Liite 1 Säädöksiä, määräyksiä, ohjeita

Hallintolaki (434/2003)

Hyvän hallinnon perusteet, 6-10 §

Laki valtion talousarviosta (423/1988), 24 b §

Sisäisen valvonnan järjestäminen ja johdon vastuu

- Viraston ja laitoksen on huolehdittava siitä, että sisäinen valvonta on asianmukaisesti järjestetty sen omassa toiminnassa sekä toiminnassa, josta virasto ja laitos vastaa.
- Sisäisen valvonnan järjestämistä johtaa ja sen asianmukaisuudesta ja riittävyydestä vastaa viraston ja laitoksen johto.

Asetus valtion talousarviosta (1243/1992)

Sisäisen valvonnan sisältö ja tavoitteet, 69 §:

- Viraston ja laitoksen johdon on huolehdittava asianmukaisista menettelyistä (sisäinen valvonta) talouden ja toiminnan laajuuteen ja sisältöön sekä niihin liittyviin riskeihin nähden.
- Menettelyillä varmistetaan talouden ja toiminnan laillisuus ja tuloksellisuus; varojen ja omaisuuden turvaaminen sekä johtamisen ja ulkoisen ohjauksen edellyttämät oikeat ja riittävät tiedot viraston ja laitoksen taloudesta ja toiminnasta.
- Menettelyiden on myös käsitettävä viraston tai laitoksen vastattavana tai välitettävänä olevien varojen hoito sekä ne viraston ja laitoksen toiminnot ja tehtävät, jotka se on antanut toisten virastojen ja laitosten, yhteisöjen tai yksityisten tehtäväksi tai joista se muuten vastaa.
- Palvelukeskuksen johto vastaa sisäisestä valvonnasta siltä osin kuin kirjanpitoyksikön tehtävät on palvelusopimuksella siirretty palvelukeskuksen tehtäväksi.

Viittaus yleisiin standardeihin ja suosituksiin, 69 a §

- Sisäisen valvonnan menettelyissä on otettava huomioon Euroopan yhteisön oikeudesta aiheutuvat viraston ja laitoksen toimintaan kohdistuvat vaikutukset sekä sisäistä valvontaa koskevat yleiset standardit ja suositukset.

Taloussäännön sisältö, 69 b §

- Taloussäännössä annetaan tarkemmat määräykset sisäiseen valvontaan ja siihen kuuluvaan riskienhallintaan vaikuttavista seikoista.

Kirjanpitoyksikön tilinpäätökseen kuuluvan toimintakertomuksen sisältö, 65 §

- Sisäisen valvonnan arviointi- ja vahvistuslausuma

Hallituksen vuosikertomuksen sisältö, 68 a § ja 68 b §

- Hallituksen vuosikertomuksen riskikatsaukset

Sisäisen valvonnan ja riskienhallinnan neuvottelukunta, 71 §

Valtiokonttorin määräys taloussäännön laatimisesta ja päivittämisestä (Dnro 481/03/2010, 23.11.2010)

- sisäisen valvonnan menettelyt, joilla johto pyrkii pitämään taloudenhoitoon liittyvät riskit hallittavalla tasolla

Valtiokonttorin ohje toimintakertomuksen laatimisesta (Dnro VK 510/03/2010, 30.11.2010)

- sisäisen valvonnan arviointi- ja vahvistuslausuma

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)

- asiakirjojen käsittelyä koskevat yleiset tietoturvallisuusvaatimukset
- tietoturvallisuuden toteuttaminen ml. toimintaan liittyvien tietoturvallisuusriskien kartoittaminen, 5 §

Työturvallisuuslaki (738/2002)

- työnantajan yleinen huolehtimisvelvoite, 8 §
- työn vaarojen selvittäminen ja arviointi, 10 §

[Viraston] riskienhallintaan liittyvät muut säädökset, määräykset, ohjeet ja asiakirjat

[*Tässä luetellaan mahdolliset muut riskienhallintaan liittyvät kansalliset tai EU-säädökset, kansainvälisistä sopimuksista tulevat määräykset, työjärjestys, taloussääntö, valtion varallisuuden ja vastuiden hallintaan liittyvät riskienhallinnan periaatteet, tietoturvaohjeet (esim. VAHTI-ohjeet), työturvallisuuden riskienhallintaoppaat, toimialakohtaiset riskienhallinnan erillisasiakirjat yms.]*

