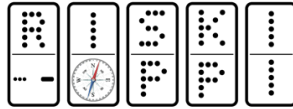




Vipuvoimaa
EU:lta
2014–2020



Vaasan yliopisto
UNIVERSITY OF VAASA

Hanke rahoitetaan Euroopan sosiaalirahaston REACT-EU tuella.
REACT-EU-hankkeet rahoitetaan osana Euroopan unionin COVID-19-pandemian johdosta toteuttamia toimia.

Moduuli 1:

Riskienhallinta digitaalisessa toimintaympäristössä



1.1 Nyt kävi digimoka!

Oppimistavoite: Tässä kappaleessa opit hahmottamaan, mitä riskit digiympäristössä tarkoittavat ja mitä näitä riskejä hallitsemalla digiympäristössä saavuttaa. Kappaleen päätteeksi kysytään 'Valintaruututehtävässä' sinulle relevantteja oppimisen aiheita ja kerrataan varautumista erääseen digimokaan. Arvioitu ajankäyttö kappaleen läpikäymiseen on 10 min.



Kenellepä ei olisi jossain vaiheessa tapahtunut jokin moka digilaitteella: ehkä kadotit älypuhelimesi tai tietokoneellesi asentui haittaohjelma.

Mokasta aiheutui sinulle varmasti monenlaista harmia, ja tilanteen korjaaminen vei aikaa. Ehkä menetit jotkin tiedot kokonaan. Saatat myös epäillä, että tietojasi on moka myötä päätynyt väärin käsiin ja väärään käyttöön niin, että niitä voidaan vielä tulevaisuudessakin mahdollisesti hyödyntää. Päätät vaihtaa heti kaikkien käytössäsi olleiden verkkopalveluiden salasanat.

Tietoturvan tärkeyttä ei turhaan korosteta toimittaessa digiympäristössä: kannattaa ottaa varmuuskopioita säännöllisesti, käyttää monivaiheista tunnistautumista jne. Tämä on kuitenkin vain yksi digitaitojen ulottuvuus.

Oletko tullut ajatelleeksi, että **riskienhallinnan taidoilla** voit tulevien uhkien hallitsemisen lisäksi myös tarkastella sitä, millaisia uhkia tapahtuneesta voi vielä seurata? Menneistä vahingoista voi ottaa oppia vastaisuuden varalle.

Tässä **Riskioppi**-ympäristössä haluamme edistää riskienhallinnan taitoja erityisesti digitaalisessa toimintaympäristössä, sekä arjessa että työssä.

Riskejä tarkastellaan aina kohdistetusti, johonkin toimintaan tai tavoitteeseen liittyen. Riskienhallinta kohdistuu mahdollisiin tuleviin tapahtumiin, joiden toteutumiseen ei itse useimmiten voi vaikuttaa. Tapahtumilla on toteutuessaan joko kielteinen tai myönteinen vaikutus tarkasteltavan toiminnan tavoitteisiin.

Riskienhallinta on **proaktiivista**. Sillä siis pyritään ennakoimaan mahdolliset toiminnan kannalta merkitykselliset tapahtumat ja määrittelemään, miten toimitaan erityisesti jonkin uhkan toteutuessa. Riskienhallinnalla voidaan myös varautua siihen, miten jonkin tapahtuman

toteutumisesta voidaan mahdollisesti hyötyä. Riskienhallinnalla epävarmuutta käsitellään sekä uhkana että mahdollisuutena.

Digimokan tarkastelu riskienhallinnan keinoilla

Riskienhallinnan keinojen avulla voit siis tarkastella, mitä seuraamuksia jo tapahtuneella mokalla oli ja miten tapahtuneesta voi ottaa opiksi jatkossa.

Pohdi tapahtunutta seuraavien kysymysten kautta:

1) Pohdi, mitkä olisivat välittömät tappiot ja mahdolliset myöhemmin toteutuvat tappiot, jos *sinun* älypuhelimesi varastettaisiin *tänään*? Seuraavassa on esimerkkejä mahdollisista tappiosta.

- I. Menetit puhelimen. Välitön tappio on vakuutuksesi omavastuu 100 € sekä uuden puhelimen ja SIM-kortin hankkimisesta aiheutuva vaiva. Sinun pitää myös asentaa ohjelmisto uudelleen.
- II. Välillisesti menetit samalla kaikki puhelimessa olevat tiedot, sillä et ollut huolehtinut niiden varmuuskopioinnista.
- III. Välillisesti joku on voinut saada laitteeltasi esille käyttäjätunnuksesi ja kontaktisi ja voi käyttää niitä väärin.

2) Miksi näin pääsi käymään?

- I. Pidet puhelinta huolimattomasti esillä väenpaljouden keskellä.
- II. Et ollut hyödyntänyt varmuuskopiointia.
- III. Tapanasi ei ole ollut käyttää näyttölukkoa.

3) Miten pienennät vastaisuudessa riskejä ja niiden toteutumisesta aiheutuvia kielteisiä vaikutuksia?

Riski on **tapahtuman todennäköisyys kertaa toteutuneen tapahtuman vaikutus**. Toinen riski voi olla suoraa seurausta siihen liittyvän riskin (eli tapahtuman) toteutumisesta.

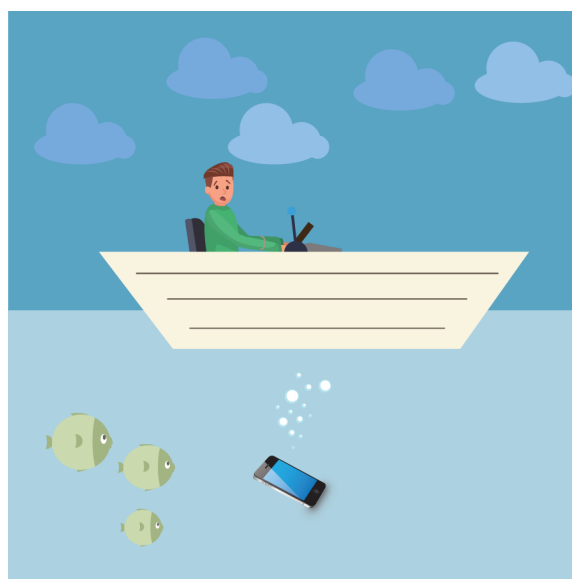
Seuraavaan taulukkoon on koottu kolme riskiä liittyen puhelimesi varastamiseen. Kun tapahtuman todennäköisyys ja vaikutus arvioidaan lukuina, voidaan jokaiselle riskille määritellä riskiluku. Sen avulla nähdään, kuinka kriittisestä riskistä on kyse kussakin tapauksessa.

	A: Tapahtuman todennäköisyys (asteikolla 1–10)	B: Tapahtuman vaikutus toteutuessaan (haitta sinulle asteikolla 1–10)	Riskiluku: A * B
Riski 1: Menetät puhelimesi, kun se varastetaan.	5 (nykyisellä varautumisella)	10	50
Riski 2: Menetät kaikki varastetun puhelimen tiedot, joista ei ole varmuuskopioita.	10	10	100
Riski 3: Varastetun puhelimen käyttäjätiedot päätyvät väärin käsiin, koska et käytä näyttölukkoa tai muuta suojausta.	10 (pahimmillaan; riippuu varkaasta)	10 (pahimmillaan; riippuu varkaasta)	100

Taulukko osoittaa, että riskin 1 toteutuessa riski 2 realisoituu varmasti. Riskin 3 toteutumisen todennäköisyys ja vaikutus ovat puolestaan epävarmoja ja riippuvat puhelimesi kähveltäjästä.

Suojautumalla riskiltä 1, eli puhelimesi menettämiseltä, ehkäiset riskien 1, 2 ja 3 aiheuttamia haittoja. Voit toimenpiteilläsi vähentää riskien 2 ja 3 seurauksia ottamalla säännöllisesti varmuuskopioita ja suojaamalla puhelimesi vähintään näyttölukolla.

Taulukosta näet, että riskin 1 toteutuessa voi sinulle aiheutuva haitta olla pahimmassa tapauksessa merkittävä. Riskin toteutuminen on aivan mahdollinen, sillä puhelinvarkauksia tapahtuu joka päivä. Riskin pienentämiseksi kannattaa siis tehdä toimenpiteitä!



Riski 2 voi toteutua esimerkiksi, jos pudotat puhelimesi järveen: tällöinkin menetät laitteella olevat tiedot. Toisaalta riski 3:n toteutuminen on tällöin epätodennäköistä, koska puhelin on järven pohjassa väärin tahojen saavuttamattomissa!

Riskienhallinta on erilaisten riskien vakavuuden arviointia eli priorisointia: kysy itseltäsi millä riskeistä 1, 2 ja 3 olisi sinulle suurin kielteinen vaikutus. Esimerkiksi riski 3 voi toteutua myös etänä tehtävän tietomurron kautta: kuinka tärkeänä pidät käyttäjätietojasi? Vai onko itse puhelin sinulle arvokkain? Minkä riskin torjumiseen sinun tulisi panostaa eniten?

Mieti erilaisia keinoja ehkäistä mainittuja riskejä. Voit esimerkiksi ehkäistä puhelimen menettämisen hankkimalla sille suojakotelon, johon kytkettävällä nauhalla kiinnität laitteen johonkin. Tällä toimenpiteellä pienennät todennäköisyyttä puhelimen varastamiselle eli riskille 1 sekä siitä aiheutuville riskeille 2 ja 3. Voit myös pienentää riskien 2 ja 3 vaikutuksia esimerkiksi ottamalla käyttöön säännöllisen varmuuskopioinnin ja näytön lukituksen.

Riskienhallinta, myös digiympäristössä, on mahdollisten tapahtumien ennakointia, vaikuttamista uhkien vaikutusten pienentämiseen sekä tapahtumaketjujen ja tapahtumien välisten riippuvuuksien tunnistamista. Seuraavan aineiston avulla opit, että riskienhallinta-ajattelu on myös mahdollisuuksien tunnistamista epävarmuudesta.

TÄSTÄ SE ALKAA!

Edellä kuvatun kärjistetyn digimoka-esimerkin tavoitteena oli johdattaa sinua riskienhallinnan ajattelun ensiaskeliin. Riskioppi-ympäristössä opit hyödyntämään riskienhallinnan oppeja uhkien torjumiseen digiympäristössä sekä tunnistamaan epävarmuudessa olevia mahdollisuuksia. Saat myös tilaisuuden harjoitella taitojasi Riskivirasto-pelissä. Tervetuloa mukaan oppimaan!



Voitko aluksi kertoa, mitkä seuraavista ovat sinulle tärkeimmät oppimisen aiheet?

- ◇ Ymmärrän paremmin, miten riski muodostuu.
- ◇ Opin hallitsemaan riskejä järjestelmällisesti.
- ◇ Opin tunnistamaan minulle relevantit digirisikit.
- ◇ Opin turvaamaan toimintani digiympäristöissä.
- ◇ Opin priorisoimaan minulle relevantit riskit.
- ◇ Opin kääntämään riskin uhkasta mahdollisuudeksi, kuten liiketoiminnaksi.



Yleisiä digiriskejä ovat mobiililaitteen menettämisestä aiheutuvat seuraukset. Sinulla on monta keinoja, joilla vähentää laitteesi katoamisen ja menettämisen aiheuttamia seurauksia. Osa toimenpiteistä on tehtävä etukäteen.

Valitse alta kaikki ne keinot, jotka ovat sinulle uusia. Kannattaa tutkia etukäteen, miten ne tehdään omalla mobiililaitteella!

- ◇ Lukitse etälukituksella ja/tai nollaa puhelin. Jos puhelin löytyy tai hankit uuden, saat palautettua tiedot, jos olet huolehtinut varmuuskopiosta.
- ◇ Vaihda heti sähköpostien ja muiden palveluiden salasana, joihin puhelimesta oli pääsy.
- ◇ Tee katoamisilmoitus esim. työnantajalle.
- ◇ Selvitä, voitko ottaa etänä kameran käyttöön, saada äänettömälläkin olevan puhelimen soimaan ja paikantaa puhelimen.
- ◇ Varoita verkostojasi mahdollisista tulevista oudoista yhteydenotoista.
- ◇ Aseta liittymään saldoraja.
- ◇ Estä kalleimmat palvelunumerot (esim. aikuisviihde).
- ◇ Käytä näyttölukossa mahdollisimman vaikeasti arvattavaa numeroyhdistelmää.

1.2 Mitä hyödyt riskienhallinnasta?

Oppimistavoite: Tässä kappaleessa opit hahmottamaan riskienhallinnan hyödyt ja vaikutusmahdollisuudet. Lopuksi vastaat monivalintatehtävään riskienhallinnan tarkoituksesta. Arvioitu ajankäyttö: 10 min.

Toimintamme tähtää tavoitteiden saavuttamiseen. **Riski kuvaa epävarmuuden vaikutusta tavoitteisiin.** Hallitsemalla riskejä turvaat tavoitteiden saavuttamisen toiminnassasi.

Monesti sanotaan, että riski otetaan, kun tavoitteena on jokin hyöty. Englanniksi puhutaan käsiteparista Risk/Reward, joka kuvaa tilannetta, jossa otettavaa riskiä (eli mahdollista tappiota) punnitaan mahdollista hyötyä vasten. Riski nähdään tilaisuutena tehdä voittoa tai kasvattaa liikevaihtoa. Joskus riskeistä puhutaan myös rahamääränä, jonka voi toiminnassaan menettää.

Haluamme kuitenkin tuoda Riskioppi-ympäristössä esille näkökulman, jossa **riskienhallinnalla turvataan tavoitteisiin pääsemistä** sellaisissa toimintaympäristöissä, joihin liittyy monenlaista

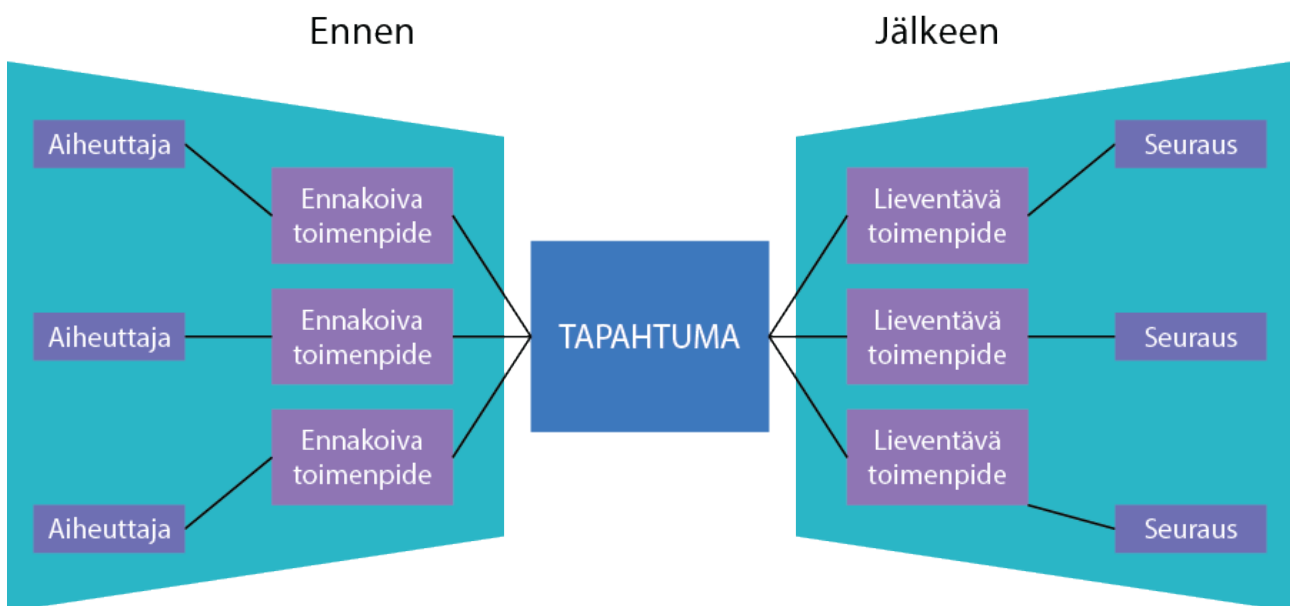
epävarmuutta. Riskienhallinnalla myös varmistetaan **toiminnan jatkuvuus** pidemmällä aikavälillä.

