VAHTI 1/2017 Ohje riskienhallintaan

SISÄLLYSLUETTELO:

1 Johdanto

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) tuottaman riskienhallintaohjeen tavoitteena on tehostaa ja yhdenmukaistaa riskienhallintaa ministeriöissä, virastoissa, laitoksissa sekä muualla julkisessa hallinnossa. Tällä ohjeella uudistetaan ”VAHTI 7/2003 Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa” vastaamaan paremmin kyber-, tietosuoja- ja tietoturvauhkien tuomiin haasteisiin ja toisaalta digitalisaation tuomiin mahdollisuuksiin.

Valtioneuvoston tietoturvallisuutta koskevan periaatepäätöksen 26.11.2009 mukaan yksi keskeisimpiä kokonaisturvallisuuden kehittämiskohteita on uhka- ja riskiarvioinnin menetelmien kehittäminen ja jatkuva riskienhallintatyö. Asetus tietoturvallisuudesta valtionhallinnossa (681/2010) tuli voimaan 1.10.2010 ja valtion virastojen oli täytettävä siinä määritetyt tietoturvallisuuden perustason vaatimukset 30.9.2013 mennessä. Yksi näistä vaatimuksista velvoittaa valtionhallinnon viranomaisen huolehtimaan sen toimintaan liittyvien tietoturvallisuusriskien kartoittamisesta. Riskienhallintaohje auttaa tässä ja edistää samalla myös yhteiskunnan turvallisuusstrategian ja Suomen kansallisen kyberturvallisuusstrategian toimeenpanoa.
.
Tällä ohjeella yhtenäistetään riskienhallinnan käytäntöjä koko valtionhallinnossa ja sitä voidaan soveltaa myös muussa julkishallinnossa sekä yksityisellä sektorilla. Jokainen organisaatio vastaa kuitenkin aina itse omista riskien käsittelyä koskevista päätöksistään ja niiden perusteella tehtävistä toimenpiteistä.

Ohjeen on laatinut VAHTI:n asettama työryhmä, jossa ovat toimineet seuraavat jäsenet:

Ari Uusikartano, ulkoasiainministeriö, puheenjohtaja
Matti Aitta, oikeusministeriö
Pyry Heikkinen, Tulli
Juho Isohanni, Väestörekisterikeskus
Katri Järvinen, Puolustusvoimat
Erja Kinnunen, Verohallinto
Tuija Lehtinen, Maanmittauslaitos
Pauli Paatsola, KEHA-keskus
Juha Pietarinen, Valtiokonttori
Riitta Pirhonen, valtiovarainministeriö
Tuomas Rouhunkoski, Maaseutuvirasto
Kimmo Rousku, valtiovarainministeriö, varapuheenjohtaja
Kari Santalahti, sisäministeriö
Niina Sipiläinen, sosiaali- ja terveysministeriö
Arto Kangas, Netum Oy, työryhmän sihteeri.

VAHTI-johtoryhmä on hyväksynyt tämän luonnoksen kokouksessaan 15.12.2016 lähetettäväksi lausuntokierrokselle.

2 Riskienhallinta johtamisen ja päätöksenteon välineenä

Riskienhallintaan kuuluvat organisaation toimintaympäristö, johdon hyväksymät, toimintaohjeet ja -mallit sekä riskienhallintapolitiikka ja -prosessi.

Riskienhallinta
Toiminto, jolla johdetaan ja ohjataan organisaation riskejä.

Riski tarkoittaa epävarmuuden vaikutusta tavoitteisiin, poikkeamaa odotetusta. Vaikutus voi olla myönteinen tai kielteinen odotettuun verrattuna.

Riskienhallinnan tarkoituksena on mahdollistaa organisaation menestyminen, toiminnan jatkuvuuden takaaminen ja tavoitteiden saavuttaminen. Tähän liittyy myös epävarmuuden huomioon ottaminen. Epävarmuus on usein uhka tai vaara, josta voi seurata jotakin negatiivista tai toiminnan kannalta epäedullista. Se voi tarkoittaa myös positiivista mahdollisuutta ja onnistumisen kautta tulevaa hyötyä tai etua, mikäli epävarmuustekijät pystytään minimoimaan tai niiltä osataan välttyä.

Riskienhallinta on osa johtamisen ja toiminnan prosesseja sekä suunnittelua ja seurantaa. Tavoitteena on, että organisaatiolla on päätöksentekoa varten ajantasainen, oikea ja riittävän kattava käsitys riskeistä sekä selkeästi määritellyt riskienhallinnan vastuut ja seurantajärjestelmä.

Kuva 1. *Riskienhallinnan viitekehys.* Jokainen organisaatio vastaa itse omista riskien käsittelyä koskevista päätöksistään ja niiden perusteella tehtävistä toimenpiteistä. *(Kuvan lähde: soveltaen ISO 31000.)*

2.1 Riskienhallinta toiminnan kehittämisen tukena ja mahdollistajana

Strategiseen suunnitteluun ja tavoitteiden asettamiseen liittyy usein odotuksia, paljon oletuksia ja suuri määrä epävarmuuksia, jotka kaikki kytkeytyvät joko olemassa olevaan tai uuteen toimintaympäristöön sekä sen mahdollisiin muutoksiin. Riskienhallinnan avulla voidaan arvioida, millaisia riskejä organisaatio on valmis ottamaan strategisten tavoitteiden asettamisessa ja miten niitä hallitaan tavoitteiden saavuttamiseksi. Esimerkiksi tulossopimuksissa ja vuosisuunnitelmissa voidaan kuvata riskienhallinnan toteuttamista ja seurantaa.

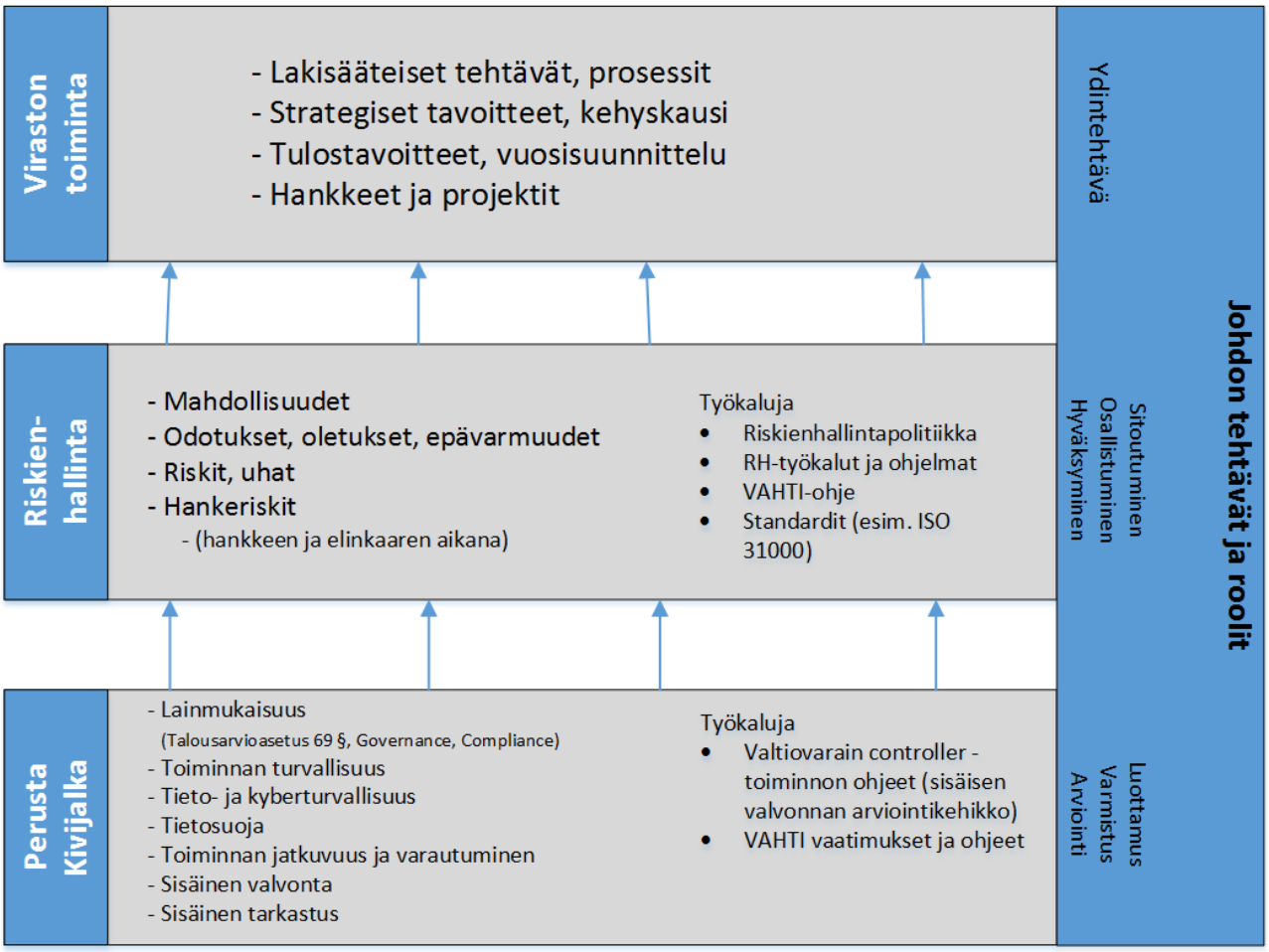
Hyvällä riskienhallinnalla varmistetaan myös hankkeiden ja projektien onnistuminen. Hankkeen tai projektin aikaisten riskien lisäksi mukaan on otettava riskit, jotka vaikuttavat hankkeessa tavoiteltavan lopputuloksen onnistumiseen ja lopputulokselle asetettujen tavoitteiden saavuttamiseen.

