

Sisäisen valvonnan ja riskienhallinnan neuvottelukunta
Suositus x.x.2017

Valtionhallinnon riskienhallintapolitiikkamalli

luonnos 15.12.2016

Taustaa saatteeksi

Riskienhallinta on osa sisäistä valvontaa ja siten jokaisen valtion viraston lakisääteinen tehtävä. Sisäisen valvonnan järjestämisestä säädetään valtion talousarviosta annetussa laissa (423/1988). Sisäisestä valvonnasta ja riskienhallinnasta on tarkempia säännöksiä talousarvioasetuksessa (1243/1992).

Valtiovarainministeriön yhteydessä on valtioneuvoston asettama sisäisen valvonnan ja riskienhallinnan neuvottelukunta, jonka tehtävänä on seurata ja arvioida sisäisen valvonnan ja sen osana olevan riskienhallinnan järjestämisen tilaa ja menettelyitä valtionhallinnossa sekä tehdä aloitteita kehittämisestä. Neuvottelukunnasta säädetään talousarvioasetuksen 71 §:ssä.

Neuvottelukunta laati vuonna 2005 suosituksen valtionhallinnon hyvästä käytännöstä sisäisessä valvonnassa ja riskienhallinnassa. Valtiovarain controller -toiminto antoi 20.12.2005 suosituksen käyttää neuvottelukunnan laatimaa asiakirjaa ja sen sisältämää arviointikehikkoa sisäisen valvonnan ja riskienhallinnan kehittämisessä ja sisäisen valvonnan arviointi- ja vahvistuslausuman valmistelemissa. Arviointikehikon käyttö on vapaaehtoista, mutta suurin osa virastoista hyödyntää joko alkuperäistä tai siitä myöhemmin kehitettyä suppeampaa arviointikehikkoa.

Neuvottelukunta on sisäisen valvonnan ja riskienhallinnan tilaa ja kehittämistä seurattessaan tunnistanut tarpeen kehittää erityisesti valtionhallinnon yhteistä riskienhallintapolitiikkaa. Neuvottelukunta selvitti keväällä 2016 ministeriöistä riskienhallinnan tilaa ja riskienhallintapolitiikan tarvetta. Tilanne vaihtelee ministeriöiden välillä, mutta riskienhallinnan kehittämiseksi on kaivattu mm. yhteisiä menetelmiä ja malleja. Selvityksen tulosten perusteella neuvottelukunta päätti valmistella riskienhallintapolitiikan mallin, jota valtionhallinnon virastot voivat hyödyntää omassa riskienhallinnassaan sekä sen kehittämisessä.

Valmisteluprosessista tähän lisää myöhemmin, mm. miten valmisteltu, miten ministeriöitä ja virastoja kuultiin.

Riskienhallintapolitiikkamalli ja ohjeaineisto on käsittelyn tässä vaiheessa koottu yhdeksi asiakirjaksi. Aineisto viedään nettiin ja tarkempi toteutus suunnitellaan erikseen.

SISÄLLYS

Johdanto.....	4
RISKIENHALLINNAN JÄRJESTÄMINEN.....	5
1 Lähtökohdat.....	5
2 Riskienhallintapolitiikka ja sen tarkoitus	5
3 Riskienhallinnan suunnittelu ja vastuutus.....	6
4 Riskienhallinnan toteuttaminen.....	7
5 Riskienhallinnan seuranta ja kehittäminen	7
6 Riskienhallinnan viestintä ja raportointi	7
7 Sisäinen valvonta, riskienhallinta ja sisäinen tarkastus	8
RISKIENHALLINTAPOLITIIKKAMALLI	9
1 Soveltamisala	9
2 Säädöspohja sekä muut määräykset ja ohjeet.....	9
3 Riskienhallinnan keskeiset käsitteet.....	9
4 Riskienhallinnan tavoitteet.....	10
5 Riskienhallinnan periaatteet	10
6 Riskienhallinnan vastuut.....	11
7 Riskienhallintaprosessi.....	12
8 Riskienhallinnan arviointi ja kehittäminen	13
9 Voimaantulo ja allekirjoitukset	13
RISKIENHALLINTAPOLITIIKAN LIITTEET	14
Liite 1 Säädöksiä, määräyksiä, ohjeita	14
Liite 2 Käsitteiden määritelmät.....	16
Liite 3 Riskienhallinnan puitteet	18
Liite 4 Riskienhallintaprosessi.....	19
Liite 5 Riskiluokittelu	22
Liite 6 Riskianalyysi: todennäköisyys ja vaikutus.....	23
Liite 7 Riskimatriisi	24
Liite 8 Riskienkäsittelysuunnitelma	25
RISKIENHALLINNAN VIITEMATERIAALIA.....	26

JOHDANTO

Valtionhallinnon riskienhallintapolitiikkamallilla tuetaan riskienhallinnan kehittämistä virastoissa. Mallin tavoitteena on selkeyttää ja yhtenäistää riskienhallinnan käsitteitä, periaatteita, tavoitteita, organisointia, vastuuta ja toimintatapoja.

Riskillä tarkoitetaan epävarmuuden vaikutusta tavoitteisiin, poikkeamaa odotetusta; vaikutus voi olla myönteinen tai kielteinen odotettuun verrattuna. Riskienhallinta tarkoittaa koordinoitua toimintaa, jolla organisaatiota johdetaan ja ohjataan riskien osalta. Riskienhallinta on osa sisäistä valvontaa ja siten jokaisen valtion viraston lakisääteinen tehtävä.

Riskienhallinta on vakiintunut osaksi mm. suunnittelua ja seurantaa. Esimerkiksi julkisen talouden suunnitelmassa¹ on katsaus valtion taloudellisiin vastuisiin ja riskeihin, hallituksen vuosikertomuksessa² ministeriöt arvioivat toimintaympäristön ja toimialan keskeisimpiä riskejä ja toimintakertomuksissaan³ virastot ottavat julkisesti kantaa riskienhallinnan asianmukaisuuteen ja riittävyyteen (sisäisen valvonnan arviointi- ja vahvistuslausuma).