Toimintamme tapahtuu kasvavassa määrin **digitaalisessa toimintaympäristössä eli digiympäristössä**. Riskioppi-ympäristön tavoitteena on lisätä osaamista **digiympäristön riskien – eli digiriskien** – hallinnan osaamista, niin arjessa kuin yritystoiminnassa. Arjen digiriskien hallinta lisää kaikkien ihmisten kyvykkyyttä toimia digiympäristössä ja täten muodostaa pohjan digiriskien hallinnalle myös yritystoiminnassa.

Kokonaisuutena riskienhallinta kattaa:

- 1) asetettuihin tavoitteisiin vaikuttavien epävarmuuksien järjestelmällisen tunnistamisen
- 2) ennakointien ja lieventävien toimenpiteiden määrittämisen ja toteuttamisen, jotta epävarmuuden vaikutuksia tavoitteisiin voidaan hallita
- 3) riskien seurannan ja viestinnän niistä asianosaisille.

Tavoitteisiin vaikuttava epävarmuustekijä voi olla jokin yllättävä tapahtuma tai muutos toiminnan olosuhteissa. Se voi olla esimerkiksi ihmisen teko tai luonnontapahtuma tai jonkin tapahtumaketjun aiheuttama muutos resurssin kysynnässä tai tarjonnassa. Epävarmuuden vaikutus tavoitteisiin voi olla negatiivinen tai positiivinen riippuen siitä, miten tavoitteet on asetettu. Riskienhallinnan kautta tarkastellaan aikaa ennen ja jälkeen tapahtuman, kuten esitetään seuraavassa kuvassa.



[Avaa kuvan täysikokoinen versio.](#) (kuvaa muokattu lähteestä AFRY)

Tässä kuvattu **rusettianalyysi** on yksi menetelmä, jolla tarkastellaan riskejä ja suunnitellaan niille hallintakeinoja. Riskin aiheuttajia kutsutaan myös riskin syiksi tai riskin lähteiksi, joita ovat esimerkiksi uhkat ja vaarat. Kuvion vasemmalla puolella olevat aiheuttajat vaikuttavat tapahtumaan, joka on analyysin keskiössä. Riskin aiheuttajien vaikutuksia pyritään estämään ja

minimoimaan ennakoivilla toimenpiteillä. Tapahtuman jälkeisiä kielteisiä seurauksia lievennetään korjaavilla toimenpiteillä. Huomaa, että tässä riskiä tarkastellaan kielteisenä tapahtumana.

Kuvan mukaisesti riskienhallinnan ytimessä on jonkin tapahtuman mahdollinen toteutuminen. Toteutuessaan tapahtumalla on seurauksia, kuten vaikutus tavoitteisiin.

Riskienhallinnassa tarkastellaan aikaa ennen ja jälkeen tapahtuman. Ennen tapahtuman toteutumista riskienhallinnan keinoilla pyritään tunnistamaan sille yksi tai useampi aiheuttaja. Toiminnan kannalta kielteisten tapahtumien toteutuminen pyritään ehkäisemään kohdistamalla aiheuttajiin ennakoivia toimenpiteitä eli hallintakeinoja. Riskienhallinnalla pyritään myös vaikuttamaan tapahtuman seurauksiin lieventävillä toimenpiteillä ja näin minimoimaan kielteiset vaikutukset tavoitteisiin **ennen tapahtuman toteutumista**.

Riskiä kuvaava epävarmuus kattaa koko kuvassa esitetyn kokonaisuuden. Avoimia kysymyksiä ovat: toteutuvatko aiheuttajat, toimivatko ennakoivat toimenpiteet, toteutuuko tapahtuma, onko lieventävillä toimenpiteillä vaikutusta, mitkä ovat tapahtuman seuraukset suhteessa asetettuihin tavoitteisiin, voiko tapahtuma toistua uudestaan jne.

Epävarmuuteen voidaan varautua myös määrittelemällä toimenpiteitä, joilla pyritään edistämään tavoitteita mahdollisesti toteutuvan tapahtuman seurausten kautta.

Haasteellista riskienhallinnassa onkin tunnistaa kaikki mahdolliset tavoitteisiin vaikuttavat tapahtumat sekä niiden aiheuttajat. Niihin voivat omalle toiminnalle asetetuista tavoitteista riippuen vaikuttaa lukuisat tapahtumat, joko kielteisesti tai negatiivisesti. Tapahtumilla on taipumus ketjuuntua ja tapahtumien ketjua voi olla vaikea ennakoida sen alkua pidemmälle.



Yhtäältä riskienhallinnalla varaudutaan ennalta **mahdollisiin ongelmiin eli negatiivisiin riskeihin** (VAHTI s. 53). Toisaalta riskienhallinta tarjoaa kokonaisvaltaisia mahdollisuuksia. Näin ollen riskien hallintaa ei kannata rajata pelkästään kielteisten tapahtumien ennakointiin ja niiden vaikutusten lieventämiseen (JOHDA s. 16).

Toimintaan liittyvää **epävarmuutta pyritään hallitsemaan kokonaisvaltaisesti**. Tavoitteiden saavuttaminen varmistetaan yhtäältä **suojautumalla negatiivisilta riskeiltä** kuten uhkilta ja vaaroilta. Toisaalta **varaudutaan hyödyntämään epävarmuudesta nousevat positiiviset mahdollisuudet**, esimerkiksi tilaisuudet luoda uutta liiketoimintaa (JOHDA s. 16, 18).

Riskienhallinnan tarkoitus on opastaa **ottamaan tavoitteisiin nähden hyväksyttäviä riskejä**, jotka eivät kuitenkaan ylitä riskinkantokykyä.

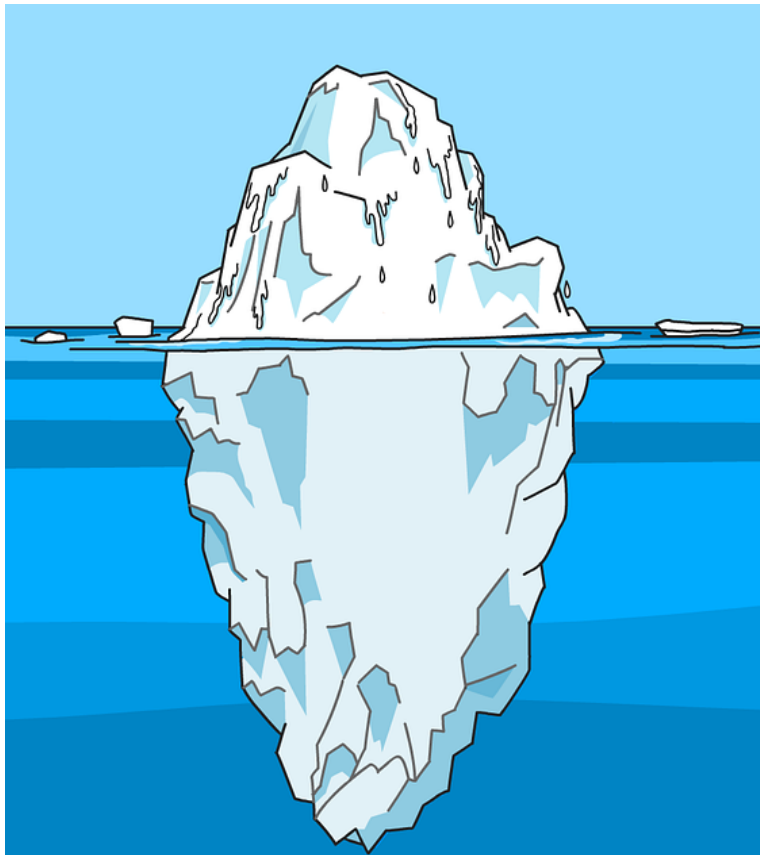
Riskienhallinnan tulisi ulottua kaikkialle, myös ihmisten arkeen ja vapaa-aikaan. Arjen riskienhallintaa on yhtä lailla auton talvirenkaiden vaihtaminen ajoissa kuin se, että pysähtyy työpäivän aikana miettimään, mikä voisi mennä pieleen ja alkaa haitata omaa työtä. (VAHTI s. 13)

Riskienhallinnalla turvataan tavoitteiden saavuttaminen omassa toiminnassa. Epävarmuutta käsitellään sekä uhkana että mahdollisuutena. Seuraavassa kappaleessa perehdymme riskienhallintaan digitaalisessa toimintaympäristössä.



Osuva metafora

Riski kuvataan usein jäävuorena.



Millä perusteella tämä on osuva metafora? Pohdi edellä lukemasi pohjalta seuraavia vastausvaihtoehtoja ja valitse niistä mielestäsi kuvaavin:

- ◇ Sekä jäävuori että riski ovat mahdollisen uhkan muodostavia kokonaisuuksia, joista vain osa on näkyvissä.
- ◇ Entiseen aikaan merenkulku pohjoisessa oli riskialtista, koska siihen sisältyi epävarmuus siitä, onko jäävuoren ajoissa havaitsemiseen käytettävissä riittävät keinot.
- ◇ Entiseen aikaan merenkulku pohjoisessa oli riskialtista, sillä siihen sisältyi epävarmuus siitä, millaiset seuraukset jäävuoreen törmääminen aiheuttaa.
- ◇ Riski voi olla paitsi uhka myös mahdollisuus, esimerkiksi tilaisuus kehittää uusia ratkaisuja uhkan havaitsemiseen ja sen kielteisten seurausten lieventämiseen.

1.3 Riskit digiympäristössä

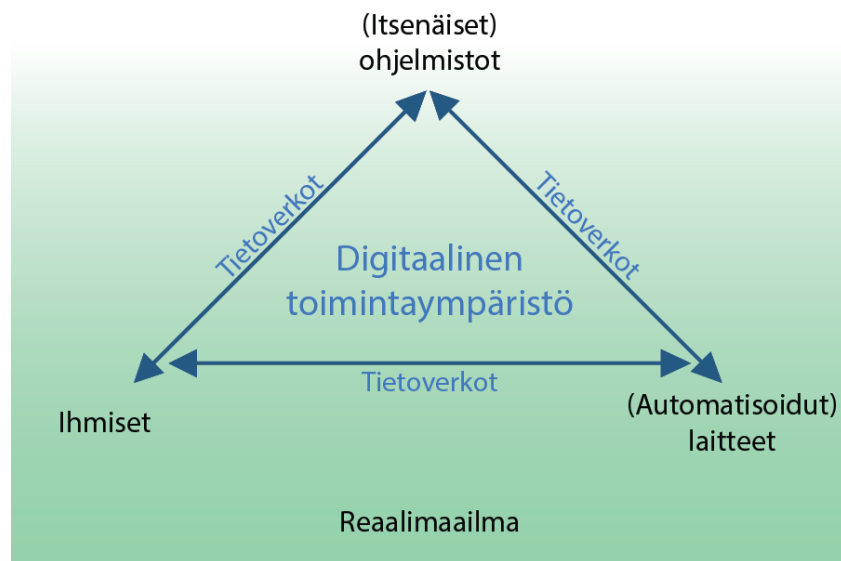
Oppimistavoite: Tämän kappaleen myötä hahmotat mikä digitaalinen toimintaympäristö on, ja mitkä ovat siinä toimimiseen vaikuttavat riskit.

Kappaleen lopussa vastaat monivalintatehtäviin digiriskeihin liittyvistä tosielämän tilanteista. Arvioitu ajankäyttö: 12 min.

Määrittelemme riskin epävarmuudeksi toiminnan tavoitteiden saavuttamisessa. Toimintamme on siirtymässä yhä laajemmin digitaaliseen ympäristöön. Tästä aiheutuu joukko uudenlaisia riskejä, joita siis nimitämme digiriskeiksi.

Digitaalinen toimintaympäristö eli digiympäristö pitää sisällään kaiken tekemisen, johon liittyy tietotekniikan, kuten ohjelmistojen, tietoverkkojen, digitaalisen median ja robotiikan, käyttö. Maksuliikenne on siirtynyt digitaaliseen ympäristöön.

Tämä toimintaympäristö on tietotekniikan, eli laitteiden, tietoverkkojen ja ohjelmistojen, välittämä ja ylläpitämä. Se on **ihmisten, automatisoitujen laitteiden ja mahdollisesti itsenäisesti toimivien ohjelmistojen** (esim. tekoälyn, kuten chatbotin) **välinen ympäristö**.



[Avaa kuvan täysikokoinen versio.](#) Kuvan lisenssi: CC BY Kompassi-hanke.

Kuvassa esitetyn mallin mukaan, ihmiset toimivat digitaalisessa toimintaympäristössä teknologian välityksellä. Tämä tapahtuu sekä toisten ihmisten että mahdollisesti itsenäisesti toimivien ohjelmistojen sekä etäohjattavien tai automatisoitujen laitteiden kanssa.

Digiympäristössä toimimisen tavoitteena voi olla esimerkiksi elannon hankkiminen ja liiketoiminta, sosiaalisten yhteyksien ylläpitäminen sekä järjestö- tai harrastustoiminta.

Kaikkeen tekemiseen, joka on riippuvaista yllä kuvattujen osien välisestä vuorovaikutuksesta voi kohdistua riskejä, mikä puolestaan luo haasteen digiympäristössä toimimiselle. Edellä mainitut riskit ovat uhkia, haavoittuvuuksia ja poikkeamia (OECD s. 33). Tällaisia epävarmuuksia voidaan ottaa riskienhallinnan kohteiksi, digiympäristössä toimimisen turvaamiseksi.

Haluamme tuoda esille näkökulman, jossa riskienhallinta on nähtävä digitaalisena kansalaistaitona. Se on paitsi kykyä käyttää riskienhallinnan välineitä myös **ennakoivaa ajattelua**, joka edistää jokaisen kansalaisen toiminnan, osallistumisen ja vaikuttamisen mahdollisuuksia digitaalisessa toimintaympäristössä.

Digiriskit

Jatkuvasti kasvava osa toiminnastamme tapahtuu tietotekniikan kautta eli digitaalisessa toimintaympäristössä, jossa tavoitteidemme saavuttamiseen vaikuttavat digitaaliseen teknologiaan ja niiden käyttöön liittyvät epävarmuudet. Nimitetään niitä siis **digiriskeiksi**.