Tavoitteiden saavuttaminen ja toiminnan onnistuminen edellyttävät riittävien toimintaedellytysten olemassaoloa.

Riskienhallintapolitiikka
Organisaation päättämät, kuvaamat ja dokumentoimat riskienhallintaan liittyvät periaatteet ja tavoitteet. Riskienhallintapolitiikka -dokumentista voidaan käyttää myös nimitystä riskienhallinnan periaatteet.

Turvallisuuden osa-alueista tähän kuuluvat mm. toiminnan turvallisuus, tieto-, kyber- ja laajemmin digitaalinen turvallisuus, tietosuoja sekä toiminnan jatkuvuus ja varautuminen. Riskienhallinnalla on tämän vuoksi hyvin keskeinen rooli myös organisaation arjen jatkuvan toiminnan sekä vaatimustenmukaisuuden takaamisessa. Sisäinen valvonnan avulla varmistetaan talouden ja toiminnan laillisuus ja tuloksellisuus sekä varojen ja omaisuuden turvaaminen. Johto vastaa sisäisen valvonnan asianmukaisuudesta. Sisäinen tarkastus arvioi sisäisen valvonnan ja riskienhallinnan asianmukaisuutta ja riittävyyttä.

Seuraavassa kuvassa on havainnollistettu viraston toiminnan ja riskienhallinnan yhteys sekä johdon tehtäviä ja rooleja. Tavoitteiden saavuttaminen ja toiminnan onnistuminen edellyttää kunnossa olevaa perustaa sekä toimivaa riskienhallintaa. Johto on näiden edistämisessä keskeisessä asemassa.

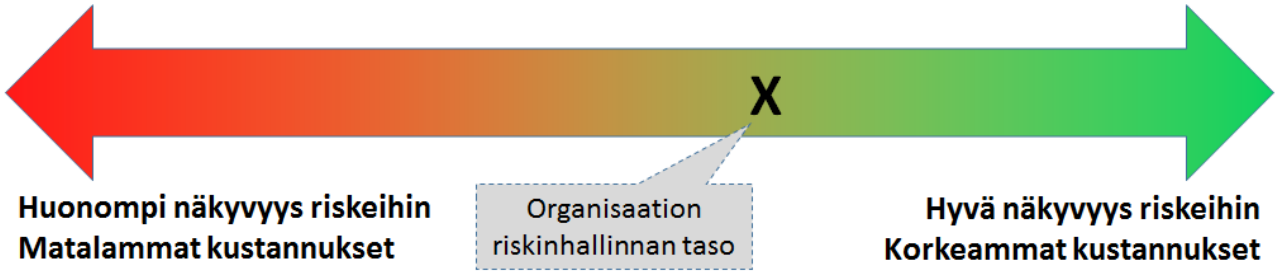


Kuva 2. *Johdon tehtävät ja roolit riskienhallinnassa. Käytettävissä olevat resurssit sekä niiden ohjaaminen ja kehittäminen vaikuttavat olennaisesti riskienhallinnassa onnistumiseen.*

Riskienhallinnan tulee olla avointa ja kattavaa. Tämä tarkoittaa, että riskien olemassaolo tulee tiedostaa ja tunnistaa sekä huolehtia siitä, että organisaation eri tasoilla olevilla päätöksentekijöillä, asiantuntijoilla ja sidosryhmillä on riittävästi tietoa riskeistä. Riskit eivät katoa ne sivuuttamalla tai huomioimatta jättämisellä. Toiminnan tukena olevien perusasioiden kuten turvallisuuden hallinnan ja jatkuvuussuunnittelun tulee olla kunnossa. Riskienhallinta auttaa asianmukaisten tavoitteiden asettamisessa ja saavuttamisessa sekä varmistaa tehtävissä onnistumisen; siis organisaation menestymisen.

2.2 Epävarmuuksien hallitseminen – uhkat ja mahdollisuudet

Riskienhallinnalla pyritään hallitsemaan epävarmuuksien vaikutuksia toimintaan. Täydellinen hallinta on mahdotonta, joten organisaatio tai toiminto määrittelee ain joko tietoisesti tai tiedostamattaan oman riskienhallintansa tason ja panostukset siihen. Riskienhallinnan on tuotettava havaittavissa olevaa lisäarvoa organisaation toiminnalle, minkä vuoksi esimerkiksi hallintatoimenpiteiden vaikutukset tulee olla mitattavissa.



Kuva 3. *Riskienhallinnan taso. Organisaatio määrittelee itse, mille tasolle se riskienhallintansa määrittelee.*

Riskienhallinnassa on keskeistä määritellä arvioinnissa löydetyille merkittävimmille riskeille tarvittavat hallintatoimenpiteet ja vastuut sekä varmistaa sovittujen hallintatoimenpiteiden eteneminen. Torjuminen esimerkiksi pidättäytymällä riskejä sisältävästä toiminnasta on tehokas uhkilta suojautumistoimenpide, mutta toiminnasta pidättäytyminen voi johtaa samalla myös positiivisten mahdollisuuksien menettämiseen. Yleisin suojautumistoimi on riskien lähteeseen vaikuttaminen siten, että riskien suuruutta tai sen merkitystä pienennetään. Samankaltainen vaikutus saavutetaan myös vaikuttamalla riskien todennäköisyyteen, jolloin myös riskin pienenemisen seurauksena onnistumisten mahdollisuudet voivat kasvaa.

Riskinsietokyky
Riskin suuruus, johon organisaatio on valmis sitoutumaan riskien määrittelyn jälkeen.

