Kokonaisvaltainen riskienhallinta

Riskienhallinnassa on kysymys järjestelmällisestä toiminnasta organisaation riskien tunnistamiseksi, analysoimiseksi ja arvioimiseksi sekä riskien käsittelystä, jotta ne vastaavat organisaation riskinottokykyä ja -halua. Parhaimmillaan riskienhallinta on luonnollinen osa päivittäistä toimintaa ja johtamista. Riskienhallinta auttaa organisaatiota päätöksenteossa asettamalla toimenpiteet tärkeysjärjestykseen ja erottamalla vaihtoehtoiset toimintatavat.

Mitä riskienhallinta on?

Yritykset ja organisaatiot pyrkivät saavuttamaan tavoitteensa ja täyttämään omistajiensa ja muiden sidosryhmiensä odotukset mahdollisimman hyvin. Tavoitteiden ja päämäärien saavuttamiseen vaikuttavat monet sisäiset ja ulkoiset tekijät, joiden vuoksi on epävarmaa, kuinka hyvin organisaatio tässä onnistuu. Epävarmuuden vaikutusta organisaation tavoitteisiin kutsutaan riskiksi. Epävarmuus ei kuitenkaan aina ole uhka vaan se voi olla myös mahdollisuus.

Riskienhallinnassa on kysymys järjestelmällisestä toiminnasta organisaation riskien tunnistamiseksi, analysoimiseksi ja arvioimiseksi sekä riskien käsittelystä, jotta ne vastaavat organisaation riskinottokykyä ja -halua. Riskienhallinnan toteutumista sekä riskien ja toimintaympäristön tilaa tulee säännöllisesti seurata ja arvioida.

Riskienhallinnan tavoitteet ja periaatteet

Kaikkeen toimintaan liittyy riskejä. Riskejä ei voida kuitenkaan aina poistaa, sillä varsinkin yritysmaailmassa riskin ottaminen on edellytys koko toiminnalle. Riskienhallinnan tavoite on tukea organisaation johtamista ja päätöksentekoa, jotta sen tavoitteisiin mahdollisesti vaikuttavat riskit ja riskien seuraukset tunnistetaan. Organisaation johto saa riskienhallinnan avulla kokonaiskuvan toimintansa merkittävimmistä riskeistä ja pystyy siten sovittamaan päätöksensä ja riskejä rajoittavat toimenpiteet riskinkantokykynsä ja riskinottohalunsa puitteisiin.

Riskienhallintaa voidaan toteuttaa organisaatiossa eri alueilla ja tasoilla, myös yksittäisissä tehtävissä ja hankkeissa. Parhaimmillaan riskienhallinta kattaa koko organisaation ja on osa toiminnan ja strategian suunnittelua, johtamista, prosesseja ja raportointia. Riskienhallinnan vastuut tulee määrittää ja ne ulottuvat organisaation johdosta aina yksittäiseen työntekijään.