Digiriski on määritelmän mukaan ”**digitaalisessa toimintaympäristössä vaikuttava, digitaaliseen toimintaympäristöön kohdistuva tai siitä johtuva riski**” (VAHTI s. 16).

Digiriskejä ovat esimerkiksi tietoturvaan, tietosuojaan, aineiston digitointiin, verkossa asiointiin ja viestintään liittyvät riskit. Digirisrien syitä ovat mm. digitaalisten järjestelmien haavoittuvuudet, jotka puolestaan avaavat uhkia. Niitä ovat esimerkiksi tietomurron tai häirinnän kohteeksi

joutuminen.

Digitaalisen toimintaympäristön riskien tarkastelun voi aloittaa kysymällä itseltään: *Mikä digiympäristössä aiheuttaa riskiä toiminnalleni eli mitkä epävarmuudet voivat vaikuttaa tavoitteideni saavuttamiseen?*

Vastauksissa varmasti päällimmäisenä nousevat esille tietoturvaan liittyvät riskit, samoin järjestelmien toimivuus ja saavutettavuus. Kärjistetysti sanottuna digitaalisessa toimintaympäristössä tarvitaan ainakin sähköä ja yhteys tietoverkkoon eli häiriöttömästi toimiva perusinfrastruktuuri. Ohjelmistojen ja verkkopalveluiden on toimittava luotettavasti kaikissa olosuhteissa. Omassa hallussa oleva tieto ei saa päätyä väärille tahoille. Rahaliikenteen on oltava turvallista.

Myös **sosiaalisessa mediassa toimiminen** avaa joukon riskejä, kuten (RAUTANEN s. 99):

- Sosiaalisessa mediassa julkaistavan viestin ymmärrettävyys, selkeys ja vaikuttavuus.
- Uudet sidosryhmät, oma rajattu toimintakenttä globaalissa verkossa, ketjut, sosiaalisuus ja henkilökohtaisuus.
- Osaaminen, vahinkojen suuruus ja globaalius.
- Vastuut, vastuiden hämärtyminen.
- Hallitsemattomuus, oikeiden työkalujen valinta.
- Suuri taloudellinen vaikuttavuus, riippuvuus ja kytkökset kansainväliseen talouteen.



Kuten edellä esitettiin, digiriskien hallintaa hankaloittaa se, ettei digitaalinen toimintaympäristö ole tarkkarajainen. **Digiriskit kytkeytyvät reaali maailmaan**, esimerkiksi ohjattaessa työkoneita digitaalitekniikalla (VAHTI s. 16–17). Tällöin digiriskit voivat kohdistua suoraan ihmisten ja ympäristön turvallisuuteen.

Digitaalisessa toimintaympäristössä voidaan vaikuttaa useisiin sen ulkopuolisiin asioihin, mutta samalla reaali maailman tapahtumat voivat vaikuttaa digitaaliseen toimintaympäristöön (VAHTI s. 70). Digiympäristö on läsnä reaali maailmassa lähes kaikkialla olevien verkottuneiden laitteiden,

kuten ympäristöään sensoreineen tarkkailevien älypuhelimien ja niiden ohjelmistojen, kautta.

Riskien määrä kasvaa digitaalisten välineiden käytön yleistymisen myötä. Ihmisten teot digitaalisessa toimintaympäristössä avaavat uusia riskejä. Lisäksi asioiden tekeminen digitaalisilla välineillä avaa uusia riskejä. Tämä on tilanne esimerkiksi silloin, kun koko toiminnan edellytyksenä on digivälineiden, niiden välisten yhteyksien ja ohjelmistojen toimivuus.

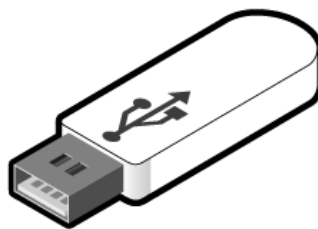
Toisaalta digitaaliset teknologiat tarjoavat välineitä vähentää tavoitteiden esteiksi muodostuvien tapahtumien vaikutuksia. Näitä toimintaa turvaavia välineitä ovat esimerkiksi tietoturvaratkaisut, kuten virustorjunta, VPN-yhteys ja käyttäjän useampivaiheinen tunnistus.

Et ole yksin digirisikien kohtaamisen ja hallinnan kanssa! Seuraavassa kappaleessa tarkastelemme tarkemmin tekijöitä, joista riski muodostuu. Tähän mennessä oppimasi pohjalta, vastaa seuraavassa muutama kysymykseen yleisistä digirisikitalanteista.



Tilanteita digirisikien maailmasta

Tässä muutama digiriskeihin liittyvä tilanne. Tehtäväsi on miettiä, mitä tilanteeseen liittyen voisit tehdä.



Tapaus 1: Tuntematon USB-muistitikku

Menet avoimen työtilan neuvotteluhuoneeseen ja huomaat pöydällä USB-muistitikun. Poimit sen ja silmäilet, löytyisikö siitä jotain yhteystietoja, kun moni organisaatio kokoontuu huoneessa. Mitään tietoa ei löydy tikusta. **Mitä teet seuraavaksi?**

- ◇ Asetan tikun tietokoneeseeni ja tutkin, jos muistitikun sisältö paljastaisi omistajan.
- ◇ Asetan muistitikun syrjään ja jatkan matkaani.



Tapaus 2: Lämpärin Webkamera

Selaillet raskaan työpäivän jälkeen nettiä läppärilläsi. Huomiosi kiinnittyy siihen, että webkameran vieressä oleva, kameran aktivoitumisen merkkivalo on syttynyt. Mikään kameraa käyttävä ohjelma ei juuri nyt pitäisi olla käytössä. **Mitä teet?**

- ◇ Antaa valon palaa vaan! Mikä lie häiriö jälleen vanhassa läppärissä.
- ◇ Laitan varmuudeksi teipin palasen kameran linssin päälle ja jatkan selailua.
- ◇ Tarkastan koneeni virus- ja haittaohjelmien poisto-ohjelmistolla



Paketin
toimitusta
yritetty

Tapaus 3: Paketin toimitus epäonnistui

Kännykkääsi saapuu tekstiviesti, jossa ilmoitetaan, että sinulle on yritetty toimittaa pakettia. Et muista juuri nyt tilanneesi mitään. Lähetysten saamiseksi sinua pyydetään maksamaan muutaman euron uudelleenohjausmaksu sopiaksesi uuden toimituksen paketille. Maksu pyydetään suorittamaan sujuvasti verkkopankin kautta viestissä olevasta linkistä. **Mitä teet?**

- ◇ Jätän viestin huomioimatta.
- ◇ Maksu on vain 2 euroa! Maksan pois ja saan mysteeripakettini.
- ◇ Nyt vähän epäilyttää. Taidan googlettaa, löytyykö muita ketkä ovat tällaisen viestin saaneet.

1.4 Digiriskit yritystoiminnassa

Oppimistavoite: Tässä kappaleessa opit tarkastelemaan digiriskejä yritystoiminnan näkökulmasta. Kappaleen lopussa vastaat tehtävään toimenpiteiden priorisoinnista, kun lähdetään yritystoiminnan digitalisaatioon. Arvioitu ajankäyttö: 12 min + lisämateriaali.

Digitaaliset teknologiat tuovat kasvupotentiaalia yritysten toiminnalle. Paljon puhutaan siitä, miten digitaalisten teknologioiden hyödyntäminen - kuten digiloikan ottaminen - luo kilpailukykyä ja esimerkiksi pohjaa ns. **datataloudelle**. Sitran mukaan datataloudessa yrityksen liiketoimintamalli perustuu tiedon käyttöön eri tavoilla. Esimerkiksi metsäkoneista voidaan kerätä dataa, jota hyödyntää kaluston käytön optimointiin yksilöllisesti jokaisessa käyttötilanteessa.

Yrityksen tulee pysyä kiinni kehityksessä jopa tässä laajassa ympäristön muutoksessa, sillä niin asiakkaat kuin kilpailijatkin ottavat digitaaliset teknologiat käyttöönsä. Nopea teknologinen muutos aiheuttaa riskejä. Hyödynnettäessä uusia digitaalisia teknologioita yrityksen toiminnassa, tulee mahdollisuuksia kuitenkin punnita suhteessa uhkiin: osataanko valita itselle tai yritykselle parhaiten sopiva teknologia, oikealta toimittajalta ja oikeaan aikaan. Riskienhallinta tarjoaa tähän välineitä.

Tarkastellaan ensin, mitä tähän muutokseen liittyvät käsitteet tarkoittavat yritystoiminnassa.

Digitisaatio tarkoittaa tilannetta, jossa jotain tuotannon, tuotteen tai palvelun ominaisuutta aletaan mittaamaan numeerisesti. Tämä voi tarkoittaa tuotannon tehokkuuden, laadun, nopeuden tai kustannusten mittaamista. Paikallisesti tai etänä kerättyä dataa analysoidaan ja hyödynnetään tuotteen parantamiseksi ja liiketoiminnan edelleen kehittämiseksi.

Digitalisaatio puolestaan tarkoittaa tilannetta, jossa yrityksen liiketoiminnassa otetaan käyttöön jokin digitaalisesti toteutettu toiminto. Tämä ei aina olennaisesti muuta liiketoiminnan tekemisen tapaa. Verkkokauppa, sähköinen tilaus- tai varausjärjestelmä ovat esimerkkejä digitaalisesti toteutetuista toiminnoista, jotka oikein toimiessaan tekevät liiketoiminnasta sujuvampaa, mutta joilla ei yleensä ole merkittävää vaikutusta liiketoiminnan perusmalliin. Koneoppimisen (eli ”tekoälyn”) laaja hyödyntäminen tulee lähitulevaisuudessa olemaan keskeinen osa digitalisaatiota monenlaisen päätöksenteon tukena, sisältöjen analysoinnin ja tuottamisen välineenä sekä asiakaspalveluiden automatisoinnissa.

Digitaalinen transformaatio taas tarkoittaa, että yrityksen liiketoiminta muuttuu logiikaltaan olennaisesti, kun otetaan käyttöön joukko muutoksia digitalisaation myötä sekä muutetaan liiketoiminta-aluetta tai liiketoimintamallia. Asiakkaalle myytävää fyysistä tuotetta voidaan esimerkiksi täydentää tietoverkon yli toteutetulla palvelulla. Tällaisia palveluita voivat puolestaan olla huoltopalvelut, etäneuvonta tai ohjelmistoina tarjottavat tuotelaajennukset. Tällöin puhutaan **tuote-palvelu –järjestelmistä**. Digitaalinen transformaatio mahdollistaa uusia liiketoimintamalleja, joissa fyysistä laitetta ei esimerkiksi myydä asiakkaalle, vaan asiakas maksaa laitteen käytöstä saamastaan hyödystä.

Digitisaatio, digitalisaatio ja digitaalinen transformaatio tuovat mukanaan erilaisia digiriskejä.

Riskienhallinnan merkitys korostuu muutostilanteissa, joissa siirrytään vanhoista toimintamalleista uusiin. Siirtymässä vanhojen toimintamallien ja digiympäristön välillä on keskeisenä riskinä, että

"... vanhemmat sukupolvet elävät ainoastaan näkyvässä ja kokevassa maailmassa, kun taas internet-sukupolvi elää virtuaalimaailmassa. Tällöin **voi pahimmillaan käydä niin, että virtuaalisen ja oikean maailman riskienhallinta ei koskaan kohtaa**. Ongelmia ratkotaan erillisinä, eikä riskeille löydetä yhteistä hallintasuunnitelmaa." (RAUTANEN s. 99)

Yritystoiminnassa digiriskien hallintaan liittyy siis myös inhimillinen ulottuvuus. Kärjistäen voidaan sanoa, että vanhalle sukupolvelle pitää opettaa digiympäristössä toimiminen, kun taas "diginatiiville" sukupolvelle pitää opettaa vanhan sukupolven käytännön taidot työn suorittamisessa.

Digitalisaation hyödyt

Digitalisaatiolla yleisesti tavoiteltuja hyötyjä toiminnalle ovat esimerkiksi seuraavat (VAHTI s. 14):

a) Tehokkuus

- Nopeus.
- Skaalautuvuus kulloisenkin tarpeen pohjalta, esimerkiksi pienet tuotantosarjat.
- Saatavuuden jatkuvuus.

b) Laatu

- Yhdenmukaisuus.
- Tarkkuus, kun virheet voidaan korjata tai estää.
- Kattavuus, joka nousee mahdollisuudesta hyödyntää dataa laajalti.

c) Kehitys

- Uudet toimintatavat, kuten automatisoidut toiminnot ja uudet käyttötavat; tekoälyn ja koneoppimisen hyödyntäminen.
- Uudet tekniikat ja tavat.
- Synergiaedut, esimerkiksi uusissa palveluissa ja yhteistyökuvioissa.

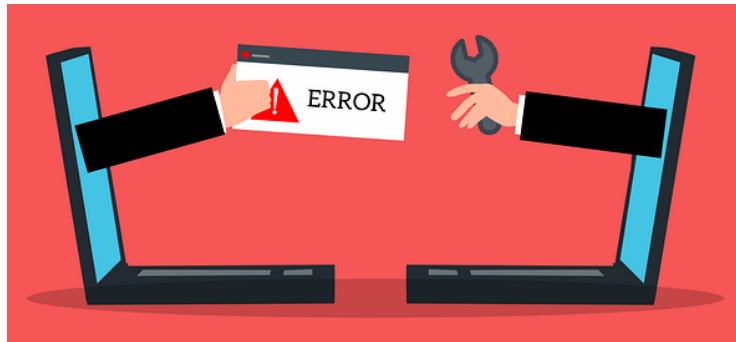
d) Yleistettävyyys

- Mukautuvuus ja hallittavuus, kuten rakenteisten osien käyttö, kopiointi ja muokkaus automatisoidusti.
- Systemaattisuus ja säännönmukaisuus, kuten toimintojen toistettavuus ja digitaalisen järjestelmän opettaminen.
- Globaalisuus, kuten verkottunut toiminta eri järjestelmissä ja niiden välillä.

Yksi keino tunnistaa digiriskejä on **käntää ylösalaisin toiminnan digitalisaatiolla tavoitellut hyödyt** (VAHTI s. 15).

Esimerkkinä hyötyjen ylösalaisin kääntämisestä voidaan ottaa tilanne, jossa tavoitellaan tehokkuutta siirtämällä yrityksen dokumentit pilvipalveluun. Pilvipalvelussa asiakirjat ovat

käytettävissä samanaikaisesti usealla eri laitteella mutta uhkaksi eli digiriskiksi muodostuvat tilanteet, joissa pilvipalvelun saatavuus katkeaa verkkohäiriön vuoksi.



Täydentävä näkökulma yritystoiminnan digiriskeihin on tarkastella epävarmuuksia, jotka liittyvät **siirtymään** aikaisemmista toimintatavoista digitaaliseen toimintaympäristöön. Muutosten kohtaaminen voi aiheuttaa työntekijöissä epävarmuutta, sillä uusien teknologioiden hallinta ja ymmärtäminen voi olla vaikeaa. Näitä epävarmuuksia voidaan nimittää **digitaalisen transformaation toteuttamisen riskeiksi**.