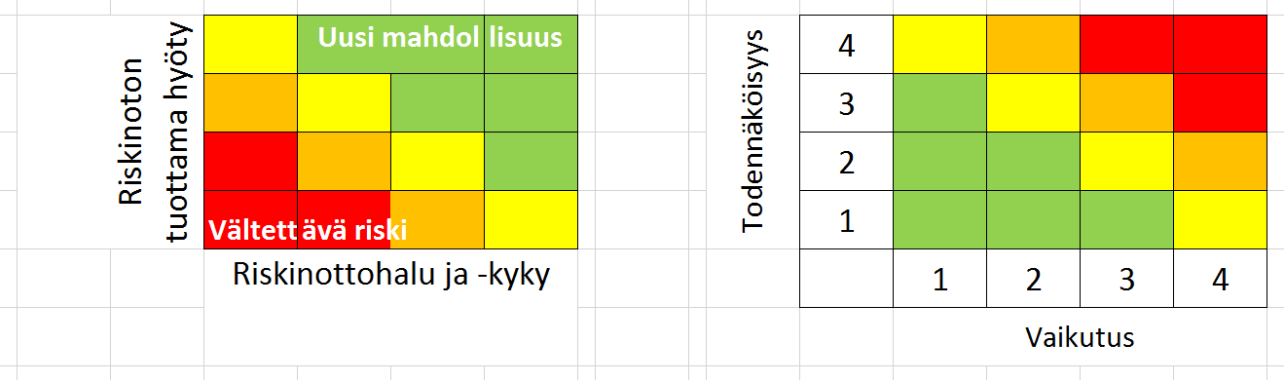
On paljon riskejä, joita ei voi mitenkään poistaa. Riskien mahdollisiin seurauksiin voidaan kuitenkin varautua etukäteen ja siten vaikuttaa mahdollisuuteen selvitä toteutuvien riskien haitallisista vaikutuksista. Riskejä voidaan myös jakaa toisen osapuolen kanssa, jolloin niiden toteutumisen vaikutukset jäävät pienemmiksi.

Riskit voidaan jättää myös käsittelemättä, mikäli suojautumistoimenpiteet eivät pienentäisi riskejä tai niiden arvioidaan olevan siedettävissä. Joihinkin riskeihin sisältyy myös mahdollisuuksia, jolloin niitä voidaan ottaa tietoisesti tai jopa lisätä.

Riskinottohalu
Riskin määrä, jonka organisaatio on valmis ottamaan pyrkiessään asettamiinsa tavoitteisiin.

Hallintatoimenpiteiden jälkeen voimaan jääviä riskejä, joihin ei voida tai haluta enää vaikuttaa, kutsutaan jäännösriskeiksi, Organisaatiolla pitää olla johtoryhmätason hyväksymä menetelmä jäännösriskien käsittelemiseksi ja niiden nostamiseksi myös johtoryhmän käsiteltäväksi.

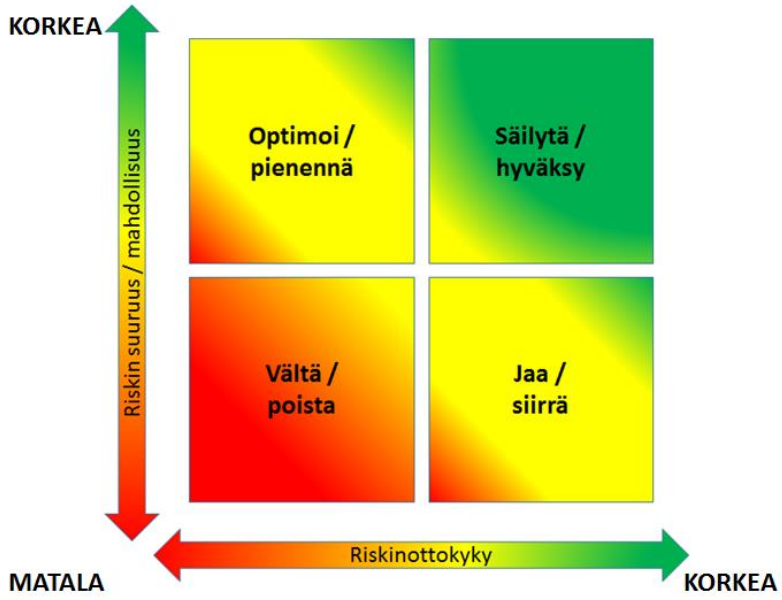
Epävarmuuksissa uhkia ja mahdollisuuksia: Perinteinen uhkien tarkastelunäkökulma:



Kuva 4. *Riskimatriisien vaihtoehtoja. Epävarmuudet voivat sisältää uhkien lisäksi myös mahdollisuuksia (vasen riskimatriisi).*

Riskien arvioinnissa on mahdollista tunnistaa niihin liittyvissä epävarmuustekijöissä myös positiivisia mahdollisuuksia. Tällöin riskin ottaminen riskinottokyvyn puitteissa voi tuottaa merkittäviä hyötyjä (kuva 4. riskimatriisi vasemmalla). Riskit, joiden ottamista tulee välttää, sisältävät useimmiten esimerkiksi ei-toivottuja operatiivisia ja vahinkotekijöitä. Näitä pääsääntöisesti uhkia sisältäviä ja haittoihin tai vahinkoihin johtavia seikkoja voi arvioida myös perinteisellä mallilla (kuva 4. riskimatriisi oikealla).

Riskienhallinnan toimenpiteiden tärkein tavoite ei aina ole poistaa tai edes pienentää kaikkia mahdollisia riskitekijöitä. Riskienhallinta voi myös auttaa organisaatiota tunnistamaan riskeihin sisältyviä mahdollisuuksia, tarvittaessa säilyttämään valittuja riskejä ja jopa lisäämään riskinottoa riskinottokykynsä puitteissa.

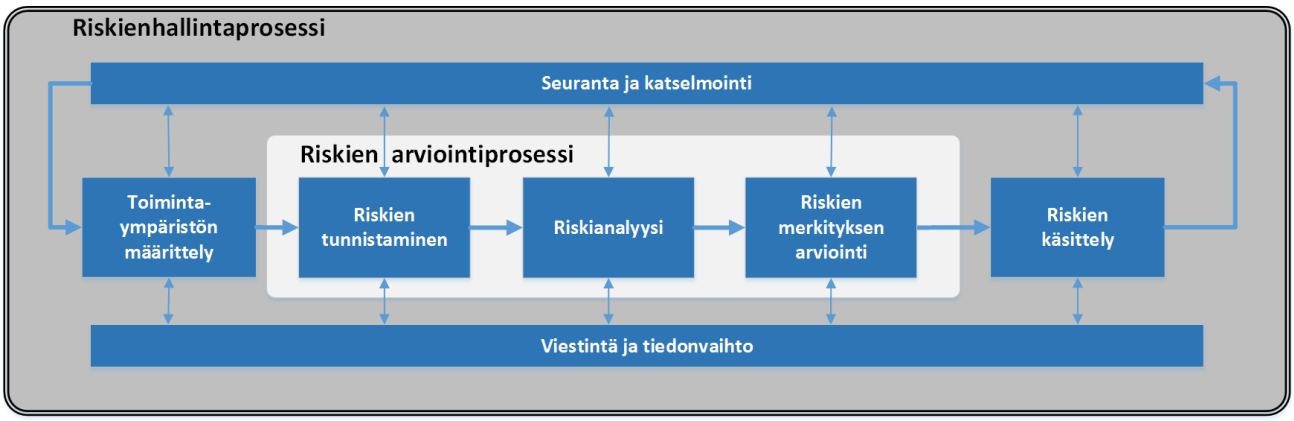


Kuva 5. *Kun riskinottokyky on pieni, on suurta uhkaa sisältäviltä riskeiltä suojauduttava. Vastaavasti kyvyn ollessa korkea on mahdollisuuksia sisältäviä riskejä helpompi sietää.*

3 Riskienhallintaprosessi

Riskienhallintaprosessi kattaa kaikki riskeille tehtävät toimenpiteet. Prosessissa noudatetaan johdon hyväksymiä riskienhallinnan toimintaohjeita ja –malleja sekä riskienhallintapolitiikkaa

Onnistunut riskienhallinta on aktiivista ja reagoi muutoksiin. Riskienhallintaa on toteutettava säännöllisesti ja sitä on kehitettävä määrätietoisesti sekä tarkoituksenmukaisesti.