Riskienhallintaa on jo kehitetty monissa virastoissa. Keskeistä on, että riskienhallinta otetaan osaksi ohjaus- ja johtamisjärjestelmää, se kattaa koko toiminnan ja toimintamalli on yhtenäinen läpi koko organisaation. Tavoitteena on, että virastolla on ajantasainen, oikea ja riittävän kattava käsitys riskeistään päätöksentekoaan varten sekä selkeästi määritellyt riskienhallinnan vastuut ja seurantajärjestelmä. Lisäksi mallilla tavoitellaan yhtenäisyyttä virastojen kesken, jotta yhteistyö helpottuu ja samoja asioita ei tarvitse suunnitella jokaisessa virastossa alusta lähtien erikseen.

Riskienhallintapolitiikka määrittelee riskienhallinnan yleiset tavoitteet, vastuut ja toteutuksen keskeiset periaatteet. Virastoissa ja eri tehtäväalueilla voi lisäksi olla riskienhallintaa ohjaavaa ja tarkentavaa lainsäädäntöä, määräyksiä, ohjeita ja toimintamalleja, jotka tulee sisällyttää viraston riskienhallinnan kokonaisuuteen.

Valtionhallinnon riskienhallintapolitiikkamalli sisältää suositellut vähimmäisvaatimukset viraston riskienhallintapolitiikkaan. Tämän lisäksi viraston tulee riskienhallinnan menettelyissään ottaa huomioon toiminnan ja toimintaympäristön erityistekijät. Virasto voi harkita, laatiiko se erillisen riskienhallintapolitiikka-asiakirjan vai sisällyttääkö asiat muihin asiakirjoihin, esim. taloussääntöön tai työjärjestykseen.

Viraston johto vastaa viraston riskienhallinnasta ja sen tehtävä on vahvistaa riskienhallintapolitiikka. Johdon näkemys sisäisen valvonnan ja riskienhallinnan merkityksestä ja toimiminen esimerkkinä luo perustan hyvän hallinnon toimivuudelle koko organisaatiossa.

¹ <http://vm.fi/valtion-talouden-kehykset>

² <http://valtioneuvosto.fi/paatokset/hallituksen-vuosikertomukset>

³ <http://www.netra.fi>

RISKIENHALLINNAN JÄRJESTÄMINEN

1 Lähtökohdat

Riskienhallintaa tarvitaan varmistamaan strategian ja tavoitteiden toteutumista, toimintaedellytyksiä ja toiminnan jatkuvuutta. Lisäksi se voi auttaa tunnistamaan uusia toimintamahdollisuuksia. Riskienhallinnalla varmistetaan myös talouden ja toiminnan laillisuutta ja tuloksellisuutta sekä hyvää hallintotapaa.

Riskienhallinta on osa sisäistä valvontaa ja siten jokaisen valtion viraston lakisääteinen tehtävä. Sisäisen valvonnan järjestämisestä säädetään valtion talousarviosta annetussa laissa (423/1988). Sisäisestä valvonnasta ja riskienhallinnasta on tarkempia säännöksiä talousarvioasetuksessa (1243/1992).

Riskienhallinta on osa viraston⁴ johtamisen ja toiminnan prosesseja sekä suunnittelua ja seuranta. Päätöksentekoa varten tarvitaan ajantasainen, oikea ja riittävän kattava käsitys riskeistä. Riskienhallinta korostuu muutostilanteissa, kun luodaan uusia toimintamalleja ja luovutaan vanhoista.

Ministeriöiden riskienhallinnan tulee kattaa myös ohjauksessa olevista virastoista, talousarvion ulkopuolella olevista valtion rahastoista, valtion liikelaitoksista ja valtion-yhtiöistä ministeriölle mahdollisesti aiheutuvat riskit.

Riskienhallinnan toteutuksessa sovelletaan yleisesti hyväksyttyjä kansainvälisiä standardeja ja suosituksia. Yleisesti tunnettuja ovat mm. ISO 31000 -riskienhallintastandardi sekä COSO ERM⁵ -viitekehys.

Tässä asiakirjassa on tukeuduttu SFS-ISO 31000 -standardiin ”Riskienhallinta. Periaatteet ja ohjeet”⁶. Standardissa on kuvattu riskienhallinnan olennaiset elementit suhteellisen tiiviisti ja selkeästi ja siitä ja sen soveltamisohjeesta on Suomen standardisoimisliiton suomennos. Kyseistä standardia on käytetty monessa virastossa riskienhallinnan viitekehyksenä.

Riskienhallinnan onnistuminen riippuu järjestelyistä, joilla se sisällytetään organisaation toimintaan. Seuraavassa esitettävien suositusten tavoitteena on auttaa organisaatiota sisällyttämään riskienhallinta ja sen kehittäminen organisaation johtamisjärjestelmään. Suositusten viitekehyksenä on käytetty standardissa esitettyjä riskienhallinnan puitteita (kuva liitteenä 3).

2 Riskienhallintapolitiikka ja sen tarkoitus

Riskienhallintapolitiikassa määritellään viraston riskienhallinnan tavoitteet, periaatteet, vastuut ja keskeiset menettelyt. Sen avulla varmistetaan ja tuetaan sitä, että

⁴ Tässä asiakirjassa käytetään yksinkertaisuuden vuoksi termiä virasto tarkoittamaan ministeriöitä, kirjanpitoyksiköinä toimivia virastoja ja laitoksia sekä tulosohtajattuja virastoja ja laitoksia. Myös talousarvion ulkopuolella olevat valtion rahastot sekä erilaiset ohjelmat ja hankkeet voivat tarpeidensa mukaan hyödyntää mallia.

⁵ Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management – Integrated Framework

⁶ Suomen standardisoimisliitto SFS Standardi SFS-ISO 31000, vahvistettu 2011-05-10

riskienhallinta otetaan osaksi ohjaus- ja johtamisjärjestelmää, se kattaa koko toiminnan ja toimintamalli on yhtenäinen läpi koko organisaation.

Virastoissa ja eri tehtäväalueilla voi olla riskienhallintaa ohjaavaa ja tarkentavaa lainsäädäntöä, määräyksiä, ohjeita ja toimintamalleja, jotka tulee sisällyttää viraston riskienhallinnan kokonaisuuteen ja ottaa huomioon riskienhallintapolitiikassa. On viraston harkinnassa, laaditaanko erillinen riskienhallintapolitiikka-asiakirja vai sisällytetäänkö sen elementit muihin asiakirjoihin, esim. taloussääntöön tai työjärjestykseen.