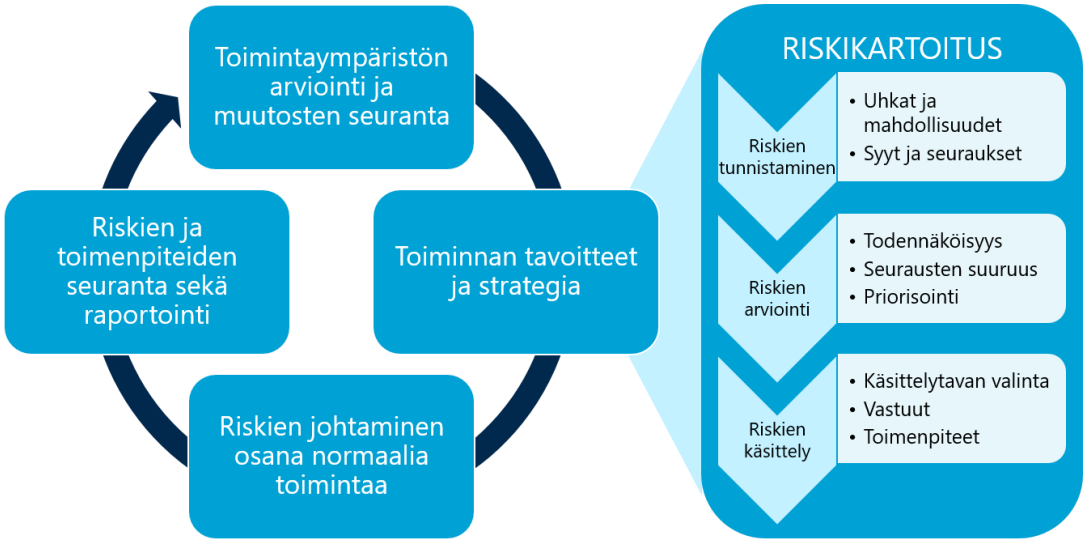
Riskienhallinnan tarkoitus on arvon luominen ja säilyttäminen. Se parantaa suorituskykyä ja tukee innovointia ja tavoitteiden saavuttamista.

a) Organisaation johtamisjärjestelmään sisälletty
b) Jäsennelty ja kattava
c) Räätälöity
d) Sidosryhmät mukaan ottava
e) Dynaaminen
f) Paras saatavilla oleva tieto
g) Inhimilliset ja kulttuuriset tekijät
h) Jatkuva kehittäminen

Riskienhallinnan periaatteet (SFS-ISO 31000:2018 Riskienhallinta. Ohjeet)

Riskienhallinnan suunnittelu ja toteutus

Riskienhallinnan toteuttaminen vaihtelee kunkin organisaation tarpeiden mukaan. Parhaimmillaan se alkaa toimintaympäristön ymmärtämisestä, toiminnan tavoitteista ja strategioista, kattaa koko organisaation ja on luonteva osa normaalia toimintaa ja johtamista. Riskienhallinnan käyttöönotto edellyttääkin yrityksen johdon vahvaa tukea ja sitoutumista.



Toimintaympäristön arviointi

Yrityksen strategian ja toiminnan suunnittelua varten on tärkeää ymmärtää ja arvioida organisaation ulkoista ja sisäistä toimintaympäristöä. Tämä palvelee myös riskienhallinnan järjestämistä.

Ulkoisen toimintaympäristön arviointi voi kattaa esimerkiksi yhteiskunnan, teknologian, talouden sekä ympäristön tilan ja kehityksen tunnistamisen. Useat eri lait ja viranomaismääräykset ohjaavat yrityksen toimintaa. Yrityksen toimialan avaintekijät ja kehityssuunnat tulee myös huomioida samoin kuin eri ulkoisten sidosryhmien odotukset.

Yrityksen sisäisestä toimintaympäristöstä arvioitavia asioita ovat esimerkiksi organisointi, toimintaperiaatteet, resurssit, osaaminen, tietojärjestelmät ja organisaation kulttuuri.

Organisointi eli yrityksen sisäinen organisaatio ja resurssit. Yrityksen organisaatiota tulee kehittää sellaiseksi, että riskienhallintaa voidaan toteuttaa kaikilla organisaatiotasoilla ja vastuut sekä valtuudet riskienhallinnan toteuttamisesta jaetaan oikein. Organisointiin liittyvät myös vahvasti riskienhallintaan suunnattavat henkilö- ja taloudelliset resurssit.

Verkostot. Toimittajien, alihankkijoiden, palveluntuottajien ja muiden sidosryhmien verkostoilla pyritään kustannustehokkuuteen ja joustavuuteen. Verkostoissa yritykset tulevat helposti riippuvaisiksi toisistaan ja myös toistensa riskeistä ja siten verkostossa tapahtuu riskin jakamista ja siirtoa. Verkostoissa riskit ja riippuvuudet syntyvät usein ketjuista, joita voi olla vaikea havaita. Kokonaisvaltaisen riskienhallinnan on huomioitava myös nämä tekijät. Ensiarvoisen tärkeää on tunnistaa liiketoimintaverkosto ja siihen liittyvät uhkatekijät.