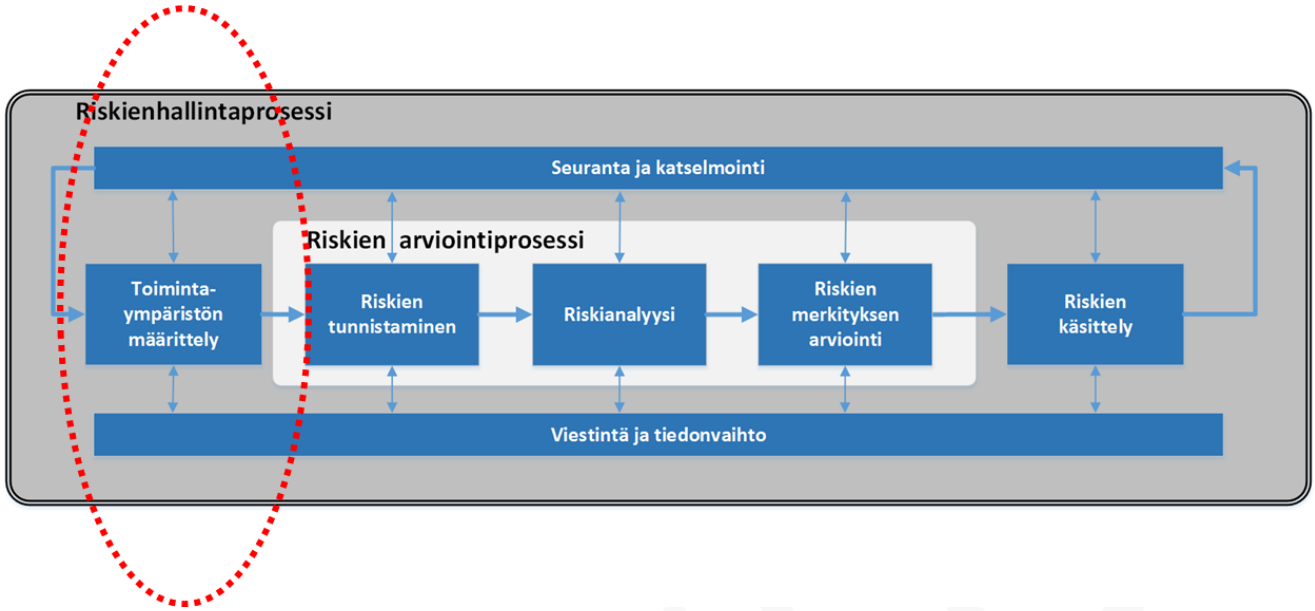


Kuva 6. *Riskienhallintaprosessi. Prosessin vaiheet ovat toimintaympäristön määritteleminen, arviointiprosessi ja tunnistettujen riskien käsittely, joista jokaiseen liittyy seuranta ja katselmointi sekä viestintä ja tiedonvaihto. (Kuvan lähde: ISO 31000.)*

3.1 Riskienhallinnan toimintaympäristön määritteleminen

Riskienhallintaprosessissa toimintaympäristön määrittely-vaiheessa tehdään riskien arvioinnin kannalta keskeiset rajaukset siitä, mitä sisällytetään riskien arviointiin ja mitä jätetään sen ulkopuolelle. Merkittävimpien riippuvuuksien tunnistaminen on myös välttämätöntä. Toimintaympäristön määrittelyn yhteydessä riskien arvioinnin kohde tarkentuu.

Toimintaympäristön määrittely
Ulkoisten ja sisäisten muuttujien sekä riskienhallintapolitiikan kattavuuden ja riskikriteerien määritteleminen.



Kuva 7. *Toimintaympäristön määrittely. Tämä vaihe tehdään ennen riskienarvioinnin toteuttamista. (Kuvan lähde: ISO 31000, muokattu.)*

Toimintaympäristön määrittelyssä otetaan huomioon ja tehdään päätökset seuraavista reunaehdoista:

- Mahdolliset syyt ja seuraukset ja miten niitä mitataan
- todennäköisyyden määrittelevät ajat, rajat ja muut tarvittavat reunaehdot
- käytettävät riskitasot ja miten riskejä tulee käsitellä
- mahdolliset riskien yhdistelmät ja miten niitä tulee ottaa huomioon.

Toimintaympäristön määrittelyssä rajataan	Toimintaympäristön määrittelyn tuloksena
• ulkoinen toimintaympäristö • sisäinen toimintaympäristö • riskienhallintaprosessin toimintaympäristö kokonaisuudessaan • riskikriteerit (miten riskejä hallitaan ja miten niitä siedetään eri tilanteissa)	• riskien tunnistamisessa tiedetään tarkemmin, mitä riskejä sisällytetään riskienhallintaan • riskien analysoinnissa osataan suhteuttaa riskien todennäköisyydet ja vaikutukset paremmin • riskien merkityksen arvioinnissa pystytään tekemään valintoja ja päätöksiä riskien käsittelyä varten.

3.2 Riskien arviointiprosessi

Arviointiprosessi on organisaation sopima ja johdon hyväksymä yhteinen menetelmä, jota käytetään riskien arviointiin. Arviointiprosessi sisältää seuraavat vaiheet:

- tunnistaminen
- analyysi
- merkityksen arviointi.

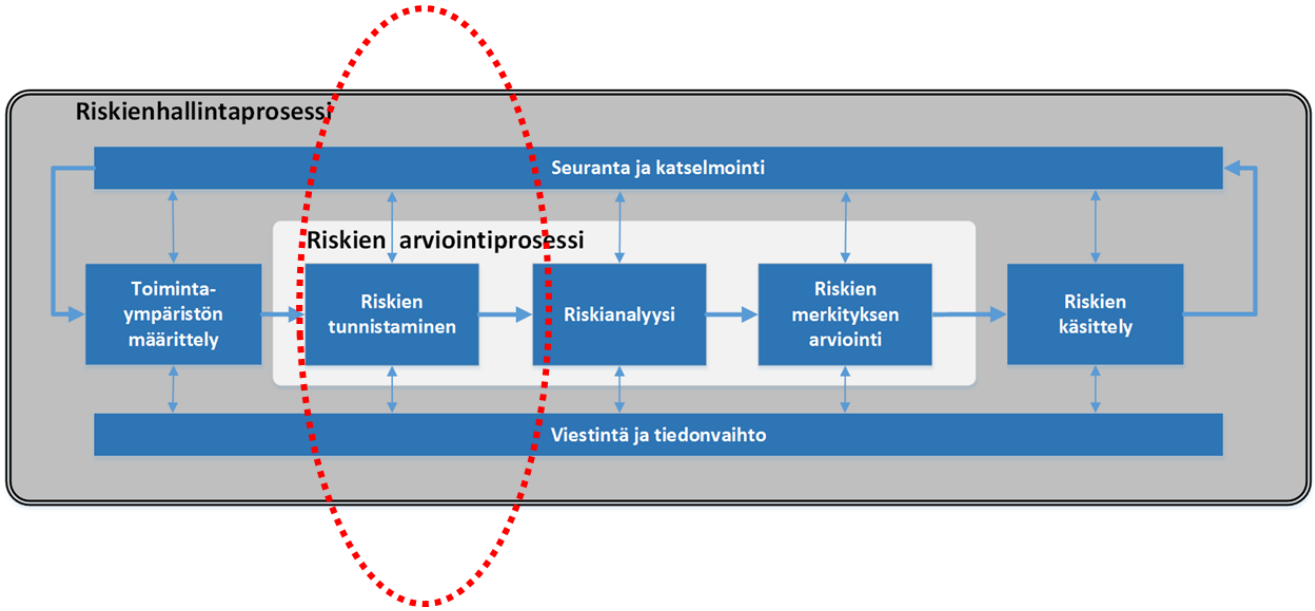
Prosessin vaiheiden on lopulta johdettava riskien käsittelyyn eli riskeihin kohdistettaviin toimenpiteisiin.

