VM 22/2017 Ohje riskienhallintaan – LIITTEET 1 - 6

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI)

SISÄLLYSLUETTELO:

LIITE 1: Riskienhallinnan käsitteitä

Käsite	Selite
digitaalinen tai digi-turvallisuus	Digitaalinen turvallisuus on digitaalisessa muodossa olevien tietojen ja niiden käsittelemisen, siirtämisen ja säilyttämisen turvallisuudesta varmistumista. Digitaalisella turvallisuudella vaikutetaan myös fyysisen ympäristön turvallisuuden toteutumiseen.
jatkuvuuden hallinta	Jatkuvuuden hallinnan tarkoituksena on mahdollistaa organisaation häiriötön toiminta kehittämällä varautumis-, jatkuvuus-, toipumis- ja valmiussuunnittelua. Suunnitelmien avulla organisaatio voi varautua erilaisiin normaaliolojen häiriötilanteisiin sekä poikkeusoloihin. Jatkuvuudenhallinta edellyttää toimintaan liittyvien riskien ja muiden toimintaan vaikuttavien riippuvuuksien tunnistamista.
jäännösriski	Riskiin käsittelyn jälkeen jäävä riski, jota ei voida tai ei haluta poistaa. Jäännösriskeihin voi sisältyä tunnistamattomia riskejä.
kyberturvallisuus	Kyberturvallisuus on turvallisuuden osa-alue, jolla pyritään digitaalisesti verkostoituneen yhteiskunnan turvallisuuteen. Kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan digitaalisten ja verkottuneiden järjestelmien häiriöiden vaikutuksiin.
otettava riski	Sellainen riski, joka halutaan ottaa uusien mahdollisuuksien saavuttamiseksi.
riski	Epävarmuuden vaikutus tavoitteisiin. Vaikutus on poikkeama odotetusta. Vaikutus voi olla myönteinen tai kielteinen suhteessa odotusarvoon. Riski kuvataan useimmiten viittaamalla tapahtumaan ja/tai seurauksiin ja ilmaistaan todennäköisyyden ja vaikutuksen yhdistelmänä.
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 esimerkiksi 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 yhden tai useamman osapuolen kanssa (esimerkiksi sopimuksin ja riskin rahoittamisella) - riskin tietoinen säilyttäminen ja sietäminen
riskien tunnistaminen	Riskien havaitsemisen ja kuvaamisen prosessi.
riskienhallinnan puitteet	Sisältää osatekijät, jotka yhdessä muodostavat organisaation riskienhallinnan järjestämisen (suunnittelun, toteutuksen, seurannan, katselmoinnin ja jatkuvan kehittämisen) perustan ja organisoinnin.
riskienhallinta	Koordinoitu toiminta, jolla johdetaan ja ohjataan, hallitaan organisaation riskejä.

Käsite	Selite
riskienhallintamalli	Organisaation sopima keino toteuttaa riskienhallintaa. Tämä ohjeistus pohjautuu SFS-ISO 31000-standardissa kuvattuun malliin.
riskienhallintapolitiikka (tai riskienhallinnan periaatteet)	Organisaation päättämät, kuvaamat ja dokumentoimat riskienhallintaan liittyvät periaatteet ja tavoitteet. Riskienhallintapolitiikka-dokumentista voidaan käyttää myös nimitystä Riskienhallinnan periaatteet.
riskienhallintaprosessi	Hallintaperiaatteiden, -menettelyjen ja -käytäntöjen järjestelmällinen soveltaminen toimintaympäristön määrittelemiseen, riskien tunnistamiseen, analysointiin, arviointiin, käsittelyyn, seurantaan ja katselmointiin sekä viestintään ja tiedonvaihtoon.
riskienkäsittelysuunnitelma	Johdon hyväksymä dokumentoitu riskien käsittelyn vastuut sisältävä toimenpidesuunnitelma.
riskikriteerit	Säännöt, joiden perusteella riskin merkittävyys arvioidaan yhdenmukaisesti. Riskikriteerit perustuvat organisaation tavoitteisiin ja sen toimintaympäristöön. Riskikriteerit voidaan johtaa standardeista, laeista, toimintaperiaatteista ja muista vaatimuksista.
riskiluokitus	Arvioitavan kohteen luokittelun apuväline, tässä ohjeessa on kuvattu pari esimerkkiä erilaisista riskiluokituksista. Keskeistä, että organisaatio käyttää omassa toiminnassaan yhteisesti sovittua, yhdenmukaista riskiluokitusta.
riskimatriisi	Riskimatriisin avulla luokitellaan riskin suuruus tapahtuman seurausten vakavuuden ja esiintymisen todennäköisyyden perusteella. Matriisi auttaa hahmottamaan riskin merkittävyyttä ja sitä, miten riski suhteutuu muihin 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 seuraa ja koordinoi tiettyä riskiä ja sen hallintaan liittyviä toimenpiteitä käytännössä.
riskinottohalu	Kyvykkyys, joka organisaatiolla on ja jonka se on valmis ottamaan tavoitteisiin pyrkiessään.
riskinsietokyky	Riskimäärä, johon organisaatiolla on valmius sitoutua riskien määrittelyn jälkeen.
riskitaso	Riskin tai riskiyhdistelmien suuruus, joka ilmoitetaan seurausten ja niiden todennäköisyyden yhdistelmänä.
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 sekä tuloksellisuus - varojen ja omaisuuden turvaaminen - oikeat ja riittävät tiedot organisaation taloudesta ja toiminnasta.

Käsite	Selite
tietosuoja	Tietosuojaan kuuluvat ihmisten yksityiselämän suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä.
tietosuojariski	Turvallisuuden ylläpitämiseksi ja asetuksen säännösten vastaisen käsittelyn estämiseksi rekisterinpitäjän tai henkilötietojen käsittelijän tulee arvioida käsittelyyn liittyvät riskit ja toteutettava toimenpiteitä näiden riskien lieventämiseksi esimerkiksi salauksella. Näiden toimenpiteiden avulla tulee varmistaa asianmukainen turvallisuustaso, muun muassa luottamuksellisuus, ottaen huomioon uusin tekniikka ja toteuttamiskustannukset suhteessa tietojenkäsittelyn riskeihin ja suojeltavien henkilötietojen luonteeseen. Tietosuojariskiä arvioitaessa tulee huomioida henkilötietojen käsittelyyn liittyvät riskit, kuten siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai laiton tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai henkilötietoihin pääsy, mikä voi aiheuttaa etenkin fyysisiä, aineellisia tai aineettomia vahinkoja.
tietoturvallisuus	Tietoturvallisuus tai tietoturva tarkoittaa kaikissa muodoissa olevien tietojen tai niitä sisältävien palvelujen, järjestelmien, tietoliikenteen tai tietovarastojen luottamuksellisuuden tai eheyden tai saatavuuden suojaamista.
uhka	Epätoivottu, kielteinen vaikutus organisaation tai järjestelmään, jossa ei ole olemassa positiivista mahdollisuutta.
varautuminen	Varautumisella tarkoitetaan sellaisia ennakoivia toimia, jotka suunnitellaan esimerkiksi häiriötilanteiden tai poikkeusolojen varalle: - valmiussuunnitelmaa, joka laaditaan esim. valmiuslain tai yhteiskunnan turvallisuusstrategiassa kuvatun velvoitteen perusteella - jatkuvuussuunnitelmaa, joka laaditaan esim. prosessin tai laajan palvelukokonaisuuden häiriötilanteiden aikaisen toiminnan valmisteluksi - toipumissuunnitelmaa, joka laaditaan järjestelmien häiriötilanteista selviytymiseksi.

LIITE 2: Riskienhallintaan velvoittavia keskeisiä säädöksiä

Kuva L2.1. *Riskienhallintaan velvoittavat lukuisat säädökset, joista keskeisimpiä on kuvassa. Eri julkishallinnon organisaatioita velvoittavat erilaiset toimintaan kohdistuvat lait ja säädökset, jotka asianomaisten organisaatioiden on itse tunnistettava.*

VALTIONEUVOSTON ASETUS TIETOTURVALLISUUDESTA VALTIONHALLINNOSSA (681/2010)

Tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava muun muassa siitä, että viranomaisen toimintaan liittyvät tietoturvallisuusriskit kartoitetaan sekä siitä, että tietojen saanti ja käytettävyys eri tilanteissa turvataan. On myös luotava menettelytavat poikkeuksellisten tilanteiden selvittämiseksi. Lisäksi viranomaisen on huolehdittava muun muassa siitä, että tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä.

LAKI VIRANOMAISEN TOIMINNAN JULKISUUDESTA (621/1999)

Viranomaisen on hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehdittava asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muista tietojen laatuun vaikuttavista tekijöistä. Viranomaisen on suunniteltava ja toteutettava asiakirja- ja tietohallintonsa samoin kuin ylläpitämänsä tietojärjestelmät ja tietojenkäsittely niin, että asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suoja, eheys ja laatu turvataan asianmukaisin menettelytavoin ja tietoturvallisuusjärjestelyin. Tässä yhteydessä tulee ottaa huomioon tietojen merkitys ja käyttötarkoitus, asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät sekä tietoturvallisuustoimenpiteistä aiheutuvat kustannukset.

KUNTALAKI (410/2015)

Sen mukaan valtuuston tulee päättää kunnan ja kuntakonsernin sisäisen valvonnan ja riskienhallinnan perusteista (14 § 7). Hallintosäännössä tulee olla myös tarpeelliset määräykset hallinnon ja talouden riskienhallinnasta (39 §, 47 §, 67 §, 90 §). Riskienvalvonnan järjestäminen tulee myös ilmetä kunnan toimintakertomuksesta (115 §). Tilintarkastajan on otettava myös kantaa, onko sisäinen valvonta ja riskienhallinta sekä konsernivalvonta järjestetty asianmukaisesti (123 §)

ASETUS VIRANOMAISTEN TOIMINNAN JULKISUUDESTA JA HYVÄSTÄ TIEDONHALLINTATAVASTA (1030/1999)

Hyvän tiedonhallintatavan toteuttamiseksi viranomaisen on selvitettävä ja arvioitava tietojen saatavuuteen, käytettävyyteen, laatuun ja suojaan sekä tietojärjestelmien turvallisuuteen vaikuttavat uhat. Lisäksi on huomioitava niiden vähentämiseksi ja poistamiseksi käytettävissä olevat keinot ja niiden kustannukset sekä muut vaikutukset.

VALMIUSLAKI (1552/2011)

Valtioneuvoston, valtion hallintoviranomaisten, valtion itsenäisten julkisoikeudellisten laitosten, muiden valtion viranomaisten ja valtion liikelaitosten sekä kuntien, kuntayhtymien ja muiden kuntien yhteenliittymien tulee valmiussuunnitelmin ja poikkeusoloissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muilla toimenpiteillä varmistaa tehtäviensä mahdollisimman hyvä hoitaminen myös poikkeusoloissa.

LAKI VALTION TALOUSARVIOSTA (423/1988)

Talousarviolain 24 b §:n mukaan 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)

Talousarvioasetuksen 69 §:ssä säädetään tarkemmin sisäisen valvonnan sisällöstä, tavoitteista ja sen järjestämistä koskevista vaatimuksista. 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,
- johtamisen ja ulkoisen ohjauksen edellyttämät oikeat ja riittävät tiedot viraston ja laitoksen taloudesta ja toiminnasta.

TYÖTURVALLISUUSLAKI (738/2002)

Työnantajan on työn ja toiminnan luonne huomioon ottaen riittävän järjestelmällisesti selvitettävä ja tunnistettava työstä, työajoista, työtilasta, muusta työympäristöstä ja työolosuhteista aiheutuvat haitta- ja vaaratekijät sekä, jos niitä ei voida poistaa, arvioitava niiden merkitys työntekijöiden turvallisuudelle ja terveydelle.

HENKILÖTIETOLAKI (523/1999)

Rekisterinpitäjän on toteutettava tarpeelliset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä tai muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojalle.

EU:N TIETOSUOJA-ASETUS (EU 679/2016)

Asetusta sovelletaan 25.5.2018 lähtien ja se korvaa vuoden 1995 henkilötietodirektiivin (95/46/EY) sekä sen kansalliseksi täytäntöön panemiseksi annetun henkilötietolain (523/1999) säännökset niiltä osin kuin henkilötietojen käsittely kuuluu asetuksen soveltamisalaan. Asetus määrittelee muun muassa

- mikä tieto on henkilötietoa ja mitkä henkilötiedot ovat erityisiä henkilötietoja (arkaluonteisia henkilötietoja),
- millä perusteilla henkilötietoja voi käsitellä ja mitä periaatteita henkilötietoja käsiteltäessä on noudatettava,
- mitkä ovat rekisteröityjen, eli henkilöiden, joiden tietoja käsitellään, oikeudet,
- mitä velvollisuuksia henkilötietojen käsittelyyn liittyy,
- millä edellytyksillä henkilötietoja voi siirtää EU:n ulkopuolelle,
- millaisia seuraamuksia asetuksen säännösten rikkomisesta voidaan määrätä.

Asetus edellyttää useissa kohden riskiperusteista lähestymistä, minkä vuoksi tässä ohjeessa kuvattua toimintamallia suositellaan sovellettavaksi myös tietosuojaa kehitettäessä.

LIITE 3: Riskienhallintapolitiikka ja puitteet

Riskienhallintapolitiikka, riskienhallinnan periaatteet

Riskienhallintapolitiikka luo perustan ja linjaukset riskienhallinnan puitteiden toteuttamiselle. Politiikan sisältö on laadittava organisaation tarpeita vastaavaksi. Yksi hyvä sisältömalli ei välttämättä sellaisenaan sovellu toiselle organisaatiolle, vaan sisältöön vaikuttavat erityispiirteet on huomioitava organisaatiokohtaisesti.

Riskienhallintapolitiikka (riskienhallinnan periaatteet) sisällysluetteloesimerkki:

RISKIENHALLINTAPOLITIIKKA
Johdanto
1 Soveltamisala
2 Säädöspohja sekä muut määräykset ja ohjeet
3 Riskienhallinnan keskeiset käsitteet
4 Riskienhallinnan tavoitteet
5 Riskienhallinnan periaatteet
6 Riskienhallinnan vastuut
7 Riskienhallintaprosessi
8 Riskienhallinnan arviointi ja kehittäminen
9 Voimaantulo ja allekirjoitukset

Sisäisen valvonnan ja riskienhallinnan neuvottelukunta on valmistellut valtionhallinnon riskienhallintapolitiikkamallin, josta valtiovarain controller -toiminto on antanut suosituksen 3.5.2017 (http://vm.fi/riskienhallinta).

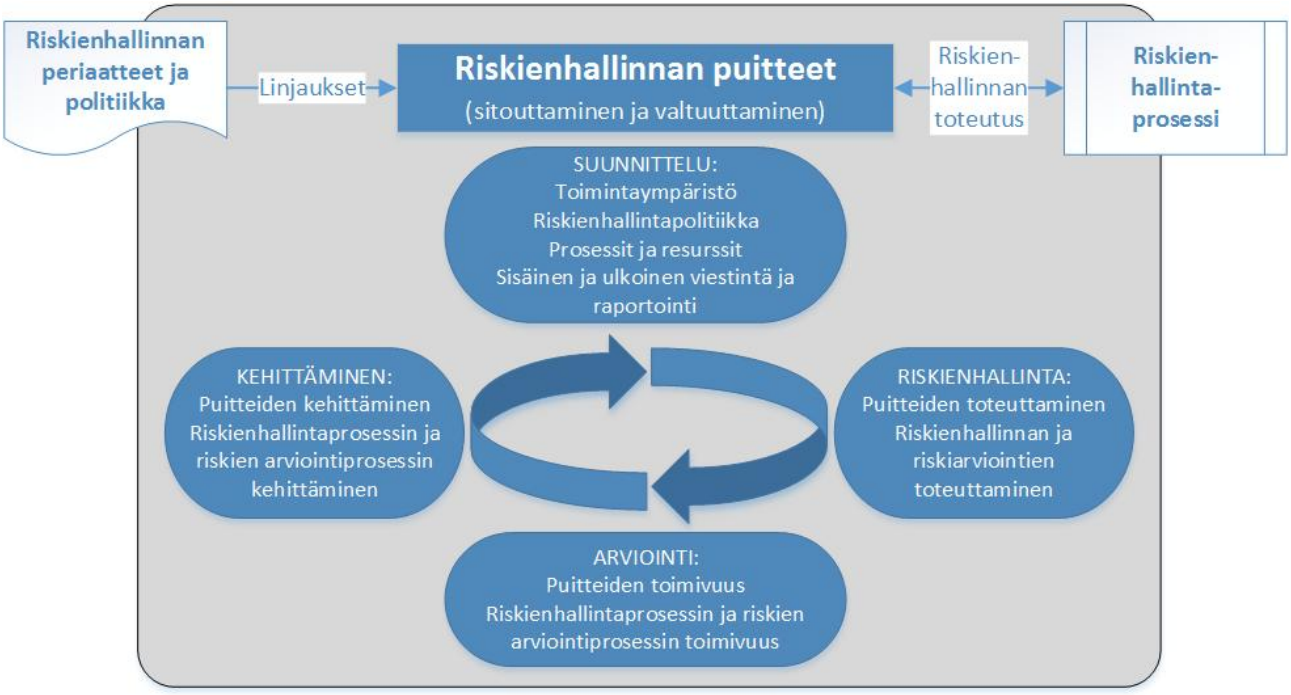
Kuva L3.1. *Riskienhallintapolitiikka osana riskienhallintaa. Riskienhallinnan periaatteet kirjataan ja kuvataan riskienhallintapolitiikassa.*

Riskienhallinnan järjestäminen, riskienhallinnan puitteet

Riskienhallinnan järjestämisessä voi käyttää apuna riskienhallinnan puitteita (osa ISO 31000-stadardia), jotka toteutetaan P-D-C-A (Plan-Do-Check-Act) menetelmää noudattaen seuraavasti:

- Suunnittelu
- Toteuttaminen
- Seuranta ja katselmointi
- Jatkuva kehittäminen

Riskienhallinnan puitteiden tarkoitus ei ole vaikuttaa johtamisjärjestelmän rakenteisiin, vaan auttaa organisaatiota sisällyttämään riskienhallinta ja sen kehittäminen organisaation johtamisjärjestelmään. Puitteiden osia ja osa-alueita on siis sovitettava organisaation käytäntöjen mukaisiksi ja johtamisjärjestelmään sopiviksi.