Viraston johto vastaa riskienhallinnasta ja sen tehtävä on vahvistaa riskienhallintapolitiikka. Johdon näkemys sisäisen valvonnan ja riskienhallinnan merkityksestä ja toimiminen esimerkkinä luo perustan hyvän hallinnon toimivuudelle koko organisaatiossa.

Riskienhallintapolitiikan käytäntöön vienti vaatii pitkäjänteistä työtä, mm. riskienhallinnan tavoitteiden ja periaatteiden viestintää, jotta henkilöstö on niistä tietoinen, sekä riskienhallinnan osaamisen kehittämistä osana henkilöstökoulutusta.

3 Riskienhallinnan suunnittelu ja vastuutus

Riskienhallinnan osa-alueita on sovitettava organisaation toimintaympäristön ja oimien käytäntöjen mukaisiksi. Eri virastoissa voidaan tarvita toisistaan poikkeavia käytännön menetelmiä. Riskienhallinta tulee liittää osaksi viraston toimintaa, päätöksentekoa, johtamista ja esimiestyötä. Myös viraston riskienhallinnan viestintää ja raportointia tulee suunnitella.

Riskienhallinta on tärkeä ottaa erityisesti strategisen suunnittelun, toiminnan ja talouden suunnittelun, tulosohjauksen sekä kehittämishankkeiden ja muutosprosessien osaksi. Esimerkiksi suunnittelun ja seurannan vuosikelloon on hyvä sisällyttää riskien arviointi ja käsittely.

Ylin johto vastaa riskienhallinnan organisoinnista sekä tehtäväjaoista. Riskienhallinnan järjestämiseksi on sovittava rooleista ja huolehdittava koko organisaation sitoutumisesta. Talousarvioasetuksen 69 §:n mukaan viraston ja laitoksen johdon on huolehdittava siitä, että virastossa ja laitoksessa toteutetaan sen talouden ja toiminnan laajuuteen ja sisältöön sekä niihin liittyviin riskeihin nähden asianmukaiset menettelyt. Johdolta edellytetään uskottavaa ja riittävän näkyvää sitoutumista. Johto ei voi delegoida kokonaisvastuuta, sen sijaan riskienhallintaan liittyviä käytännön tehtäviä voidaan delegoida.

Riskienhallinnan järjestämisessä on otettava huomioon organisaation sisäinen ja ulkoinen toimintaympäristö sekä organisaation erityispiirteet (esim. tehtäväalue, resurssit), joilla on vaikutusta riskienhallintaan. Vastuiden tulee perustua toiminnan vastuisiin mm. säädösten, työjärjestyksen ja taloussäännön mukaisesti, jotta riskienhallinta ei ole toiminnasta irrallista.

Riskienhallintapolitiikkamallin luvussa 6 on kuvattu riskienhallinnan vastuita. Vastuut tulee muokata viraston toimintaan ja organisointiin sopiviksi. Tässä yhteydessä voidaan kirjata tarvittaessa myös vastuutahojen tavoitteet ja konkreettiset toimenpiteet, mitä vastuu sisältää. Ministeriön riskienhallintapolitiikassa on hyvä kuvata mahdolliset vastuut hallinnonalan riskienhallinnan ohjauksessa ja koordinoinnissa.

4 Riskienhallinnan toteuttaminen

Riskienhallinnan käytännön toteutusta auttaa, jos johdon tukena on nimetty henkilö koordinoimassa prosessia ja kehittämistä. Työtä voidaan edistää myös koordinointi- tai tukiryhmällä, jossa on kattavasti viraston eri osa-alueita tuntevia henkilöitä. Tehdävät voivat vaihdella virastoittain riskienhallinnan toteutustavan mukaan. Jäsenten ei tarvitse olla riskienhallinta-asiantuntijoita. Ryhmä voi olla myös jo olemassa oleva ryhmä, jonka tehtäviin riskienhallinnan tuki luontevasti liittyy. Näin saadaan huolehdittua riskienhallinnasta viraston kaikissa toiminnoissa.

Systemaattinen riskienhallinta on tärkeää erityisesti hankkeissa ja projekteissa, sillä kertaluonteisuutensa vuoksi niissä on lähes kaikki uutta ja historiatietoa riskeistä ei ole välttämättä olemassa. Riskienhallintaa ei pidä rajata vain hanke- tai projektihallintoon, vaan mukaan on otettava myös tavoiteltavan lopputuloksen sisältämät mahdolliset uudet riskit. Toimintatapojen, välineiden ja raportoinnin tulisi olla yhdenmukaisia viraston toimintaan liittyvän riskienhallinnan kanssa.

Riskienhallintaa toteutetaan käytännössä viraston riskienhallintaprosessin mukaisesti. Prosessi on kuvattu lyhyesti riskienhallintapolitiikkamallin luvussa 7.

5 Riskienhallinnan seuranta ja kehittäminen

Viraston toimintaympäristön ja riskien muuttuessa myös riskienhallintapolitiikkaa tulee arvioida ja mukauttaa toimintaympäristöön sopivaksi. Riskienhallinnan tilaa ja toimivuutta on arvioitava säännöllisesti ja määriteltävä arvioinnin tulosten perusteella kehittämiskohteet.

Sisäisen valvonnan ja riskienhallinnan arviointi tulee tehdä vähintään vuosittain ja esittää arvioinnin tulokset sekä keskeiset kehittämiskohteet toimintakertomuksessa (sisäisen valvonnan arviointi- ja vahvistuslausuma).

6 Riskienhallinnan viestintä ja raportointi

Viraston hyvään johtamiseen kuuluvat riittävät tiedot organisaation riskeistä ja niiden hallintatoimista. Vuosittaisessa toimintakertomuksessa sisäisen valvonnan arviointi- ja vahvistuslausumassa esitetään arviointi sisäisen valvonnan ja siihen sisältyvän riskienhallinnan asianmukaisuudesta ja riittävydestä sekä olennaisimmista kehittämistarpeista.

Valtionhallinnon virastojen toiminta kytkeytyy toisten virastojen sekä muiden yhteistyökumppaneiden ja sidosryhmien toimintaan. Virastojen tehokas riskienhallinta edellyttää riittävää tiedonvaihtoa näiden kanssa. Merkittävistä riskeistä ja riskienhallintatoimista tulee viestiä tulosohjaavalle ministeriölle.