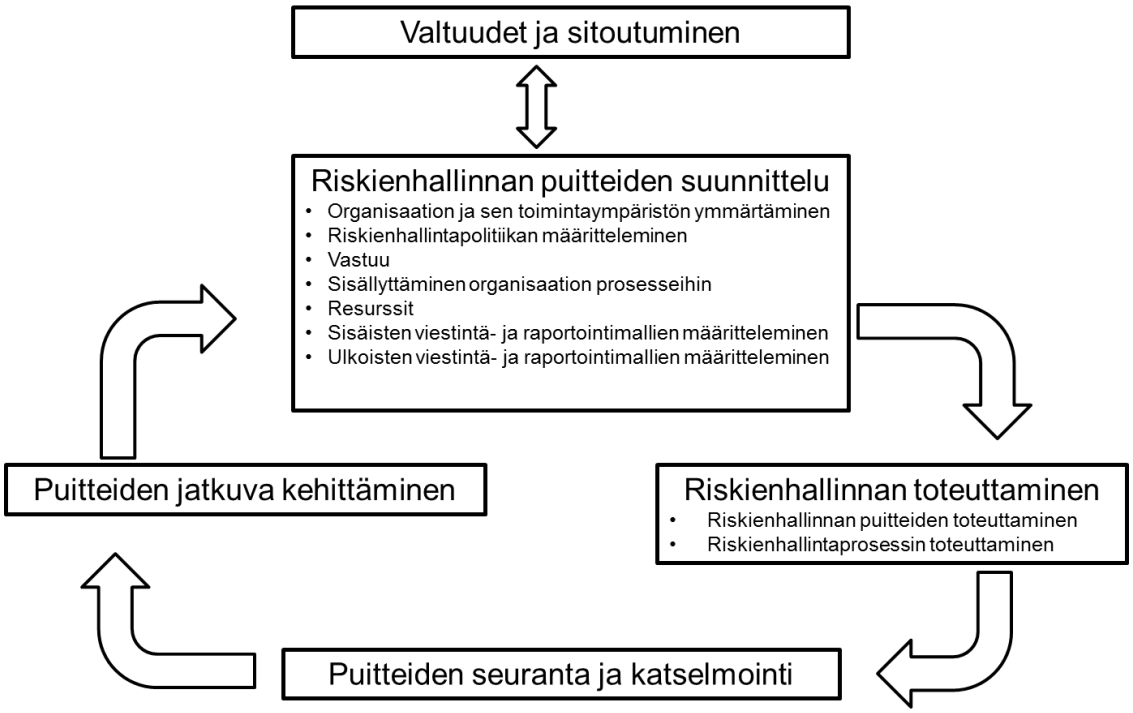
Liite 2 Käsitteiden määritelmät

[Seuraavassa hakemistossa on riskienhallinnan keskeisimpiä käsitteitä määrittelyineen. [Virasto voi valita itselleen olennaisimmat ja täydentää tarvittaessa.]