Kuva L3.2. *Riskienhallinnan puitteiden avulla huolehditaan jatkuvasta kehittymisestä.*
Lähde: Kuva perustuu standardiin SFS-ISO 31000.

LIITE 4: Riskienhallinnan standardeja ja hyviä käytäntöjä

Tämä liite sisältää kuvauksia aiheista:

- ISO 31000 Riskienhallinta
- COSO-ERM-riskienhallinta (tiivistelmä)
- PESTLE-malli
- Vaikutusanalyysi (BIA, Business Impact Analysis)
- Tietoriskianalyysi
- Tietojärjestelmäympäristön ja sovelluskehityksen riskien arviointi
- Riskienhallinnan tasot esimerkki
- Riskienhallinnan vastuukuvaus – esimerkkinä RACI-malli
- Riskienhallintasuunnitelma tai riskisalkku
- Riskienhallinta vuosikelloissa, esimerkkejä
    - Riskienhallinta TTS-vuosikellossa
    - Riskienhallinnan vuosikello – esimerkkejä
    - Riskienhallinta osana vuosisuunnitelmaa

ISO 31000 Riskienhallinta

Tässä ohjeessa on hyödynnetty standardia SFS-ISO 31000 Riskienhallinta. Se on standardointiorganisaation ISO (*International Organization for Standardization*) julkaisema standardi, joka antaa selkeän rakenteen organisaation riskienhallinnan kehittämiseen. Standardissa riskienhallinta jaetaan kolmeen pääkohtaan:

- **Riskienhallinnan periaatteet:** Organisaation johdon päättämät riskienhallintaan liittyvät periaatteet ja tavoitteet, jotka on kuvattu riskienhallintapolitiikka tai -periaatteet dokumentissa.

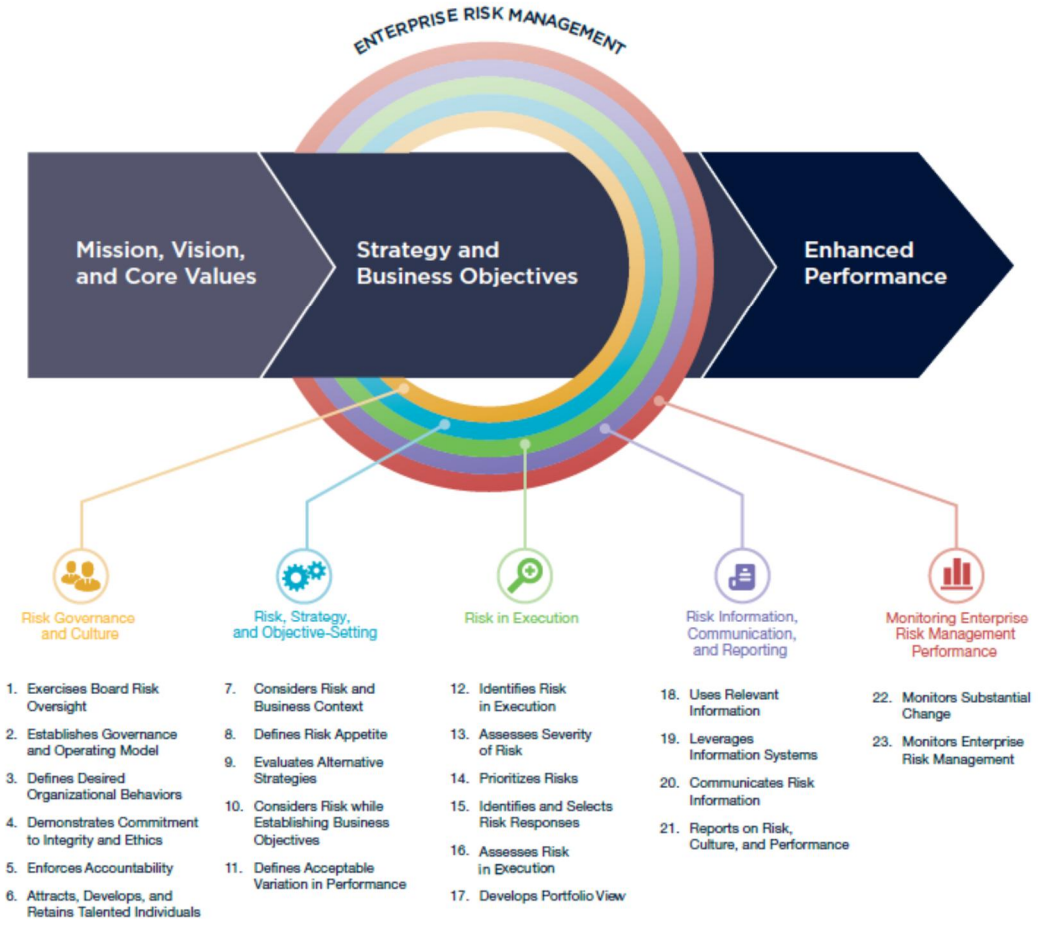
- **Riskienhallinnan puitteet:** Koostuvat osatekijöistä, jotka yhdessä muodostavat organisaation riskienhallinnan suunnittelun, toteutuksen, seurannan, katselmoinnin ja jatkuvan kehittämisen perustan ja organisoinnin.

- **Riskienhallinnan prosessi:** Sisältää hallintaperiaatteiden, -menettelyjen ja -käytäntöjen järjestelmällisen soveltamisen viestintään ja tiedonvaihtoon sidosryhmien kanssa, toimintaympäristön määrittelemiseen liittyviin toimintoihin sekä riskien tunnistamiseen, analysointiin, arviointiin, käsittelyyn, seurantaan ja katselmointiin.

ISO 31000 -standardi on kaupallinen kansainvälinen riskienhallinnan malli, joka soveltuu sellaisenaan riskienhallinnan toteuttamisen viitekehykseksi tai sillä voidaan täydentää muiden ISO-hallintajärjestelmästandardien (mm. ISO 9000 Laadunhallinta, ISO 14000 Ympäristöjohtaminen, ISO 26000 Yhteiskuntavastuu, ISO 27000 Tietoturvallisuuden hallinta, ISO 55000 Omaisuudenhallinta, OHSAS 18001 Työterveys- ja työturvallisuusjohtaminen, ym.) vaatimustenmukaisuutta.

COSO-ERM-riskienhallinta (tiivistelmä)

Sisäisen valvonnan lähtökohdista ja sisäisen valvonnan riskienhallinnan tarpeisiin on tuotettu kansainvälinen ja erityisesti yrityksissä laajalti käytössä oleva kaupallinen COSO tai COSO-ERM (*The Committee of Sponsoring Organizations of the Treadway Comission, Enterprise Risk Management*) riskienhallinnan malli (tässä kuvattu luonnos/ehdotus ao. mallin uudesta versiosta).



Kuva L4.1. *COSO-ERM viitekehys. (Kuvan lähde: COSO-ERM.)*

PESTLE-malli

Riskien arvioinnissa voi käyttää apuna myös PESTLE-mallia, jossa riskien juurisyitä arvioidaan tarkemmin. Toisin sanoen arvioidaan niitä syitä, jotka mahdollistavat heikkouksia ja joilla on vaikutuksia organisaation toimintaan. PESTLE-mallissa arvioidaan seuraavia juurisyitä:

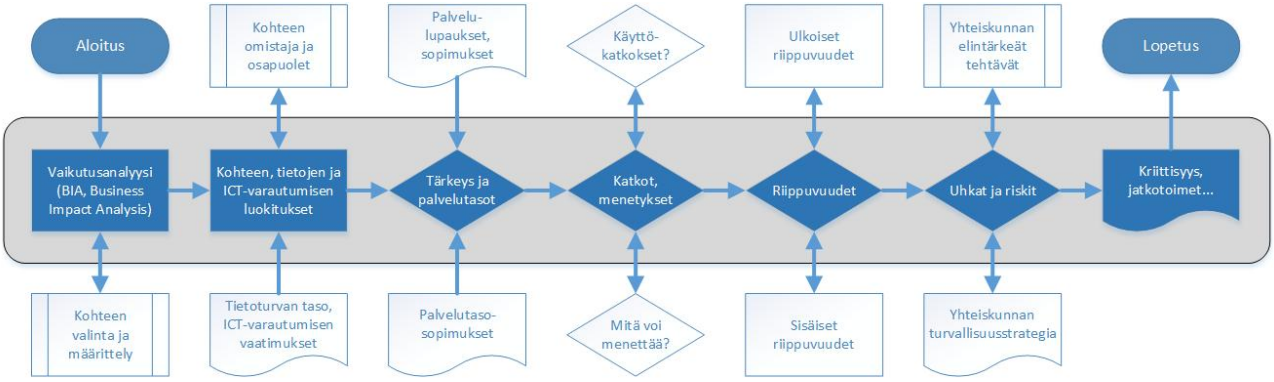
P	Politiikka (Politics)	Valtio-ohjaus, säätely, poliittinen ohjaus, verotus.
E	Talous (Economy)	Talouskasvu tai –lasku, korot, inflaatio, vaihtokurssit.
S	Yhteiskunta (Society)	Kulttuuri, terveys, ikääntyminen, turvallisuus, väestönkasvu, työllisyys.
T	Teknologia (Technology)	Automaatio, tuotekehitys, teknologinen muutos.
L	Laki (Law)	Lainsäädäntö, tullit, tietoturva, hankinta, työsuojelu, ICT.
E	Ympäristö (Environment)	Sää, ilmasto, ilmastonmuutos, ympäristötietoisuus.

PESTLE-mallia voi käyttää riskienarvioinnissa myös toimintaympäristön muutosten hahmottamiseen ja näiden muutosten aiheuttamien riskien tunnistamiseen.

Vaikutusanalyysi (Business Impact Analysis, BIA)

Vaikutusanalyysillä tarkoitetaan toiminnan keskeyttävien tai toiminnan jatkuvuutta häiritsevien uhkien tunnistamista sekä toimintaan liittyvien riippuvuuksien tunnistamista. Tieto- ja kyberturvallisuuden näkökulmasta vaikutusanalyysissä erityisesti valtionhallinnon tai muun julkisen sektorin organisaation toiminnan kannalta tarkasteltavia asioita ovat muun muassa

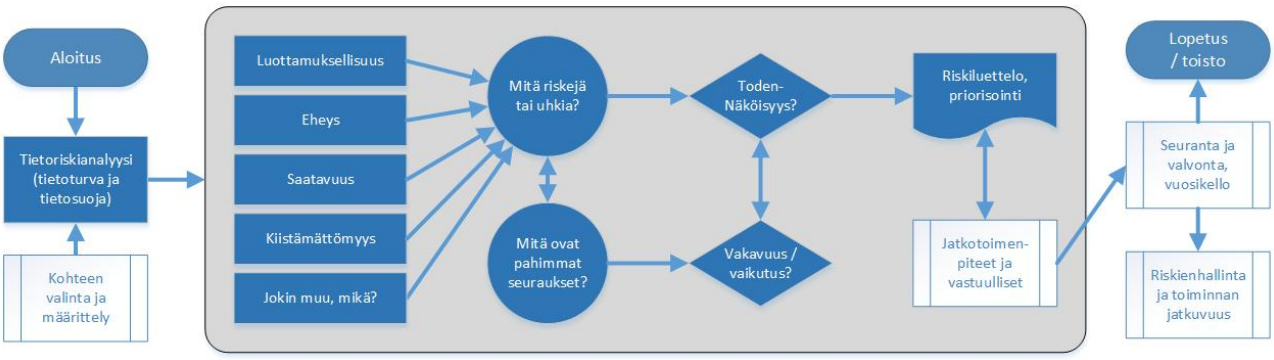
- Vaikutukset omaan operatiiviseen toimintakykyyn.
- Vaikutukset säädösperusteisten tehtävien suorittamiseen (vrt. myös yhteiskunnan elintärkeät tehtävät)
- Vaikutukset yhteiskunnalle
- Riippuvuussuhteet ja niiden vaikutukset:
    - Oman organisaation riippuvuus toisesta osapuolesta tai palvelusta tai toisista organisaatioista tai palveluista
    - Toisen organisaation tai palvelun riippuvuus oman organisaation tuottamasta palvelusta tai toiminnasta



Kuva L4.2. *Huolellisesti toteutetulla vaikutusanalyysillä (ns. BIA-analyysi) voidaan selvittää esimerkiksi palvelun tai järjestelmän tärkeys, kriittiset riippuvuudet, toimintaa uhkaavat riskit ja uhat sekä tarvittavat jatkokehitystoimet.*

Tietoriskianalyysi

Tietoriskianalyysin voi keveimmillään toteuttaa arvioimalla riskejä ja uhkia, jotka kohdistuvat luottamuksellisuuteen, eheyteen, saatavuuteen ja kiistämättömyyteen.



Kuva L4.3. *Tietoriskianalyysissä arvioidaan kohdetta tietoturvallisuuden peruskäsitteiden kautta ja kartoitetaan todennäköisimmät riskit ja uhat sekä kuvataan niiden pahimmat seuraukset.*

Tietojärjestelmäympäristön ja sovelluskehityksen riskien arviointi

Tietojärjestelmäympäristön riskien arviointiin on olemassa useita tarkastelu- ja toteutustapoja. Tietojärjestelmien riskejä liittyy esimerkiksi suorituskykyyn, jota voidaan tarkastella järjestelmän teknisen kapasiteetin ja todellisen käyttövarmuuden näkökulmista. Käyttövarmuutta voidaan tarkastella toimintavarmuuden, huollettavuuden ja huoltovarmuuden näkökulmista.

Tietojärjestelmän ja sovelluskehityksen tietoturvauhkien ja riskien kartoituksessa voidaan käyttää apuna esimerkiksi yleisiä vapaasti saatavilla olevia malleja ja menetelmiä (esim. OWASP Top-10). Haastatteluin ja pistokokein tehtyjen tarkastusten lisäksi voidaan tehdä muun muassa penetraatiotestejä ja teknisiä haavoittuvuusskannauksia, joihin voidaan yhdistää murtoharjoituksia esimerkiksi tietoverkon rajapintaa tai palveluihin kirjautumisessa käytettävien ratkaisujen ja järjestelmien testaamiseksi.

Sovellusten ohjelmistokoodi voi sisältää paljon riskejä. Useimmiten ohjelmistokoodin riskien kartoittaminen vaatii kohteena olevaa ohjelmistokoodia ymmärtävää ohjelmistoalan ammattilaista, joka ymmärtää myös tietoturvallisuutta ja riskienhallintaa kattavasti.