Se, mikä ennen toimi hyvin, ei välttämättä ole paras tapa tehdä sama asia digitaalisessa toimintaympäristössä. Siirtymää suunniteltaessa yrityksen kannattaa kartoittaa, miten **riskit periytyvät tai muuttuvat** jokaisen toiminnon osalta, kun ne siirretään digitaaliseen toimintaympäristöön.

Digiriskit ja liiketoiminnan globaalisuus

Digitaalisten teknologioiden yleistymisen ja liiketoiminnan globalisaatio ovat edenneet rinnakkain. Digitaalinen teknologia on yksi tekijä, joka on mahdollistanut liiketoiminnan globaalisuuden. Lukuisat toisiinsa liittyvät tekijät ovat lisänneet liiketoiminnan riskejä, joista digiriskien kannalta olennaisia ovat muun muassa seuraavat (pohjautuen TARKKALA 2020):

- **Hankinnan kansainvälistyminen** mm. etäisyyksien ja potentiaalisten toimittajien lukumäärän hallitseminen.
- **Toimitusketjujen monimutkaistuminen**. Kun tahoja on suurempi määrä, tulee riskienhallinnassa huomioida koko toimitusketju eikä rajoittua ensimmäiseen toimittajatasoon. Uhkana on, että kaikille ketjun tasoille ei ole näkyvyyttä.
- **Liiketoimintaprosessin vaiheiden ulkoistaminen** kolmansille osapuolille.
- **Lean-operaatiokehitys** pyrkimyksineen minimoida varasto-, kapasiteetti- ja työntekijäpuskurit.
- Nopeat ja voimakkaat **kysyntä- ja tarjontavaihtelut**. Tietoverkossa toimivat botit voivat hoitaa tarjoukset ja ostot.
- Maailman nopea muuttuminen **uudenlaisine 'digikonflikteineen'** kuten disinformaatio ja kyberterrorismi. Lisäksi resurssipula energiasta, sähköverkon mahdollinen ylikuormittuminen ja GPS järjestelmien häiriöt.

Opi lisää

Yritystoiminnan digiriskien tarkastelua voidaan täydentää kahdella englanninkielisellä konseptilla. **Digital risk**(McKinsey 2017) viittaa digitaaliseen teknologiaan liittyviin riskeihin ja **digital transformation risks** (Deloitte 2018) viittaa digitalisaation hyödyntämisen ja toisaalta hyödyntämättä jättämisen riskeihin.

Konsulttiyhtiö McKinsey & Companyn raportissa [”The Future of Risk Management in the Digital Era”](#) kuvataan seitsemän komponenttia, joilla yritys voi rakentaa riskienhallintaa digitaalisia teknologioita hyödyntävässä liiketoiminnassaan. Raportti on laadittu **rahoitusalan** näkökulmasta. (lisätehtävän laajuus: 70 sivua)

Konsulttiyhtiö Deloitteen raportissa [”Future of risk in the digital era”](#) esitetään riskien jakaminen digitaaliseen transformaatioon liittyviin riskeihin ja transformaation jälkeisiin riskeihin. (lisätehtävän laajuus: 30 sivua)



Tapaus: Digiloikan ottaminen

Kuvittele tilanne, jossa mentoroimasi yritys harkitsee digiloikan ottamista siirtämällä myyntinsä verkkopohjaiseksi. Yritys pyytää sinulta neuvoja tähän muutokseen liittyvän epävarmuuden haltuun ottamiseen.



Mitkä alla luetelluista ovat tärkeimpiä keinoja varmistaa mahdollisimman sujuva muutos? Priorisointi on olennaista riskienhallinnassa; valitse siis seuraavista enintään kolme mielestäsi tärkeintä keino.

- ◇ Digiasiantuntijuuden varmistaminen yrityksessä.
- ◇ Henkilöstön osallistaminen muutoksen suunnitteluun.
- ◇ Digimuutoskoulutusten tarjoaminen koko henkilöstölle.
- ◇ Tarkka selvitys etukäteen siitä, mitä lisäarvoa digitalisaation avulla voidaan saavuttaa ja kenties menettää.
- ◇ Ensisijaisesti yrityksen ylimmän johdon on tärkeää olla tietoinen tulevista muutoksista.
- ◇ Tärkeintä on nopeus! Digitalisaatioon tulee lähteä välittömästi, koska sitä kautta laajennetaan asiakaskuntaa.
- ◇ Tehokkuus kasvaa, kun jokainen järjestelmä siirretään digitaaliseksi samanaikaisesti. Tällöin henkilöstön ei tarvitse työskennellä rinnakkain kahdessa järjestelmässä.
- ◇ Kaikki yrityksen dokumentaatio skannataan digitaaliseen muotoon. Näin lisätään tehokkuutta ja säästetään paperiarkistoinnissa.
- ◇ Uutena toimintatapana hankitaan tekoälyä hyödyntävä Chatbot täydentämään asiakaspalvelua verkkosivuilla.

2.1 Mistä riski muodostuu?

Oppimistavoite: Tässä kappaleessa opit tunnistamaan, mistä tekijöistä riskit muodostuvat. Riskienhallinnan keskeiset tekijät ovat toiminnan tavoite, tapahtuma, sen todennäköisyys ja vaikutus. Kappaleen lopussa vastaat ”Yhdistä parit” -tehtävään liittyen riskin eri osia kuvaaviin tilanteisiin.

Arvioitu ajankäyttö: 15 min.

ISO 31000 -standardin määritelmän mukaan **riski on epävarmuuden vaikutus tavoitteisiin**.

Epävarmuus tarkoittaa puutteellista tietoa jonkin tapahtuman todennäköisyydestä, toteutumisen ajankohdasta ja toistuvuudesta sekä vaikutuksesta toiminnan tavoitteisiin.

Epävarmat seikat voivat olla tavoitteiden kannalta sekä kielteisiä (negatiivisia) että myönteisiä (positiivisia). Arkikielessä synonyymejä riskille ovat muun muassa uhkatekijä, vahingonvaara ja tappionuhka, eli riski mielletään haitalliseksi tapahtumaksi. **Uhka** tarkoittaa yksinkertaisimmillaan sitä, että saattaa tapahtua jokin ei-toivuttu tapahtuma.

Kuitenkin ISO 31000 -määritelmän mukaan **riski voi olla sekä uhka että mahdollisuus**:

- Riski on siis epävarmuuden vaikutus tavoitteisiin ja "*... vaikutus on poikkeama odotetusta. Se voi olla myönteinen, kielteinen tai molempia, ja se voi käsitellä, luoda tai saada aikaan mahdollisuuksia ja uhkia.*" (ISO 31000 s. 6)

Riskeistä keskusteltaessa on kuitenkin hyvä tiedostaa, että jotkin muut määritelmät tarkastelevat riskejä yksinomaan uhkina.

Riskienhallinnalla varaudutaan paitsi suojautumaan uhkien toteutumiselta myös hyödyntämään toiminnan epävarmuuteen liittyviä mahdollisuuksia. Standardin mukaan yksi mahdollinen riskinkäsittelytapa on "*... riskin ottaminen tai lisääminen jonkin mahdollisuuden hyödyntämisen takia*" (ISO 31000 s. 18).

"Kaava" riskin määrittelylle

Riskin määrittely voidaan esittää seuraavana ”kaavana”:

riski = tapahtuman todennäköisyys * tapahtuman vaikutus tavoitteisiin

Käydään seuraavaksi läpi riskienhallinnan kannalta keskeisiä tekijöitä tämän yhtälön pohjalta.

Tavoite on se päämäärä, joka riskienhallinnalla käsiteltävällä toiminnalla pyritään saavuttamaan. Tavoitteet voivat olla yhtä lailla taloudellisia, henkilökohtaisia tai yhteiskunnallisia. Samalla toiminnalla voi olla useita tavoitteita eri aikajäniteillä. Digiriskien hallinnassa tavoite voi liittyä yhtä lailla elannon hankkimiseen työssä tai itsensä toteuttamiseen harrastuksessa.

Tapahtuma on ainutkertainen tai toistuva. Tapahtumalle voi olla useita syitä. Tapahtuma voi myös koostua useasta samanaikaisesta tai peräkkäisestä tapauksesta. (VAHTI s. 18)

Tapahtumaksi voidaan tulkita myös muutos olosuhteissa, kuten muutos toiminnan kannalta keskeisen resurssin saatavuudessa. Muutos olosuhteissa saattaa olla seurausta useiden tapahtumien yhteisvaikutuksesta.

Vaara (engl. hazard) on tekijä tai olosuhde, joka voi aikaansaada haitallisen tapahtuman (JOHDA s. 226). Vaaratilanteiden hallinta onkin erityinen alueensa riskienhallinnassa.

Riskienhallinnan kannalta tapahtuma voi olla tunnistettu, tunnistamaton tai kokonaan tuntematon. Haasteellista onkin tunnistaa tavoitteisiin mahdollisesti vaikuttavat tapahtumat sekä varautua riittävässä määrin tunnistamattomien sekä tuntemattomien tapahtumien seurauksiin.

Käsitteellä **riskitekijät** tarkoitetaan riskien aiheuttajia tai myötävaikuttajia. Jonkin riskitekijän vuoksi tietty tapahtuma voi olla merkittävä uhka tavoitteille. Riskienhallinnassa tehdään ero syiden ja niiden seurausten välillä. Riskienhallinnassa puututaan tapahtumien syihin, jotta voidaan hallita tapahtumien seurauksia. (OECD s. 35) Myös seurausten laajuuteen tai vakavuuteen voidaan ennakoivasti pyrkiä vaikuttamaan.

Välitön riski on sellainen, jonka lähde vaikuttaa suoraan kohteeseen, kuten toiminnan tavoitteisiin. Välillinen riski puolestaan vaikuttaa epäsuorasti kohteeseen. Välillisiä riskejä on usein vaikeampi tunnistaa kuin välittömiä riskejä. Välilliset riskit voivat myös olla ketjuuntuneita riskejä. (VAHTI s. 57)

Todennäköisyys: riskiin kuuluu tapahtuma, jonka toteutuminen on odotettavissa jollain todennäköisyydellä. Todennäköisyys tarkasteltavan tapahtuman toteutumiselle on aina arvio. Siihen vaikuttavat arvioinnin aikaiset olosuhteet sekä ennakoitavissa olevat olosuhteiden muutokset. Tietyissä olosuhteissa tarkasteltavan tapahtuman toteutuminen on todennäköisempää kuin toisissa olosuhteissa.

Tapahtuma voi toteutua esimerkiksi vain joissakin olosuhteissa tai lähes aina. Tapahtuman todennäköisyys voidaan myös arvioida lukuarvona.

Olennaista on, että tietyn toiminnan riskejä arvioitaessa käytetään yhdenmukaista asteikkoa. Näin ollen mahdolliset tapahtumat voidaan priorisoida niiden todennäköisyyden pohjalta. Tällöin ne asetetaan keskinäiseen tärkeysjärjestykseen.

Vaikka tapahtumalla olisi tilastotietojen valossa tietty todennäköisyys toteutua, on omaan toimintaan vaikuttavan tapahtuman todennäköisyyden arviointi kuitenkin subjektiivinen arvio. Se tehdään tiettyinä hetkenä. Tilastotietoa ei aina edes ole saatavilla, jolloin todennäköisyys arvioidaan pitkälti oman kokemuksen pohjalta. Riskienhallinnassa on hyväksyttävä, ettei aina löydy keinoja laskea tapahtuman todennäköisyyttä.

Vaikutus: tapahtuman toteutuminen voi aikaansaada useita eritasoisia vaikutuksia liittyen esim. ihmisiin, resursseihin, omaisuuteen, ympäristöön tai digitaalisiin järjestelmiin (VAHTI s. 25).

Riskienhallinnan näkökulmasta vaikutukset voivat olla sekä kielteisiä että myönteisiä riippuen siitä, miten toiminnan tavoitteet on määritelty. Kuvaava esimerkki saman tapahtuman vaihtelevista

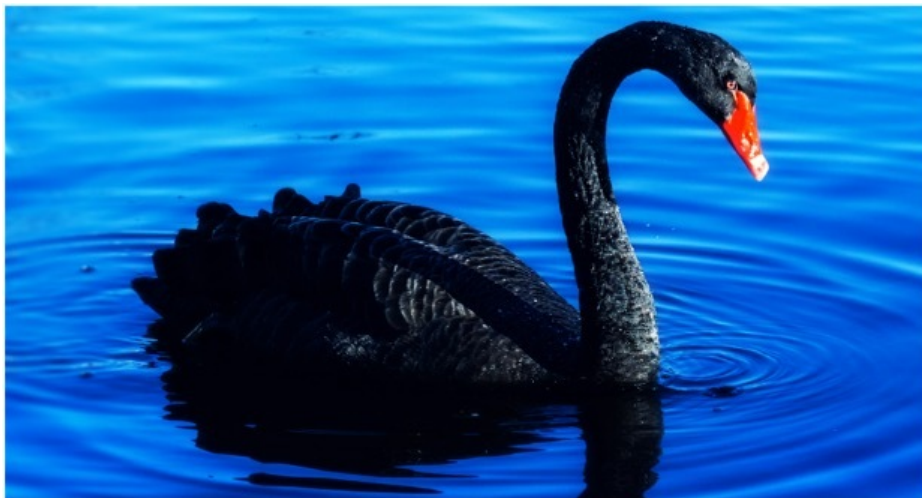
vaikutuksista on, että *"sateen toteutumisen vaikutus voi olla 0 euroa normaalille toimistotyölle tai vaikkapa 100 000 euroa ulkoilmakonsertille"* (IIVARI & LAAKSONEN s. 118).

Vaikutus voidaan käsittää poikkeamana odotetusta:

- **Positiiviset tapahtumat** (engl. upside), ovat esim. liiketoimintamahdollisuuksia, jotka merkitsevät realisoituessaan liiketoiminnan tai kannattavuuden kasvua. (JOHDA s. 16) Näistä käytetään myös nimitystä positiivinen riski.
- **Negatiivisten tapahtumien** (engl. downside) vaikutus on miinusmerkkinen tavoitteisiin nähden. Realisoituessaan negatiivinen riski esimerkiksi lisää kustannuksia tai pienentää kannattavuutta. (JOHDA s. 16) **Haavoittuvuus** on tarkasteltavan toiminnan tai kohteen piirre, joka mahdollistaa sen, että uhka aiheuttaa toteutuessaan negatiivisen vaikutuksen; esim. varkauden uhka voi realisoitua siitä, että fyysisessä suojauksessa on haavoittuvuus kuten rikkinäinen lukitus (IIVARI & LAAKSONEN s. 118).
- **Läheltä piti -tilanne** on toteutunut tapahtuma, jolla ei ollut vallinneissa olosuhteissa olennaista kielteistä vaikutusta toimintaan. Kielteinen vaikutus onnistuttiin ehkäisemään omalla toiminnalla tai oltiin onnekkaita. Toisenlaisissa olosuhteissa tapahtumalla olisi voinut ollut merkittävä kielteinen vaikutus. (VAHTI s. 19, 73) Läheltä piti -tilanteita ei tule painaa villaisella, vaan niistä pitää ottaa opiksi.

Riskienhallinnassa arvioidaan tapahtuman todennäköisyyden lisäksi sen vaikutus tavoitteisiin. Vaikutus voi olla esimerkiksi vähäinen, kohtalainen, merkittävä tai kriittinen. Vaikutus voidaan arvioida myös resurssin, kuten rahan tai työpanoksen, kautta. Seuraus näihin on joko positiivinen tai negatiivinen.