Riskien tunnistaminen				Riskianalyysi		Riskin merkityksen arviointi		Riskin käsittely				Lisätietoja
Riskin tunniste	Riskiluokka	Riski (riskin nimi)	Riskin kuvaus (mistä riski johtuu, mitä voi tapahtua toteutuessa):	Todennäköisyys	Vaikutus	Riskin suuruus (T x V)	Toimenpidetarpeet riskin käsittelylle (vakavuus/sietokyky)	Toimenpide-ehdotukset riskin käsittelylle	Toimenpiteiden vapaamuotoinen (sanallinen) kuvaus	Vastuuhenkilö	Tavoiteaikataulu (mihin mennessä	
St01	1 Strateginen	Raaka-aine (kahvi) loppuu.	Ei ole käyty kaupassa tai automaattinen raaka-aineen tilatiedottaminen ei toimi. Kahvia on voitu myös varastaa.Asiakas ei saa hänelle luvattua (odottamaansa) kahvia ajallaan ja kieltäytyy sopimuksen allekirjoittamisesta.	4 Lähes varma	4 Kriittinen	16 Sietämätön riski	4 Huomioitava riski	4 Vaatii välittömiä toimenpiteitä	Luotava prosessi tai tehtävä, jolla riski ehkäistään. Liittyy St02, Hr01 ja Hr02.	Kalevi Keittiövastaava	Yhden (1) viikon kuluessa.	
St02	1 Strateginen	Suodatinpaperi loppuu.	Ei ole käyty kaupassa tai automaattinen raaka-aineen tilatiedottaminen ei toimi. Suodatinpaperit on voitu myös rikkoa tai varastaa.Asiakas ei saa hänelle luvattua (odottamaansa) kahvia ajallaan ja kieltäytyy sopimuksen allekirjoittamisesta.	4 Lähes varma	3 Merkittävä	12 Sietämätön riski	4 Huomioitava riski	4 Vaatii välittömiä toimenpiteitä	Luotava prosessi tai tehtävä, jolla riski ehkäistään. Liittyy St01, Hr01 ja Hr02.	Kalevi Keittiövastaava	Yhden (1) viikon kuluessa.	
St03	1 Strateginen	Vedenjakelukatkos.	Vedenjakelun keskeytyksestä ei ole tiedotettu. Tai jos on tiedotettu, on unohdettu varata kahvinkeittoon tarvittavaa vettä. Asiakas ei saa hänelle luvattua (odottamaansa) kahvia ajallaan ja kieltäytyy sopimuksen allekirjoittamisesta.	3 Todennäköinen	2 Kohtalainen	6 Merkittävä riski	3 Huomioitava riski	3 Luotava suunnitelma pienentämiseksi	Hankittava riittävästi termospulloja, jotta vaikutuksia voidaan pienentää. Liittyy St03.	Timo Pomottaja, työnjohto	Kuukauden kuluessa.	
St04	1 Strateginen	Sähkönjakelukatk	Suunniteltu (tiedotettu) tai	2	2	4	1	1	Riski tiedoksi	Timo Pomottaja	Puolivuosittain	

Kuva 8. *Esimerkki riskiarvioinnista. Tässä ohjeessa on käytetty havaintoesimerkkinä kuvitteellista kahvinkeitin-tapausta, joka on kokonaisuudessaan liitteessä kuusi.*

3.2.1 Riskien tunnistaminen

Tunnistamisen tavoite on havaita ja kuvata kaikki merkittävät riskit ja mahdollisuudet, riskien lähteet, vaikutusalueet, tapahtumat, mukaan lukien olosuhteiden muutokset ja niiden syyt sekä mahdolliset seuraukset. Tunnistamiseen osallistuvien henkilöillä on oltava tarkasteltavan toiminnan riittävä asiantuntemus. Tunnistamisessa on otettava huomioon organisaatioon vaikuttavat tekijät riippumatta siitä, onko riskien lähde organisaation itsensä hallinnassa.



Kuva 9. *Riskien tunnistaminen. Riskejä tunnistettaessa ne kirjataan mahdollisimman kattavasti. (Kuvan lähde: ISO 31000, muokattu.)*

Riskien tunnistaminen sisältää seuraavat vaiheet:

- tunnistetaan tekijät, jotka voivat estää, haitata tai viivästyttää tavoitteiden saavuttamista
- tunnistetaan myös mahdollisuuksien menettämisestä tai hyödyntämättä jättämisestä aiheutuvat riskit, joiden seurauksena voidaan menettää tilaisuus tuloksellisempaan ja tehokkaampaan toimintaan
- luodaan riskeistä ja mahdollisuuksista kattava luettelo sellaisten tapahtumien perusteella, jotka voivat mahdollistaa tai estää asetettujen tavoitteiden saavuttamista tai sellaisten tapahtumien perusteella, jotka voivat parantaa, haitata, nopeuttaa tai viivästyttää niitä
- kirjataan luetteloon riskit riippumatta siitä, onko niiden lähde organisaation hallinnassa ja myös siinä tapauksessa, että lähde tai syy ei ole selvillä.

Riskiluokka määritellään organisaatiossa valitun jaottelun mukaisesti. Riskit voidaan jakaa luokkiin esimerkiksi seuraavasti (lisää esimerkkejä on liitteessä viisi):

- strategiset, joilla on vaikutusta esimerkiksi tavoitteiden saavuttamiseen
- operatiiviset, joilla on vaikutusta esimerkiksi toiminnan tai palvelun laadun toteutumiseen
- taloudelliset, joilla on vaikutusta esimerkiksi rahoitukseen sekä yleensä talouteen ja varojen käyttöön
- vahinkoriskit, joilla on vaikutusta esimerkiksi käytössä oleviin resursseihin (ihmiset, koneet ja laitteet, toimitilat, ym.).

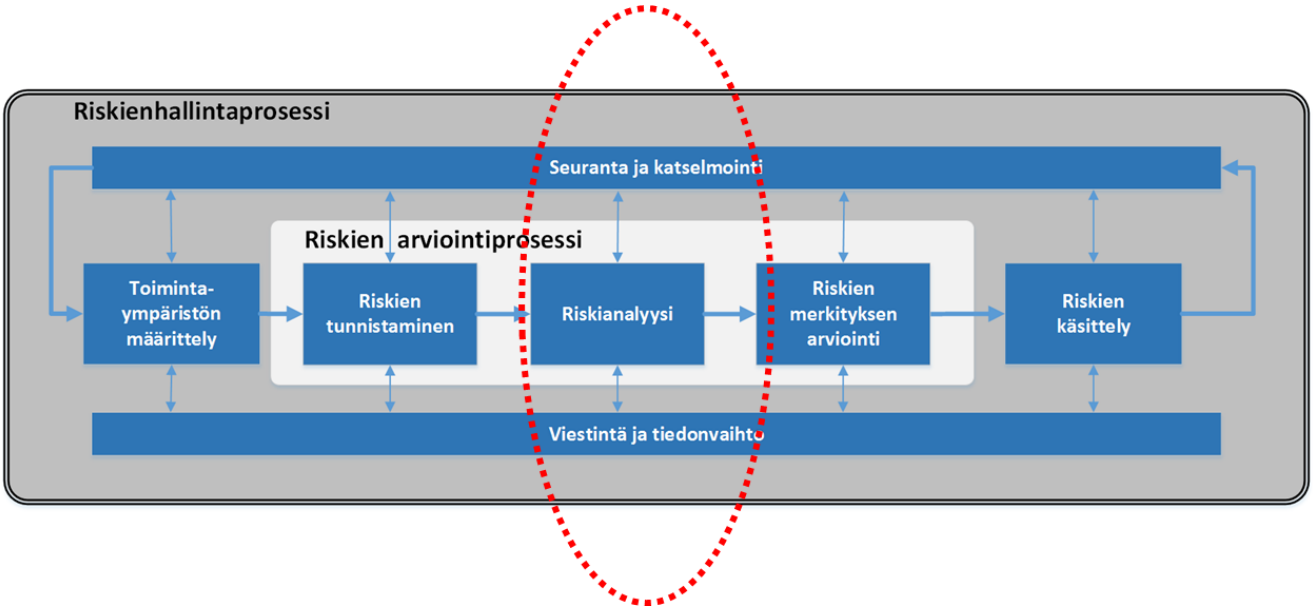
Riskien tunnistamisen yhteydessä	**Riskien tunnistamisvaiheen tuloksena**
• kirjataan kaikki olennaiset riskit • havaitaan mahdollisesti myös uusia ja aiemmin tunnistamattomia riskejä • tunnistetaan mahdolliset riippuvuuksista johtuvat riskit	• muodostuu työ-/asialista niistä riskeistä, joiden todennäköisyyttä ja vaikutusta tulee arvioida analyysivaiheessa • tiedetään tarkemmin toimintaa uhkaavat ja vaarantavat riskitekijät • tulevat esiin myös ne riskit, jotka sisältävät aikaisemmin tunnistamattomia mahdollisuuksia