7 Sisäinen valvonta, riskienhallinta ja sisäinen tarkastus

Sisäinen valvonta tarkoittaa menettelyjä, joilla varmistetaan

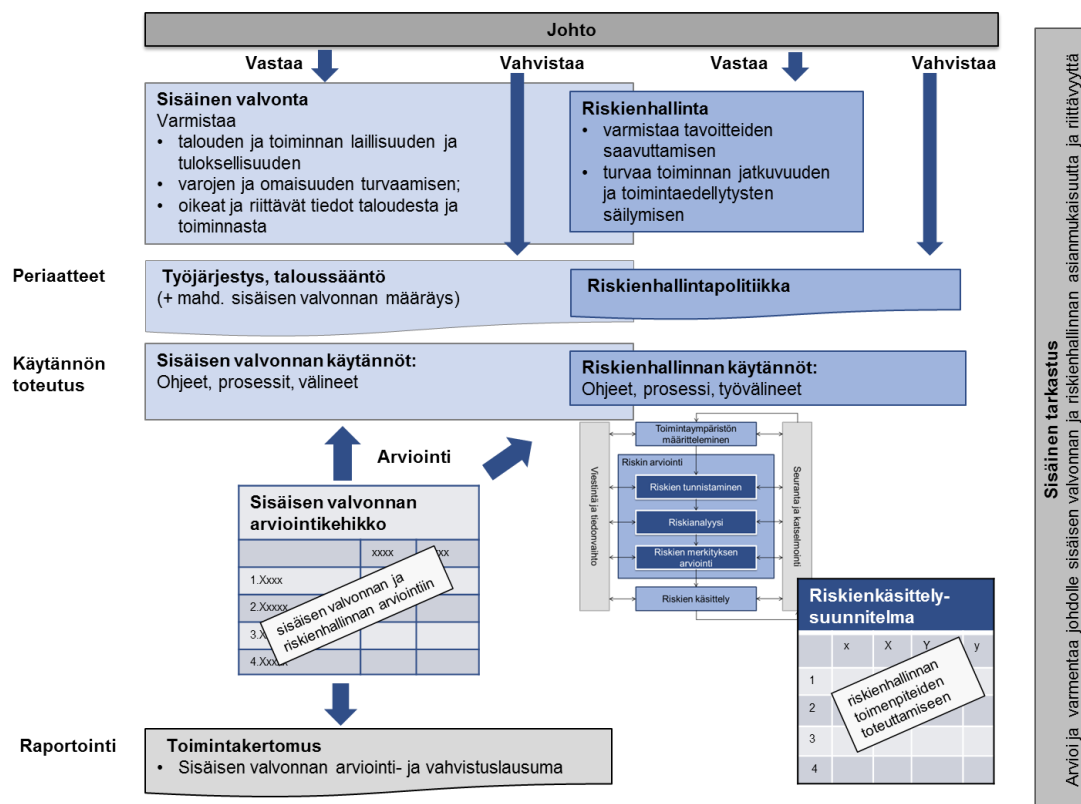
- talouden ja toiminnan laillisuus ja tulokellisuus;
- varojen ja omaisuuden turvaaminen;
- oikeat ja riittävät tiedot viraston ja laitoksen taloudesta ja toiminnasta.

Menettelyt ovat osa ohjaus- ja toimintaprosesseja ja organisointitratkaisuja. Sisäinen valvonta on koko organisaation asia, se varmistaa tavoitteiden ja hyvän hallinnon toteutumisen. Sisäisen valvonnan asianmukaisuudesta vastaa johto.

Riskienhallinta tarkoittaa koordinoitua toimintaa, jolla organisaatiota johdetaan ja ohjataan riskien osalta. Se on systemaattista ja jatkuvaa toimintaa, jonka avulla tunnistetaan, analysoidaan, arvioidaan, käsitellään ja seurataan riskejä. Riskienhallinnan avulla varmistetaan tavoitteiden saavuttaminen ja turvataan toiminnan jatkuvuus ja toimintaedellytysten säilyminen.

Sisäisen tarkastuksen tehtävä on selvittää johdolle sisäisen valvonnan ja riskienhallinnan asianmukaisuus ja riittävyys. Sisäinen tarkastus arvioi näiden toimivuutta ja tehokkuutta sekä tukee asiantuntijana organisaation kaikkia tasoja riskienhallinnan toteuttamisessa.

Seuraavassa kuvassa on esitetty sisäisen valvonnan ja riskienhallinnan elementtejä ja työvälineitä.



Kuva 1. Riskienhallinta, sisäinen valvonta ja sisäinen tarkastus

RISKIENHALLINTAPOLITIIKKAMALLI

Riskienhallintapolitiikka sisältää [viraston] riskienhallintaan liittyvät periaatteet ja tavoitteet. Tavoitteena on selkeyttää ja yhtenäistää riskienhallinnan käsitteitä, periaatteita, tavoitteita, organisointia, vastuuta ja toimintatapoja. Riskienhallinta otetaan osaksi ohjaus- ja johtamisjärjestelmää, se kattaa koko toiminnan ja toimintamalli on yhtenäinen läpi koko organisaation.

1 Soveltamisala

Tässä asiakirjassa esitettyä [viraston] riskienhallintapolitiikkaa sovelletaan ... [virastokohtaiset täsmennykset, mahdolliset organisaatio- tai tehtävärajaukset sekä ministeriöissä maininta mahdollisesta soveltamisesta hallinnonalan virastoissa].

Riskienhallinta on ennakoiva näkökulma toimintaan ja osa asioiden valmistelua. Se kattaa kaikki toiminnot, sekä oman toiminnan että toiminnan, josta organisaatio vastaa lainsäädännön, sopimusten tai muiden velvoitteiden nojalla.

2 Säädöspohja sekä muut määräykset ja ohjeet

Riskienhallinta on osa sisäistä valvontaa ja siten jokaisen valtion viraston lakisääteinen tehtävä. Valtion talousarviosta annetussa lain (423/1988) 24 b §:ssä säädetään sisäisen valvonnan järjestämisestä. Talousarvioasetuksen (1243/1992) 69 ja 69 b § sisältävät tarkempia säännöksiä sisäisestä valvonnasta ja riskienhallinnasta.

Tietoturvallisuusasetuksessa (681/2010) säädetään asiakirjojen käsittelyä koskevat tietoturvallisuusvaatimukset ja tietoturvallisuustoimenpiteet, 5 §:ssä tietoturvallisuusriskien kartoittaminen.