Jäännösriski	Riskiin käsittelyn jälkeen jäävä riski, jota ei voida tai ei haluta poistaa. Jäännösriskeihin voi sisältyä tunnistamattomia riskejä.
Riski	Epävarmuuden vaikutus tavoitteisiin. Vaikutus on poikkeama odotetusta. Vaikutus voi olla myönteinen tai kielteinen odotettuun vaikutukseen verrattuna.
Riskianalyysi	Prosessi, jolla pyritään ymmärtämään riskin luonne ja määrittämään riskitaso. Riskianalyysi on riskin merkityksen arvioinnin ja riskin käsittelyä koskevien päätösten perusta. Riskianalyysi sisältää riskin suuruuden arvioinnin.
Riskien arviointi	Kokonaisprosessi, joka kattaa riskien tunnistamisen riskianalyysin ja riskin merkityksen arvioinnin
Riskien käsittely	Riskin muokkaamisprosessi, jossa päätetään erimerkiksi seuraavista toimenpiteistä: - riskin torjuminen tai poistaminen päättämällä olla aloittamatta tai jatkamatta riskin aiheuttavaa toimintaa - riskin ottaminen tai lisääminen jonkin mahdollisuuden saavuttamiseksi - riskin lähteen tai syyn poistaminen - todennäköisyyden muuttaminen tai todennäköisyyteen vaikuttaminen - seurausten muuttaminen tai vaikutuksiin varautuminen - riskin jakaminen toisen osapuolen tai osapuolten kanssa - riskin säilyttäminen ja sietäminen tietoon perustuvalla päätöksellä
Riskien tunnistaminen	Riskien havaitsemisen ja kuvaamisen prosessi
Riskienhallinta	Koordinoitu toiminta, jolla organisaatiota johdetaan ja ohjataan riskien osalta.
Riskienhallintapolitiikka	Organisaation päättämät ja dokumentoimat riskienhallintaan liittyvät periaatteet ja tavoitteet.
Riskienhallintaprosessi	Hallintaperiaatteiden, -menettelyjen ja -käytäntöjen järjestelmällinen soveltaminen toimintaympäristön määrittelemiseen, riskien tunnistamiseen, analysointiin, arviointiin, käsittelyyn, seurantaan sekä viestintään ja tiedonvaihtoon.
Riskienkäsittelysuunnitelma	Johdon hyväksymä dokumentoitu riskien käsittelyn vastuutettu toimenpidesuunnitelma
Riskikriteerit	Säännöt, joiden perusteella riskin merkittävyys arvioidaan yhdenmukaisesti. Riskikriteerit perustuvat organisaation tavoitteisiin ja sen toimintaympäristöön. Riskikriteerit voivat olla johdettu standardeista, laeista,

	toimintaperiaatteista ja muista vaatimuksista.
Riskiluokitus	Arvioitavan kohteen luokittelun apuväline.
Riskimatriisi	Riskimatriisin avulla luokitellaan riskin suuruus tapahtuman seurausten vakavuuden ja esiintymisen todennäköisyyden perusteella. Matriisi auttaa hahmottamaan riskin merkittävyyttä ja miten riski sijoittuu suhteessa toisiin riskeihin.
Riskin hallintakeino	Riskiä muuttava toimenpide. Hallintakeinoja ovat kaikki riskiä muuttavat prosessit, toimintaperiaatteet, laitteet, käytännöt tai muut toimenpiteet. Hallintakeinoilla ei aina välttämättä ole haluttua tai oletettua muutosvaikutusta.
Riskin merkityksen arviointi	Prosessi, jossa riskianalyysin tuloksia riskikriteereihin vertaamalla määritetään, onko riski tai sen suuruus hyväksyttävä tai siedettävä. Riskin merkityksen arviointi auttaa riskin käsittelypäätöksissä.
Riskin omistaja	Henkilö tai taho, jolla on vastuu ja valtuudet hallita riskiä. Usein määritellään lisäksi riskitoimenpiteiden vastuuhenkilö, joka käytännössä seuraa ja koordinoi tiettyä riskiä.
Riskitaso	Riskin tai riskiyhdistelmien suuruus, joka ilmoitetaan seurausten ja niiden todennäköisyyden yhdistelmänä (esim. vaikutuksen ja todennäköisyyden tulo)
Sisäinen tarkastus	Sisäisen tarkastuksen tehtävä on selvittää johdolle sisäisen valvonnan asianmukaisuus ja riittävyys.
Sisäinen valvonta	Menettelyt, joilla varmistetaan - talouden ja toiminnan laillisuus ja tuloksellisuus; - varojen ja omaisuuden turvaaminen; - oikeat ja riittävät tiedot viraston ja laitoksen taloudesta ja toiminnasta.