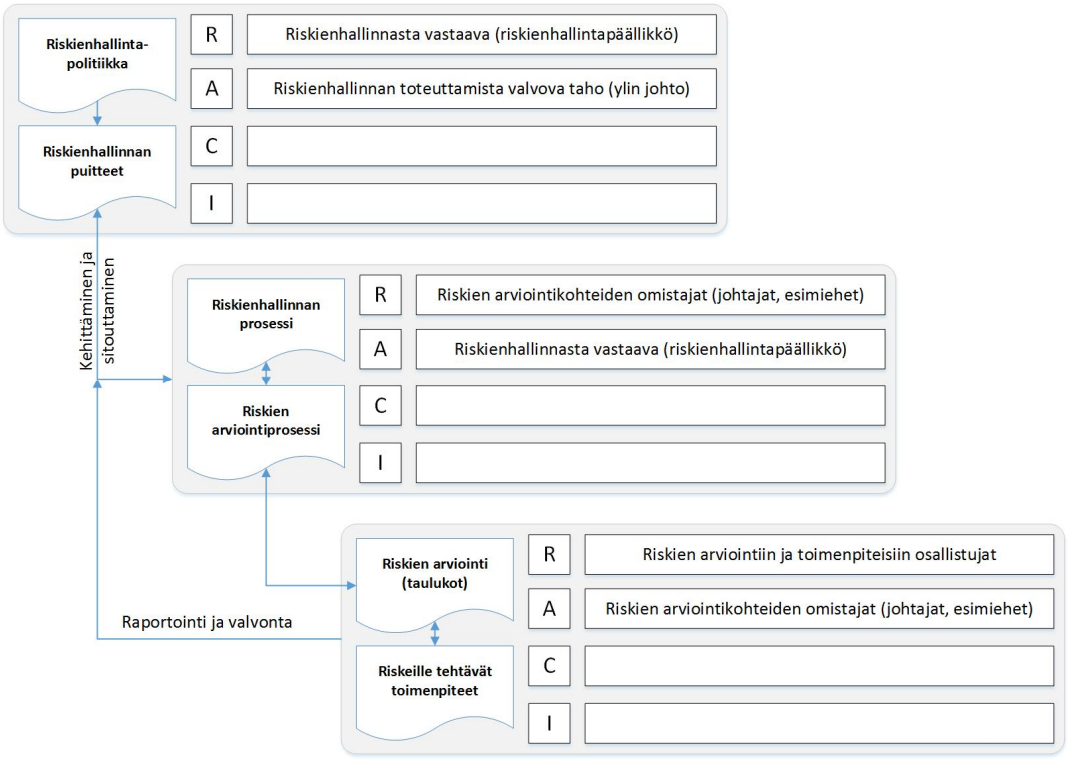
Riskienhallinnan tasot esimerkki

Kuva L4.4. *Riskienhallintaa voi käsitellä myös organisaatiotasoittain.*

Riskienhallinnan vastuukuvaus – esimerkkinä RACI-malli

Riskienhallinnan vastuiden kuvaamisessa suositellaan sovellettavaksi RACI-mallia:

- **R = responsible (vastuullinen)**
  - Vastuullinen henkilö (R) suorittaa annetun tehtävän tai on osa suoritustiimiä
  - jokaisella tehtävällä on ainakin yksi R-henkilö
- **A = accountable (vastuussa oleva)**
  - Vastuussa oleva henkilö (A) valvoo, että tehtävä tulee valmiiksi
  - jokaisella tehtävällä on vain yksi vastuuhenkilö
- **C = consulted (neuvonantaja)**
  - Henkilöltä (C) voidaan kysyä ohjeita ja neuvoja tehtävän suorittamiseen
  - jokaisella tehtävällä voi olla nollasta lukemattomaan neuvonantajaan
- **I = informed (tiedotettava)**
  - Henkilöä (I) tiedotetaan tehtävän suorittamisesta, jokaisella tehtävällä voi olla nollasta lukemattomaan tiedotettavaa

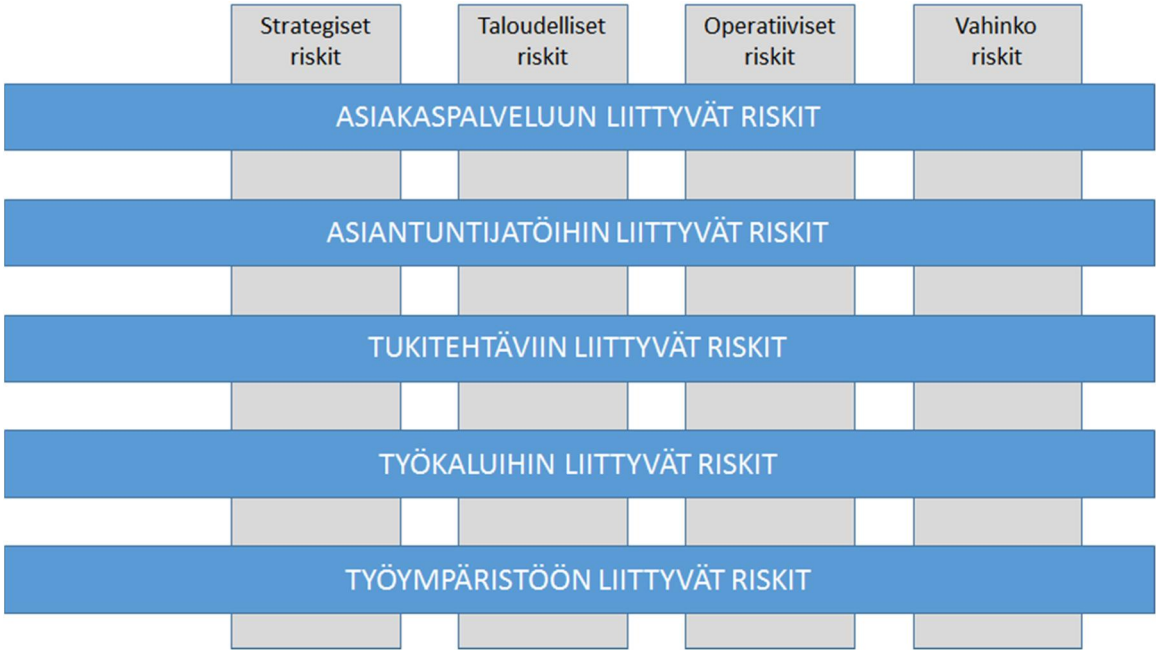


Kuva L4.5. *Riskienhallinnan vastuut voidaan kuvata myös RACI-mallilla.*

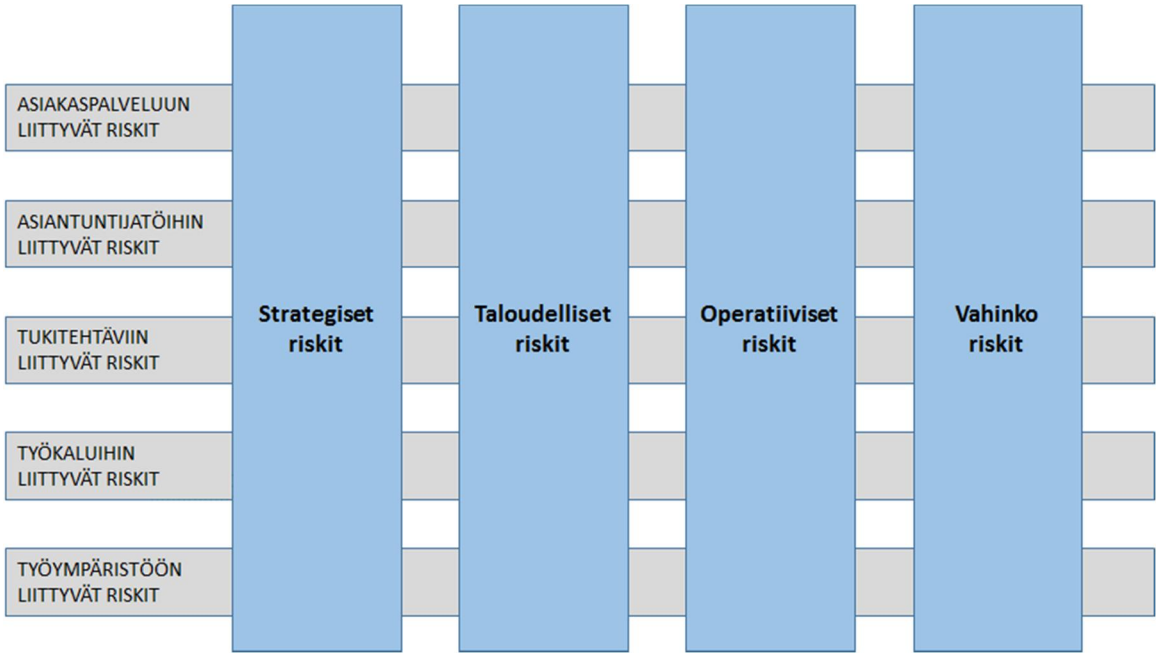
Onnistuneessa RACI-mallissa useimmiten ylemmän tason vastuullinen henkilö (R) on alemman tason vastuussa oleva henkilönä (A). Neuvonantajan (C) ja tiedotettavan (I) roolit ja tehtävät voivat vaihdella organisaatioittain ja organisaatioiden sisälläkin niin paljon, että ne on jätetty kaavion selvyyden vuoksi kuvaamatta.

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. Organisaatio vastuuttaa yleensä riskienhallintapäällikön tai muun riskeistä vastaavan henkilön valvomaan riskien arviointia ja toimenpiteiden etenemistä sekä riskienhallinnan kehittymistä.



Kuva L4.6. *Riskejä voidaan tarkastella riskisalkussa luokittelun tai tehtävien mukaan. Tässä esimerkkinä tarkastelun painottaminen tehtäviin tai osa-alueisiin.*



Kuva L4.7. *Riskejä voidaan tarkastella riskisalkussa luokittelun tai tehtävien mukaan. Tässä esimerkkinä tarkastelu riskiluokittain.*

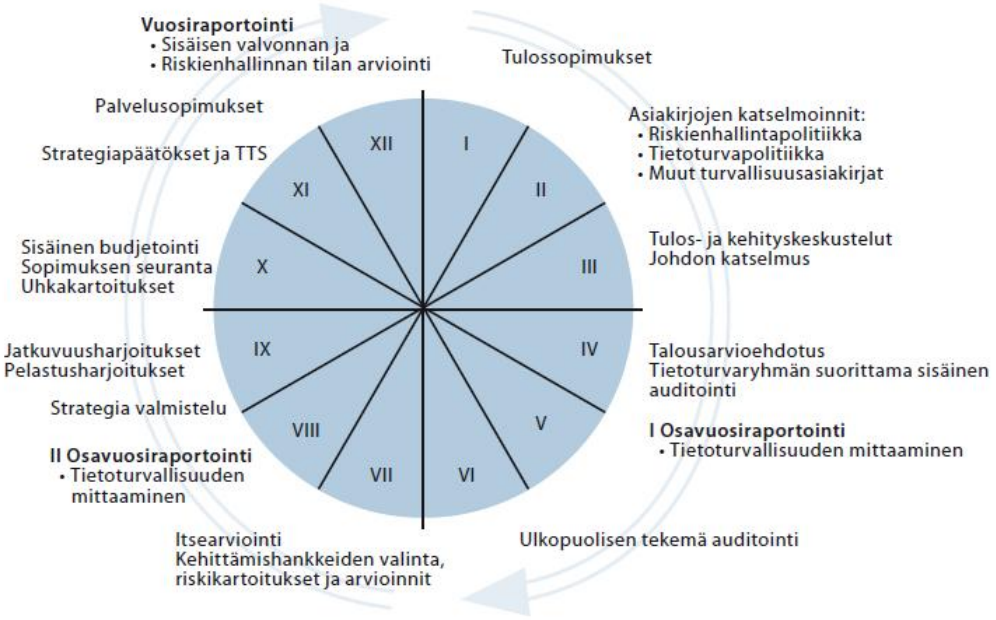
Kuva L4.8. *Riskejä voidaan tarkastella riskisalkussa luokittelun ja yksiköiden matriisina. Lopputuloksena tällaisesta tarkastelusta voidaan saada selville organisaation olemassaolon ja toiminnassa menestymisen kannalta kriittisimmät riskit sekä onnistumisen edellytykset.*

Riskienhallintasuunnitelman tai riskisalkun avulla organisaation ylimmälle johdolle voidaan raportoida koko organisaation riskienhallinnan tilanne. Kokonaistilanteen tarkastelun hyödyistä tärkeimpiin kuuluu se, että riskeille tehtäviin toimenpiteisiin käytettävät resurssit (ihmiset, ajankäyttö, raha ym.) voidaan jakaa tasapuolisemmin. Tällöin kaikki yksittäiset riskit voidaan suhteuttaa muihin riskeihin ja varmistua, että mitään olennaista riskiä ei unohdeta käsitellä. Riskienhallintasuunnitelma tai riskisalkku mahdollistaa myös aiemmin toteutettujen riskienkäsittelytoimenpiteiden soveltamisen tehokkaasti uusiin riskeihin. Organisaationtasoisen riskienhallintasuunnitelman tai riskisalkun avulla riskejä voidaan myös tarkastella esimerkiksi yksikkökohtaisesti tai riski- tai suuruusluokittain.

Riskienhallinta vuosikelloissa, esimerkkejä

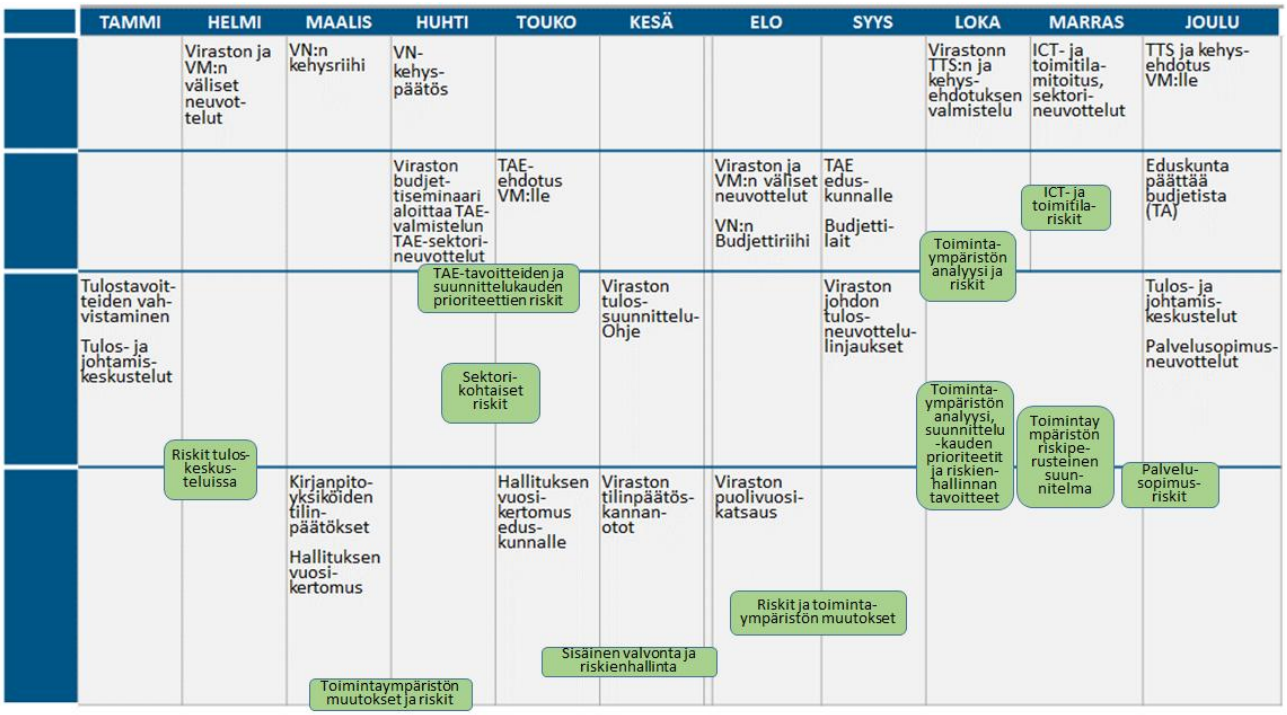
Riskienhallinnan vuosittaiset toimenpiteet tulee kuvata vuosikelloon. Vuosikello voi olla organisaation toiminnan ja talouden suunnittelun (TTS) vuosikello tai erillinen riskienhallinnan vuosikello.