Vaikutuksen arviointi tehdään pitkälti kokemuksen pohjalta. Haasteena on kuitenkin se, että olemme alttiita omien kokemustemme puolueellisuuteen. Olemme esimerkiksi taipuvaisia puoltamaan omia ennakkokäsityksiämme tukevaa informaatiota. Olemme myös taipuvaisia etsimään päätöksenteon pohjaksi lähteitä, jotka puoltavat ja vahvistavat aikaisempia olettamuksiamme. Tämän vuoksi tapahtumien todennäköisyyden ja vaikutuksen arviointi tulisi pohjautua useamman ihmisen arvioon.



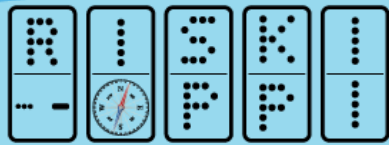
Riskienhallintaan kuuluu epävarmuuden kanssa toimeen tuleminen: niin tunnistettavien ja tuntemattomien tapahtumien kuin myös uhkien ja mahdollisuuksien. Käsitteellä **musta joutsen** viitataan kielteiseen tapahtumaan, jota ei pystytä ennakoimaan. Sillä on toteutuessaan suuri vaikutus ja jälkikäteen tarkasteltuna se näyttää ilmeiseltä uhkalta. Mustia joutsenia ei osaa odottaa kohtaavansa, joten vastaavasti tällaiset tapahtumat ovat täysin odottamattomia ja yllätyksellisiä.

Yhteenveto

Riskien tunnistaminen on riskienhallinnan ensimmäinen vaihe. Tunnistamiseen liittyy:

- Tavoitteisiin vaikuttavien mahdollisten tapahtumien tunnistaminen.
- Kunkin tunnistetun tapahtuman todennäköisyyden arviointi.
- Tunnistetun tapahtuman mahdollisten kielteisten vaikutusten arviointi tavoitteisiin nähden.
- Tunnistetun tapahtuman mahdollisten myönteisten vaikutusten arviointi tavoitteisiin nähden.

Varsinkin kun negatiivinen riski on toteutunut, on tärkeää pysähtyä ottamaan siitä opiksi. Kun tapahtuman syyt, kulku ja vaikutukset selvitetään, voidaan vähentää tai estää saman riskin toteutuminen uudelleen. Opittu on usein tärkeää jakaa myös oman yhteisön kesken.



TEHTÄVÄ!

Tapaus: Riskitilanne työmaalla

Alla on kolmen kuvan sarja tilanteesta työmaalla. Yksi toiminnan tavoitteista on turvallinen työskentely, jolloin riski on että työntekijä loukkaantuu. Aiemmin lukemasi pohjalta, **yhdistä kuva ja sitä parhaiten kuvaava käsite.**

Riskin lähde	
Vaara	
Läheltä piti -tilanne	

2.2 Riskien luokittelu

Oppimistavoite: Tässä kappaleessa opit tarkastelemaan tavoitteisiisi kohdistuvaa epävarmuutta. Sitä tarkastellaan riskien luokittelujen avulla eri näkökulmista. Kappaleen lopussa vastaat tehtäviin riskien luokittelusta. Arvioitu ajankäyttö: 15 min + lisäaineisto 10-40 min.

Riskien luokittelu pohjautuu esimerkiksi niiden olemukseen tai siihen, mihin toimintoihin ne vaikuttavat. Vaikka näillä luokitteluilla voidaan tunnistaa selkeärajaisia riskilajeja, voi yksi ja sama tapahtuma käytännössä kohdistua useaan riskiluokkaan.



Käymme seuraavassa läpi muutaman luokittelun ja tarjoamme linkkejä lisätietoon. Nämä luokittelut täydentävät toisiaan.

1) Tietoiset ja tiedostamattomat

Riskit voivat olla tietoisia tai tiedostamattomia. Vain tiedostettuihin riskeihin kyetään kohdistamaan hallintatoimenpiteitä. (JOHDA s. 82) Yritystoimintaa käynnistettäessä tai muuhun toimintaan lähdettäessä puhutaan tietoisesta riskin ottamisesta.

2) Sisäiset ja ulkoiset

Sisäiset riskit kohdistuvat omaan toimintaan eli tavoitteisiin, valintoihin, tekoihin ja tekemättä jättämisiiin.

Ulkoiset riskit ovat tapahtumia, joiden toteutumiseen ei voi vaikuttaa omalla toiminnalla, mutta joiden vaikutuksiin voidaan varautua.

3) Välittömät ja välilliset

Välitön riski vaikuttaa toimintaan suoraan, välillinen riski puolestaan jonkin muun toiminnan kautta tai osana. Välillisiin riskeihin puuttuminen voi olla vaikeaa tai ei ollenkaan omissa käsissä. (JOHDA s. 82)

Riskit voivat myös olla ketjuutuneita tai verkottuneita.

4) Neljä riskilajia

Yleisesti riskit luokitellaan neljään riskilajiin, joita ovat strategiset riskit, talouden riskit, operatiiviset riskit ja vahinkoriskit. (JOHDA s. 76)

a) Strategiset riskit liittyvät siihen, että toiminnassa ”tehdään vääriä valintoja tai hukataan mahdollisuuksia” (SRHY). Näitä ovat mm. liiketoiminnan kehittymiseen liittyvät riskit, liiketoimintaympäristöön liittyvät riskit, markkinariskit, maineriskit, globaaleista ilmiöistä johtuvat riskit ja teknologiariskit. (JOHDA s. 77)

Lue lisää: <https://riskikompassi.fi/riskien-luokittelu/strategiset-riskit/> (lisätehtävä: 10 min)

b) Taloudelliset riskit ”tarkoittavat organisaation vakavaraisuuteen, pääomien riittävyyteen ja rahaprosessien toimivuuteen liittyviä epävarmuuksia”. Riskit voivat johtua muutoksista esimerkiksi pääomien saatavuudessa, valuuttakursseissa ja koroissa. (SRHY) Taloudellisiin riskeihin sisältyvät myös mm. kirjanpidon riskit, sopimusriskit ja vastapuoliriskit (JOHDA s. 77).

- Vastapuoliriskejä ovat esimerkiksi **luottoriskit** jotka ovat potentiaalisia koko sen ajan, kun yritys on toimittanut asiakkalleen tuotteen mutta ei ole vielä saanut siitä maksua. Luottoriskien hallinta toteutetaan noudattamalla selkeää prosessia jossa määritellään mitä tehdään ja missä vaiheessa tehdään, jos asiakas jättää laskun maksamatta. (JOHDA s. 183)

Lue lisää: <https://riskikompassi.fi/riskien-luokittelu/taloudelliset-riskit/> (lisätehtävä: 10 min)

c) Operatiiviset riskit ovat seurauksia ”tapahtumasta, joka aiheutuu riittämättömistä tai toimimattomista sisäisistä prosesseista, järjestelmistä tai ihmisistä” (SRHY). Niistä käytetään myös nimitystä **toiminnalliset riskit**.

Operatiivisia riskejä ovat mm. tuotannolliset riskit, tuottavuusriskit, projektiriskit, sopimus- ja vastuusriskit, tietoturvallisuusriskit ja informaatioteknologiaan liittyvät riskit. (JOHDA s. 77) Resurssiriski on riski menettää resursseja, kuten avainhenkilöstöä tai kalustoa. Maineriski on uhka sille, että maine heikkenee julkisuudessa esille tuotujen kielteisten seikkojen kautta.

Lue lisää: <https://riskikompassi.fi/riskien-luokittelu/operatiiviset-riskit/> (lisätehtävä: 10 min)

d) Vahinkoriskit liittyvät mahdollisiin tapaturmiin, rikoksiin tai palo- ja vuotovahinkoihin. Vahinkoriskien hallintaan on käytettävissä vakuutuksia. Riskejä voikin luokitella myös sen pohjalta, ovatko ne vakuutettavia vai ei-vakuutettavia (JOHDA s. 82).

Lue lisää: <https://riskikompassi.fi/riskien-luokittelu/vahinkoriskit/> (lisätehtävä: 10 min)



Riskilajit

Osoita seuraavat digiympäristössä toimimisen epävarmuudet niihin riskilajeihin, joihin koet ne eniten kuuluvaksi.

Markkinatutkimuksen mukaan käyttäjät suosivat puhelimissa kosketusnäyttöjä. Pysymme silti vanhoissa, hyväksi todetuissa fyysisissä nappuloissa.	Strateginen riski
Tietoturvan parantamiseksi otetun lainan korot nousevat lähes kolminkertaiseksi.	Vahinkoriski
Työntekijä ohittaa potentiaalisesti ison asiakkaan sähköpostiviestin, koska luulee sitä roskapostiksi.	Taloudellinen riski
Vesiputket vuotavat serverihuoneeseemme. Tärkeitä tietoja tuhoutuu.	Operatiivinen riski

Kumpi seuraavista riskeistä voisi olla luonteeltaan tietoinen ja kumpi tiedostamaton?

Joudumme satunnaisesti käyttämään ulkoisia, avoimia WLAN-verkkoja.	Tietoiset riskit
Aurinkomyrsky lamauttaa maailman tietoyhteydet kerralla.	Tiedostamattomat riskit

Kumpi seuraavista riskeistä tulee ulkoa ja kumpi sisäisesti?

Yritykseemme kohdistuu toimintaamme lamauttavia palvelunestohyökkäyksiä.	Sisäiset riskit
Työntekijä tekee huolimattoman somepäivityksen paljastaen uuden tuotteemme tiedot kilpailijalle.	Ulkoiset riskit

Valitse välittömien ja välillisten riskien välillä:

Virhe kassajärjestelmässä aiheutti sen, että asiakkailta on peritty liikaa maksuja.	Välittömät riskit
Annoimme tuotteemme kokeiltavaksi somevaikuttajalle ja hän haukkui tuotteen kanavallaan.	Välilliset riskit

2.3 Digiriskien luokittelu

Oppimistavoite: Tässä kappaleessa opit hahmottamaan digiriskien moninaisuuden sekä sen, miten ne kuuluvat eri riskilajeihin. Kappaleen päätteeksi vastaat tehtäviin erilaisissa tilanteissa ilmenevistä digiriskeistä. Arvioitu ajankäyttö: 12 min.

Digiriskin määritelmä on siis: ”**digitaalisessa toimintaympäristössä vaikuttava, digitaaliseen toimintaympäristöön kohdistuva tai siitä johtuva riski**” (VAHTI s. 16).

Tarkastellaan seuraavassa digiriskejä muutaman luokittelun kautta. Kirjassa ”Johda riskejä” ehdotetaan jakoa yhtäältä **tietoriskeihin** ja toisaalta **IT-riskeihin** (JOHDA s. 176). Käydään seuraavaksi läpi nämä kaksi kategoriaa.

Tietoriskit



Tietoriskit vaarantavat tietoturvallisuutta. Tietoriskit ovat uhkia tiedon aitoudelle, vastuullisuudelle, kiistämättömyydelle ja luotettavuudelle. Tietoriskit vaarantavat tiedon luottamuksellisuuden, eheyden ja käytettävyyden säilymisen (JOHDA s. 176)

Tietoturvariskit kohdistuvat organisaatiolle tai yksilölle tärkeään tietoon. Organisaatiolle tietoturva tarkoittaa, että toiminnan kannalta tärkeät tiedot on suojattu. Tietoturvariskit voivat kohdistua esimerkiksi (JOHDA s. 176):

- **Tiedon saatavuuteen**, jolloin tietoa tarvitsevat pääsevät siihen käsiksi.
- **Tiedon luottamuksellisuuteen**, jolloin tieto päätyy tahoille, joilla ei ole oikeutta siihen.
- **Tiedon aitouteen ja eheyteen** eli tiedon pysymiseen muuttumattomana järjestelmässä, johon se on tallennettu.

Tietosuoja-riskit koskevat henkilöön yhdistettävän tiedon taltioinnin ja käsittelyn riskejä. Tietosuojan tarkoitus on suojata **henkilötietoja** niin, että niitä käsitellään turvallisesti ja että tiedot ovat sellaisten tahojen saavuttamattomissa, joilla ei ole oikeutta niihin.

Henkilötietoja ovat esimerkiksi nimi, kotiosoite, puhelinnumero, sähköpostiosoite ja IP-osoite. Tietosuojaan kuuluu myös yksilön oikeus nähdä sekä saada poistettua hänestä kerätyt tiedot. Siihen sisältyy lisäksi se, että henkilötiedot on suojattu valtuudettomalta tai henkilöä vahingoittavalta käytöltä (JOHDA s. 225). Uhkat, jotka loukkaavat tietosuoja, ovat ilmeisiä digiriskejä.

Tietosuojaan, tietoturvallisuuteen ja kyberturvallisuuteen liittyviä riskejä käsitellään tarkemmin Riskioppi-ympäristön moduulissa 3.

IT-riskit



IT-riskit liittyvät epävarmuuksiin informaatioteknologiaa hyödyntävien palveluiden tuottamisessa, hankinnassa ja hallinnassa (JOHDA s. 176), esimerkiksi tietyn teknologian valitsemiseen. Näissä digiriskeissä epävarmuus todennäköisemmin suurenee, mitä uudempi tai vähemmän käytetty teknologia on kyseessä.

IT-riskejä ovat myös käytettävyyssongelmat, kuten että tilattu järjestelmä kyllä täyttää toimittajalle annetun määritelmän, mutta sen käyttäminen koetaankin hankalaksi. Järjestelmän käyttöliittymää ei ole testattu loppukäyttäjillä riittävästi.

IT-riskeihin liittyy myös digiympäristön infrastruktuurin kohdistuvat uhkat ja haavoittuvuudet, alkaen sähköön saatavuudesta ja datansiirtoyhteyden luotettavasta toimivuudesta.

Muita digirisriskien luokkia

Viestintään liittyviä digiriskejä ovat esim. sosiaalisen median julkaisut joko sisällöltään (viestejä on vaikea saada poistettua tai muutettua, kun ne kerran on julkaisu) tai julkaisujen **metatietojen** osalta. Esimerkiksi julkaistaessa valokuvaa, saattaa kuvatiedoston metatiedoissa ilmetä arkaluontoista tietoa itsestä. Viime aikoina on myös varoitettu siitä, että someen julkaistavissa valokuvassa ei saa näkyä avaimia, koska niiden hammastus voidaan saada näkyviin kuvaa suurentamalla.



Uudenlaisia digiriskejä ovat **koneoppimisen eli tekoälyn hyödyntämisen riskit**. Tekoälyyn liittyvien riskien hallintaan on yhdysvaltalainen NIST-organisaatio (National Institute of Standards and Technology) julkaisemassa hallintakehyksen otsikolla ”AI Risk Management Framework”.

NIST:n kehyksen mukaan tekoälyjärjestelmien mahdolliset haitat kohdistuvat:

1) Ihmisiin eli yksilöön, ryhmään/yhteisöön, tai yhteiskuntaan.

2) Organisaatioon/yritykseen tai järjestelmään, kuten rahoitusjärjestelmään tai toimitusketjuun.