3.2.2 Riskianalyysi

Analyysin avulla luodaan perusta päätöksille siitä, mitä ja miten riskejä käsitellään. Analyysissä arviot todennäköisyydestä ja vaikutuksista perustuvat osallistujien subjektiivisiin näkemyksiin, jolloin voi olla vaikea muodostaa yhteistä käsitystä riskin tasosta. Sen vuoksi on tärkeää kirjata mahdolliset mielipiteisiin tai muihin epävarmuustekijöihin perustuvat seikat riittävän selkeästi myöhemmin tapahtuvaa päätöksentekoa varten. Analyysi voi perustua kvantitatiiviseen (määrällinen, numeerisesti esitettävään) tai kvalitatiiviseen (laadulliseen, kuvailevaan esitykseen) tarkasteluun tai niiden yhdistelmään.

Riskianalyysi
Todennäköisyys: 1. Epätodennäköinen 2. Mahdollinen 3. Todennäköinen 4. Lähes varma
Vaikutus: 1. Vähäinen 2. Kohtalainen 3. Merkittävä 4. Kriittinen

Strategisten riskien ja uusien mahdollisuuksien arviointi perustuu monissa tapauksissa kvalitatiiviseen tarkasteluun. Riskienoton tuottamaa hyötyä voidaan arvioida esimerkiksi taloudellisilla, toiminnallisilla tai laadullisilla kriteereillä. Riskinottohalua ja -kykyä voidaan arvioida esimerkiksi meneillään olevilla muilla uudistuksilla tai hankkeilla, käytettävissä olevilla resursseilla ja osaamisella sekä taloudellisilla mahdollisuuksilla.



Kuva 10. *Riskianalyysi. Arvioitavana ovat riskin luonne ja suuruus. (Kuvan lähde: ISO 31000, muokattu.)*

Operatiiviset ja vahinkoriskit voidaan usein analysoida arvioimalla riskien toteutumisen todennäköisyyttä ja niiden vaikutuksia. Todennäköisyyden ja vaikutuksen arvioinnissa käytetään yleensä ennalta määrättyä asteikkoa.

Esimerkki analyysiasteikosta:

- Todennäköisyyden arviointi, esimerkkinä neliportainen asteikko:
    1. **Epätodennäköinen:** Tapahtuma toteutuu vain poikkeuksellisissa oloissa. Mahdollisuus toteutumiseen on tällöin enimmäkseen teoreettinen. Esimerkiksi silloin, kun riskin ei tiedetä aikaisemmin toteutuneen.
    2. **Mahdollinen:** Tapahtuma saattaa toteutua joissakin olosuhteissa tai tapauksissa. Tapahtuma on toteutunut joskus omassa organisaatiossa tai muualla.

3. **Todennäköinen:** Tapahtuman tiedetään tai odotetaan toteutuvan mitä suurimmalla todennäköisyydellä.
4. **Lähes varma:** Tapahtuma toteutuu tai on toteutunut usein ja on tapahtunut useita ”läheltä piti”-tilanteita.

- Vaikutuksen arviointi, esimerkkinä neliportainen asteikko:

1. **Vähäinen:** Riskin toteutumisesta voi aiheutua vähäistä haittaa strategisen tavoitteen saavuttamiselle. Toteutumisella on vähäinen vaikutus organisaation toimintaan.

2. **Kohtalainen:** Riskin toteutuminen viivästyttää tai heikentää selvästi mahdollisuuksia saavuttaa yhtä tai useampia strategisista tavoitteista. Seuraus tai tapahtuma, jonka vuoksi ei tarvitse keskeyttää toimintaa, mutta saatetaan joutua muuttamaan toiminnallisia suunnitelmia. Tapahtumasta voi aiheutua vähäisiä kustannuksia. Maine luotettavana toimijana vaarantuu.

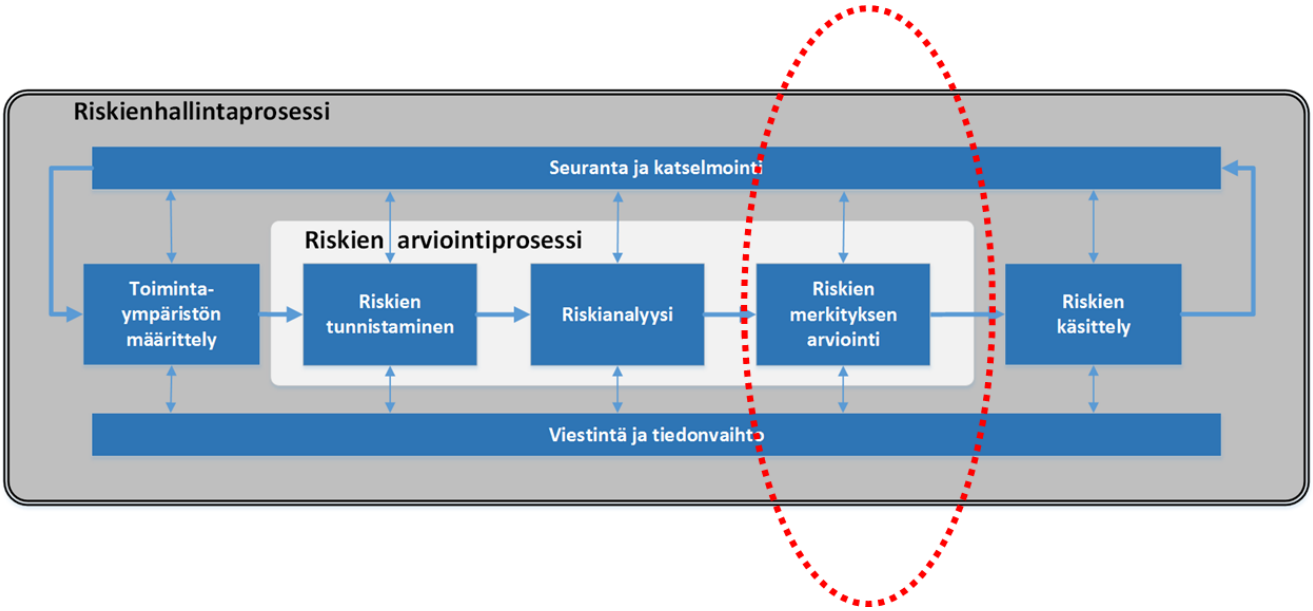
3. **Merkittävä:** Riskin toteutuminen vaikeuttaa, hidastaa tai muutoin vaarantaa merkittävällä tavalla tärkeän strategisen tavoitteen saavuttamisen. Toteutuminen voi aiheuttaa merkittävää vahinkoa tai kustannuksia. Seuraus tai tapahtuma, jonka vuoksi toiminta joudutaan keskeyttämään, tai tapahtuman seurauksena aiheutuu vähäistä suurempia kustannuksia. Tapahtumasta voi aiheutua myös omaisuuden rikkoontumista. Yksittäisten ihmisten terveys tai henki voi vaarantua. Maine luotettavana toimijana heikentyy merkittävästi.