Riskienhallinta TTS-vuosikellossa



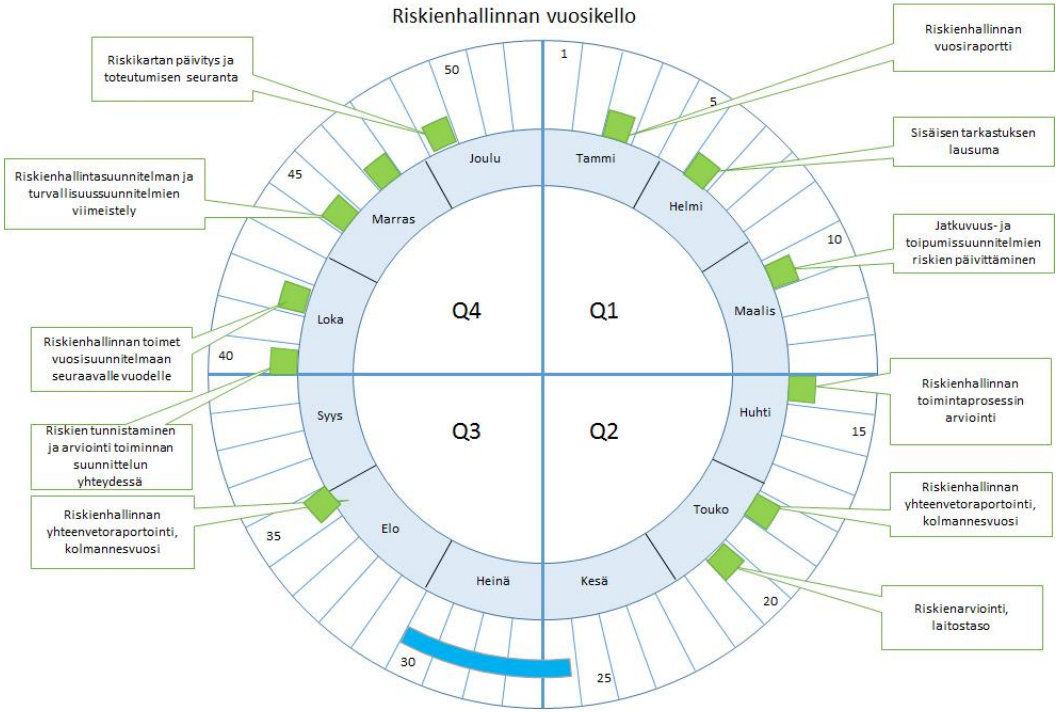
Kuva L4.9. *Esimerkki TTS-vuosikellosta, joka sisältää myös riskienhallinnan asioita. (Kuvan lähde: VAHTI 3/2007.)*

Riskienhallinta osana vuosisuunnitelmaa

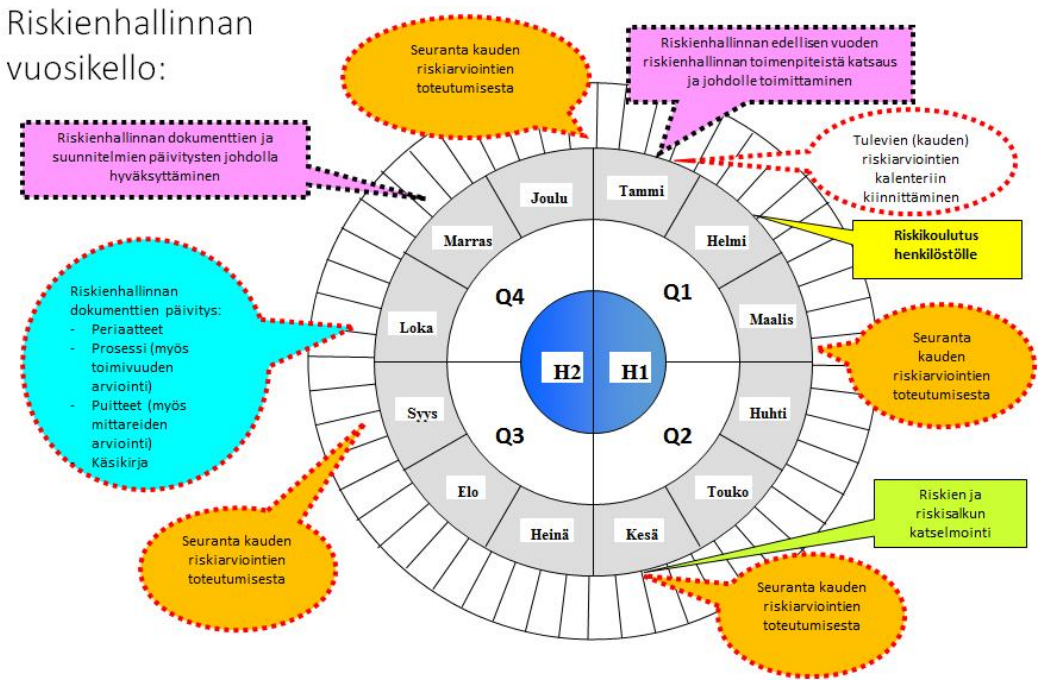


Kuva L4.10. *Esimerkki vuosisuunnitelmasta, johon on sisällytetty riskienhallinnan toimia.*

Riskienhallinnan vuosikello – esimerkkejä



Kuva L4.11. *Esimerkki riskienhallinnan vuosikellosta*



Kuva L4.12. *Esimerkki riskienhallinnan vuosikellosta*

LIITE 5: Riskien luokittelu ja arviointi – esimerkkejä ja menetelmiä

Tämä liite sisältää kuvauksia ja esimerkkejä seuraavista aiheista:

- Riskien luokittelu ja arviointitasot
    - Riskien luokittelu
    - Riskien analysoinnissa käytettäviä asteikkoja
- Riskimatriisit
- Riskienhallinta ISO 31000 perustuvan prosessin mukaisesti
    - Toimintaympäristön määritteleminen
    - Riskien arviointiprosessi
        - Riskien tunnistaminen
        - Riskianalyysi
        - Riskien merkityksen arviointi
    - Riskien käsittely ja hallinta
    - Viestintä ja tiedonvaihto
    - Seuranta ja katselmointi
- Yksinkertaistettu riskienhallintaprosessi
- Yksinkertaistettu riskien seurantamalli
- Tärkeiden kumppaneiden riskien arviointi ja riskien huomioon ottaminen
- Riskien arvioinnin kuvitteellinen käyttötapaus: Kahvinkeitin
    - Kahvinkeittimeen liittyvien asioiden riskiarvioinnin kuvaus
    - Kahvinkeittimeen liittyvien asioiden riskiarviointi – tietojen vienti taulukkoon
    - Yhteenveto case Kahvinkeittimen riskien arvioinnista
- Riskien käsittelytavat käytännössä

Esimerkkejä riskien luokitteluista ja arviointitasoista

Yleisimmin riskit luokitellaan neljään pääluokkaan:

- **Strategiset riskit**, joilla tarkoitetaan vääriin valintoihin tai mahdollisuuksien menettämiseen johtavia riskejä.

- **Operatiiviset riskit**, joilla tarkoitetaan mm. prosessien toimimattomuudesta tai ihmisten toiminnassa epäonnistumisesta johtuvia riskejä.

- **Taloudelliset riskit**, joilla tarkoitetaan mm. pääoma-, markkina- tai talousprosessien epäonnistumisiin johtavia riskejä.

- **Vahinkoriskit**, joilla tarkoitetaan muun muassa vaaran tai vahingon toteutumisen mahdollisuuksista johtuvia riskejä.

Riskien luokitteluun ei ole yhtä ainoaa kaikille sopivaa mallia tai tapaa. Organisaation riskien luokittelu tulee suunnitella ja toteuttaa organisaation toiminnan erityispiirteet huomioon ottaen. Luokittelun suunnittelussa voi hyödyntää esimerkiksi toiminnan tai vaaran mukaan lähestymistä:

Toiminnan lähtökohdat riskien luokittelussa	**Vaaran tunnistaminen riskien luokittelussa**
Strategiaan ja suunnitteluun liittyvät riskit	Omaisuusvahingon vaara
Toimintaympäristöön liittyvät riskit	Keskeytysvahingon vaara
Johtajuuteen ja esimiestyöhön liittyvät riskit	Vahingonkorvausvastuu
Prosesseihin ja palveluihin liittyvät riskit	Henkilövahinkojen vaara
Kumppanuuksiin ja resursseihin liittyvät riskit	Liiketoiminnan menettämisen vaara
Henkilöstöön ja työn tekemiseen liittyvät riskit	Rikoksen kohteeksi joutumisen vaara

Esimerkkejä riskien luokittelusta

Esimerkki 1 (yleisin)	**Esimerkki 2**	**Esimerkki 3**
Strategiset riskit	Johtamisen riskit	Markkinariskit
Operatiiviset riskit	Omaisuusriskit	Likviditeettiriskit
Taloudelliset riskit	Henkilöstöriskit	Vastapuoliriskit
Vahinkoriskit	Teknologiariskit	Luottoriskit
		Sopimusriskit
Esimerkki 4	**Esimerkki 5**	Lainsäädäntöriskit
Henkilöriskit	Ulkoiset riskit	Toimintariskit
Maineriskit	Sisäiset riskit	Malliriskit
Tietoriskit	Vahinkoriskit	Henkilöriskit
Omaisuusriskit		Tietoriskit
Ympäristöriskit		Turvallisuusriskit

On huomattava, että organisaation riskienhallinnan toteuttamisen kannalta on parempi ratkaisu käyttää pientä kuin suurta määrää riskiluokkia. Yksittäiset riskit voidaan usein sijoittaa moneen eri luokkaan, mutta tällöin vastuu riskeille tehtävistä toimenpiteistä jakautuu. Esimerkiksi, jos riskiluokkia on kahdeksan tai enemmän, luokittelu ja luokkaan sijoittaminen voisi käytännössä muodostua mahdottomaksi. Riski voisi pahimmillaan kuulua jokaiseen luokkaan, mikä tekee valintapäätöksistä työläitä ja kohtuuttoman aikaa vieviä. Käytännössä riski kannattaa sijoittaa siihen luokkaan, johon se luontevimmin tai suurimmalta osaltaan kuuluu. Luokkaan sijoittamisessa voi käyttää myös perusteena sitä, missä luokassa riskille todennäköisimmin tehdään sovitut tai tarvittavat käsittelytoimenpiteet.

Riskien analysoinnissa käytettäviä asteikkoja

Riskejä voidaan analysoida esimerkiksi seuraavasti (organisaatio itse päättää käyttämästään riskien arviointitaulukosta ja tasojen määrästä):

Esimerkki 1		**Esimerkki 2**	
Todennäköisyys	**Vaikutus**	**Todennäköisyys**	**Vaikutus**
4. Lähes varma	4. Kriittinen	5. Lähes varmaa	5. Erittäin merkittävä
3. Todennäköinen	3. Merkittävä	4. Todennäköinen	4. Merkittävä
2. Mahdollinen	2. Kohtalainen	3. Mahdollinen	3. Huomattava
1. Epätodennäköinen	1. Vähäinen	2. Harvinainen	2. Vähäinen
		1. Epätodennäköinen	1. Erittäin vähäinen

Esimerkki 1 selitteet käsitteille:

- 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.

Esimerkki 2 selitteet käsitteille:

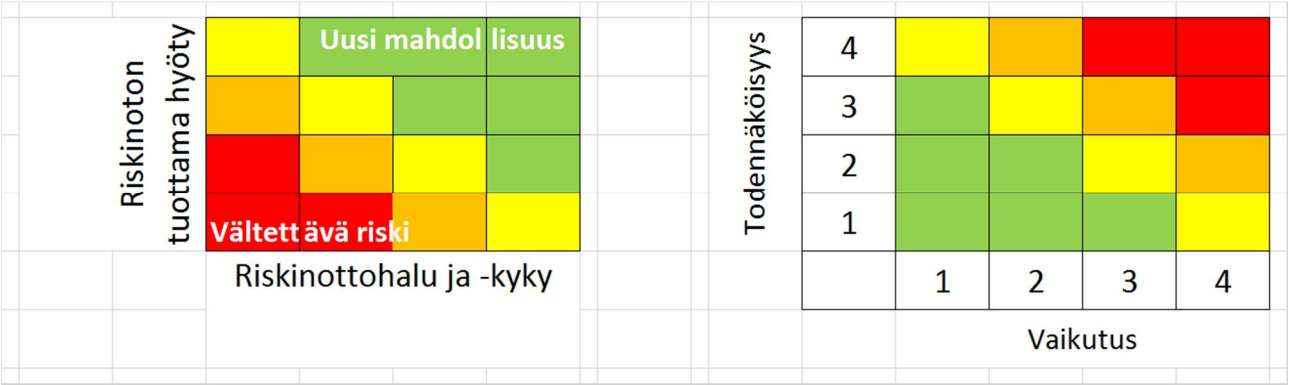
- **Riskin todennäköisyyttä** voidaan mitata asteikolla 1-5 esimerkiksi seuraavasti:
    1. Riskin toteutuminen on erittäin epätodennäköistä (ei ole tapahtunut)
    2. Riskin toteutuminen harvinaista (on joskus tapahtunut)
    3. Riskin toteutumisen mahdollista (on tapahtunut joskus meillä tai tapahtunut muualla useammin kuin kerran)
    4. Riskin toteutuminen on todennäköistä (on odotettavissa, että tapahtuu, tapahtunut meillä useamman kerran ja/tai ollut ”läheltä piti” tilanteita)
    5. Riskin toteutuminen on lähes varmaa (toteutuu lähitulevaisuudessa).

- **Riskin toteutumisen vaikutuksia** voidaan mitata asteikolla 1-5 esimerkiksi seuraavasti:
    1. Riskin vaikutukset ovat erittäin vähäiset. Erittäin pieniä häiriöitä toiminnalle, ei vaikuta tavoitteiden saavuttamiseen
    2. Riskin vaikutukset ovat vähäiset. Pieniä häiriöitä toiminnalle, kaikki tai lähes kaikki tavoitteet saavutetaan
    3. Riskin vaikutukset ovat huomattavat. Toiminnan hidastuminen, osa tavoitteista jää saavuttamatta
    4. Riskin vaikutukset ovat merkittäviä. Toiminnan huomattava vaikeutuminen, suuri osa tavoitteista jää saavuttamatta
    5. Riskin vaikutukset ovat erittäin merkittävä. Toiminnan lamaantuminen, tavoitteiden saavuttamisessa epäonnistutaan täysin.

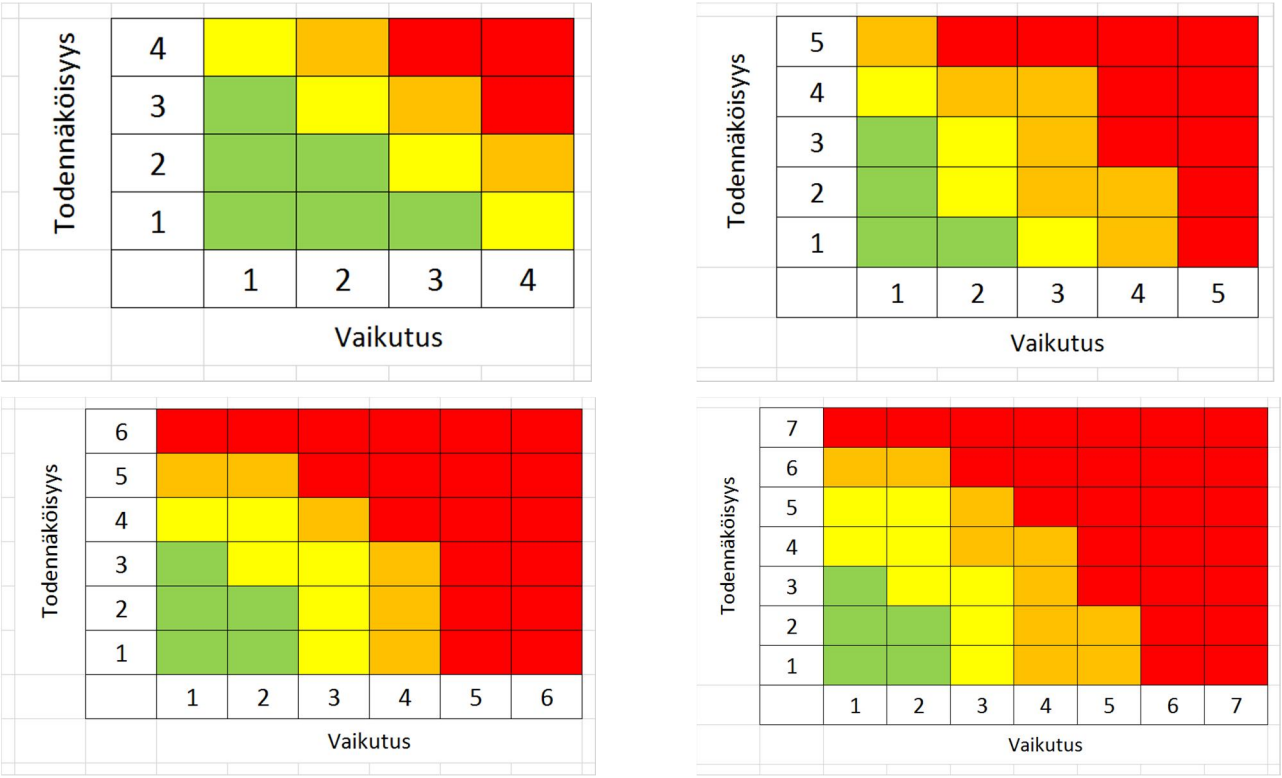
Huomaa, että esimerkeissäkin esitetyt käsitteet ovat riskienhallintaan tyypillisesti liittyvistä epävarmuustekijöistä johtuen vain suuntaa-antavia. Niiden perusteella ei voi näin ollen muodostaa tarkkoja kvantitatiivisia mittareita.

