sen tehokkuuden alustavan arvion laatimista yhdessä liiketoimintayksiköiden johtajien ja eri toimintojen avainhenkilöiden kanssa. Riippumatta arvion toteutustavasta sen perusteella olisi päätettävä kattavamman ja perusteellisemman selvityksen tarpeesta ja toteutuksesta.
- Muu henkilökunta – Organisaation johdon ja muun henkilökunnan olisi mietittävä, kuinka he huolehtivat vastuistaan tämän mallin valossa ja keskusteltava esimiestensä kanssa riskienhallinnan vahvistamisesta. Sisäisten tarkastajien olisi pohdittava, kuinka laajasti he keskittyvät riskienhallintaan.
- Viranomaiset – Tämän mallin avulla voidaan edistää yhteistä näkemystä organisaation riskienhallinnasta, mm. sen mahdollisuuksista ja rajoituksista. Viranomaiset voivat käyttää mallia luodessaan odotuksia joko sääntöjen tai ohjeiden muodossa tai tarkastaessaan valvomiaan organisaatioita .
- Ammatilliset järjestöt – Sääntöjä laativien ja muiden ammatillisten järjestöjen, jotka opastavat esim. rahoitushallinnossa sekä sisäisessä ja ulkoisessa tarkastuksessa, olisi pohdittava normejaan ja ohjeitaan tämän mallin pohjalta. Kaikki osapuolet hyötyvät, kun käsitteistö ja terminologia yksinkertaistuu.
- Kouluttajat – Tämä malli voisi sopia aiheeksi parannuskohteita pohtivaan akateemiseen tutkimukseen tai analyysiin. Jos raportti hyväksytään riskienhallinnan yhteisymmärryksen pohjaksi, sen käsitteistö ja termit omaksutaan todennäköisesti myös korkeakouluopetuksessa.

Raportti luo perustan yhteisymmärrykselle, jonka avulla kaikki osapuolet voivat puhua samaa kieltä ja viestiä entistä tehokkaammin. Organisaation johto pystyy arvioimaan riskienhallintaprosessiaan normien pohjalta, vahvistamaan sitä ja kehittämään organisaatiotaan sovittujen tavoitteiden suuntaan. Samalla tutkimus voi tulevaisuudessa rakentua jo tehdylle työlle. Sitä paitsi lainsäätäjät ja viranomaiset kykenevät ymmärtämään entistä paremmin organisaation riskienhallintaa, myös sen hyötyjä ja rajoituksia. Kun kaikki osapuolet käyttävät samaa riskienhallintamallia, hyödyt kyetään myös realisoimaan.