Säädöksistä on lisätietoa liitteessä 1.

Muut asiakirjat, joissa määritellään riskienhallintaa

[Tässä kohdassa tai liitteessä luetellaan muut asiakirjat, joissa määritellään viraston riskienhallintaa, sekä viraston riskienhallintapolitiikan liittymät ja rajaukset näihin. Näitä ovat esim. muu kuin em. lainsäädäntö, työjärjestys, taloussääntö, valtion varallisuuden ja vastuiden hallintaan liittyvät riskienhallinnan periaatteet, tietoturvaohjeet/politiikat (esim. VAHTI-ohjeet), työturvallisuuteen liittyvät riskienhallintaoppaat sekä toimialakohtaiset riskienhallinnan erilliset asiakirjat.]

3 Riskienhallinnan keskeiset käsitteet

Seuraavassa on esitetty määrittelyt keskeisimmistä riskienhallinnan käsitteistä. Laajempi luettelo käsitteistä on liitteenä 2. [Lisäksi voidaan viitata muuhun määrittelydokumenttiin tai standardiin.]

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

Riskienhallinta tarkoittaa koordinoitua toimintaa, jolla organisaatiota johdetaan ja ohjataan riskien osalta. Se on systemaattista ja jatkuvaa toimintaa, jonka avulla tunnistetaan, analysoidaan, arvioidaan, käsitellään ja seurataan riskejä.

Riskienhallintapolitiikka sisältää organisaation riskienhallintaan liittyvät periaatteet ja tavoitteet.

Riskienhallintaprosessi on menettely riskien arviointiin (tunnistamiseen, analysointiin, merkityksen arviointiin), käsittelyyn, seurantaan ja viestintään.

Riskienkäsittelysuunnitelma on dokumentti, joka sisältää riskit ja niille tehtävät toimenpiteet, vastuut, käsittelyn tavoiteaikataulut, raportoinnin ja seurannan.

4 Riskienhallinnan tavoitteet

Riskienhallinnan avulla varmistetaan tavoitteiden saavuttaminen sekä turvataan toiminnan jatkuvuus ja toimintaedellytysten säilyminen.

Riskienhallinnan tavoitteena on tukea ennakoivaa johtamista. Tämä lisää strategioissa ja tulossopimuksissa määriteltyjen tavoitteiden saavuttamisen sekä säädettyjen ja määrättyjen tehtävien toteutumisen todennäköisyyttä. Riskienhallinta parantaa myös uusien toimintamahdollisuuksien tunnistamista. Riskienhallinnan avulla voidaan myös varmistaa talouden ja toiminnan laillisuutta ja tuloksellisuutta.

Riskienhallinnan tavoitteena on vahvistaa hyvää johtamis- ja hallintotapaa sekä luoda luotettavaa perustaa päätöksenteolle ja suunnittelulle sekä operatiiviselle toiminnalle. Riskienhallinta edellyttää toimivia johtamisrakenteita ja -järjestelyjä, joilla menettelyt riskien hallitsemiseksi sisällytetään toimintaan. Riskienhallinta on olennainen osa tulosohejausta ja -johtamista sekä toiminnan ja talouden prosesseja, hankkeita ja päivittäisen toiminnan toteuttamista.

Riskienhallinnan tavoitteena on varmistaa talouden ja toiminnan laillisuus ja tuloksellisuus, varojen ja omaisuuden turvaaminen sekä johtamisen ja ulkoisen ohjauksen edellyttämät oikeat ja riittävät tiedot taloudesta ja toiminnasta.

5 Riskienhallinnan periaatteet

[Viraston] riskienhallinta on osa koko valtionhallinnon riskienhallintaa. Virastot tuottavat palveluita myös toisille virastoille sekä toimivat keskenään yhteistyössä ja verkostoissa. Riskienhallintaa koskeissa päätöksissä ja toimenpiteiden määrittelyssä otetaan huomioon, että niillä saattaa olla vaikutuksia myös muihin virastoihin.

Riskienhallinta luo lisäarvoa auttamalla onnistumaan. Riskienhallinta edesauttaa tavoitteiden saavuttamista ja toiminnan tason havaittavaa ja mitattavaa kehittymistä. Riskienhallinta edesauttaa päivittäisen toiminnan, turvallisuuden, lakien ja viranomaisten vaatimusten noudattamista. Sillä voidaan edistää myös projektinhallintaa, toimintojen ja hallintotavan tehokkuutta sekä julkisuuskuvaan liittyvien uhkien hallintaa.

Riskienhallinta on olennainen osa johtamista. Riskien tunnistaminen ja hallinta on osa ennakoivaa johtamista. Riskienhallinta on osa johdon vastuuta sekä olennainen osa suunnittelun ja seurannan prosesseja, hankkeita ja operatiivista toimintaa sekä niihin liittyvää päätöksentekoa. Riskienhallinnan onnistuminen edellyttää johdolta näkyvää sitoutumista. Johdon sitoutuminen ja esimerkki on perustana hyvän hallinnon toimivuudelle koko organisaatiossa.

Riskienhallinta on osa päätöksentekoa. Riskitietoista kulttuuria edistetään kaikessa päätöksenteossa. Riskienhallinnassa otetaan huomioon epävarmuus, sen luonne ja käsittely-

mahdollisuudet. Tämä auttaa päätöksentekijöitä ennakoimaan ja tekemään tietoisia valintoja, asettamaan asioita tärkeysjärjestykseen ja erottamaan vaihtoehtoiset toimintatavat.

Riskienhallinta on järjestelmällistä, jäsenneltyä ja ajantasaista. Järjestelmällinen, ajan- tasainen ja jäsennelty riskienhallinnan toimintamalli lisää tehokkuutta ja toiminnan yhdenmu- kaisuutta. Tähän kuuluvat olennaisena osana myös toimenpiteet riskien käsittelemiseksi.

Riskienhallinta on avointa, kattavaa ja se perustuu parhaaseen saatavilla olevaan tie- toon. Riskienhallinnan onnistumisen kannalta on tärkeää, että eri tasoilla olevat päätöksen- tekijät, asiantuntijat ja sidosryhmät otetaan tarkoituksenmukaisella tavalla mukaan riskienhal- lintatyöhön.