Organisaation riskienhallinnan kannalta hallintaprosessin muotoseikkoihin syventymistä tärkeämpää on tunnistaa riskejä ja suunnitella toimenpiteitä.

Esimerkkejä riskimatriiseista

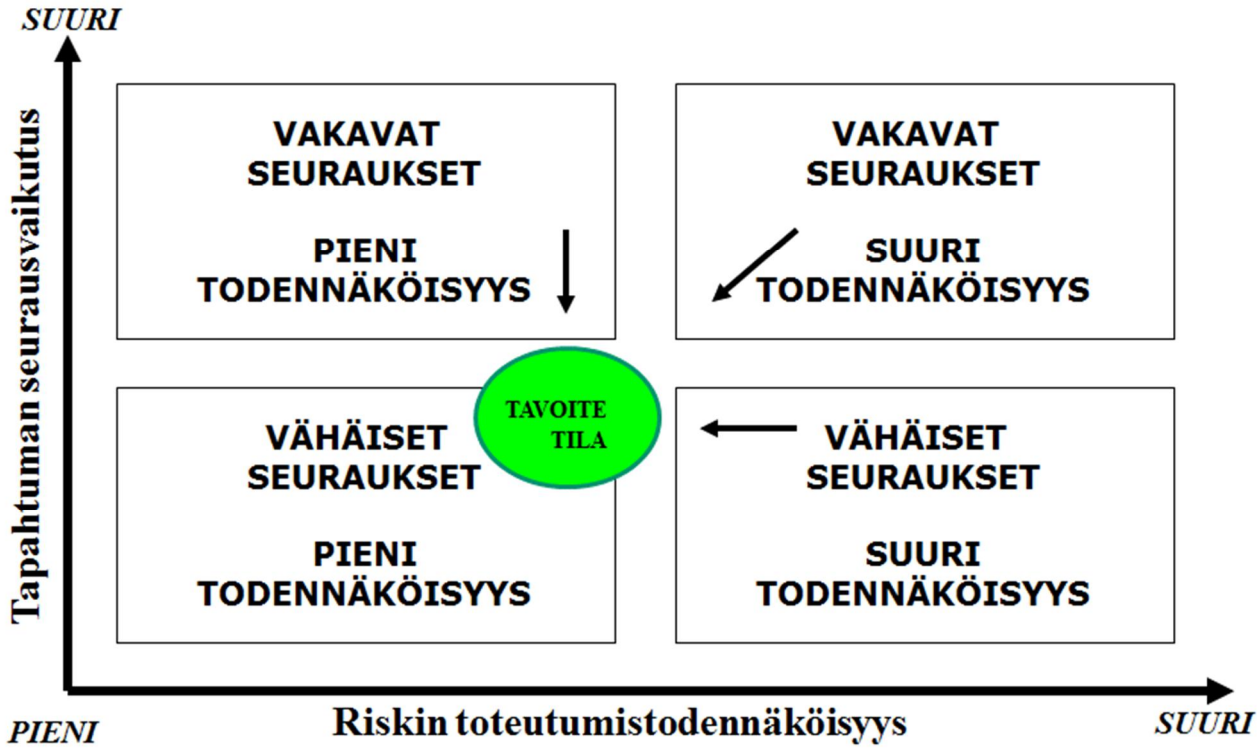


Kuva L5.1. *Riskimatriisit ja niissä olevien tasojen määrät voivat vaihdella organisaation riskienhallinnan tarpeista riippuen esimerkiksi sen mukaan, mitä merkitystä riskin arvolla tai riskinottokyvyllä riskienhallinnalle ja riskien käsittelylle on.*



Kuva L5.2. *Erilaisia riskimatriiseja. Perinteiseen uhkanäkökulmaan perustuvat riskimatriisit voivat vaihdella organisaatioittain paljonkin.*

Useimmiten riskin todennäköisyys voi olla suhteellisesti korkea, koska esimerkiksi jo pitkään tunnistetulle ja usein toteutuville riskille voi olla helpompaa tehdä vastatoimenpiteitä. Joissakin tapauksissa riskin toteutumisen todennäköisyys voi olla hyvin pieni, mutta toteutumisen vaikutukset todella suuria.

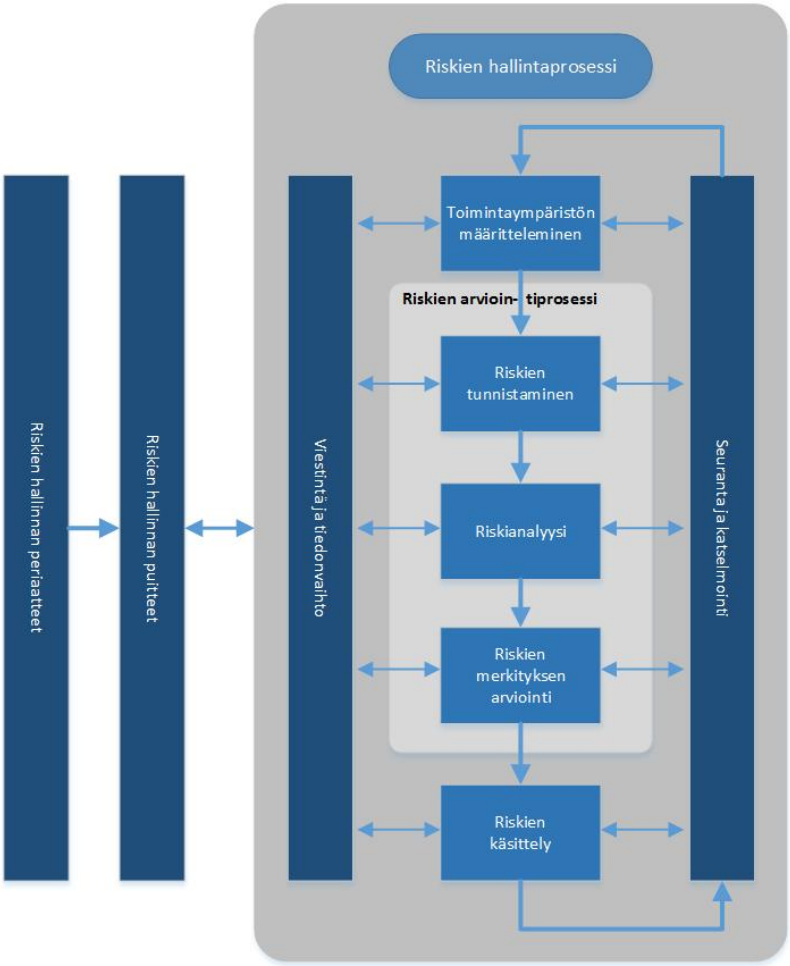


Kuva L5.3. *Riskien arvioinnin nelikenttä. Yksinkertainen seurausten ja vaikutusten arvioinnin kehys.*

ISO 31000:n mukainen riskienhallinnan prosessi

ISO 31000 perustuvaan riskienhallinnan ja riskien arviointiprosessiin sisältyvät

- toimintaympäristön määritteleminen
- riskienarviointi, jonka vaiheet ovat:
  - riskien tunnistaminen
  - riskianalyysi
  - riskien merkityksen arviointi
- riskien käsittely ja hallinta
- viestintä ja tiedonvaihto
- seuranta ja katselmointi.



Kuva L5.4. *Riskienhallinnan prosessin tärkeimmät elementit. Lähde: Kuva perustuu standardiin SFS-ISO 31000.*

Toimintaympäristön määritteleminen

Toimintaympäristön määrittelyssä toteutetaan riskien arvioinnin kannalta keskeiset rajaukset. Tämä tarkoittaa sen määrittelyä, mitä sisällytetään riskien arviointiin ja mitä jätetään arvioinnin ulkopuolelle. Riippuvuuksien tunnistaminen on välttämätöntä, mutta kaikkia riippuvuuksiin liittyvien tahojen riskejä on käytännössä mahdotonta ottaa huomioon. Toimintaympäristön määrittely yhteydessä myös riskien arvioinnin kohde yleensä tarkentuu.

Riskien arviointiprosessi

Riskien arviointiprosessin kaksi ensimmäistä vaihetta eli riskien tunnistaminen (riskien kirjaaminen) ja riskianalyysi (useimmiten todennäköisyyden ja vaikutuksen arviointi) ovat riskien arviointeihin osallistuneille tutuimmat toimenpiteet. Riskien merkityksen arviointi on useimmiten huomattavasti vaikeampaa, koska siinä tulee käsiteltäväksi myös subjektiivisia näkökulmia liittyen esimerkiksi siihen, kenen kannalta riskin merkitystä tarkastellaan.

Riskien tunnistaminen

Riskien tunnistamisen yhteydessä tulee kirjata riskien kaikki arvioinnin kohteeseen liittyvät tunnistettavissa olevat riskit. Riskien tunnistamisen (kirjaamisen) yhteydessä ei anneta yksittäisille riskeille todennäköisyyden tai vaikutuksen arvoja, koska arvojen kirjaaminen voi viedä huomion muualle ja siten olennaisesti haitata riskien tunnistamista.

Riskianalyysi

Riskianalyysissä arvioidaan riskikohtaisesti todennäköisyyttä ja vaikutuksia. Suositeltavaa on käyttää esimerkiksi 4 x 4 tai 5 x 5 riskimatriisia, jolloin vältetään ainakin 3 x 3 riskimatriisin käytölle tyypillinen riskien arvioiminen käyttäen eniten keskimmäisiä arvoja.

Ellei erityisen painavia syitä ole, riskimatriisista ei ole suositeltavaa tehdä siitä kovin moniportaista. Esimerkiksi jo 6 x 6 tai 7 x 7 -riskimatriisi voi johtaa kiinnittämään lähtökohtaisesti enemmän huomiota menetelmiin kuin varsinaiseen riskien analysointiin – puhumattakaan sitä monitasoisemmista riskimatriiseista.

Riskimatriiseissa tulisi ottaa huomioon myös riskeihin sisältyvät positiiviset mahdollisuudet. Kun tarkastellaan uusia mahdollisuuksia sisältäviä riskejä (ns. hyvät riskit) suhteessa vältettäviin riskeihin (ns. huonot riskit), ei kvantitatiivinen tarkastelu riskimatriisin muodossa ei ole toimivin tapa. Sen sijaan tulisi suosia kvalitatiivista tai jotain muuta kuin riskimatriisiin perustuvaa kvantitatiivista tarkastelutapaa

Riskien merkityksen arviointi

Riskien merkityksen arviointiin saadaan toteutettua helposti pelkistettyjä matemaattisia malleja, mutta painotuksia ja erityispiirteitä huomioivia ominaisuuksia on käytännössä mahdotonta sisällyttää geneerisiin valmismalleihin. Lineaarisesta tarkastelusta poikkeavat organisaatiokohtaiset arviointitavat edellyttävät siis suunnittelua ja muutosten tekemistä arvioinnissa käytettävään työkaluun.

Esimerkiksi yksinkertainen kertolasku *todennäköisyys* 2 x *vaikutus* 4 tuottaa saman tuloksen kuin *todennäköisyys* 4 x *vaikutus* 2. Voi olla lähes mahdotonta päättää pelkästään numeerisen arvon perusteella, kumpi tämän esimerkin luvuista 8 on toista vakavampi, vaikka käytännössä merkityksessä voi olla suuri ero. Yleensä riskin yleisempi esiintyminen ei kuitenkaan ole niin vakavaa kuin mahdollinen toteutumisesta aiheutuva vaikutus.

Riskien käsittely ja hallinta

Riskien käsittelyssä määritellään riskille jatkotoimenpiteet ja nimetään jatkotoimenpiteiden suorittamisesta vastuullinen henkilö. Useimmiten tässä yhteydessä määritellään myös vähintään alustava tavoiteaikataulu toimenpiteille ja nimetään taho, jolle toimenpiteiden suorittamisesta vastaavan henkilön on raportoitava.

Viestintä ja tiedonvaihto

Riskienhallinnan onnistumisen kannalta on välttämätöntä, että osapuolet viestivät keskenään riskeistä ja niille tehtävistä toimenpiteistä. Tiedonvaihto on myös tärkeää kehittämisen ja kehittymisen varmistamisessa.

Seuranta ja katselmointi

Riskienhallintatoimenpiteiden toteutumista on seurattava. Useimmiten seurantatilaisuuksia nimitetään katselmointitilaisuuksiksi ja niihin osallistuu vähintään organisaation riskienhallinnan vastuuhenkilö (esim. riskienhallintapäällikkö) sekä riskien omistajat.

Esimerkki yksinkertaistetusta riskienhallintaprosessista

Kuva L5.5. *Riskienhallinnan voi toteuttaa myös yllä kuvatun mukaisella vuosittain toistettavalla prosessilla.*

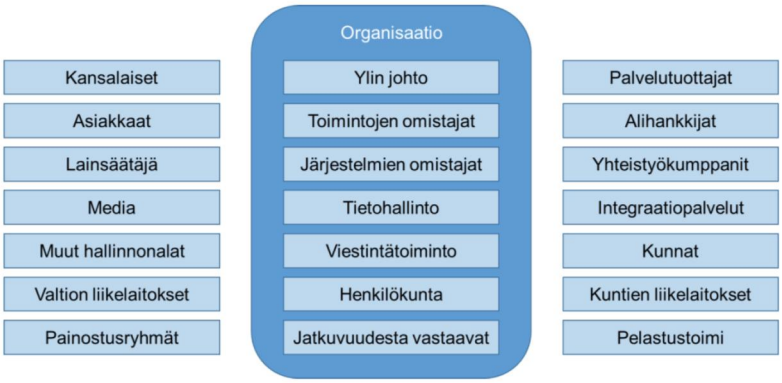
Esimerkki yksinkertaistetusta riskien seurantamallista

Tavoite	*Toimenpide*	*Aikataulu*	*Riskit*	*Riskienhallinta-toimepiteet*	*Tilanne*
1. Sähköinen asiointi ja palvelut ovat asiakaslähtöisiä	**1.1 Sähköinen asiointi** Edistetään sähköistä asiointia viraston järjestelmissä.	2017-2020	Rahoitus puuttuu.	Priorisoidaan digitalisoinnin toimenpiteitä tärkeys- ja vuositasolla.	Tarkoitetut lisäpalvelut ja ratkaisut eivät ole toteutuneet luvatusti. Sähköistä asiointia ei ole pystytty edistämään.
2. Asiakkaiden palvelu toteutuu tehokkaasti	**2.1 Tietojärjestelmät** Varmistetaan, että järjestelmät ovat helppokäyttöisiä, turvallisia ja valvottavissa olevia.	2016	Itse toteutut tukitoimet ja järjestelyt jäävät tarpeettomiksi.	Hyödynnetään valtion yhteisiä ratkaisuja tukitoimiin ja niihin liittyviin järjestelyihin.	Toteutunut onnistuneesti.
	2.2 Erillisjärjestelmä Huolehditaan erillisen järjestelmän X ajantasaisuudesta.	2016-2020	Järjestelmän päivitykset jäävät tekemättä, koska rahoitus puuttuu.	Tulosohjaajalle tietoa lisää tilanteesta ja sitotuminen rahoituksen järjestämiseen.	Toimintaprosessia ei ole voitu digitalisoida rahoituksen edelleen puuttuessa.