Toimintajärjestelmät. Toimintajärjestelmillä tarkoitetaan erilaisia yrityksen liiketoimintaan liittyviä hallintajärjestelmiä. Näistä tunnetuimpia ovat laadunhallinnan järjestelmät (ISO 9000-sarja), ympäristöjärjestelmät (ISO 14000-sarja) ja turvallisuusjohtamisjärjestelmät (ISO 45001 Työterveys- ja työturvallisuusjohtaminen). Näiden lisäksi toimintajärjestelmiä ovat tietoturvallisuuteen liittyvät järjestelmät (ISO/IEC 27000-sarja) ja elintarviketurvallisuusjärjestelmät (ISO 22000 Elintarviketurvallisuus). Toimintajärjestelmien sisältämät tiedot tulee hyödyntää myös riskienhallintaa kehitettäessä. Lisäksi yrityksen luotettavuus paranee, kun sillä on käytössään dokumentoidut toimintajärjestelmät, joista voidaan kertoa asiakkaille ja muille intressitahoille.

Hallinnointi- ja ohjausjärjestelmiä (Corporate Governance) koskevien suositusten tavoitteena on yhtiöiden toimintatapojen yhtenäistäminen, toiminnan läpinäkyvyyden parantaminen, sijoittajille ja osakkeenomistajille annettavan tiedon yhtenäistäminen sekä tiedonkulun tehostaminen. Suosituksissa otetaan kantaa myös riskienhallinnan järjestämiseen. Keskuskauppakamari suosittaa näitä alun perin pörssiyhtiöille suunnattuja sääntöjä myös osuuskunnille, säätiöille ja pk-yrityksille. Sisäisen valvonnan ja riskienhallinnan merkitys on kasvussa myös julkisyhteisöissä.

Toiminnan tavoitteet ja strategia

Riskienhallinta on olennainen osa yrityksen johtamista ja strategiatyötä. Toimintasuunnitelmia ja strategiaa valmisteltaessa on syytä arvioida yrityksen merkittävimpien riskien ja riskienhallinnan tila. Parhaiten tämä hahmotetaan järjestelmällisellä ja säännöllisesti päivitettävällä riskien kartoituksella. Uusien ja muuttuneiden riskien vaikutukset voidaan siten huomioida strategiaa laadittaessa.

Riskien kartoitus, arviointi ja priorisointi

Riskien kartoituksella tunnistetaan ja arvioidaan organisaation toimintaa uhkaavat tekijät. Kartoitus antaa johdolle yleiskuvan yrityksen riskitilanteesta toiminnan ja strategian suunnittelun tueksi. Myös muun kartoituksiin osallistuvan henkilöstön tietoisuus riskeistä ja yrityksen toiminnasta paranee.

Arvioimalla tunnistettujen riskien todennäköisyyden ja seurausten merkityksen, yritys voi valita ja kohdentaa riskienhallintatoimenpiteet sopivimmalla tavalla. Kartoituksen yhteydessä löytyykin usein toimenpide-ehdotuksia toiminnan häiriöttömyyden ja keskeytymättömyyden varmistamiseksi. Riskikartoitukset tulee säännöllisesti päivittää ja tarvittaessa kokonaan uusia aina oman toiminnan tai toimintaympäristön merkittävästi muuttuessa.

Riskikartoituksia on hyvä tehdä kaikilla organisaation tasoilla. Johdon tarkastelussa korostuvat merkittävimmät yrityksen strategiaan, talouteen ja toiminnan johtamiseen liittyvät uhkat ja mahdollisuudet. Eri organisaatioyksiköiden kartoituksissa painopiste on taas enemmän toiminnallisissa ja vahinkoriskeissä. Työn riskien arvioiminen sisältyy osaltaan yrityksen riskikartoitusten kokonaisuuteen. Varsinaisten liiketoimintayksiköiden lisäksi tulee muistaa kartoittaa myös tukitoimintojen riskit.