4. **Kriittinen:** Riskin toteutuminen estää tai keskeyttää kokonaan esimerkiksi toiminnan kannalta tärkeän strategisen tavoitteen saavuttamisen tai jonkin organisaation tuottaman kriittisen prosessin tai palvelun. Toteutumisesta voi seurata suurta vahinkoa tai kustannuksia myös muille. Seuraus tai tapahtuma, jonka vuoksi toiminta joudutaan keskeyttämään ja se estyy pitkähköksi ajaksi. Tapahtumasta voi aiheutua merkittäviä kustannuksia organisaation tai valtionhallinnon näkökulmasta katsottuna. Suuren ihmisjoukon terveys tai henki vaarantuu ja sillä voi olla vaikutusta laajalti koko yhteiskunnan toimintaan. Suomen maine tai asema kansainvälisissä yhteyksissä vaarantuu.

Riskejä analysoitaessa:	**Riskien analysoinnin tuloksena:**
• on mahdollista muodostaa käsitys siitä, mitä riskejä voi ottaa, miten usein tai todennäköisesti jokin riski voi toteutua • saadaan muodostettua käsitys siitä, mitä riskin ottamisesta tai toteutumisesta voi seurata	• on kirjattuna yhteinen (paras saatavilla oleva) näkemys riskikohtaisista todennäköisyyksistä ja vaikutuksista • on luotu perusta riskien merkityksen arvioinnille eli päätöksenteolle siitä, mitä riskeille tullaan tekemään tai jätetään tekemättä.

3.2.3 Riskien merkityksen arviointi

Merkityksen arvioinnin tavoitteena on auttaa tekemään päätöksiä, mitä riskejä on tarpeen käsitellä ja mikä on käsittelyn tärkeysjärjestys. Arvioinnin yhteydessä voi käydä ilmi, että jotkut riskit täytyy arvioida uudelleen tai että tarvitaan muu täydentävä analyysi. Merkityksen arvioinnin yhteydessä voidaan päättää, että joitakin havaittuja riskejä ei käsitellä.



Kuva 11. *Riskien merkityksen arviointi. Kuvassa mainittujen vaiheiden lisäksi merkityksen arvioinnin yhteydessä päätetään mahdollisista täydennys- tai uudelleenarviointitarpeista. (Kuvan lähde: ISO 31000, muokattu.)*

Riskin suuruuden perusteella muodostuu tarve käsittelylle ja toimenpiteitä vaativalle päätöksenteolle esimerkiksi seuraavasti:

- **Kriittinen tai ei siedettävissä oleva riski.** Tällainen riskitekijä vaatii yleensä välittömiä toimia.
- **Merkittävä tai nopeasti toimenpiteitä vaativa riski.** Yleensä tämänkaltaiselle riskille on luotava suunnitelma, jolla sitä hallitaan, esimerkiksi sen pienentämisen osalta.
  Huomioitava tai seurattava riski. Välittömät toimenpiteet eivät ole välttämättömiä, mutta riskiä ja sen kehittymistä on seurattava.
- **Ei riskiä tai hyvin matala riski.** Ei vaadi välittömiä toimenpiteitä.

- **Jäännösriski.** Sellainen riski tai riskin osa, joka jää tehtyjen toimenpiteiden jälkeen voimaan, vaikka riskin vaikutusta tai todennäköisyyttä on pienennetty.

- **Otettava riski.** Riski, joka halutaan ottaa uusien mahdollisuuksien saavuttamiseksi.

Merkityksen arvioinnissa tulisi ottaa huomioon seuraavaa:

- **Ajan vaikutus.** Vähäiseltä tuntuvan riskin merkitys voi ajan kuluessa muuttua olennaisesti. Riski voi pienentyä tai kasvaa.

- **Psykologiset tai inhimilliset vaikutukset.** Näiden muuttujien vuoksi esimerkiksi erilaisten riskien sieto-, käsittely- tai tunnistamiskyky voi vaihdella yksilöittäin.

- **Riippuvuudet.** Riskit voivat olla toisistaan riippuvaisia, jolloin kerrannaisvaikutukset voivat olla sekä uhkina että mahdollisuuksina merkittäviä. Riippuvuus voi olla myös riskin alkuperästä johtuva ja liittyä useisiin eri osapuoliin. Sidosryhmiin kuuluvilla osapuolilla voi olla suuri vaikutus riskin todennäköisyyteen ja vaikutusten laajuuteen.

Riskien merkitystä arvioitaessa	Merkityksen arvioinnin tuloksena
• päätetään, mitä riskien suhteen tehdään • arvioidaan toimenpiteiden tärkeyttä ja kiireellisyyttä	• käytettävissä on työlista tehtävien vastuuttamista ja tavoiteaikataulujen asettamista varten

3.3 Riskien käsittely

Käsittelyprosessissa päätetään riskikohtaisista toimenpiteistä. Toimenpiteille nimetään vastuulliset (tekijä ja tekemisen valvoja, vrt. myös vastuukuvauksia ja vastuurooleja selventävä RACI-malli, liite 4). Käsittelyvaihtoehdot ovat useimmiten seuraavia (vrt. samaan riskiin voi kohdentua yksi tai useampi vaihtoehto):

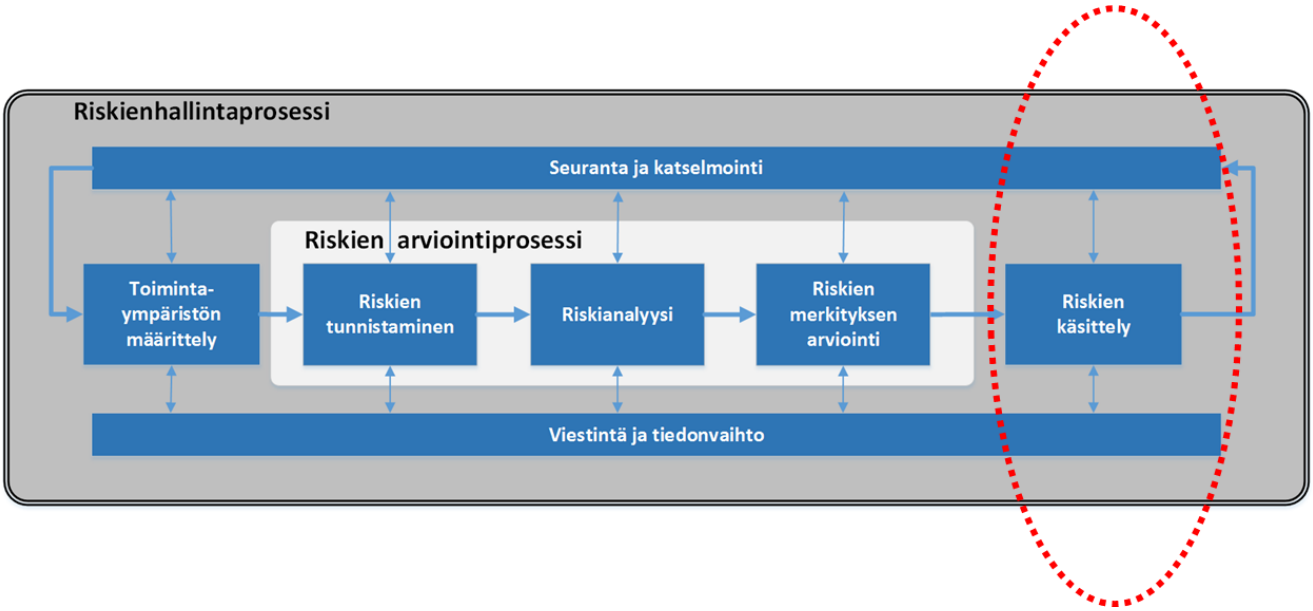
- torjuminen, esim. pidättäytymällä riskejä aiheuttavasta toiminnasta
- riskin ottaminen tai lisääminen jonkin mahdollisuuden saavuttamiseksi
- riskin syyn poistaminen
- riskin toteutumisen todennäköisyyteen vaikuttaminen
- riskin toteutumisen seurauksiin varautuminen tai vaikuttaminen
- riskin jakaminen osittain tai kokonaan yhden tai useamman osapuolen kesken
- tilanteen säilyttäminen sellaisenaan.

Yhteen riskiin voi kohdentua näistä yksi tai useampi toimenpide. Käsittelyn on oltava säännöllisesti toistuva prosessi, jossa päätetään toimenpiteet ja vastuulliset riskeille ja linjataan mahdollisten jäännösriskien sietämisestä.