Tekoälyn riskit voivat olla luonteeltaan teknisiä liittyen tekoälyjärjestelmien tarkkuuteen, luotettavuuteen, vankkuuteen (engl. robustness), resilienssiin (eli toimintakykyisenä pysymiseen) tai turvallisuuteen.

Tekoälyn riskit voivat olla myös sosioteknisiä liittyen tekoälyn mallin selitettävyyteen, tulkittavuuteen, yksityisyyden suojaan, turvallisuuteen sekä painottumien ja vinoumien (engl. bias) hallintaan.

Opi lisää tekoälyn riskeistä: Traficom on julkaissut raportin "[Tekoälyn soveltamisen kyberturvallisuus ja riskienhallinta](#)" (2021). Voit perehtyä siihen tarkemmin, jos aihe kiinnostaa sinua.

Digiriskit osana toiminnan riskien kokonaisuutta

Digiriskit liittyvät muihin riskilajeihin. Esimerkiksi uhka kyberrikoksen uhriksi joutumisesta on paitsi digiriski myös osa vahinkoriskiä.

IT-riskit ovat teknologiariskejä, joita voidaan tarkastella myös strategisina riskeinä (JOHDA s. 77). Esimerkkinä tästä olkoon tilanne, jossa ollaan valitsemassa teknologiatoimittajaa. Strategisia riskejä ovat tässä valintatilanteessa mm. epävarmuus siitä, missä laajuudessa lopulta sitoudutaan olemaan riippuvaisia valitusta teknologiatoimittajasta. Riskinä on, että jäädäänkö tällöin ulkopuolelle tulevista uusista teknologisista kehittymismahdollisuuksista.

Digiriskejä ei tule tarkastella erillään muista riskeistä, jotka kohdistuvat digitaalisessa toimintaympäristössä tarkasteltavaan toimintaan. Riskien tarkastelun tulee olla kokonaisvaltaista.

Esimerkiksi Internetissä tapahtuvaan liiketoimintaan kohdistuu joukko harjoitettavan liiketoiminnan riskejä sekä digiriskejä. Jos liiketoimintana on esimerkiksi maahantuoda ja myydä verkkokaupassa varaosia, kohdistuvat toiminnassa hallittavat riskit yhtä lailla esimerkiksi varaosien saatavuuteen kuin verkkokaupan ja maksuliikenteen luotettavaan toimivuuteen.

Seuraavassa taulukossa on esimerkinomaisesti esitetty kokoelma digiriskejä ja yleisiä liiketoiminnan riskejä digiympäristössä.

Digiriskejä	Yleiset riskilajit liittyen digiympäristössä toimimiseen
Tietosuoja- ja tietoturvariskit, tietoturvallisuusriskit, kyberturvallisuusriskit Tekniset häiriöt: esim. tahattomat tai huoltoon liittyvät käyttökeskeytykset ja yhteyskatkokset Tahallinen häirintä ja hyökkäykset: esim. palvelunesto, tietoliikennehäirintä, identiteettivarkaus Tieto-omaisuuteen kohdistuva kyberrikollisuus: esim. tietomurto, teollisuusvakoilu, kiristys, petos, identiteettivarkaus Tietoriskit: esim. tiedon luottamuksellisuuteen, eheyteen, käytettävyyteen, aitouteen ja luotettavuuteen liittyvät riskit Henkilöön ja ympäristöön kohdistuvat turvallisuusriskit: esim. riskit lisätyn todellisuuden järjestelmien käytössä ja laitteiden automaattiohjauksessa Tekoälyn riskit IT-riskit: esim. IT-palveluiden tuottamiseen, hankintaan ja hallintaan liittyvät riskit Tuoteriskit: esim. digituotteen tai -palvelun riskit kuten uhkat että tuote ei vastaa asiakkaan tarpeeseen tai tuotteen käytöstä on haittaa asiakkaalle Viestinnän riskit: esim. sosiaalisessa mediassa	Strategiset riskit: esim. valitaan väärä teknologiapartneri tai sitoudutaan rajalliseksi osoittautuvaan teknologiaan Taloudelliset riskit: esim. investoinnit digiteknologiaan Operatiiviset riskit: esim. riittämätön ohjeistus työntekijöille aiheuttaa tietosuoja- ja tietoturvariskejä Vahinkoriskit: esim. digitaalinen laite varastetaan tai rikkoutuu tai työntekijä tuhoaa tahattomasti yrityksen tietoja

Taulukon esitys ei ole kattava, mutta varmasti huomaat jo sen pohjalta, kuinka laaja riskienhallinnan kenttä voi olla. Kuitenkin järjestelmällisellä lähestymistavalla voit ottaa sen haltuun oman toimintasi turvaamisen kannalta relevantilla tavalla.

Opi lisää: riskienhallinta IT-projektissa

Keskeinen digiriski on käytettävän teknologian uutuus ja mahdollinen testaamattomuus kaikissa mahdollisissa olosuhteissa. Tällöin voidaan käyttää termiä "NISK" eli Newness Risk. Epävarmuus tulee esimerkiksi siitä, että vasta kun teknologian hyödyntämisessä on päästy käyntiin, päästään kokeilemaan että toimiiko valittu teknologia omaan tarkoitukseen. Uutuuden riskeihin liittyy myös epävarmuus, milloin ohjelmiston uskaltaa päivittää uusimpaan versioon, mikäli nykyinen versio on toiminut hyvin.

Digiriskeihin liittyy myös epävarmuus, että kesken IT-projektin tulee tarjolle uusi teknologia, joka saattaa olla parempi ratkaisu, kun se teknologia, jota alun perin aiottiin käyttää.

Katso video: <https://www.youtube.com/watch?v=25N3h8JOY00> ["Riskien hallinta"; Jouni Huotari, JAMK, 2017, 00:00 – 11:10 asti]



Seuraavassa tutustut mahdollisiin riskeihin, jotka liittyvät digiympäristössä toimimisen epävarmuuksiin. **Valitse kuhunkin tilanteeseen sopivin selitys sille, mikä tekijä juuri tässä on kulloinkin riskinä?**

Tapaus 1: Tietoturvariski



Kuvittele tilanne, jossa olet verkkosivujen valmistukseen keskittyneen yrityksen toimitusjohtaja. Kehitystyössä hyödynnetään useita erilaisia järjestelmiä, joissa käsitellään myös henkilötietoja. Työ sujuu helpommin nyt kun kaikkiin keskeisiin tietojärjestelmiinne on asetettu sama, kaikille yhteinen salasana. Näin jokainen työntekijä pääsee helposti ja nopeasti käsiksi kaikkiin tietoihin.

Mikä muodostaa tässä tapauksessa keskeisimmän **tietoturvariskin**?

- ◇ Se, että käytössä on liian monta järjestelmää
- ◇ Se, että kaikissa järjestelmissä on sama salasana
- ◇ Se, että kaikki pääsevät käsiksi henkilötietoihin
- ◇ Se, että asiointi on helppoa ja nopeaa

Tapaus 2: Tietosuojaariski



Saat yhteydeoton, jossa Henkilö X kertoo pitävänsä eräästä asiakkaallemme tekemästämme verkkosivustosta. Nyt hän haluaisi tietää kenen verkkosivuista on kyse, sillä mitään yhteystietoja ei sivuston kautta ole saatavilla. Henkilö X kysyy sähköpostiviestissään että voisimmeko antaa hänelle asiakkaamme yhteystiedot. **Mitä vastaat?**

- ◇ Ilman muuta, sivusto kuuluu asiakkaallemme Y. Tässä hänen yhteystietonsa.
- ◇ Valitettavasti emme voi luovuttaa asiakkaidemme yhteystietoja ulkopuolisille ilman lupaa. Mikäli haluat, voin kuitenkin välittää heille yhteydenottopyyntönne.
- ◇ En varmaankaan saisi sanoa, mutta se oli vaatetusalan pienyritys paikkakunnalta Y.

Tapaus 3: IT riski



Kehitteillä on uusi ohjelmointirajapinta, joka kuulemma tulee mullistamaan koko verkkosivujen kehittämisalan. Mikä olisi hyvä lähestymistapa tähän?

- ◇ Nyt ei ole hyvä hetki siirtyä täysin tähän, koska teknologia on vielä kehitteillä.
- ◇ Täysillä mukaan! Näin varmistamme edelläkävijyytemme.
- ◇ Otetaan uusi teknologia nyt testikäyttöön, mutta ei vielä siirretä toimintaa sen varaan.
- ◇ Alamme seuraamaan teknologian kehitystä ja reagoimme tarvittaessa.



Jäikö jokin käsitellyistä aiheista vielä mietityttämään sinua?

- ◇ Kaikki hyvin! Jatketaan.
- ◇ Haluan henkilökohtaista opastusta tähän aiheeseen.

2.4 Case: Digiriskeistä Etelä-Pohjanmaalla

Oppimistavoite: Tässä kappaleessa opit 'elävän elämän' esimerkkien kautta, miten digirismit ilmenevät yritystoiminnassa. Kappaleen lopussa vastaat valintatehtävään toiminnallesi olennaisista digiriskeistä. Arvioitu ajankäyttö: 12 min + lisätehtävä.

Etelä-Pohjanmaalla toteutettiin 2021–2023 digitaalisiin riskeihin, niiden hallintaan ja osaamiseen liittyvä KOMPASSI-hanke. Edellä mainittuihin teemoihin liittyen hankkeessa haastateltiin eri toimialoilta yhteensä 25:tä yritys- ja julkisen organisaation edustajaa.

Tähän tehtävään on poimittu KOMPASSI-hankkeen tuottamasta aineistosta tuloksia ja ajankohtaisia käytännön esimerkkejä. **Tunnistatko 'tosielämän esimerkeistä' myös omaan toimintaasi vaikuttavia riskejä?**

Teema 1: Mille taholle riskienhallinta kuuluu?

Useissa organisaatioissa **riskienhallinta** digitaalisessa toimintaympäristössä mielletään **vahvasti IT-ammattilaisten kentäksi**. IT-ammattilaisen rooli digirismitien hallinnassa on keskeinen, mutta se ei yksinään riitä, sillä kaikkien toiminta ratkaisee riskienhallinnassa onnistumisen.

Digirismitien varautumiseen on erilaisia tapoja. Ensinnäkin osalla yrityksistä on joko käytössään **riskienhallinnan standardi** ISO 31000 tai ne voivat **soveltaa** omassa toiminnassaan standardien mukaista riskienhallintaprotokollaa. Tällöin riskienhallinta on sekä strategista että kokonaisvaltaista ja kattaa yrityksen toiminnan. Mukaan voidaan lukea myös digitaalinen toiminta, strategiselta tasolta aina käytännön toimiin asti, ja näiden toimien tarkastelu myös toimintaympäristön mahdollisten ja todennäköisten vaikutusten kautta. IT-ammattilaisten toiminta on tässä osa koko organisaation toiminnan ja sen tulevaisuuden hallintaa.

Toiseksi yrityksen strateginen riskienhallinta voi olla vähäistä, mutta sillä voi kuitenkin olla oma **IT-asiiantuntija**, jonka tehtäviin kuuluu vastata organisaation digitaalisesta toiminnasta ja turvallisuudesta. Yhtenä digirismitien hallintakeinona voi tällöin olla henkilöstön kouluttaminen, ohjeistaminen ja muistuttaminen mahdollisten riskien osalta.

Kolmanneksi yritys voi täydentää omaa IT-toimintaansa tai kokonaan ostaa **ulkopuoliselta palveluntarjoajalta IT-tukipalvelut** ja esim. **riskikartoituksia**. Tähän voi liittyä myös digiympäristöissä mahdollisesti realisoituvien riskien seuranta ja hallinta. Lisäksi IT-palveluiden tarjoaja voi tehdä asiakasorganisaatioilleen testejä, joilla mitataan, kuinka hyvin henkilöstö osaa torjua erilaisia digiriskejä. Usein palveluntarjoajat myös kouluttavat asiakasyritysten henkilökuntaa.

Neljänneksi ja viimeiseksi, kun yrityksissä kehitetään uusia digitaalisia palveluja tai kehitetään niiden käyttämiä järjestelmiä, niin monesti jo tässä vaiheessa IT-asiantuntijoiden kanssa pyritään **ennakoimaan ja ottamaan huomioon mahdollisia riskejä**.

Riskienhallinnassa **suurilla tai ketjuihin kuuluvilla yrityksillä** on yleensä **käytössään enemmän asiantuntijaresursseja ja keinoja kuin pk-yrityksillä**. Usein ne ovat myös paremmin näkyvillä digitaalisissa ympäristöissä, ja ovat siten myös potentiaalisia kohteita erilaisille ulkopuolelta tuleville negatiivisille riskeille, kuten tietojen kalastelu- ja verkkohyökkäysyrityksille.

Etenkin hyvin pienissä yrityksissä voi olla vähäiset riskienhallinnan resurssit, jolloin hallinnan mekanismeina saattavat korostua esimerkiksi protokolla tietojen säilyttämiselle, virusturva tietokoneissa ja yleinen ”varovaisuus ja varpaillaan olo”. On kuitenkin huomattava, että pienetkin toimijat ovat monesti osa toimitusketjuja, ja mikäli joku haluaa aiheuttaa häiriötä, hyökkäys voi tapahtua tämän ns. heikoimman lenkin kautta, vaikka häiriön varsinaisena kohteena olisikin joku ketjun näkyvämpi yritys.

’Elävän elämän’ esimerkkejä digiriskeistä maakunnassa:

- Rahaa pyritään säästämään sillä, että otetaan yhdet yhteiset tunnukset digijärjestelmään ja jaetaan tämä tunnus useammalle työntekijälle.
- Riskien hallintaan kuuluu, että osataan tunnistaa, mitkä viestit ja puhelut ovat luotettavia ja mitkä eivät. Viesteillähän yritellään kalastella yritykseen tietoja.
- Kun organisaatiossa on uusia tai väliaikaisia työntekijöitä, miten tässä tilanteessa otetaan haltuun tietoturvariskit? Millä tavoin organisaation pitäisi olla valmistautunut siihen, että ulkopuolelta voi tulla mitä tahansa sähköpostia, joka näyttää aivan oikeanlaiselta, mutta ei olekaan?
- Työntekijät voivat kokea digitalisaation kautta toteutuvan työn- ja prosessien seurannan negatiivisena asiana. Työnantajan haasteena on osoittaa, että palkanmaksu nopeutuu, kun työaikatiedot siirtyvät digitalisaation avulla nopeammin kuin paperimerkinnät. Lisäksi seurannassa on kyse työturvallisuudesta, kun työntekijälle tulee digitaalisesti tieto, että työntekijät pääsevät etäällä oleviin työkohteisiin ja sieltä pois (metsäala).
- Mikroyrityksissä ei välttämättä mietitä tietomurtoja ja hakkerointia, tai miten epävarmuustilanteessa toimitaan.
- Jos esimerkiksi pienessä yrityksessä yhtiökumppani menehtyy, ongelmana on, mitä kautta häneen liittyneitä digitaalisia asioita päästään hoitamaan. Tällaista tulisi miettiä etukäteen.
- Monella pienellä alihankkijayrityksellä voi olla pitkään jatkuneet, vakiintuneet yhteistyösuhteet isompiin yrityksiin. Entä jos iso yritys ei yhtäkkiä ostakaan niiltä enää? Mitäs sitten tehdään, kun pitäisi saada uusia asiakkaita, mutta yrityksellä ei ole edes nettisivuja? Nykyäänhän yritys ei oikein ole olemassa, jos sitä ei netistä löydy.
- Haasteena on meille sopivimpien digitalisaation ja järjestelmien tunnistaminen. Pitäisi osata ja tietää laajasti digitalisaatiosta toimialallamme. Uhkana on, että tehdään väärä valinta ja sitoudutaan siihen.
- Uuden tietojärjestelmän käyttöönotossa (teollisuus) tietojen siirto vanhasta järjestelmästä uuteen ei onnistunut. Vaihtoehtoinenkin tietojensiirto jätti tietoihin virheitä, jotka puolestaan näkyivät ongelmina tuotannossa. Tietojen liikuttelu järjestelmästä toiseen isoissa määrin on iso riski.