Riskien tunnistaminen

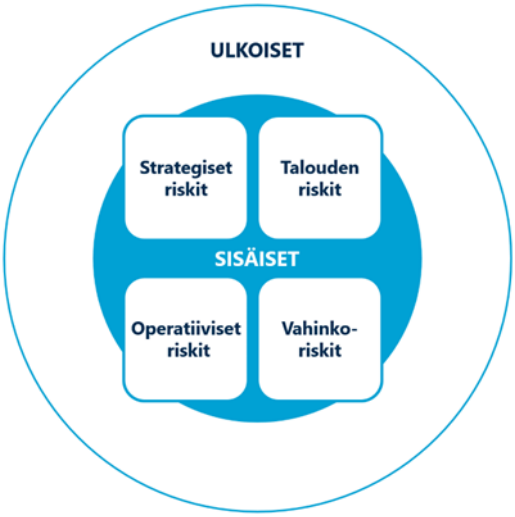
Yrityksen riskejä voidaan luokitella eri tavoin. Usein käytetty jako on **strategisiin**, **taloudellisiin**, **operatiivisiin** ja **vahinkoriskeihin**. Riskien tarkastelu ja arviointi näistä eri näkökulmista antaa monta kertaa paremman kuvan yrityksen uhkien ja mahdollisuuksien koko laajuudesta sekä riskien riippuvuuksista ja vaikutuksista toisiinsa. Yksittäinen riski ei useinkaan ole selkeästi vain esimerkiksi vahinkoriski, vaan sillä voi toteutuessaan olla myös toiminnallisia, taloudellisia ja strategisia vaikutuksia.

Strategiset riskit

- Liikestrategia
- Yrityskulttuuri, johtaminen
- Kilpailijat ja markkinat
- Asiakkuudet
- Verkostot ja kumppanit
- Sääntely ja lainsäädäntö

Talouden riskit

- Pääoma ja rahoitus
- Maksuvalmius
- Hinta- ja valuuttariskit
- Tuottavuus
- Luottotappiot
- Väärinkäytökset



Operatiiviset riskit

- Raportointi ja mittarit
- Tietojärjestelmät ja –turva
- Digitalisaatio, teknologia
- Palvelut, tuotteet, prosessit
- Henkilöstö
- Vastuut ja sopimukset
- Viestintä

Vahinkoriskit

- Kiinteistöt (palo, vuoto)
- Rikollinen toiminta
- Kuljetukset ja liikenne
- Työtapaturmat
- Koneet ja laitteet
- Tuotannontekijät
- Ympäristö

Riskien tunnistaminen voi tapahtua käyttäen apuna erilaisia tarkistuslistoja tai käsiteltävän aihepiirin asiantuntijoiden ryhmätyöskentelynä. Riskien arvioimiseksi on kehitetty myös erityisiä päättelymenetelmiä, kuten HAZOP, HACC tai RCA.

Riskeistä pyritään tunnistamaan niiden syyt ja seuraukset. Syyt tai riskin lähteet voivat usein olla myös yrityksen oman toiminnan ulkopuolella. Riskin toteutumisen seuraukset vaihtelevat esimerkiksi taloudellisista vaikutuksista ja toiminnan häiriintymisestä henkilövahinkoihin ja yrityksen maineen vahingoittumiseen.

Riskien arviointi ja priorisointi

Riskin suuruus tulee arvioida, jotta riskit voidaan priorisoida eli asettaa ne niiden merkittävyyden mukaiseen järjestykseen. Riskin suuruus koostuu yleensä kahdesta tekijästä, vahingon seurausten vakavuudesta ja vahingollisen tapahtuman todennäköisyydestä. Riskin suuruutta kuvataan riskiluvulla, joka saadaan seurausten vakavuuden ja tapahtuman todennäköisyyden tulona. Luokittelussa käytetään usein kolmi- tai viisiportaista asteikkoa.