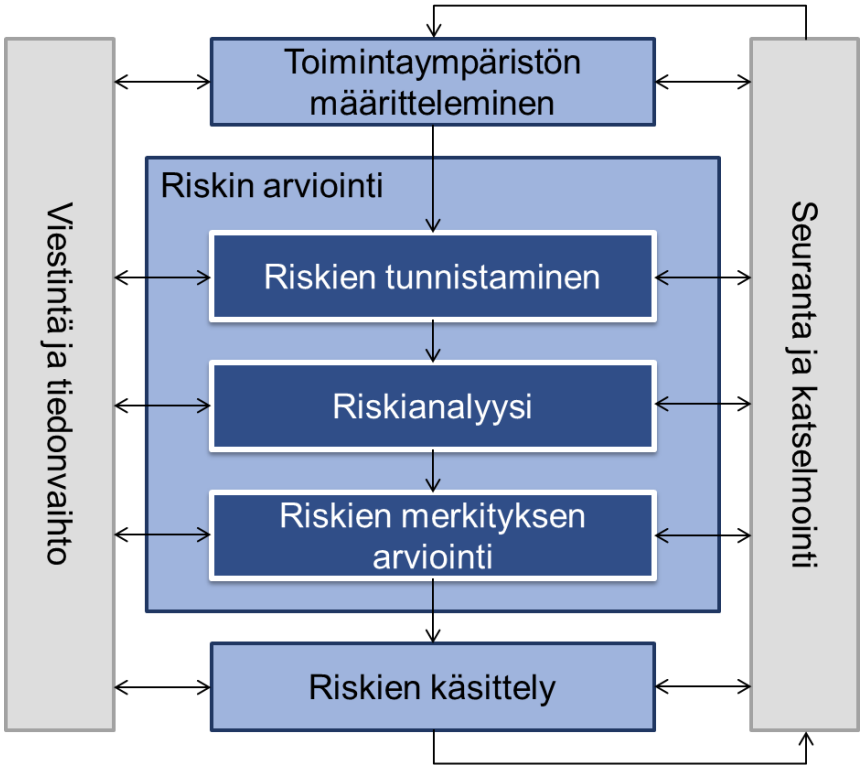
Liite 3 Riskienhallinnan puitteet



lähde: SFS-ISO 31000, SFS:n luvalla

Liite 4 Riskienhallintaprosessi

Seuraavassa on kuvattu *[viraston]* riskienhallintaprosessi. *[Viraston tulee sovittaa prosessi omaan riskienhallintaansa sopivaksi ja kirjata tarvittavat organisaatiokohtaiset ohjeet.]*



Kuva Riskienhallintaprosessi, SFS ISO 31000, SFS:n luvalla

1.1 Toimintaympäristön määritteleminen

Riskienhallintaprosessin toimintaympäristön määrittelyvaiheessa tehdään riskien arvioinnin keskeiset rajaukset, ts. mitä sisällytetään arviointiin ja mitä jätetään ulkopuolelle. Tässä vaiheessa määritellään myös riskikriteerit, joita hyödynnetään myöhemmässä vaiheessa riskien merkityksen arvioinnissa ja käsittelytapaa valittaessa. Näissä otetaan huomioon mm. strategia, tavoitteet, toimintaympäristö, sidosryhmät, säädökset ja muut vaatimukset. Riskikriteereissä määritellään myös, millä tasolla riskistä tulee hyväksyttävä tai siedettävä.

1.2 Riskien arviointi

Riskien arviointiin kuuluvat riskien tunnistaminen, riskianalyysi eli riskien todennäköisyyden ja vaikutusten analyysi, sekä riskien merkityksen arviointi.

1.2.1 Riskien tunnistaminen

Riskien tunnistamisvaiheessa tavoitteena on havaita kaikki merkittävät riskit ja niiden lähteet, vaikutusalueet, tapahtumat ja niiden syyt sekä mahdolliset seuraukset. Tässä kootaan tieto toimintaa ja tavoitteiden saavuttamista vaarantavista riskeistä sekä niistä riskeistä, jotka sisältävät mahdollisuuksia, joita ei ole aikaisemmin tunnistettu. Riskien tunnistamisessa tulee olla mukana riittävän laajasti asiantuntijoita kattavuuden varmistamiseksi.

Riskien tunnistamisvaiheessa saadaan aikaan luettelo niistä riskeistä, joiden todennäköisyyttä ja vaikutusta arvioidaan riskianalyysivaiheessa. Tunnistettujen riskien jäsentämiseksi käytetään luokittelua (liite 5): 1. Strategiset riskit, 2. Operatiiviset riskit, 3. Taloudelliset riskit, 4. Vahinkoriskit.