- Yrityksen ulkopuolelta ostetuissa taloushallinnon palveluissa sisältyy tilanteita, joissa palveluntarjoajalle tulee ohjelma- tai tietojärjestelmäpäivitys ja tämän seurauksena jotkut asiat eivät enää toimi kuten aiemmin. Digitalisaatioon kuuluvat muutokset ovat stressaavia, koska ne tuovat lisätyötä omalle organisaatiolle.
- Kyberhyökkäykset ovat suuri uhka. Koetun hyökkäyksen seurauksena tilausjärjestelmät olivat poissa käytöstä kaksi kuukautta (kaupan ala). Tänä aikana tilauksia hoidettiin perinteisesti puhelimella soittamalla ja paperille kirjaamalla.
- Vaikka oman organisaation tietoturva olisi turvattu, niin olennainen kysymys on, että ovatko yhteistyökumppanintietoturva-asiat kunnossa, jotta sinne jaettua tietoa ei pääse leviämään kolmansille osapuolille?
- Kiristyshyökkäys kohdistui asiakasyritykseen, jossa yrityksen kaikki tiedot oli viety. Tietovarkaat eivät heti ilmaisseet tekoaan, vaan odottivat muutaman kuukauden, jotta varmuuskopiotkin olivat saastuneet, ja kertoivat vasta sitten teostaan ja asentamastaan haittakoodista. Rikolliset tuntuvat pääsevän liian helpolla: heidän ei tarvitse onnistua kuin kerran, mutta yrityksen itsensä on onnistuttava kaiken aikaa.
- Valokuituverkon tarjoajan järjestelmä oli hakkeroitu ja siksi nettiyhteys ei toiminut lainkaan.
- Ennen pärjättiin paperikartoilla (alkutuotanto), mutta nyt käytössä on GPS ja puhelimessa karttaohjelmat, eikä ilman näitä oikein osaa enää toimia.

Teema 2: Digitaalisista riskeistä palvelualoilla

Teeman 1. johdantotekstissä kirjoitettu pätee sellaisenaan myös palvelualojen kohdalla (ks. teksti em. kohdassa). Edellisen lisäksi palvelualoilla on omia erityisiä piirteitä, jotka nousevat esiin riskienhallinnan yhteydessä.

KOMPASSI-hankkeen asiantuntijahaastatteluiden perusteella erityisesti **hyvinvointi- ja terveys- sekä henkilöstö- ja yrityspalveluissa** digitaalisten palveluiden **riskejä tiedostetaan ja tunnistetaan jo järjestelmien kehittämisvaiheessa**. Tässä vaiheessa myös tietoturva-asiantuntija, joko sisäisenä tai ulkoisena palveluna, on tärkeä yhteistyökumppani. Palveluiden tietoturvaan liittyvää tietoa voidaan saada myös muiden organisaatioiden kanssa toteutetuissa yhteiskehittämisen hankkeissa, testeissä ja piloteissa.

Palveluja tarjotaan ja käytetään useimmiten **suojaetuilla yhteyksillä**, joilla turvataan niin asiakkaan kuin oman organisaation tietoturvaa.

Lisäksi **tietoturva-asiantuntija** (oman organisaation ja/tai ulkoisen palveluntuottajan) tekee riskeihin liittyvää **seurantaa ja tilannearvioita**. Tietoturva-asiantuntijat eivät kuitenkaan voi hallita koko riskipotentiaalia, jossa on myös mukana käyttäjien omalla toiminnallaan luomat riskit.

Erityisen merkittävää palvelualoilla on, että riskejä ei kohdata ja poisteta vain omien organisaatioiden osalta, vaan usein myös palveluja käyttävien asiakkaiden osalta. Digitaalisessa toimintaympäristössä palveluiden käyttöön liittyvät riskit pyritään kohtaamaan yhdessä palveluyrityksen / organisaation, palvelun asiakkaiden, sekä palvelun pohjalla olevan IT-järjestelmän tarjoajan kanssa.

Teeman 1. kohdalla esitetyt esimerkit ”elävästä elämästä” pätevät suurelta osin myös palvelualojen yrityksissä ja julkisissa organisaatioissa. Seuraavassa on kuitenkin listattu sellaisia esimerkkejä, jotka nousivat KOMPASSI-hankkeen eri palvelualojen asiantuntijahaastatteluissa esiin.

'Elävän elämän' esimerkkejä digiriskeistä palvelualoilta:

- Jos sähköpostiosoitteensa tai muita tietoja antaa mihin vain, mitä siitä seuraa ja voiko näistä seurauksista tulla jotain kerrannaisvaikutuksia?
- Sosiaalisessa mediassa toimimiseen liittyvä riski on esimerkiksi oman julkaistun materiaalin poistaminen. Ei välttämättä osata ajatella, että some-julkaisulla voidaan hätäpäissään tehdä vahinkoa joko itselle tai toiselle organisaatiolle.
- Miten suhtautua, jos joku tarjoaa puhelimitse vaikka edullista sähkösopimusta, mutta tarjouksen laskemiseksi myyjän laskuri vaatii henkilötunnuksesi? Vaikka se olisi ihan oikea myyntitilanne, pitäisi osata tehdä pikaisesti riskianalyysi siitä, mitä henkilötunnuksen antaminen voi pahimmillaan tarkoittaa.
- Riskinä ovat omien työntekijöiden tai asiakkaiden henkilötietoihin liittyvät väärinkäytökset, kuten identiteettivarkaudet ja asiakastietojen varkaudet.
- Potentiaalisena uhkana rekrytointitilanteessa on, että yksinomaan digitaalisesti toteutettava henkilöhaastattelu muuttaa havaintoja verrattuna havaintoihin, joita saataisiin suorassa henkilön kohtaamisessa.
- Monelle työntekijälle tuottaa hankaluuksia se, että tieto ja asiat ovat sirpaleina monessa järjestelmässä, joista moni vaatii kirjautumisen, salasanat ja tunnistautumisen monella tavalla.
- Pitkään työelämässä olleilla voi olla muutoshaluttomuutta ja ajatus siitä, että työelämää ei ole jäljellä enää montaa vuotta ja siksi uuden opettelu ei välttämättä kiinnosta.
- Digitalisoidut palvelut voivat aiheuttaa eriarvoisuutta käyttäjien kesken. Esimerkiksi osa sosiaali- ja terveyspalveluja (myös työllisyyspalveluja) käyttävistä ei osaa tai muutoin kykene käyttämään digitaalisia palveluja.
- Isot asiakasyritykset ovat kokeneet kyberhyökkäyksiä, jolloin yritys on voinut olla viikon tai kaksikin toimimaton, kun edes printterit eivät ole toimineet.

Lisätehtävä: Perehdy KOMPASSI-hankkeen selvityksiin kokonaisuudessaan [täällä](#).



Mitkä yhteenvedossa kuvatuista digiriskeistä ovat mielestäsi merkittävimpiä oman toimintasi kannalta? Valitse alla olevista listasta kolme tärkeintä riskiä, joiden hallintaan organisaatiossasi pitää kiinnittää huomiota välittömästi.

- ◇ Suoraan omaan toimintaan kohdistuvat kyberhyökkäykset
- ◇ Verkkorikollisuuden uhriksi joutuminen
- ◇ Henkilökohtaisuus asiakassuhteissa kärsii, kun yhteydenpito hoidetaan digitaalisissa kanavissa
- ◇ Digitalisaation aiheuttama luottamuspula työntekijöissä
- ◇ Digiosaamisen puute organisaatiossa
- ◇ Organisaation tarkoituksenmukainen näkyvyys netissä
- ◇ Järjestelmien päivityksien aiheuttamat ongelmat
- ◇ Tarve käyttää useita eri järjestelmiä rinnakkain
- ◇ Yhteistoiminnan jatkuvuuden suunnittelu etukäteen asiakasyrityksen kanssa, sen digitoimintojen lamaantuessa kyberhyökkäyksessä

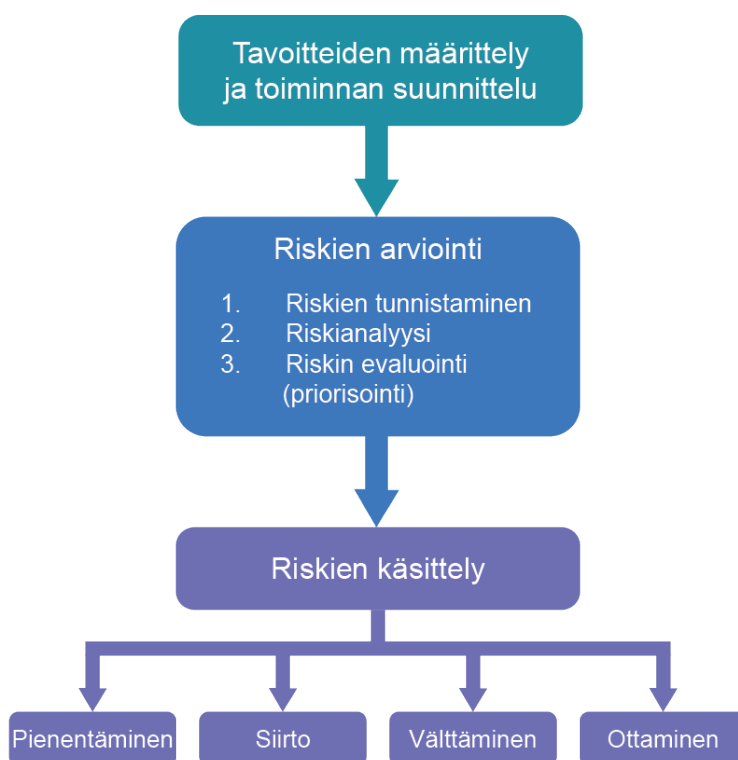
3.1 Prosessi riskienhallinnalle

Oppimistavoite: Tässä kappaleessa opit hahmottamaan riskinhallintaprosessin keskeiset vaiheet. Niihin liittyviä toimenpiteitä kuvataan yksityiskohtaisemmin tulevissa kappaleissa 4-6. Kappaleen lopussa vastaat tehtävään erään yleisen digiriskin toteutumisesta. Arvioitu ajankäyttö: 10 min.

Riskienhallinta etenee rinnakkain muun toiminnan kanssa. Sillä pyritään turvaamaan asetettujen tavoitteiden saavuttaminen toimintaan liittyvästä epävarmuudesta huolimatta.

Riskienhallintaan on käytettävissä monenlaisia menetelmiä ja prosesseja, joissa määritellään sen vaiheet. Riskienhallinnan standardit ja prosessit eroavat toisistaan esimerkiksi siinä, miten riskin käsite määritellään. Tässä aineistossa tarkastelemme riskiä uhkan ohella myös mahdollisuutena.

Yleiskäyttöisen riskinhallintaprosessin määrittelyssä lähdemme liikkeelle sen ydinvaiheista. Seuraavassa kuvatut vaiheet pohjautuvat OECD:n suositukseen digitaaliseen turvallisuuteen kohdistuvien riskien hallinnasta (OECD s. 38). Ne vastaavat standardissa SFS-ISO 31000:2018, tai lyhyemmin ISO 31000, määriteltyä riskienhallinnan prosessia.



[Avaa kuvan täysikokoinen versio.](#)

Prosessin vaiheet ovat pääpiirteiltään seuraavat:

TAVOITTEIDEN MÄÄRITTELY OSANA TOIMINNAN SUUNNITTELUA: Riskienhallintaprosessin alkuvaiheessa määritellään tavoitteet toiminnalle, johon liittyviä riskejä halutaan hallita. Tavoitteet voivat olla yhtä lailla henkilökohtaisia tai yrityksen, muun organisaation tai yhteiskunnankin asettamia. Tavoitteet voivat olla määrällisiä tai laadullisia. Käynnistettävä toiminta suunnitellaan

tavoitteiden pohjalta, ja toimintaan kohdistuvat epävarmuudet otetaan käsittelyyn.

RISKIEN ARVIOINTI sisältää kolme alivaihetta:

I. Riskien tunnistamiseen on käytettävissä useita menetelmiä, kuten SWOT-analyysi. Toiminnalle asetettuihin tavoitteisiin liittyy yleensä useita riskejä, ja ne muodostavat kokonaisuuden, jossa riskit ovat keskenään riippuvaisia. Tällöin puhutaan esimerkiksi ketjuuntuneista riskeistä, joiden tunnistaminen edellyttää myös käsitystä siitä, miten riskit ovat ketjuuntuneet toisiinsa.

II. Riskianalyysissä tarkastellaan epävarmuuden mahdollisia vaikutuksia tavoitteiden saavuttamiselle. Analyysissä tarkastellaan mm. riskien syitä ja lähteitä, eri riskien keskinäistä riippuvuutta sekä riskien negatiivisia ja positiivisia seurauksia.

III. Riskin arvioinnissa arvioidaan jokaisen tunnistetun riskin merkittävyys riskiin liittyvän tapahtuman todennäköisyyden ja sen vaikutuksen pohjalta. Tältä pohjalta riskit priorisoidaan.

RISKIEN KÄSITTELY: Päätetään, millä toimenpiteillä jokainen käsittelyyn valittu riski muutetaan hyväksyttävälle riskitasolle niin, että suunniteltu toiminta voidaan aloittaa tai sitä kannattaa jatkaa. Edellä tehty riskien priorisointi luo pohjan hallintatoimenpiteiden valitsemiselle. Hallintatoimenpiteitä on neljän tyyppisiä:

- I. Riskin pienentäminen
- II. Riskin siirto kolmannelle osapuolelle
- III. Riskin välttäminen
- IV. Riskin ottaminen.

Prosessin kautta hahmotetun kokonaisuuden hallitsemiseksi laaditaan **riskienkäsittelysuunnitelma**. Siinä määritellään mm. tunnistetut riskit ja niihin kohdistettavat hallintatoimenpiteet, vastuuhenkilöt, käsittelyn tavoiteaikataulut sekä vaatimukset riskien seurannalle ja raportoinnille. Suunnitelman toteuttaminen etenee rinnakkain muun toiminnan kanssa.

Riskienhallintaprosessin vaiheet käydään läpi yksityiskohtaisemmin seuraavissa kappaleissa. Pääset myös harjoittelemaan mm. tavoitteiden kirjaamista.



Tapaus: Avoin WLAN ja riskien käsittely

Kuvittele tilanne, että käytit kuukausi sitten työmatkallasi kahvilan avointa WLAN-verkkoa ja nyt paljastui, että työkoneellesi on pesiytynyt haittaohjelma.