Kuva L5.6. *Riskien seurantaa voi toteuttaa myös yllä kuvatun mukaisella pelkistetyllä mallilla.*

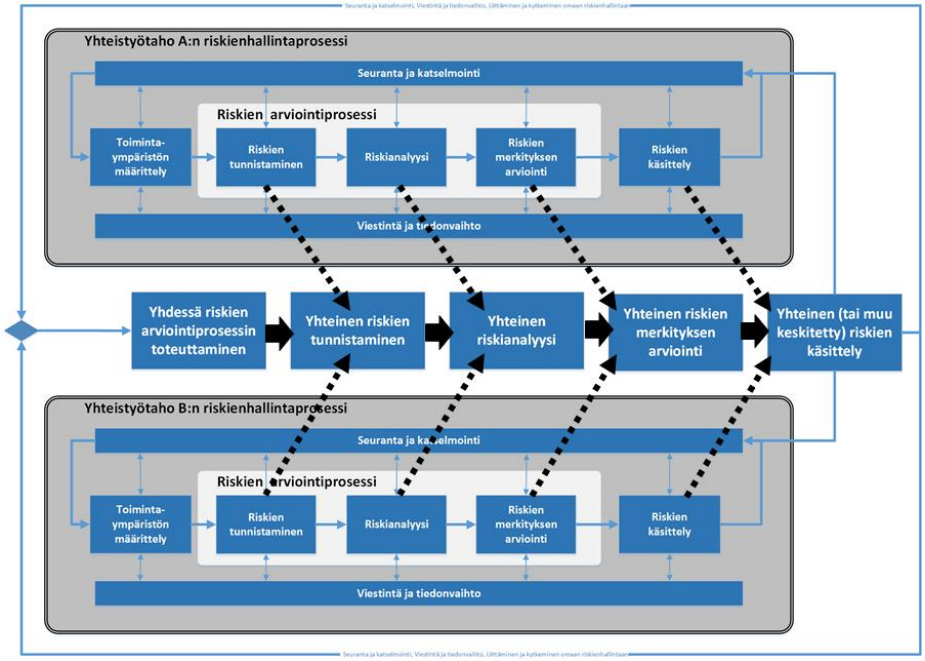
Tärkeiden kumppaneiden riskien arviointi ja riskien huomioon ottaminen

Toimintaverkostot voivat olla hyvin moniportaisia, jolloin riskienhallinnassa ensimmäinen tehtävä on tunnistaa riittävän laajasti sidosryhmät. Tämän jälkeen tulee tunnistaa oman toiminnan kannalta tärkeimmät osapuolet ja kumppanit. Lisäksi tunnistaa mitä riskejä yhteistyöhön liittyy tai millä yhteistyötahojen riskeillä voi olla vaikutusta omaan toimintaan (yhteistyön kohteeseen liittyvät riskit).



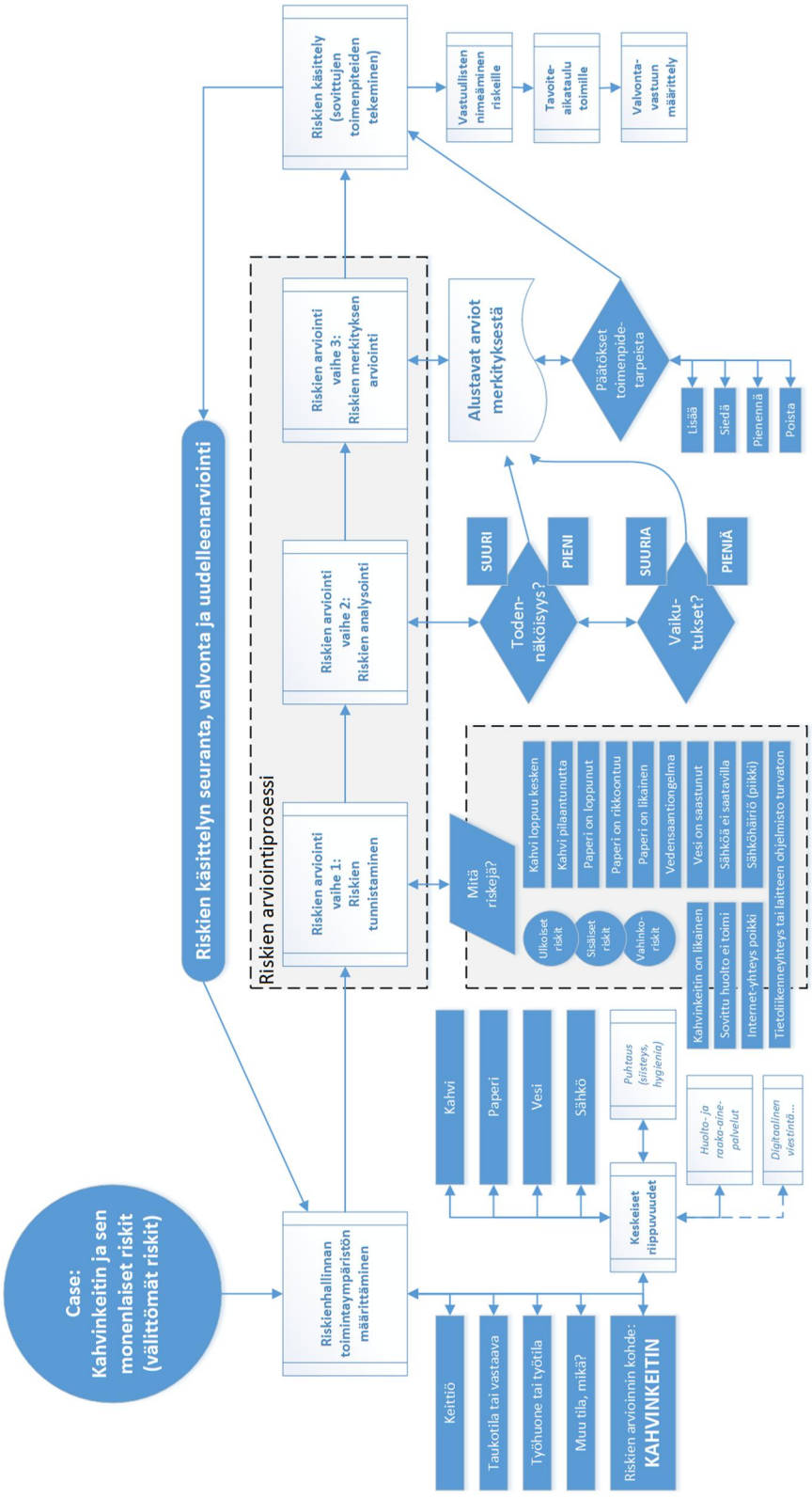
Kuva L5.7. *Organisaation sidosryhmät. Esimerkkejä sisäisistä ja ulkoisista sidosryhmistä. (Kuvan lähde: VAHTI 2/2016.)*

Kumppanin ja kumppaneiden riskien arvioinnissa tulee tehdä yhteistyötä. Osapuolten on kartoitettava aluksi keskenään riskienhallinnan tavoitteet ja riskienhallinnassa sovellettavat periaatteet. Niihin liittyen on määriteltävä myös sovellettavat riskienhallinnan menetelmät (käytännössä minkälaista prosessia eri osapuolet käyttävät kunkin osapuolen omassa riskien arvioinnissa). Yhteisessä riskien arvioinnissa on suunniteltava prosessin pääkohdat (riskien tunnistaminen, riskianalyysi ja riskien merkityksen arviointi). Riskien käsittely, jossa nimetään riskeille omistajat ja päätetään riskeille tehtävistä toimenpiteistä, on suunniteltava huolellisesti, jotta riskejä käsitellään kaikkien mukana olevien osapuolten kannalta oikeudenmukaisesti ja tasapuolisesti.



Kuva L5.8. *Esimerkki kumppaneiden riskien arvioinnin toteuttamistavasta. Lähde: Kuva perustuu standardiin SFS-ISO 31000*

- ***Esimerkki riskien arvioinnista, kuvitteellinen käyttötapaus: Kahvinkeitin -*** **Kahvinkeittimeen liittyvien asioiden riskiarvioinnin kuvaus**



Kuva L5.9. *Riskienhallinta ja riskien arviointi edellyttää onnistuakseen riittävän laajaa ja monipuolista kokonaistarkastelua.*

Kahvinkeittimeen liittyvien asioiden riskiarviointi – tietojen vienti taulukkoon

Riskin tunniste	Riskiluokka	Riski (riskin nimi)	Syyt ja tekijät riskin taustalla - miksi riski voi toteutua?	Seurauksia riskin toteutumisesta - mitä voi tapahtua?	Todennäköisyys		Vaikutus		Riskin suuruus (T x V)	Toimenpidetarpeet riskin käsittelylle (vakavuus/sietokyky)	Toimenpide-ehdotukset riskin käsittelylle	Toimenpiteiden vapaamuotoinen (sanallinen) kuvaus	Vastuuhenkilö	Tavoitealkutaulu (mihin mennessä toimenpiteitä)	Tavoitteen tarkastus (päivämäärä)	Tarkastaja (riskin toimenpiteiden valvoja)	Liittyykö riskin mahdollisuus (1 = kyllä, 2 = ei)	Sanallinen kuvaus mahdollisuudesta (mitä voi saavuttaa)	Lisätietoja
St01	1	Strateginen	Raaka-aine (kahvi) loppuu.	Ei ole käyty kaupassa tai automaattinen raaka-aineen tilatiedottaminen ei toimi. Kahvia on voitu myös rikkoa tai varastaa.	4	Lähes varma	4	Kriittinen	16	Sietämätön riski	4	Huomioitava riski	Vastli vaihtoehtoja toimenpiteitä	Luotava prosessi tai tehtävä, pila riski ehkäistään. Liittyy St02, Hr01 ja Hr02.	Kalevi Keittövastaava	Yhden (1) viikon kuluessa.	Kahden (2) viikon kuluessa.	Unto Monottaja, yksikönjohtaja	1	Kyllä	Voidaan parantaa valmiutta myös ruuhkahuippuihin merkittävästi.
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.	3	Merkittävä	3	Huomioitava riski	12	Sietämätön riski	4	Huomioitava riski	Vastli toimenpiteitä toimenpiteitä	Luotava prosessi tai tehtävä, pila riski ehkäistään. Liittyy St01, Hr01 ja Hr02.	Kalevi Keittövastaava	Yhden (1) viikon kuluessa.	Kahden (2) viikon kuluessa.	Unto Monottaja, yksikönjohtaja	1	Kyllä	Paramus ei ole merkittävä, mutta on kuitenkin.
St03	1	Strateginen	Vedenjakelukatkos.	Vedenjakelun keskeytyksestä ei oie tiedotettu. Tai jos on tiedotettu, on unohdettu varata kahvinkeittoon tarvittavaa vettä.	Asiakas ei saa hänelle luvattua (odottamaansa) kahvia ajallaan ja kieltäytyy sopimuksen allekirjoittamisesta.	2	Kohtalainen	6	Merkittävä riski	3	Huomioitava riski	Luotava suunnitelma pienentämiseksi	Hankittava riittävästi termospulloja, jotta vaikutuksia voidaan pienentää. Liittyy St03.	Timo Pomottaja, työnjohto	Koukauden kuluessa.	Parin kuukauden kuluessa.	Unto Monottaja, yksikönjohtaja	1	Kyllä	Voidaan parantaa valmiutta myös ruuhkahuippuihin merkittävästi.
St04	1	Strateginen	Sähkönjakelukatkos.	Suunniteltu (tiedotettu) tai odottamaton katkos sähkönjakelussa.	Asiakas ei saa hänelle luvattua (odottamaansa) kahvia ajallaan ja kieltäytyy sopimuksen allekirjoittamisesta.	2	Mahdollinen	2	Kohtalainen	4	Huomioitava riski	2	Ei riskiä	Seurattava riskin kehittymistä	Riski tiedoksi.	Timo Pomottaja, työnjohto	Puolivuosittain.	Seuraava riskiarviointi.	Riskienarviointi-ryhmä	2	Ei	
Hr01	4	Henkilöstö	Raaka-aine (kahvi) loppuu.	Ei ole käyty kaupassa tai automaattinen raaka-aineen tilatiedottaminen ei toimi. Kahvia on voitu myös varastaa.	Henkilöstön tauot eivät onnistu odotetusti. Tulee kireä työilmapiiri.	4	Lähes varma	2	Kohtalainen	8	Merkittävä riski	3	Huomioitava riski	Luotava suunnitelma pienentämiseksi	Luotava prosessi tai tehtävä, pila riski ehkäistään. Liittyy Hr02, St01 ja St02.	Kalevi Keittövastaava	Koukauden kuluessa.	Parin kuukauden kuluessa.	Matti Vekkäinen, hallintojohtaja	1	Kyllä	Voidaan parantaa valmiutta myös ruuhkahuippuihin merkittävästi.
Hr02	4	Henkilöstö	Suodatinpaperi loppuu.	Ei ole käyty kaupassa tai automaattinen raaka-aineen tilatiedottaminen ei toimi. Suodatinpaperit on voitu myös rikkoa tai varastaa.	Henkilöstön tauot eivät onnistu odotetusti. Tulee kireä työilmapiiri.	4	Lähes varma	2	Kohtalainen	8	Merkittävä riski	3	Huomioitava riski	Luotava suunnitelma pienentämiseksi	Luotava prosessi tai tehtävä, pila riski ehkäistään. Liittyy Hr01, St01 ja St02.	Kalevi Keittövastaava	Koukauden kuluessa.	Parin kuukauden kuluessa.	Matti Vekkäinen, hallintojohtaja	1	Kyllä	Paramus ei ole merkittävä, mutta on kuitenkin.
Hr03	4	Henkilöstö	Vedenjakelukatkos.	Vedenjakelun keskeytyksestä ei oie tiedotettu. Tai jos on tiedotettu, on unohdettu varata kahvinkeittoon tarvittavaa vettä.	Henkilöstön tauot eivät onnistu odotetusti. Tulee kireä työilmapiiri.	2	Kohtalainen	6	Merkittävä riski	3	Huomioitava riski	Luotava suunnitelma pienentämiseksi	Hankittava riittävästi termospulloja, jotta vaikutuksia voidaan pienentää. Liittyy St03.	Timo Pomottaja, työnjohto	Koukauden kuluessa.	Parin kuukauden kuluessa.	Matti Vekkäinen, hallintojohtaja	1	Kyllä	Voidaan parantaa valmiutta myös ruuhkahuippuihin merkittävästi.
Hr04	4	Henkilöstö	Sähkönjakelukatkos.	Suunniteltu (tiedotettu) tai odottamaton katkos sähkönjakelussa.	Henkilöstön tauot eivät onnistu odotetusti. Tulee kireä työilmapiiri.	2	Mahdollinen	2	Kohtalainen	4	Huomioitava riski	2	Ei riskiä	Seurattava riskin kehittymistä	Riski tiedoksi.	Timo Pomottaja, työnjohto	Puolivuosittain.	Seuraava riskiarviointi.	Riskienarviointi-ryhmä	2	Ei	
Va01	6	Vahinko	Tulipalo	Kahvinkeitin syttyy tuleen.	Rakennus palaa. Tietoja voi menettää. Henkilöitä hengenvaarassa. Infraa (huonelaut. telokoneet. työdist) tuhoutuu paljon. Seurauksista voi seurata laaja vesivahinko.	2	Mahdollinen	4	Kriittinen	8	Merkittävä riski	3	Huomioitava riski	Laadittava suunnitelma pienentämiseksi	Selvitettävä keinot pienentää riskiä. Laadittava suunnitelma. Seurautuset osin samanlaisia kuin Va02.	Risto Karhu, turvallisuusvastaava	Koukauden kuluessa.	Parin kuukauden kuluessa.		2	Ei	
Va02	6	Vahinko	Vesivahinko	Kahvin keittämisen yhteydessä vesivahinko.	Vesivuoto voi johtaa veden rakenteisiin, jonka seurauksena korjaus ja remontointitoimenpiteitä.	2	Mahdollinen	4	Kriittinen	8	Merkittävä riski	3	Huomioitava riski	Laadittava suunnitelma pienentämiseksi	Selvitettävä keinot pienentää riskiä. Laadittava suunnitelma. Seurautuset osin samanlaisia kuin Va01.	Risto Karhu, turvallisuusvastaava	Koukauden kuluessa.	Parin kuukauden kuluessa.		2	Ei	
Hr05	4	Henkilöstö	Työhyvinvointimyys kasvaa	Henkilöstö ei saa kahvia	Henkilöstön tauot eivät onnistu odotetusti. Tulee kireä työilmapiiri.	2	Mahdollinen	3	Merkittävä	6	Merkittävä riski	3	Huomioitava riski	Luotava suunnitelma pienentämiseksi	Laadittava ehdotus riskin pienentämisestä.	Timo Pomottaja, työnjohto ja Taneli Tukimies, työsuojeluvastaava	Koukauden kuluessa.	Parin kuukauden kuluessa.		1	Kyllä	Toimenpiteiden seurauksena työtyytyväisyys voi myös kasvaa.
Op01	2	Operatiivinen	Pesu puuttuu	Siivous ei ole toteutunut.	Pikkityessään estää kahvin keittämisen.	2	Mahdollinen	2	Kohtalainen	4	Huomioitava riski	2	Ei riskiä	Seurattava riskin kehittymistä	Riski tiedoksi.	Timo Pomottaja, työnjohto	Puolivuosittain.	Seuraava riskiarviointi.	Riskienarviointi-ryhmä	2	Ei	
Te01	5	Teknologinen	Päivitys puuttuu	Internet-yhteys ei toimi. huolto ei saa tietoa huoltotarpeesta.	Pikkityessään estää kahvin keittämisen.	2	Mahdollinen	2	Kohtalainen	4	Huomioitava riski	2	Ei riskiä	Seurattava riskin kehittymistä	Liittyy Te02. Tiedoksi.	Yks Ylläpitäjä, atk-tuki	Puolivuosittain.	Seuraava riskiarviointi.	Riskienarviointi-ryhmä	2	Ei	
Te02	5	Teknologinen	Tekninen vika	Internet-yhteys ei toimi. huolto ei saa tietoa huoltotarpeesta.	Joko heti tai myöhemmin estää kahvin keittämisen.	2	Mahdollinen	3	Merkittävä	6	Merkittävä riski	3	Huomioitava riski	Luotava suunnitelma pienentämiseksi	Luotava suunnitelma ja toteutusehdotus varayhteydestä. Liittyy Te01	Yks Ylläpitäjä, atk-tuki	Koukauden kuluessa.	Parin kuukauden kuluessa.		1	Kyllä	Varayhteyttä voidaan mahdollisesti käyttää myös muihin tarpeisiin.
Ta01	3	Taloudellinen	Kustannusten nousu	Kahvin hinta maailmalla kasvaa odottamattoman korkealle.	Budjetti ylittyy (rahat loppuvat). Tai kahvia ei voi enää keittää ja asiakkaat ja työntekijät ovat ilman kahvia.	1	Epätodennäköinen	4	Kriittinen	4	Huomioitava riski	2	Ei riskiä	Seurattava riskin kehittymistä	Riski tiedoksi.	Tina Tarkka, talousjohtaja	Vuosittain	Seuraava riskiarviointi.	Riskienarviointi-ryhmä	2	Ei	
Ta02	3	Taloudellinen	Kahvinkeitin menetetään.	Kahvinkeitin nikkonbu tai esim. varastetaan. Uushankinta.	Kallis investointi laitteeseen ja mahdollisesti sen laajaan käyttöön. Mali voi vaihtua, jolloin vanhat varaosat eivät enää käy. Käyttökoulutus uudelleen.	1	Epätodennäköinen	3	Merkittävä	3	Huomioitava riski	2	Ei riskiä	Seurattava riskin kehittymistä	Riski tiedoksi.	Tina Tarkka, talousjohtaja	Vuosittain	Seuraava riskiarviointi.	Riskienarviointi-ryhmä	1	Kyllä	Uusi keitin.
Op02	2	Operatiivinen	Toiminta keskeytyy	Kahvi (raaka-aine) on myrkyllistä/myrkytetyä.	Koko toimitila joudutaan evakuoimaan ja työnteko keskeytymään esim. viikoiksi.	1	Epätodennäköinen	4	Kriittinen	4	Huomioitava riski	2	Ei riskiä	Seurattava riskin kehittymistä	Riski tiedoksi.	Taneli Tukimies, työsuojeluvastaava	Puolivuosittain.	Seuraava riskiarviointi.	Riskienarviointi-ryhmä	2	Ei	