Riskien käsittelyssä on otettava huomioon myös se, että käsittelyprosessi itsessään voi aiheuttaa uusia riskejä. Esimerkiksi käsittelytoimenpiteiden epäonnistuminen tai tehottomuus voi synnyttää uusia riskejä.

Riskienhallintaa tukee riskienkäsittelysuunnitelman laatiminen, sen toteuttaminen ja säännöllinen seuranta. Suunnitelmasta käytetään usein myös nimitystä riskisalkku. Suunnitelman pääkohdiksi valitaan usein mm.

- riskit ja niiden käsittelytavat
- suunnitelman hyväksyjätahot ja toteuttamisvastuulliset
- riskeille tehtävät toimenpiteet
- käsittelyn tavoiteaikataulut, raportointi ja seuranta.



Kuva 12. *Riskien käsittely. Sovittujen toimenpiteiden toteuttamista on valvottava aktiivisesti. (Kuvan lähde: ISO 31000, muokattu.)*

Riskien käsittelyssä päätetään	Riskien käsittelyvaiheen tuloksena
• riskien omistajat • riskienhallintatoimenpiteet • toteutusaikataulut • valvontavastuut	• kokonaisnäkemys riskeistä, niiden tasosta, käsittelytoimenpiteistä, vastuista ja aikataulusta

3.4 Riskien seuranta, katselmointi ja viestintä

Riskienhallintakeinojen vaikuttavuus ja tehokkuus varmistetaan seurannan ja katselmoinnin avulla. Niiden on oltava suunniteltu osa riskienhallintaprosessia ja vastuut on määriteltävä ja viestittävä selvästi. Seurantaan ja katselmointiin kuuluu valvontaa ja tarkastuksia, joita voidaan tehdä määrävälein tai tapauskohtaisesti.

Seurantaan ja katselmointiin sisältyvät toimintaympäristön sisäisten ja ulkoisten muutosten, riskien muutosten ja riskikriteerien muutostarpeiden havaitseminen. Riskienhallintaprosessissa muodostuvan dokumentaation ja tallenteiden tulee olla jälkikäteen todennettavissa. Tämä on tärkeää organisaation oppimisen, kustannusten seurannan ja säädösperusteisten toimien osoittamisen kannalta.

Riskien seurannassa ja katselmoinnissa	Seurannan ja katselmoinnin tuloksena
• arvioidaan riskienhallinnan ja riskien käsittelyn tavoitteiden onnistumista	• voidaan puuttua tilanteisiin, joissa riskit ovat vaarassa jäädä käsittelemättä • tiedetään, miten organisaation riskienhallinnassa onnistutaan

Riskien tunnistaminen, analysointi ja niiden merkityksen arviointi edellyttävät arvioinnin kohteena oleviin riskeihin ja toimintaympäristöön liittyvien osapuolten välistä viestintää. Myös riskien käsittely edellyttää niihin liittyvien osapuolten välistä aktiivista ja säännöllistä tiedonvaihtoa niin kauan kuin riski on olemassa.

Riskienhallinnan viestinnässä	**Viestinnän tuloksena**
• varmistetaan jokaisessa vaiheessa olennaisten osapuolten kesken tarvittavasta tiedonvälityksestä	• tieto riskeistä tavoittaa tahot, joiden tulee olla niistä tietoisia • on mahdollista jakaa riskienhallinnassa ja riskien käsittelyssä tarvittavaa tietoa toimenpiteistä ja valvonnasta vastuullisten kesken

4 Riskienhallinnan viitekehyksiä ja apuvälineitä

Riskienhallinnan toteuttamiseen on löydettävissä apuvälineitä kaikenkokoisille organisaatioille ja erilaisiin käyttötarpeisiin.

Riskienhallinnan standardit Riskienhallinnan hallintamallin luomisessa ja kokonaisuuden ohjaamisessa organisaatio voi käyttää apunaan esimerkiksi kansainvälisiä standardeja, joissa kuvataan mm. hallintamalli, periaatteet ja hyvät käytännöt. Standardeja voidaan käyttää yleisinä tukikehikkoina ja prosessien sekä menetelmien kattavuuden arviointityökaluina. Standardin valintaa ja käyttöön ottamista ohjaavat esim. laatuun tai toimialaan perustuvat syyt. Tässä ohjeessa kuvattu prosessi pohjautuu ISO 31000-standardiin.	***Riskienarviointityökalu*** Tämän ohjeen liitteenä on yksinkertainen riskienarvioinnin työkalu käyttöohjeineen. Organisaatio voi käyttää omaa jo käytössään olevaa arviointityökalua ja menetelmiä. Liitteen työkalu on tarkoitettu ensisijaisesti niille organisaatioille, joilla ei vielä ole riskienarviointityökalua tai jotka ovat tyytymättömiä nykyiseen ratkaisuunsa.	***Riskienhallintasuunnitelma tai riskisalkku*** Riskienhallinta vaatii riskien käsittelyn ja niihin kohdistuvien toimenpiteiden seurannan koordinointia ja vertailua. Tämä koskee erityisesti suuria organisaatioita, joissa riskien arviointia tehdään organisaation eri osissa. Tällöin käytetään usein kokoavaa hallintasuunnitelmaa, josta voidaan käyttää nimitystä riskisalkku.
Riskienhallinta vuosikellossa Riskienhallinnan vuosittaiset toimenpiteet tulee kuvata vuosikelloon. Se voi olla organisaation toiminnan ja talouden suunnitteluun (TTS) tarkoitettu tai erillinen riskienhallintaa varten laadittu vuosikello.	***Riskienhallinnan ja arvioinnin apuvälineitä*** - riskienhallinnan standardit - keskeytysanalyysit - sovelluskehityksen riskienarviointimenetelmät - tietoriskien arviointimallit - riskienarviointityökalut - riskienhallinnan vastuiden kuvaamismallit - vuosikellot - riskisalkut	***Riskienhallinnan vastuukuvausmallit*** Riskienhallinnan vastuiden kuvaamisessa voi soveltaa esimerkiksi RACI-mallia. RACI-mallissa R tarkoittaa vastuullista (*responsible*), A vastuussa olevaa (*accountable*), C neuvojaa (*consulted*) ja I tiedotettavaa (*informed*) toimijaa tai osapuolta.
Tietoriskien arviointimallit Tietoihin ja tietojenkäsittelyyn liittyviä riskejä, ts.tietoriskejä, voidaan arvioida haastatteluin tarkastelemalla saatavuuteen, eheyteen ja luottamuksellisuuteen sekä kiistämättömyyteen liittyviä riskejä. Tietoriskien arviointien lisäksi kartoitetaan tarvittaessa teknisiä riskejä..	***Keskeytysanalyysit*** Organisaatio voi käyttää toiminnan jatkuvuussuunnittelun tukena keskeytys- ja vaikutusanalyysejä, joiden avulla kartoitetaan ja tarvittaessa myös arvioidaan pahimpia toiminnan keskeyttäviä, toimintaa häiritseviä tai muuten toimintaan haitallisesti vaikuttavia uhkia sekä niiden vaikutuksia laaja-alaisemmin sen toimintaan	***Sovelluskehityksen riskienarviointimenetelmät*** Sovelluskehityksen menetelmien ja prosessien arvioinnissa keskitytään mm. ohjelmistovirheistä tai inhimillisistä virheistä johtuvien riskien ja heikkouksien tunnistamiseen.

LIITTEET – erillinen tiedosto

LIITE 1 Riskienhallinnan käsitteitä
LIITE 2 Riskienhallintaan velvoittavia keskeisiä säädöksiä
LIITE 3 Riskienhallintapolitiikka ja puitteet
LIITE 4 Riskienhallinnan standardeja ja hyviä käytäntöjä
LIITE 5 Riskien luokittelu, arviointi ja käsittely – esimerkkejä ja menetelmiä
LIITE 6 Riskien toteutumisskenaarioita