1.2.2 Riskianalyysi

Riskianalyysissa tavoitteena on muodostaa käsitys tunnistetuista riskeistä. Tässä vaiheessa tarkastellaan riskin syitä ja lähteitä, niiden myönteisiä ja haitallisia seurauksia sekä arvioidaan riskin toteutumisen todennäköisyyttä ja vaikutusta ennalta määritellyllä asteikolla (liite 6):

Todennäköisyys: 1. Epätodennäköinen, 2. Mahdollinen, 3. Todennäköinen, 4. Lähes varma.

Vaikutus: 1. Vähäinen, 2. Kohtalainen, 3. Merkittävä 4. Kriittinen.

Riskianalyysin tuloksena saadaan aikaan

- yhteinen näkemys riskikohtaisista todennäköisyyksistä ja vaikutuksista
- näkemys riskin toteutumiseen vaikuttavista tekijöistä ja riippuvuuksista; syystä, miksi riski voi toteutua
- perusta riskien merkityksen arvioinnille eli päätöksenteolle siitä, mitä riskeille tehdään tai jätetään tekemättä

1.2.3 Riskien merkityksen arviointi

Riskien merkityksen arvioinnin tavoitteena on auttaa tekemään päätöksiä, mitä riskejä on tarpeen käsitellä ja mikä on käsittelyn tärkeysjärjestys. Riskit saadaan järjestykseen todennäköisyyden ja vaikutuksen mukaan. Riskimatriisi (liite 7) auttaa hahmottamaan riskien merkittävyyttä ja sen arvioimista, onko riski hyväksyttävissä vai tarvitaanko käsittelyä.

Vaikka yksittäinen riski ei ole merkittävä, yhdessä toisen riskin kanssa siitä saattaa tulla merkittävä. Arvioinnissa tulee myös huomioida jo mahdollisesti tehdyt/suunnitellut toimenpiteet,

arvioida ovatko ne riittäviä, vai onko jäännösriski sellainen, että tulee miettiä muita toimenpiteitä riskin hallitsemiseksi.

Riskien merkityksen arvioinnista syntyy

- järjestetty luettelo riskeistä
- yhteinen näkemys käsiteltävistä riskeistä toimenpiteiden suunnittelemiseksi

1.3 Riskien käsittely

Riskien käsittelyssä määritellään jatkotoimenpiteet ja nimetään vastuullisen henkilöt sekä alustava tavoiteaikataulu. Tässä vaiheessa päätetään myös siitä, onko jäännösriskien taso siedettävä. Käsittelyvaihtoehtoja voivat olla:

- riskin torjuminen esim. pidättäytymällä riskiä aiheuttavasta toiminnasta
- riskin ottaminen tai lisääminen jonkin mahdollisuuden saavuttamiseksi
- riskin lähteen poistaminen
- riskin todennäköisyyden muuttaminen
- riskin vaikutusten muuttaminen
- riskin jakaminen toisten osapuolten kanssa
- riskin säilyttäminen tietoon perustuvalla päätöksellä

Yhteen riskiin voi kohdentua näistä yksi tai useampi.

Toimenpiteet, niiden tärkeysjärjestys, vastuut sekä aikataulut dokumentoidaan **riskienkäsittelysuunnitelmaan**. Toimenpiteiden tulee olla oikeassa suhteessa riskin kokoon nähden ja ne tulee toteuttaa oikealla organisaatiotasolla. Myös jäännösriskit dokumentoidaan, jotta niitä voidaan seurata ja tarvittaessa käsitellä uudelleen. Riskienkäsittelysuunnitelman hyväksyy viraston ylin johto. Merkittävimmät riskit ja niiden hallintatoimenpiteet tulee viedä asianomaisiin suunnitelmiin ja niiden seuranta seurantaraportteihin.