Riskienhallinta on muutoksiin reagoivaa ja jatkuvaa kehittämistä. Riskienhallinnan avulla muutokset havaitaan ja niihin voidaan reagoida viipymättä. Riskienhallinta on mukana orga- nisaation toiminnassa sen eri osa-alueita kehitettäessä. Toimiva ja läpinäkyvä riskienhallinta korostuu erityisesti muutoksissa, joissa kehitetään uusia toimintamalleja ja luovutaan van- hoista.

Riskienhallinta toteutetaan organisaation tarpeiden mukaan. Riskienhallinnan järjeste- lyssä otetaan huomioon organisaation rakenne sekä toiminnan laatu, laajuus ja monimuotoi- suus. Riskienhallinnan järjestelyt sovitetaan yhteen ulkoisen ja sisäisen toimintaympäristön ja riskien mukaan.

Riskienhallinta kattaa myös yhteistyökumppaneiden toiminnan. Ulkopuolelta hankitta- vissa palveluissa riskienhallinnan kokonais- ja valvontavastuu on aina virastolla. Palvelun- tuottajien riskienhallinnan järjestelyjen riittävä taso tulee varmistaa sopimuksilla.

6 Riskienhallinnan vastuut

Tässä esitetään, kuinka riskienhallinnan vastuut ja roolit on määritelty *[virastossa]*. Tärkeää on, että jokainen sisäistää oman vastuunsa ja sen luonteen osana riskienhallintakokonaisuut- ta. *[Jos vastuut eivät ole riskienhallintapolitiikassa, lisätään maininta: Riskienhallinnan vastuut on kirjattu...].*

Riskienhallinnan vastuista päättää *[virastokohtainen säädösten ja työjärjestyksen mu- kainen taho]*.

[Viraston ylin johto, määrittää virkanimikkeen mukaan (ministeriössä kansliapääl- likkö / virastossa viraston päällikkö)] vastaa sisäisen valvonnan ja riskienhallinnan järjes- tämisestä, vahvistaa riskienhallintapolitiikan sekä hyväksyy sisäisen valvonnan arviointi- ja vahvistuslausuman. Käytännön tehtäviä voidaan delegoida organisaatiossa, mutta vastuu on johdolla.

Johtoryhmät: Riskienhallinta on osa ohjaus- ja johtamisjärjestelmää ja johtoryhmätyöskente- lyä kaikilla organisaatiotasolla. Viraston ylin johtoryhmä *[määrittää tähän virastokohtaises- ti]* käsittelee virastotaseiset riskit ja riskienhallintatoimenpiteet.

Johtajat, päälliköt ja esimiehet vastaavat oman organisaatioyksikkönsä *[osastonsa, yksik- könsä, toimintonsa, ryhmänsä, vastuualueensa]* riskienhallinnasta ja sen toimeenpanosta, tunnistavat oman organisaatioyksikön toimintaan liittyviä riskejä sekä ilmoittavat ja raportoivat niistä asiaankuuluvalla tavalla eteenpäin.

Hankkeen tai projektin omistaja, hanke/projektipäällikkö, työryhmän vetäjä vastaa riskienhallinnasta osana hanke-/projekti/työryhmähallintoa. Hankkeiden, projektien ja työryhmien riskienhallinta sisältää erityisesti työn läpiviemiseen ja tavoitteiden saavuttamiseen liittyvien riskien tunnistamisen, analysoinnin, käsittelyn ja raportoinnin. Näiden riskienhallinnassa mukaan on otettava myös tavoiteltavan lopputuloksen sisältämät mahdolliset uudet riskit.

Henkilöstö arvioi ja tunnistaa mahdollisia omaan työhönsä liittyviä riskejä sekä ilmoittaa niistä ja poikkeamista esimiehelleen tai *[muulle asiaankuuluvalla taholla, virastokohtainen]*. Henkilöstön on huomioitava voimassa olevat ohjeet ja määräykset. Johdon on varmistettava, että koko henkilöstö on näistä tietoinen ja koulutus ja perehdytys on ollut riittävä.

Riskienhallinnan vastuuhenkilö(t) / koordinaattori(t) / asiantuntija(t) / ryhmä(t): *[Viraston]* riskienhallinnan vastuuhenkilö on *[nimike tai muu yksilöinti]* / on määritelty *[asiakirjassa]*. Henkilön vastuulla on seurata riskienhallinnan tilaa, koordinoita riskienhallintaa ja menettelyiden yhdenmukaisuutta, tukea riskienhallinnan prosessissa sekä kehittää riskienhallinnan menettelyitä.

[Seuraava viraston tarpeen mukaan: Vastuuhenkilön tukena on riskienhallinnan koordinointi/ yhteistyöryhmä [ryhmänä voi toimia jo olemassa oleva ryhmä, jonka tehtäviin riskienhallinta voidaan kytkeä], jossa on [organisaatioyksiköiden] nimeämiä toimintaa hyvin tuntevia henkilöitä. Ryhmä toimii riskienhallintaprosessin valmistelevana ryhmänä sekä riskienhallinnan kehittämisen tukena. Ryhmän avulla riskienhallinnan toteutukseen saadaan laajempaa koko virastoa tuntevaa asiantuntemusta ja näkemystä.]

[Tarvittaessa: Ministeriön rooli ja vastuu hallinnonalan riskienhallinnan ohjauksessa: Ministeriö vastaa hallinnonalan riskienhallinnan [tarvittavat luonnehdinnat asioista, vastuista ja toteutuksesta, mm. ohjausprosesseista, joihin liittyy].]