Yhteenveto Kahvinkeitin-käyttötapauksen riskien arvioinnista

Yhteenvetona voidaan suoritetun (kuvitteellisen) riskiarvioinnin perusteella todeta, että

- Strategisiksi luokiteltavia riskejä tunnistettiin yhteensä 4 kpl
- Henkilöstöriskeiksi luokiteltavia riskejä tunnistettiin yhteensä 5 kpl
- Vahinkoriskeiksi luokiteltavia riskejä tunnistettiin yhteensä 2 kpl
- Operatiivisiksi luokiteltavia riskejä tunnistettiin yhteensä 2 kpl
- Taloudellisiksi riskeiksi luokiteltavia riskejä tunnistettiin yhteensä 2 kpl
- Teknologiariskeiksi luokiteltavia riskejä tunnistettiin yhteensä 2 kpl

Riskien merkityksen arvioinnin yhteydessä voitaisiin tämän kuvitteellisen esimerkin perusteella todeta, että

- 2 kpl riskejä vaatii välittömiä toimenpiteitä
- 8 kpl riskejä vaatii suunnitelman tunnistettujen riskien pienentämiseksi

Riskien käsittelyn esimerkkitoimenpiteet voisivat olla seuraavat: Riskeille nimettiin omistajat. Päätettiin jatkotoimista. Sovittiin myös raportointitapa ja tahot, joille riskeille tehtävistä toimenpiteistä raportoidaan.

Käytännön esimerkkejä riskien käsittelytavoista

Tyypillisiä riskien käsittelyvaihtoehtoja ovat:

- **riskin torjuminen**
  - esimerkiksi pidättäytymällä riskin aiheuttavasta toiminnasta
- **riskin ottaminen**
  - tai riskin lisääminen jonkin mahdollisuuden saavuttamiseksi
- **riskin lähteen poistaminen**
  - tai muu riskin lähteeseen vaikuttaminen
- **riskin todennäköisyyteen**
  - varautuminen tai muu todennäköisyyden muuttaminen
- **riskin seurauksiin varautuminen**
  - tai muu seurausten muuttaminen
- **riskin jakaminen**
  - osittain tai kokonaan jonkin toisen osapuolen tai toisten osapuolten kesken
- **riskin säilyttäminen**
  - sellaisenaan

Riski voidaan torjua pidättäytymällä riskin aiheuttavasta toiminnasta. Esimerkiksi on tunnistettu riskiksi (teemat: terveys/henki, liikenne, tietojärjestelmähanke, henkilöstö, yleisnäkökulma), että…

- …jonkin tietyn valtion alueella on henkilöihin kohdistuva suuri hengen tai terveyden vaara, jolloin päätetään, että ei mennä eikä lähetetä ihmisiä kyseisen valtion alueelle.

- …liikenneolosuhteet ovat vaikeat sään takia, jolloin päätetään, että ei mennä ainakaan vaikeimmille liikenneolosuhdealueille.

- …tietojärjestelmähankkeen kustannukset ovat täysin kohtuuttomat, jolloin päätetään, ettei hanketta käynnistetä lainkaan.

- …henkilöstöä ei ole tai sitä ei voi lisätä riittävästi toteuttamaan asiakaspalvelua, jolloin päätetään olla järjestämättä asiakkaille palvelua.

- …yksinkertaisesti jätetään tekemättä riskiä sisältävät hankkeet ja tehtävät.

Riskin ottaminen tai riskin lisääminen jonkin mahdollisuuden saavuttamiseksi, kun…

- …jonkin tietyn valtion alueella on henkilöihin kohdistuva suuri hengen tai terveyden vaara, mutta todetaan esimerkiksi humanitäärisen avun tarve ja nähdään kyseisen avun tarjoamisen kautta suuret mahdollisuudet pelastaa ihmishenkiä ja sen seurauksena edistää rauhanponnisteluita.

- …liikenneolosuhteet ovat vaikeat sään takia, mutta todetaan saavutettavan enemmän etua sillä, että olosuhteista huolimatta lähdetään liikkeelle ja kannustetaan muitakin lähtemään liikkeelle.

- …tietojärjestelmähankkeen kustannusten olevan huomattavan korkeat, mutta todetaan lopputuloksen tuovan merkittäviä etuja ja päätetään ottaa riski ja käynnistää hanke.

- …henkilöstöä ei ole tällä hetkellä riittävästi toteuttamaan asiakaspalvelua, mutta päätetään kuitenkin tuottaa palvelua niillä resursseilla, jotka ovat käytettävissä. Tiedotetaan palvelun saatavuudesta, vaikka se lisääkin riskiä siitä, että asiakasyhteydenottoja tulee enemmän.

- …yksinkertaisesti tarkastellaan saatavia hyötyjä ja etuja sekä otetaan hallitusti jopa lisää riskiä, jotta onnistuminen olisi odotettua suurempi.

Riskin lähteen poistaminen toimenpiteenä tilanteessa, jossa…

- …jonkin tietyn valtion alueella on esimerkiksi rokotteella torjuttavissa oleva henkilöihin kohdistuva tautiepidemiasta johtuva suuri hengen tai terveyden vaara. Päätetään toteuttaa kattava rokotuskampanja, jonka ansiosta hengen tai terveyden vaara poistuu.

- …liikenneolosuhteet ovat vaikeat esimerkiksi teiden lumisuudesta johtuen. Päätetään aurata lunta pois, jolloin kaaosta aiheuttava lumen määrä ajoteillä vähenee ja riski pienenee.

- …tietojärjestelmähankkeen kustannusten olevan kohtuuttoman korkeat, jolloin päätetään käyttää yhteistyökumppania. Seurauksena hankkeen toteuttaakin omalla riskillään kumppani, joka sitoutuu tarjoamaan ratkaisun siedettävään kiinteään hintaan. Tällöin korkeiden kustannusten ja odottamattomien kustannusten nousujen riski minimoituu tai jopa poistuu.

- …henkilöstöä ei ole tällä hetkellä riittävästi toteuttamaan asiakaspalvelua ja riskinä on palvelutason heikkeneminen. Tehdään päätös rekrytoida ja kouluttaa tehtäviin tarvittava määrä kattamaan myös ruuhkahuippujen tarpeet esimerkiksi sijaisjärjestelyin, jolloin riski voidaan poistaa.

- …yksinkertaisesti tarkastellaan riskin syytä ja pyritään vaikuttamaan siihen, että riskin alkuperäinen syy ei enää vaikuttaisi tai mahdollistaisi riskin toteutumista.

Riskin todennäköisyyteen varautuminen tai muu todennäköisyyden muuttaminen tilanteessa, jossa…

- …jonkin tietyn valtion alueella on esimerkiksi 90 %:n todennäköisyydellä rokotteella estettävissä oleva taudin tartuntavaara. Päätetään rokottaa kaikki maahan syystä tai toisesta vierailemaan menevät ihmiset, jolloin tämä toimenpide vähentää merkittävästi riskin toteutumisen todennäköisyyttä.

- …liikenneolosuhteet ovat vaikeat esimerkiksi teiden liukkauden vuoksi. Päätetään käyttää ajoneuvoissa talvirenkaita sekä mahdollisuuksien mukaan hiekoittaa tai suolata teitä ja jalkakäytäviä, jolloin liukkaudesta johtuvien riskien toteutumisen todennäköisyydet pienenevät.

- …tietojärjestelmähankkeen kustannukset ovat korkeat ja riskinä ovat odottamattomat ylimääräiset kustannukset esim. resurssien käytettävyydestä ja aikataulun pettämisestä johtuen. Kuvataan riskit hankesuunnitelmaan ja sopimuksin velvoitetaan osapuolet huolehtimaan riittävän osaavan henkilöstön jatkuvasta käytettävyydestä esimerkiksi varahenkilökäytäntöjä hyödyntäen. Tällä tavoin voidaan ainakin osin pienentää ammattitaitoisen henkilöstön poissaoloista johtuvien riskien toteutumisen todennäköisyyttä.

- …henkilöstöä ei ole tällä hetkellä riittävästi vastaamaan ruuhkahuippujen aikaiseen palvelutarpeeseen. Päätetään palkata ja kouluttaa satunnaisesti ja nopeasti paikalle saatavia ruuhka-apulaisia sekä varataan myös näiden ruuhka-apulaisten työskentelyä varten työnteossa tarvittavat välineet ja puitteet (esim. etätyömahdollisuus). Näin todennäköisyys asiakaspalvelun ylikuormittumiseen pienenee merkittävästi ja mahdollisuudet ruuhkahuippujen työkuorman purkamiseen etätyönä pienentää myös todennäköisyyttä sille, että työtiloja ei riitä kaikille.

- …yksinkertaisesti tarkastellaan riskin todennäköisyyttä ja siihen vaikuttavia tekijöitä ja suunnitellusti varaudutaan toimenpiteillä, jotka pienentävät toteutumisen todennäköisyyttä.

Riskin seurauksiin ennalta varautuminen tai muu seurausten muuttaminen, kun…

- …jonkin tietyn valtion alueella on melko suuri taudin tartuntavaara. Hankitaan etukäteen lääkkeitä tai varmistetaan nopea lääkäripalveluiden saatavuus sen varalle, että tautitartuntoja alkaa esiintyä.

- …liikenneolosuhteet ovat vaikeat esimerkiksi teiden liukkauden vuoksi. Hankitaan ajoneuvoihin kattavampi vakuutus ja/tai pienempi omavastuuosuus vahinkojen varalle.

- …tietojärjestelmähankkeen kustannukset ovat korkeat ja riskinä ovat odottamattomat ylimääräiset kustannukset hankkeen aikana. Näihin varautumiseksi budjetoidaan käytettävissä olevia varoja tai varaudutaan käyttämään toiseen hankkeeseen varattuja varoja riskejä sisältävän hankkeen odottamattomiin kustannuseriin.

- …henkilöstöä ei ole tällä hetkellä riittävästi vastaamaan ruuhkahuippujen aikaiseen puhelinpalvelutarpeeseen. Ostetaan niin kutsuttu ”ylivuoto” etukäteen laadittavan sopimuksen ja sopimuksessa sovittujen ehtojen mukaisesti palveluntarjoajalta tai kumppanilta, joka on sitoutunut palvelusopimuksen puitteissa varmistamaan palveluhenkilöstön kapasiteetin riittävyydestä.

- …yksinkertaisesti tarkastellaan mitä riskin toteutumisesta voi seurata ja varaudutaan kykyyn selvitä seurauksista.

Riskin jakaminen osittain tai kokonaan jonkin toisen osapuolen tai toisten osapuolten kesken, esimerkiksi tilanteessa, jossa…

- …jonkin tietyn valtion alueella on suuri hengen tai terveyden vaara. Sovitaan yhteistyöhön liittyvien toimien osalta kumppanitahon kanssa maassa vierailevien osalta vuorottelua tai muuta sijaisjärjestelyä, jolloin varmistetaan, etteivät kaikki riskit ole ainoastaan omalla vastuulla.

- …liikenneolosuhteet ovat vaikeat esimerkiksi teiden liukkauden vuoksi ja kaikkia suunniteltuja kuljetuksia ei pystyttäisi omin voimin toimittamaan ajoissa. Etukäteen suunnitellun varasuunnitelman mukaan toteutetaan kumppanin kanssa esimerkiksi yhteiskuljetuksia, jolloin olosuhteista johtuvien aikatauluviiveiden vaikutusta voitaisiin kompensoida toimitusten tavanomaista hitaamman mutta käytännössä huomattavasti kattavamman kokonaiskapasiteetin avulla.

- …tietojärjestelmähankkeen kustannukset ovat korkeat ja riskinä ovat odottamattomat ylimääräiset kustannukset hankkeen aikana. Tiedetään kumppanilla olevan samanlaisen järjestelmän hankintatarve, jolloin päätetään toteuttaa hankinnat yhtäaikaisesti ja mahdollisuuksien mukaan toteuttaa yhteinen järjestelmä. Tällöin ylimääräisten kustannusten jakajia on enemmän.

- …henkilöstöä ei ole tällä hetkellä riittävästi hoitamaan kaikkia tarvittavia palvelupisteitä ja samanaikaisesti tunnistetaan suuri ”hukkakapasiteetin” riski. Tällöin voidaan perustaa yhteispalvelupisteitä, joissa palveluhenkilöstö on kouluttautunut hoitamaan esimerkiksi kahden tai useamman eri organisaation palveluita saman pisteen kautta. Näillä toimilla minimoidaan ja jaetaan riskiä palveluhenkilöstön ”tyhjäkäynnistä” (odottelusta).

- …yksinkertaisesti arvioidaan riskejä myös siitä näkökulmasta, kuinka niitä voidaan joko jakaa tai siirtää myös toisen vastuulle sopimuksin tai yhteistoimintaa laajentamalla.