Riskin suuruus = Vahingon seuraukset * Tapahtuman todennäköisyys

Kun kaikkien tunnistettujen riskien suuruudet on arvioitu, voidaan ne asettaa kaikki yhtäläiseen suuruusjärjestykseen ja alkaa miettiä niiden vähentämiseksi tarvittavia toimenpiteitä ja riskien hallintakeinoja.

Riskien hallintakeinot

Tyypillisiä riskienhallintakeinoja ovat **välttäminen**, **pienentäminen**, **siirtäminen** tai **pitäminen**. Näitä keinoja voidaan käyttää joko erillisinä, mutta yleensä riskin hallitseminen on eriasteinen yhdistelmä edellä mainittuja toimia. Näiden toimien lisäksi riskien hallintakeinoihin liittyy myös olennaisesti yrityksen liiketoiminnan jatkuvuussuunnittelu

Kokonaisvaltaisessa riskienhallinnassa eri hallintakeinoilla tulee pyrkiä poistamaan liiketoimintaa uhkaavat riskit ja käyttämään hyödyksi kaikki mahdollisuudet, joilla yritys saavuttaa liiketoimintansa tavoitteet.

Riskin välttäminen. Kaikkien riskien toteutumista tulisi ensisijaisesti yrittää välttää, koska ne aiheuttavat joko välittömiä taloudellisia menetyksiä tai välillisiä epäedullisia seurauksia. Näin ei kuitenkaan ole välttämättä kaikkien liikeriskien osalta, koska riskin toteutuminen myönteisenä on myös mahdollista. Näissäkin tapauksissa on kuitenkin varauduttava riskin toteutumisen kielteisiin seurauksiin. Vain harvat riskit ovat kokonaan poistettavissa.

Riskin pienentäminen tähtää vahinkotapahtuman todennäköisyyden tai seurausten pienentämiseen. Riskin pienentäminen voi olla riskin a) jakamista tai b) vahingontorjuntaa

Riskin siirtäminen ja pitäminen. Riskin siirtäminen merkitsee riskialttiin toiminnan siirtämistä sopimuksen perusteella jollekin toiselle osapuolelle. Yleisin tapa on siirtää riskin taloudelliset seuraamukset vakuutusyhtiön kannettavaksi vakuutussopimuksella. Yritys voi myös siirtää riskejä sisältävää omaisuuttaan tai riskipitoisia toimintojaan sopimusteitse toisen yrityksen kannettavaksi esimerkiksi kuljetus- tai alihankintasopimuksilla. Riskin pitäminen yrityksen omalla vastuulla voi olla johdon tietoinen valinta. Yritys voi myös olla tiedostamatta riskin olemassaoloa tai on arvioinut sen liian alhaiseksi.

Liiketoiminnan jatkuvuussuunnittelu tarkoittaa kaikkien niiden toimenpiteiden muodostamaa kokonaisuutta, jonka avulla yritys pyrkii varmistamaan päivittäisen liiketoimintansa jatkumisen myös vakavien häiriöiden jälkeen. Jatkuvuussuunnittelun tärkein dokumentti ja työkalu on liiketoiminnan jatkuvuussuunnitelma, jossa kuvataan kirjallisesti vastuut ja toimenpiteet vakavassa häiriötilanteessa. Tyypillisiä vakavia liiketoimintaan kohdistuvia häiriötilanteita ovat esimerkiksi yrityksen toimitiloihin kohdistunut suuri tulipalo, laaja vesivahinko, vakava tietovuoto sekä laajamittaisen yrityksen tietoverkon tai tietojärjestelmän käyttöhäiriö.

Riskienhallintapolitiikka

Riskienhallintapolitiikka sisältää perusteet riskienhallintapäämäärien ja -tavoitteiden määrittelylle sekä katselmoinnille. Riskienhallintapolitiikka laaditaan riskitekijöiden tunnistamisen, arvioinnon ja priorisoinnin jälkeen, jotta keskeisimmät riskienhallinnan tasoa kehittävät toimenpiteet saadaan kerättyä. Samalla voidaan varmistua siitä, että politiikka soveltuu yrityksen toiminnan luonteeseen.