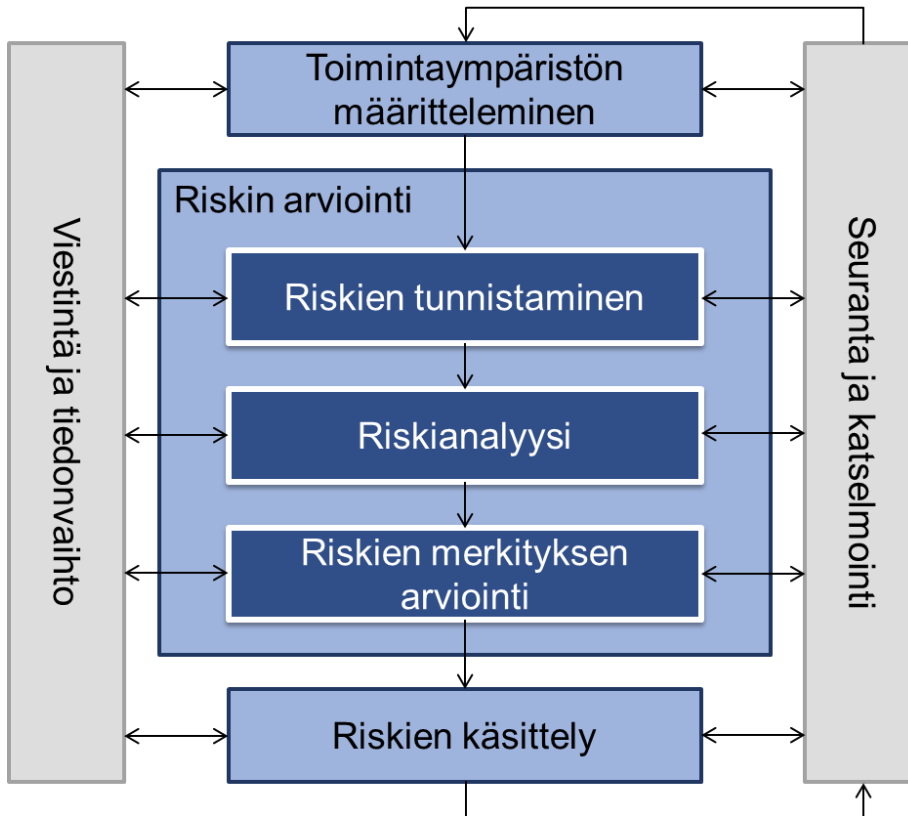
Sisäinen tarkastus selvittää johdolle sisäisen valvonnan ja riskienhallinnan asianmukaisuutta ja riittävyyttä. Sisäinen tarkastus arvioi näiden toimivuutta ja tehokkuutta sekä tukee asiantuntijana organisaation kaikkia tasoja systemaattisen riskienhallinnan toteuttamisessa. Sisäinen tarkastus ei ole vastuussa riskienhallinnan järjestämisestä ja toteuttamisesta.

7 Riskienhallintaprosessi

[Viraston] riskienhallinnan käytännön prosessi on kuvattu *[liitteessä 4 / erillisessä kuvauksessa]*.

Riskienhallinta on osa *[viraston ohjausjärjestelmää / johtamisjärjestelmää / johtamista / toimintaa]*. Riskienhallinnan keskeiset vaiheet sisältyvät vuosikelloon ja ne liittyvät *[tähän kirjaan tarvittavat prosessit]*. Riskien kokonaisarviointi eli koko virastotason keskeisten alueiden riskikartoitus tai niiden päivitys tehdään *[vuosittain...]*.

[Seuraavassa on kuvattu riskienhallintaprosessi SFS-ISO 31000 -standardin mukaisesti.]



Kuva 2. Riskienhallinnan prosessi, lähde: SFS-ISO 31000

Tunnistettujen riskien jäsentämiseksi käytetään luokittelua: 1. Strategiset riskit, 2. Operatiiviset riskit, 3. Taloudelliset riskit, 4. Vahinkoriskit. Näiden kuvaukset ovat liitteessä 5.

Riskien toteutumisen todennäköisyyttä ja vaikutusta arvioidaan seuraavilla asteikolla (liite 6):
 Todennäköisyys: 1. Epätodennäköinen, 2. Mahdollinen, 3. Todennäköinen, 4. Lähes varma.
 Vaikutus: 1. Vähäinen, 2. Kohtalainen, 3. Merkittävä 4. Kriittinen.

8 Riskienhallinnan arviointi ja kehittäminen

[Viraston] riskienhallintaa seurataan ja arvioidaan säännöllisesti [tähän kuvataan miten, esim. johtoryhmässä ja miten usein, sekä mitä sisäinen tarkastus tekee sisäisen valvonnan ja riskienhallinnan asianmukaisuuden ja riittävyyden varmistamiseksi]. Arvioinnin tulosten perusteella määritellään kehittämiskohteet [ja näiden käsittely/ ylimmän johdon vahvistaminen]. Toimintakertomukseen kirjataan arvioinnin tulos sekä keskeiset kehittämiskohteet sisäisen valvonnan arviointi- ja vahvistuslausumaan.

9 Voimaantulo ja allekirjoitukset

RISKIENHALLINTAPOLITIIKAN LIITTEET

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 riittävydestä 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 laatisesta 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

[luetellaan tarvittavat tässä]