Riskien käsittelyn tuloksena syntyy

- kokonaisnäkemys riskeistä, niiden tasosta, käsittelytoimenpiteistä, vastuista ja aikataulusta

1.4 Seuranta

Seuranta ja katselmointi ovat tärkeä osa riskienhallintaprossin loppuun viemistä, jotta varmistetaan valittujen keinojen vaikuttavuus ja tehokkuus ja tiedetään, miten organisaation riskienhallinnassa onnistutaan. Tähän vaiheeseen sisältyvät toimintaympäristön sisäisten ja ulkois-

ten muutosten sekä riskien muutosten havaitseminen sekä riskikriteerien muutostarpeet. Seuranta- ja katselmointitoimet voivat olla määrävälein tapahtuvia tai tilannekohtaisia ja niihin liittyvät vastuut on määriteltävä.

Tässä vaiheessa voidaan puuttua tilanteisiin, joissa riskit ovat jäämässä käsittelemättä.

1.5 Viestintä ja tiedonvaihto

Riskien arviointi edellyttää toimintaympäristöön ja riskeihin liittyvien eri osapuolten välistä viestintää. Viestinnän ansiosta tieto riskeistä tavoittaa ne, joiden tulee olla niistä tietoisia, ja riskienhallinnassa ja riskien käsittelyssä tarvittavaa tietoa saadaan jaettua toimenpiteistä ja valvonnasta vastuullisten kesken. Riskienhallinnan viestintä tulee sisällyttää riskienkäsittely-suunnitelmaan.

Riskienhallinnan viestintään sisältyvät kaikki oleelliset riskit ja käsittelytoimet. Tähän kuuluu myös riittävä tiedonvaihto viraston, yhteiskumppaneiden ja sidosryhmien välillä. Viraston merkittävistä riskeistä ja riskienhallintatoimista raportoidaan tulosohjaajalle.

Liite 5 Riskiluokittelu

Riskien luokitus auttaa riskien kokonaisuuden hahmottamisessa. Seuraavassa on esitetty yleinen luokittelu, jota suositellaan käytettäväksi riskien arvioinnissa. *[Tarvittaessa virasto voi tarkentaa alajaotteluin tai käyttää muuta, viraston riskienhallintaa paremmin palvelevaa jaottelua.]*

1. Strategiset riskit

esim. strategia, toimintaympäristö, suhdannevaihtelut, säädösmuutokset, johtamisjärjestelmä, organisaatiorakenne, arvot, eettiset periaatteet, viestintä, maine, sidosryhmät, yhteistyökumppanit

2. Operatiiviset riskit

esim. toiminnan tavoitteet, toiminnan suunnittelu ja organisointi, päätösten toimeenpano, henkilöstö, prosessit, hankinnat, sopimukset, laatu, asiakkaat, toimitilat, työvälineet, teknologia, tiedon hallinta, tietojärjestelmät, tietoturva, kyberturvallisuus

3. Taloudelliset riskit

esim. rahoitus, budjetointi, talouden suunnittelu, varojen käyttö, omaisuus, taloudelliset vastuut, valtiontakaukset ja -takuut, talouden raportointi

4. Vahinkoriskit

esim. toimitilaturvallisuus, koneet, laitteet, työsuojelu, työterveys, tapaturmat, henkilöturvallisuus, matkustus, ympäristön pilaantuminen

Liite 6 Riskianalyysi: todennäköisyys ja vaikutus

Seuraavassa on esitetty yleiset arviointiasteikot. *[Tarvittaessa virasto voi tarkentaa tai käyttää muuta, viraston riskienhallintaa paremmin palvelevaa.]*

Riskin todennäköisyys

1. Epätodennäköinen: Tapahtuma toteutuu vain poikkeuksellisissa oloissa. Lähinnä teoreettisesti mahdollinen, ei tiedetä tapahtuneen.