Riskienhallintapolitiikan tavoitteena on taata riskitekijöiden ja niiden edellyttämien korjaavien toimenpiteiden huomioon ottaminen kaikilla yrityksen liiketoiminnan osa-alueilla. Parhaimmillaan se on lyhyt ja ytimekäs johdon tahdonilmaisu yrityksen riskienhallinnan tilasta ja kehittämisestä.

Riskienhallintapolitiikka antaa yrityksen vastuuhenkilöille ylätason toimintamallin, jonka toteuttamiseen koko yrityksen henkilökunta johdon lisäksi sitoutuu. Siinä määritellään riskienhallintaan liittyvät vastuut ja velvoitteet, varataan tarvittaviin resurssit ja määritetään mittaus- ja raportointikeinot.

Riskienhallintapolitiikasta ja riskienhallinnan toimintamallista tulee viestittää koko henkilöstölle, mutta myös monet ulkopuoliset sidosryhmät, kuten asiakkaat, alihankkijat ja tavarantoimittajat ovat kiinnostuneita yrityksen riskienhallinnan järjestämisestä.

Riskien käsittely

Riskien käsittelyllä pyritään saattamaan yrityksen toimintaa uhkaavat riskit halutulle tasolle käyttäen valittuja riskien hallintakeinoja. Kullakin riskillä tulee olla omistaja, joka vastaa siitä, että toimenpiteet toteutetaan ja että riskin tilaa mitataan ja seurataan. Usein se on liiketoiminnasta vastuussa oleva yksikkö.

Riskienhallinnan toimenpiteiden käytännön toteuttamisesta voi vastata jokin muukin taho kuin riskin omistaja. Se voi olla esimerkiksi talous- tai tietohallinto tai vaikkapa kunnossapitotoiminto. Käytännössä tämä tarkoittaa sitä, että riskien käsittelysuunnitelmat liitetään osaksi yrityksen johtamis- ja toiminta-prosesseja.

Seuranta ja raportointi

Riskienhallinnan toteuttaminen ja kehittäminen edellyttää prosessin jatkuvaa parantamista. Jatkuva parantaminen taas edellyttää johdon sitoutumista, resursseja, joustavaa yrityskulttuuria, virheistä oppimista ja omalle yritykselle sopivien työkalujen ja mittareiden käyttöä.

Riskien mittaaminen ja seuranta on parhaimmillaan systemaattista toimintaa, jonka tavoitteena on varmistaa että riskien hallintakeinot ovat vaikuttavia ja tehokkaita. Seurannalla saadaan lisätietoa riskeistä

ja voidaan analysoida tapahtumia sekä muita turvallisuushavaintoja. Lisäksi säännöllisen seurannan avulla havaitaan ulkoisen ja sisäisen toimintaympäristön muutokset ja tunnistetaan uudet tai muuttuneet riskit.

Kokonaisvaltaista riskienhallintaa tulisi toteuttaa jatkuvana prosessina, eikä suinkaan yhtenä erillisenä projektina. Hyvät käytännöt ovat osoittaneet, että kokonaisvaltaisen riskienhallinnan toimintamalli voidaan integroida osaksi yrityksen liiketoiminnan suunnitteluprosesseja tai vuosisuunnittelua. Tällä tavoin kokonaisvaltaisesta riskienhallinnasta saadaan myös merkittäviä hyötyjä.

Lisätietoja:

Riskienhallinnan toteuttamisessa huomioitavista periaatteista löytyy lisätietoa esimerkiksi kansainvälisistä standardeista:

SFS-ISO 31000. Riskienhallinta. Periaatteet ja ohjeet

SFS-EN IEC 31010:2019 – Riskienhallinta. Riskien arviointimenetelmät