Riskin säilyttäminen sellaisenaan

- …jonkin tietyn valtion alueella on suuri hengen tai terveyden vaara, mutta todetaan, että riski on olemassa ja riskistä huolimatta mennään ko. valtion alueelle.

- …liikenneolosuhteet ovat vaikeat esimerkiksi teiden liukkauden vuoksi, mutta todetaan olosuhteiden olevan yhtä vaikeat kaikille ja päätetään liukkaudesta huolimatta lähteä liikkeelle (jalkaisin tai ajoneuvolla).

- …tietojärjestelmähankkeen kustannukset ovat korkeat ja riskinä ovat odottamattomat ylimääräiset kustannukset, mutta todetaan riskin olevan. Käynnistetään hanke ja toivotaan, ettei riski toteudu.

- …henkilöstöä ei ole tällä hetkellä riittävästi kaikkien ruuhkahuippujen hoitamiseen, mutta todetaan tilanne ja otetaan riski siitä, että palvelua vaille jääneet asiakkaat joko lähettävät reklamaatioita tai vaihtavat asiointinsa muualle.

- …yksinkertaisesti todetaan riski ja päätetään, että riskille, sen todennäköisyydelle tai syille ei tehdä mitään. Jätetään myös riskin seurauksiin varautumistoimet suunnittelematta (esimerkiksi sellaisessa tilanteessa, jolloin riskiä ei voi poistaa tai riskin pienentämisen kustannukset ovat kohtuuttoman suuria tai riskiä ei yksinkertaisesti voi poistaa).

LIITE 6: Riskien kuviteltuja toteutumisskenaarioita

Tässä liitteessä on kuviteltuja esimerkkejä riskien toteutumisskenaarioista:

- Strateginen riski, seurauksena onnistuminen tai epäonnistuminen
- Taloudellinen riski, seurauksena onnistuminen tai epäonnistuminen
- Operatiivinen riski, seurauksena onnistuminen tai epäonnistuminen
- Projektinhallintaan liittyvien riskien haitat ja mahdollisuudet
- Muita riskien toteutumisskenaarioita
    - Henkilöstöön liittyvä riski (esim. sairastuminen)
    - Toimitilojen menettäminen (esim. omat tilat tai konesalitilat, esim. vesivahinko/tulipalo)
    - Laaja kyberturvallisuusriski toteutuu (esim. palvelunestohyökkäys)
    - Laaja tietovuoto (esim. salasanat ja käyttäjätunnukset, tai salassa pidettävien asiakirjojen vuotaminen)

Strateginen riski, seurauksena onnistuminen tai epäonnistuminen

Organisaatio tunnistaa tutkimuslaitosten ennusteiden perusteella palvelutoimintansa toimintaympäristön pitkän aikavälin (vaikuttaa viiden seuraavan vuoden ajan) kehittämiseen liittyvät vaihtoehdot, joita käytännössä ovat:

a) Investoinnin lykkääminen ja määrätietoinen pysyttäytyminen vanhassa toimintamallissa. Muutosten toteuttaminen vasta mahdollisimman myöhäisessä vaiheessa, jolloin vanha toimintamalli ja siihen liittyvät teknologiat ovat tulleet täysin peruuttamattomasti elinkaarensa päähän.
Riskeinä mainitaan muun muassa viivyttelystä aiheutuvien kustannushyötyjen menettäminen ja myöhempien investointien nykyistä korkeampi kustannusvaikutus.

b) Suuren kertainvestoinnin toteuttaminen pitkäaikaisen rahoituksen turvin uuteen toimintamalliin ja sen vaatimiin teknologioihin.
Riskeinä mainitaan mahdolliset uusien teknologioiden yhteensopivuusongelmat ja näistä johtuvat ennalta tuntemattomat kustannusvaikutukset.

Jos organisaatio valitsee vaihtoehdon a, joka on lyhyen aikavälin tarkastelussa vaihtoehtoa b vähemmän riskejä sisältävä, jolloin esimerkkejä seurauksista ovat seuraavat:

- Onnistuminen: Käytössä ollut toimintamalli teknologioineen ei vanhentunutkaan niin nopeasti kuin ennustettiin ja uusien teknologioiden yhteensovittamisessa ilmeni kohtuuttoman suuria yhteensopivuusongelmia. Organisaatio otti riskin ja seuraukset eivät olleet ennustetun mukaisia → rahaa ei säästynyt, mutta rahaa ei myöskään kulunut odotettua enempää.

- Epäonnistuminen: Käytössä olevaan toimintamalliin liittyvät teknologiat vanhentuivat odotettua nopeammin ja käyttäjät omaksuivat uudet teknologiat käyttöön hyläten samalla vanhat teknologiat kokonaan. Organisaatio päätti ottaa riskin (siirtää uudistamistoimia), mutta riski toteutui ja toimintaympäristön muutokset pakottivat organisaation siirtymään uuteen toimintamalliin sekä sen vaatimiin teknologioihin nopeutetulla aikataululla. Tällöin muun muassa kustannukset olivat nopeuttamisesta johtuen 50 % korkeampia, minkä lisäksi samaan aikaan piti ylläpitää vanhaa toimintamallia ja siihen liittyviä vanhoja teknologioita. Kokonaiskustannus oli viiden vuoden tarkastelujaksolta yli kolminkertainen verrattuna siihen, että olisi heti valittu vaihtoehto b.
- Pahimmassa tapauksessa seuraus: Käyttäjät hylkäävät organisaation toimintamallin ja siihen liittyvien teknologioiden käyttämisen kokonaan, mutta organisaatio ei voi lopettaa palveluaan. Lisäksi palveluntarjoajat eivät uusi palvelusopimuksia ja lopettavat kaiken

ylläpidon kyseisen toimintamallin käyttämille teknologioille, jolloin päivitykset jäävät tekemättä. Organisaatio ajautuu teknologian ”umpikujaan”, josta on todella hankalaa ja kallista siirtyä uusiin teknologioihin ja toimintamalleihin. Lisäksi taloudellinen tilanne estää tarvittavan rahoituksen saamisen.

Tässä kuvattua esimerkkiä voi tarkastella valintaan vaikuttaneiden päätösten näkökulmasta strategisena riskinä, jonka seuraukset olivat talouteen vaikuttavia. Esimerkkiä voi tarkastella toteutuneiden seurausten osalta myös taloudellisena riskinä.

Taloudellinen riski, seurauksena onnistuminen tai epäonnistuminen

Organisaatio arvioi uusien palveluidensa suosion olevan voimakkaassa kasvussa ja päättää rekrytoida huomattavan paljon uusia erityisasiantuntijoita pysyviin työsuhteisiin palvelun tuottamisen tueksi. Samaan aikaan tunnistetaan kuitenkin riskin myös kysynnän tasaantumisesta ja automaation kautta tulevasta mahdollisuudesta entistä vähentää henkilötyötarvetta. Esimerkkejä seurauksista:

- Onnistuminen: Palveluiden suosio todellakin kasvoi merkittävästi ja niiden laajentumisen myötä erityisasiantuntijoiden työpanoksen tarve ei poistunut. Palveluiden kokonaisuuden moninkertaistuminen ei olisi ollut mahdollista ilman riittävää henkilöstöä. Organisaatio otti riskin, kysyntään liittynyt riski ei toteutunut sellaisenaan ja organisaatio onnistui hyödyntämään asiantuntijakapasiteetin onnistuneesti lisäten palveluidensa kokonaistarjontaa merkittävästi. Näin aluksi korkealta tuntuneiden henkilöstökustannusten suhteellinen osuus pieneni jatkuvasti.
- Epäonnistuminen: Palveluiden kysyntä tasaantui ja jopa merkittävästi odotettua nopeammin, minkä seurauksena erityisasiantuntijoiden työpanoksesta ei enää tarvittu kuin enintään 10 % maksimitarpeen aikaiseen tilanteeseen verrattuna. Organisaatio ei piitannut riskistä ja riski toteutui. Seurauksena organisaation henkilöstökustannukset pysyivät korkeina ja henkilöstöjärjestelyistä syntyi uusia odottamattomia lisäkustannuksia, joiden kattamiseen ei oltu varauduttu.

Tässä kuvattua riskiä voi tarkastella taloudellisena (kustannuksia aiheuttavana) riskinä. Esimerkkiä voi tarkastella myös operatiivisena riskinä, jonka seurauksilta välttymisen ansiosta mahdollistetaan kasvua tai jonka toteutuessa seurauksina ovatkin toiminnan toteuttamiseen nähden moninkertaiset kustannukset.

Operatiivinen riski, seurauksena onnistuminen tai epäonnistuminen

Organisaatio päättää toteuttaa toisen organisaation kanssa yhteisen myös käyttötarkoitukseltaan rajoitettua tietoa sisältävän tietovaraston. Myös muut kyseisiä tietoja tarvitsevat saavat tarvitsemansa tiedot suoraan käyttöönsä tietovarastosta digitaalisessa muodossa, ajantasaisina ja ilman toimitusviiveitä. Riskeinä tunnistetaan mm. tietovuodot, joilta suojautumiskeinona nähdään kyseisen tietovaraston toteuttamatta jättäminen. Nämä kaksi organisaatiota päättävät ottaa riskin ja toteuttaa projektin, jonka seurauksina voi olla esimerkiksi:

- Onnistuminen: Tietojen digitaalinen muoto ja digitaalisesti saataville asettaminen nopeuttavat päätöksentekoprosesseja ja niiden vaatimaa tiedonkulkua merkittävästi. Lisäksi syntyy tuntuvia säästöjä tietojen hakemiseen ja toimittamiseen liittyneiden henkilötyön ja postimaksujen lähes kokonaan poistuttua. Huomataan myös, että pelättyjä tietovuotoja ei ole tapahtunut tai aiheutettu. Seurauksena ovat kaikkien osapuolten merkittävät kustannussäästöt.

- Epäonnistuminen: Tietovuodoilta suojautumisen varalle luodaan useita erilaisia käyttöoikeustasoja, joiden sisäistäminen edellyttää erillisiä kurssimuotoisesti pidettäviä koulutuksia. Kaikki käyttäjät eivät pääse odotetusti koulutuksiin ja heidän pääsynsä

tietovarastossa oleviin tietoihin viivästyy esimerkiksi viikkoja kurssiaikataulujen takia, jolloin joudutaan turvautumaan perinteisiin tiedonvälittämistapoihin. Lisäksi havaitaan, että koulutuksista huolimatta luvattomia tietojen käsittelyitä tapahtuu usein ja toisinaan epäillään tapahtuvan myös suoranaisia tietovuotoja. Seurauksena ovat sujuvan käytön mahdollistavat teknologiat, joiden käyttö ja käyttäjien koulutus sekä ongelmiin puuttuminen vaativat kuitenkin huomattavan paljon aikaa ja investointeja. Näin todellisuudessa alun perin arvioidut kustannussäästöt eivät toteudu lähellekään odotetussa määrin.

Tässä kuvattua riskiä voi tarkastella operatiivisena riskinä, jonka toteutumisen välttäminen voi varmistaa merkittävät taloudelliset säästöt. Samanaikaisesti riskin vaatimat suojautumistoimet tai riskin toteutuminen voivat kuitenkin aiheuttaa paljon prosessiin liittyviä lisätoimenpiteitä, joilla useimmiten on lisäksi taloudelliset vaikutukset.

Projektinhallintaan liittyvien riskien haitat ja mahdollisuudet

Esimerkkinä onnistumisia ja epäonnistumisia jatkuvan palvelun ratkaisuun liittyvissä projektikäytännöissä:

- Onnistumisen mahdollisuuksia:
    - Monitoimittajaympäristössä on useita osapuolia ja ammattitaitoinen ote, minkä ansiosta riskienhallinta on automaattisesti osa säännöllisiä sovittuja kokouskäytäntöjä.
    - Näkökulmia riskeihin saadaan useista eri lähteistä (kaikilta osallistujilta).
    - Kokemusta kertyy ja opit voidaan jatkojalostaa ja hyödyntää toistuvasti, jolloin ensikertaisuuden riskit vähenevät merkittävästi.
    - Priorisointitoimissa ja merkitysten arvioinnissa saadaan yhteinen ja yhteneväinen näkemys riskeistä ja niidenkäsittelytarpeista.

- Epäonnistumisen mahdollisuuksia:
    - Riskejä on useimmiten vähintään kymmeniä, jopa sata, jolloin riskien läpikäynti voi olla puuduttavaa ja tuntua raskaalta.
    - Opitut riskit jäävät ”kummittelemaan” päällimmäisiksi ja sokeudutaan uusille ja erilaisille riskeille – riskeistä muistetaan tällöin vain vanhat, yleisimmät ja tyypillisimmät.
    - Uusia riippuvuussuhteisiin liittyviä riskejä ei tunnisteta riittävästi.
    - Eri toimintaympäristöt eivät ole yhteensopivia.

Muita riskien toteutumisskenaarioita

Seuraavissa esimerkeissä riskin toteutuminen aiheuttaa pääsääntöisesti haittoja tai vahinkoja. Onnistumiset tai muut positiiviset vaikutukset ovat seuraavissa esimerkeissä pääasiassa välillisiä. Niitä ilmenee esimerkiksi tilanteissa, joissa etukäteen suunnitellut ja harjoitellut suojautumistoimet tai varautumistoimet auttavat suojautumaan myös joltain muulta kuin tässä luetellulta riskiltä.

Henkilöstöön liittyvä riski (esimerkiksi sairastuminen)

Laaja influenssaepidemia tai vastaava voi johtaa tilanteeseen, jossa työntekijöitä on ennakoimattoman tilanteen takia yksinkertaisesti liian vähän. Tämä voi johtaa muun muassa kiireen ja työpaineen vuoksi tilanteisiin, joissa tietojen turvallisen käsittelyn tapoja ja sääntöjä rikotaan.

Seurauksena voi olla esimerkiksi:

- Tietojen joutuminen sivullisten haltuun tai tietovuoto.
- Puutteellisen informaation perusteella tehdyt päätökset, joista seuraa jollekin päätöksen osapuolelle taloudellisia menetyksiä.

Toimitilojen menettäminen (esimerkiksi omat tilat tai konesalitilat, vesivahinko tai tulipalo)

Tulipalo, tulva tai vesivahinko voi johtaa tilanteeseen, jossa menetetään käytettävissä olevia työ-/toimitiloja tai esimerkiksi konesalitiloja. Toisinaan käy myös niin, että tietyn riskin toteutuminen itsessään ei aiheuta suurta vahinkoa, mutta riskin toteutumisen seurauksena tehtävät toimet johtavat varsinaista alkusyytä suurempiin seurausvaikutuksiin – esimerkiksi silloin, kun sinänsä pienen tulipalon sammuttaminen aiheuttaakin laajat vesivahingot.

Laaja kyberturvallisuusriski toteutuu (esimerkiksi palvelunestohyökkäys)

Laajalla palvelunestohyökkäyksellä voidaan pahimmillaan lamaannuttaa koko organisaation tietojärjestelmistä ja digitaalisista tiedoista riippuva toiminta. Laajamittaisessa palvelunestohyökkäyksessä tulisi pystyä tunnistamaan riskeinä myös mahdollinen tietoverkon ja pääsynvalvonnan muu samanaikainen heikentyminen, jota hyödyntäen vihamieliset tahot pystyvät tekemään tietomurtoja tai saamaan pääsyn salassa pidettävään tietoon.

Laaja tietovuoto (esimerkiksi salasanat ja käyttäjätunnukset tai salassa pidettävien asiakirjojen vuotaminen)

Tietovuoto voi tapahtua esimerkiksi verkon tai siihen liitettyjen tunnistamis- ja suojaamisratkaisujen heikkouksien vuoksi. Tietovuodon voi myös aiheuttaa yksittäinen henkilö, joka saa suuren tietomassan haltuunsa esimerkiksi kopioimalla ja julkaisemalla sen avoimessa verkossa sen jälkeen joko vahingossa tai tarkoitushakuisesti.

Laajan tietovuodon seurauksena voi olla esimerkiksi:

- alueellinen sekaannus ja tietojen paljastumisesta johtuva kohu
- valtakunnallinen ongelmatilanne jälkiselvittelyineen
- kansainvälinen selkkaus tai valtioiden välisten suhteiden viilentyminen
- kolmansiin osapuoliin kohdistuva haitta tai vahinko
- organisaation maineen menetys
- hankala/kallis selvitystyö, mihin kaikkiin järjestelmiin on päästy tunkeutumaan
- tietojärjestelmien uudelleen asentaminen (sekä siitä aiheutuva kustannus ja järjestelmän pois käytöstä oleminen).