2. Mahdollinen: Tapahtuma saattaa tapahtua joissakin tapauksissa. Tapahtuma on sattunut joskus meillä tai muualla.

3. Todennäköinen: Tapahtuma toteutuu tai on toteutunut usein tai on tapahtunut useita "läheltä piti" -tilanteita.

4. Lähes varma: Tapahtuman odotetaan toteutuvan mitä suurimmalla todennäköisyydellä.

Riskin vaikutus

1. Vähäinen: Riskin toteutumisesta voi aiheutua vähäistä haittaa strategisen tavoitteen saavuttamiselle.

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

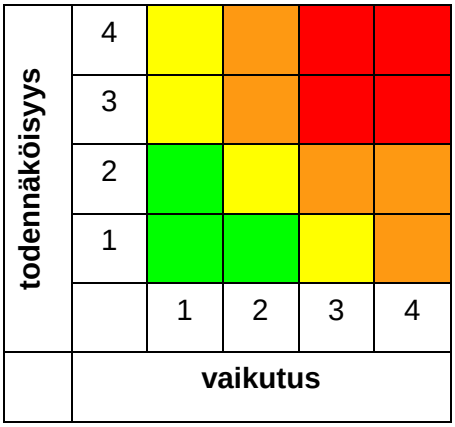
3. Merkittävä: Riskin toteutuminen vaikeuttaa, hidastaa tai muutoin vaarantaa merkittävällä tavalla tärkeän strategisen tavoitteen saavuttamista. Riskin toteutuminen voi aiheuttaa merkittävää vahinkoa tai kustannuksia. Seuraus tai tapahtuma, jonka vuoksi toiminta joudutaan keskeyttämään, taikka tapahtuman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

4. Kriittinen: Riskin toteutuminen estää tai keskeyttää kokonaan toiminnan kannalta tärkeän strategisen tavoitteen saavuttamisen. Riskin 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 koko valtionhallinnon näkökulmasta katsottuna. Suuren ihmisjoukon terveys tai ihmishenkiä

vaarantuu ja sillä voi olla vaikutusta laajasti koko yhteiskunnan toimintaan. Suomen maine tai asema kansainvälisissä yhteyksissä vaarantuu.

Liite 7 Riskimatriisi

Riskien tasoja voidaan kuvata matriisilla, johon riskit sijoittuvat todennäköisyyden ja vaikutuksen mukaan. Värit auttavat hahmottavaan riskien merkittävyyttä ja tarvittavia toimenpiteitä.



Riskitasosta voidaan johtaa käsittelyn tarve

Taso	**Käsittelyn tarve**
Kriittinen riski (riskiluku 9-16)	• vaatii yleensä välittömiä toimia • edellyttää jatkuvaa seurantaa
Merkittävä riski (riskiluku 4-8)	• tehtävä suunnitelma riskin pienentämiseksi • seurattava
Kohtalainen riski (riskiluku 3-4)	• ei välttämättä tarvita toimenteitä • seurattava riskiä ja sen mahdollista kehittymistä
Matala riski (riskiluku 1-2)	• ei vaadi akuutteja toimenpiteitä

Lisää matriiseja on mm. VAHTI-riskienhallintaohjeessa.

Liite 8 Riskienkäsittelysuunnitelma

Esimerkkitaulukko riskienhallintaprosessin tueksi ja riskienkäsittelysuunnitelmaksi.

Riskin nimi	Riskin kuvaus	Riski-luokka	Toden-näköi-syys	Vaikutus	Riskitaso	Käsittelyn tarve	Toimenpiteen kuvaus	Vastuu-henkilö	Aikataulu	Tilanne

Lisää aineistoa on mm. VAHTI-riskienhallintaohjeessa.

Riskienhallinnan viitemateriaalia

Riskikompassi www.riskikompassi.fi

SFS-ISO 31000 -standardi ”Riskienhallinta. Periaatteet ja ohjeet”

SFS, Tekninen raportti, ISO/TR 31004:fi ”Riskienhallinta. Ohjeita standardin ISO 31000 sovel-tamisesta.

COSO ERM –viitekehys: Committee of Sponsoring Organizations of the Treadway Commis-sion, Enterprise Risk Managemet – Integrated Framework

INTOSAIn hyvän hallinnon ohjeistus: International Organization of Supreme Audit Institutions, INTOSAI GOV 9130

VAHTI-ohjeet

Ohje riskienhallintaan, Valtiovarainministeriön julkaisuja 22/2017, http://urn.fi/URN:ISBN:978-952-251-862-0

Riskienhallintatyökalu - Excel - perusversio

Riskienhallintatyökalu - Excel - laajempi versio

Ohje riskienhallintatyökaluun