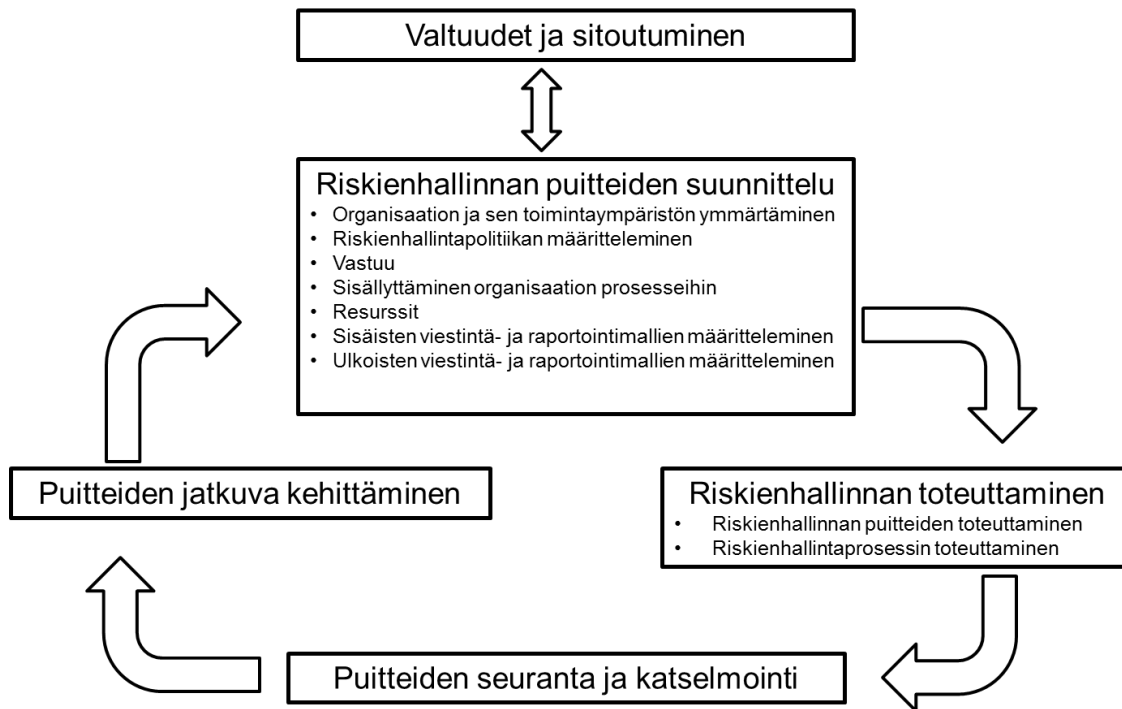
LIITE 2 KÄSITTEIDEN MÄÄRITELMÄT

Seuraavassa hakemistossa on riskienhallinnan keskeisimpiä käsitteitä määrittelyineen. Lisää määrittelyitä on SFS-ISO 31000 -standardissa.

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 tarkastus arvioi sisäisen valvonnan toimivuutta ja tehokkuutta sekä tukee asiantuntijana organisaation kaikkia tasoja riskienhallinnan toteuttamisessa.
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.

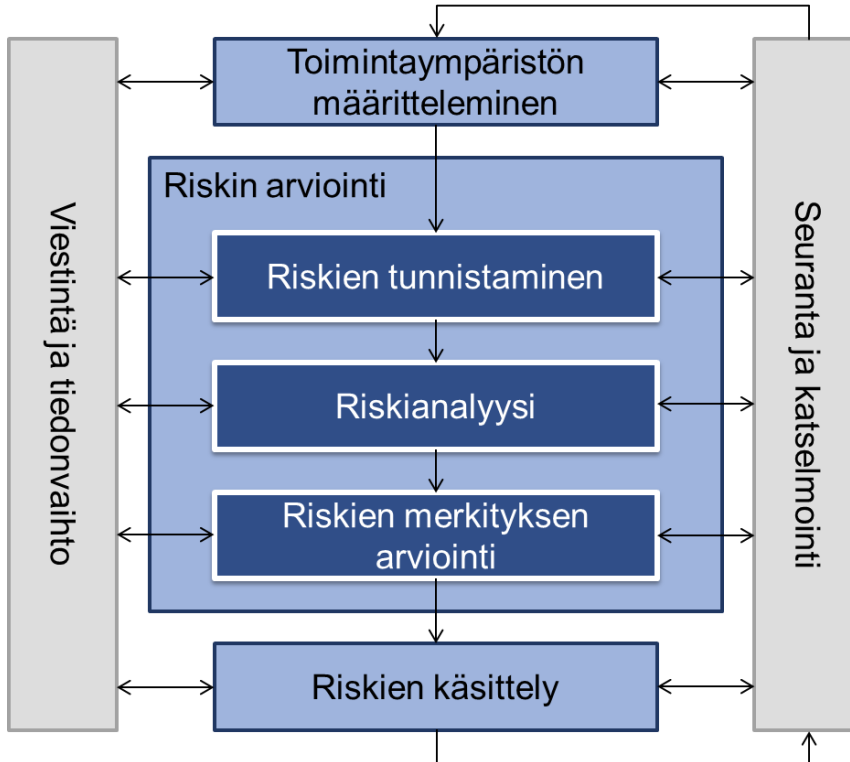
LIITE 3 RISKIENHALLINNAN PUITTEET



lähde: SFS-ISO 31000

LIITE 4 RISKIENHALLINTAPROSESSI

Seuraavassa on kuvattu riskienhallintaprosessi SFS-ISO 31000 -standardin mukaisesti.



1 Toimintaympäristön määrittäminen

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.

2 Riskien arviointi

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

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 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.

2.2 Riskianalyysi

Riskianalyysissa tavoitteena on muodostaa käsitys tunnistetuista riskeistä. Tässä vaiheessa 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
- perusta riskien merkityksen arvioinnille eli päätöksenteolle siitä, mitä riskeille tehdään tai jätetään tekemättä

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.

Riskien merkityksen arvioinnista syntyy

- järjestetty luettelo riskeistä
- yhteinen näkemys käsiteltävistä riskeistä toimenpiteiden suunnittelemiseksi

3 Riskien käsittely

Riskien käsittelyssä määritellään jatkotoimenpiteet ja nimetään vastuullisen henkilöt sekä alustava tavoiteaikataulu. 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**. Riskienkäsittelysuunnitelman hyväksyy viraston ylin johto.

Riskien käsittelyn tuloksena syntyy

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

4 Seuranta

Riskienhallinnassa seuranta ja katselmointi ovat osa prosessia, jotta varmistetaan valittujen keinojen vaikuttavuus ja tehokkuus ja tiedetään, miten organisaation riskienhallinnassa onnistutaan. Tähän vaiheeseen sisältyvät toimintaympäristön sisäisten ja ulkoisten 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 myös puuttua tilanteisiin, joissa riskit ovat jäämässä käsittelemättä.

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 riskienkäsittelysuunnitelmaan.

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

Seuraavassa on esitetty yleinen luokittelu, jota suositellaan käytettäväksi riskien arvioinnissa. Tarvittaessa sitä voi tarkentaa alajaotteluin tai käyttää muuta, viraston riskienhallintaa paremmin palvelevaa jaottelua.

1. Strategiset riskit

esim. strategia, toimintaympäristö, suhdannevaihtelut, säädosmuutokset, johtamisjärjestelmä, organisaatorakenne, 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

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 merkittäväällä 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 tai henki 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 henki 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 hahmottamaan riskien merkittävyyttä ja tarvittavia toimenpiteitä.

todennäköisyys	4				
	3				
	2				
	1				
		1	2	3	4
	vaikutus				

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 toimenpiteitä • seurattava riskiä ja sen mahdollista kehittymistä
Matala riski (riskiluku 1-2)	• ei vaadi akuutteja toimenpiteitä

LIITE 8 RISKIENKÄSITTELYSUUNNITELMA

Yksinkertainen taulukko riskienhallintaprosessin tueksi ja riskienkäsittelysuunnitelmaksi

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

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 soveltamisesta.

VAHTI-riskienhallintaohje (valmisteilla)

Riskienarvioinnin kevyt työväline (Excel, valmistellaan VAHTI-riskienhallintaohjeen yhteydessä)