Yhdistä seuraavassa tarvittavat toimenpiteet niiden käytännön toteutuksiin.

Riskin pienentäminen	Laaditaan kattavampi ohjeistus siitä, miten tietoturvariskeihin voidaan varautua paremmin.
Riskin siirtäminen	Yrityksen vastuuvakuutus korvaa osan aiheutuneista kuluista.
Riskin välttäminen	Osaamme toimia avoimessa WLAN-verkossa tietoturvallisesti.
Riskin ottaminen	Saastunut tietokone otetaan uudelleen käyttöön vasta täydellisen uudelleenasetamisen jälkeen.

4.1 Tavoitteiden kirjaaminen

Oppimistavoite: Tässä kappaleessa oppiminen kohdistuu taulukon täyttämiseen, johon kirjaat tavoitteita joihin kohdistuvia riskejä haluat ottaa hallintaan. Arvioitu ajankäyttö: 10 min.

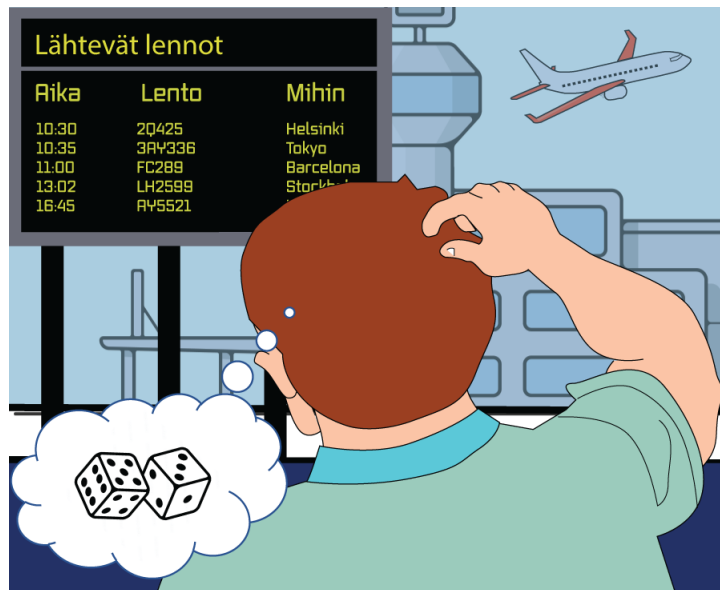
Riskienhallintaprosessi siis käynnistyy toiminnan tavoitteiden tarkastelemisesta.

Kaikella toiminnallamme yksilöinä tai organisaation jäseninä on tiedostettuja ja tiedostamattomiakin tavoitteita. Yhdistyksen, yrityksen tai muun organisaation toiminnalla on hyvinkin täsmällisiä tavoitteita, joiden saavuttamiseen pyritään yhdessä muiden organisaation jäsenten kanssa. Uusi ja käynnistettävä toiminta suunnitellaan asetettuja tavoitteita vasten.

Kirjaamalla ylös toiminnan tavoitteet voidaan niiden saavuttamista turvata riskienhallinnan keinoilla, kuten ennakoimalla epävarmuuksia, jotka voivat toteutuessaan estää tavoitteiden saavuttamisen.

Tavoitteiden kirjaamisen yhteydessä voidaan punnita, mitkä tavoitteet ovat ehdottomia ja mistä voidaan joustaa. Kun tiedostetaan, että epävarmuudessa voi olla paitsi uhkia myös mahdollisuuksia, voidaan jo toiminnan ja tavoitteiden kirjaamisessa ottaa huomioon tarttuminen epävarmuudesta nouseviin mahdollisuuksiin.

Toimintaa tarkasteltaessa voidaan myös päättää, missä rajoissa on valmiuksia muuttaa tavoitteita, esimerkiksi olosuhteiden muuttuessa ja uusien mahdollisuuksien avautuessa.



Riskienhallinta ilman tavoitteiden määrittelemistä on kuin lähtisi matkalle ilman päämäärää.



Tavoitteiden kirjaaminen

Tavoitteiden kirjaamiseen voidaan käyttää seuraavaa yksinkertaista taulukkoa ([lataa taulukon pohja täältä pdf-muodossa](#)). Tavoitteiden määrittely ja toiminnan kuvaus tehdään rinnakkain. Joskus kuvauksen laatimisessa on luontevaa lähteä liikkeelle tavoitteiden asettamisesta ("*mitä halutaan saavuttaa*"), toisinaan taas toiminnan kuvauksesta ("*mitä halutaan tehdä*").

Tavoitteet voivat olla määrällisiä, esimerkiksi tietty liikevoitto toiminnassa, tai laadullisia, esimerkiksi että saavutetaan jokin vaikutus johonkin yhteisöön. Eri tavoitteiden saavuttamiselle voi olla erilaiset aikataulut. Taulukossa tavoitteita voi olla useampia, ja ne voivat rakentua toistensa päälle, eli Tavoite 2 mahdollistuu Tavoitteen 1 saavuttamisen pohjalta jne.

Tämänlaisen taulukon täyttäminen yhdessä muiden toimintaan osallistuvien kanssa on luonteva väline keskustella siitä, miten yhteiset tavoitteet mielletään yrityksen tai muun organisaation sisällä.

Toiminnan kuvaus:	Ehdottomat tavoitteet:	Joustavat tavoitteet:	Missä rajoissa on valmiuksia muuttaa tavoitetta; missä olosuhteissa, minkä vuoksi ja miltä osin tavoitetta voidaan muuttaa?
	Tavoite 1	Tavoite 3	Kuvaus 1
	Tavoite 2	Tavoite 4	Kuvaus 2
	Jne.	Jne.	Jne.

[Avaa taulukon täysikokoinen versio.](#)

Kun olet kirjannut tavoitteet tämän tehtävän myötä, siirrytään seuraavaan kappaleeseen tarkastelemaan tavoitteisiin vaikuttavien epävarmuuksien hallintaa.

Tai jos haluat ensin oppia riskeihin liittyvistä sisäisistä ja ulkoisista vaatimuksista yritystoiminnassa, lue seuraava kappale 4.2.

VASTAA KUITENKIN ENSIN KYSYMYKSEEN:

Millaisena koit edellisen taulukon käyttämisen tavoitteiden kuvaamiseen?

- ◇ Hyödyllisenä – taulukko on täytetty osaltani!
- ◇ En koe tällaista taulukkoa relevanttina.
- ◇ Tarvitsen opastusta taulukon täyttämiseen.

4.2 Sisäiset ja ulkoiset vaatimukset

Oppimistavoite: Tässä kappaleessa opit keskeisiä yritystoiminnan sisäisiä ja ulkoisia vaatimuksia liittyen digiympäristössä toimimiseen. Vaatimusten täyttäminen on monesti pakollinen osa toiminnan tavoitteita. Kappaleen lopussa vastaat tehtävään tietosuojan riskikartoituksesta. Arvioitu ajankäyttö: 10 min.

Yritystoiminnan tavoitteisiin sisältyy joukko täytettäviä vaatimuksia, jotka voidaan jakaa organisaation sisäisiin ja ulkoisiin vaatimuksiin. Tästä näkökulmasta riskienhallinta on osa yritystoiminnan vaatimusten toteuttamista (engl. compliance) (JOHDA s. 20).

Sisäiset vaatimukset ovat riskienhallinnan seikkoja, jotka on kirjattu esimerkiksi organisaation missioon, visioon, arvoihin, strategiaan ja toimintaohjeisiin. Organisaation päivittäinen

riskienhallinta nojaa näihin vaatimuksiin. (JOHDA s. 20)

Ulkoiset vaatimukset ovat riskienhallinnan seikkoja, joista on määrätty lainsäädännössä, esimerkiksi kirjanpitolaisissa ja EU:n tietosuoja-asetuksessa, sekä säädöksissä, kuten ympäristösäädöksissä. Niitä on myös suositeltu riskienhallintastandardeissa ja toimialan suosituksissa. Ulkoiset vaatimukset voivat tulla myös asiakkailta esimerkiksi sopimuksissa. (JOHDA s. 20)

Yrityksissä riskienhallinnan johtamista määrittäviä lakeja ja direktiivejä ovat muun muassa tilinpäätösdirektiivi, osakeyhtiö-, tilintarkastus-, kirjanpito-, ja arvopaperimarkkinalaki. Esimerkiksi kirjanpitolain mukaan yrityksen toimintakertomuksessa on arvioitava liiketoiminnan kehittymiseen vaikuttavia merkittävimpiä riskejä ja epävarmuustekijöitä. (JOHDA s. 22–23)

Julkishallinnon organisaatioita velvoittavat riskienhallintaan erilaiset sen toimintaan kohdistuvat lait ja säädökset kuten työturvallisuuslaki, henkilötietolaki, valmiuslaki. [Lue lisää riskienhallinnasta julkishallinnossa.](#)

Osa vaatimuksista liittyy erityisesti digiympäristössä toimimiseen.

Digiympäristön vaatimukset: tietosuoja

Digitaaliseen toimintaympäristöön liittyy joukko ulkoisia vaatimuksia. Esimerkiksi EU:n tietosuoja-asetus (General Data Protection Regulation, GDPR) koskee henkilötietojen käsittelyä EU:n jäsenvaltioissa. Verkkopalveluiden käyttäminen kerää paljon henkilötietoja, joiden tietosuoja on verkkopalvelusta vastaavan organisaation eli rekisterinpitäjän vastuulla. Henkilötietojen käsittelyn kohteena olevan henkilön oikeuksia ovat muun muassa tiedonsaantioikeus, oikeus saada tiedot oikaistua sekä oikeus tietojen poistamiseen ja tietojenkäsittelyn vastustamiseen.



Ulkoisiin vaatimuksiin kuuluu myös muun muassa ilmoitusvelvollisuus tietovuodoista ja tietoturvaloukkauksista viranomaisille 72 tunnin kuluessa. Tietyt kriteerit täyttävät yritykset ovat veloitettuja nimeämään tietosuojavaltuutetun. Viranomaiset voivat määrätä tuntuja maksuja yritykselle tietosuoja-asioiden laiminlyönnistä. Tietosuojaan liittyvien riskien hallinta ilmentää organisaation mainetta luotettavana toimijana ja luo pohjaa asiakkaiden luottamukselle. (JOHDA s. 28)

Teoksessa ”Johda riskejä” esitetään seuraava tarkistuslista tietosuojan riskikartoituksen toteuttamiselle (JOHDA s. 28–29):

1. Nykytilan kartoitus

- Millä tavoin henkilötietoja käsitellään tällä hetkellä organisaatiossa?
- Kuka organisaatiossa omistaa kerättävän tiedon
- Täyttääkö henkilötietojen käsittely voimassa olevat tietosuojavaatimukset?
- Ovatko kaikki organisaation jäsenet tietoisia tietosuojavaatimuksista?
- Ovatko tietosuojaa koskevat sopimukset ajan tasalla?

2. Tietosuojatason määrittäminen

- Määritetään organisaation tietosuojatase ja sen toteuttaminen organisaation toiminnassa.
- Arvioidaan miten tietosuojatase tulee kehittymään omalla toimialueella.

3. Vastuuhenkilöiden asettaminen

- Määritellään, kenen tai keiden vastuulle tietosuoja-asiat kuuluvat organisaatiossa.

Selvitetään, tuleeko organisaation nimitä erityinen tietosuojavastaava.

'PESTLE' toimintaympäristön hahmottamiseen

PESTLE-analyysiä voidaan käyttää kattavan käsityksen muodostamiseen yrityksen toimintaympäristöstä, siinä tapahtuvissa muutoksissa ja muutosten vaikutuksista yritystoiminnan tavoitteisiin.

PESTLE-analyysin kautta tarkastellaan miten seuraavat tekijät ja niihin liittyvät epävarmuustekijät voivat vaikuttaa yrityksen toimintaan:

- **Politiikka** (Politics) kuten valtio-ohjaus, säätely, verotus, rajoitukset ja finanssipolitiikka.
- **Talous** (Economy) kuten talouden suhdanteet, korot, inflaatio, valuuttakurssit ja kuluttajien käytössä olevat varat.
- **Yhteiskunta** (Society) kuten ikärakenne, kansanterveys, turvallisuus, työllisyys, käsitykset työurista, väestönkasvu ja ostokäyttäytyminen.
- **Teknologia** (Technology) kuten automaatio, tuotekehitys, innovaatiot ja käynnissä olevat teknologiset muutostrendit.
- **Laki** (Law) lainsäädäntö kohdistuen mm. vientiin ja tuontiin, hankintaan, työsuojeluun, informaatioteknologiaan, kuluttajasuojaan ja tasa-arvoon.
- **Ympäristö** (Environment) kuten ilmastoon ja ilmastomuutokseen liittyvät seikat, raaka-aineiden saatavuus ja ympäristötietoisuus.

Kaikki analyysillä tunnistetut näkökulmat voivat osoittautua riskeiksi tai niiden juurisyiksi. Näitä seikkoja kannattaa hyödyntää, kun yritys tekee SWOT-analyysiin. Sen idea on tarkastella yhtä aikaa

vahvuuksia, heikkouksia, mahdollisuuksia ja uhkia. SWOT-analyysin laatiminen esitellään kappaleessa 5.1.



Tietosuojaan riskikartoitus

Valitse alla olevasta listauksesta kaikki ne kohdat tietosuojaan riskikartoituksen toteuttamiselle, jotka ovat mielestäsi kunnossa omassa organisaatiossasi.

- ◇ Olemme varmistaneet, että jokainen henkilökuntamme jäsen tietää millä tavoin henkilötietoja tällä hetkellä organisaatiossamme käsitellään.
- ◇ Olemme määritelleet kuka organisaatiossa omistaa kerättävän tiedon.
- ◇ Tiedämme, täyttääkö henkilötietojen käsittely organisaatiossamme voimassa olevat tietosuojavaatimukset.
- ◇ Kaikki organisaatiomme jäsenet ovat tietoisia tietosuojavaatimuksista.
- ◇ Tietosuoja koskevat sopimuksemme ovat ajan tasalla.
- ◇ Kaikki organisaatiomme jäsenet tietävät, mikä on organisaatiomme tietosuojataso ja miten sitä toteutetaan toiminnassamme.
- ◇ Olemme arvioineet, miten tietosuojataso tulee kehittymään omalla toimialueellamme.
- ◇ Tietosuoja-asiat kuuluvat organisaatiossamme sen jokaiselle jäsenelle.
- ◇ Tiedämme, tuleeko meidän nimetä tietosuojavastaava.

5.1 Riskien tunnistaminen

Oppimistavoite: Tässä kappaleessa opit, mitä erilaisia menetelmiä on käytettävissäsi riskien tunnistamiseen. Kappaleen lopussa teet harjoituksen SWOT-analyysistä. Arvioitu ajankäyttö: 12 min.

Riskien arvioinnin ensimmäinen vaihe on **riskien tunnistaminen**. Tavoitteena riskienhallinnassa on tunnistaa kaikki sellaiset seikat, joilla voi olla myönteistä tai kielteistä vaikutusta asetettujen tavoitteiden saavuttamiseen. Kyse on siis muun muassa mahdollisten tapahtumien ja olosuhteiden muutosten ennakoimisesta.

Yksi lähtökohta riskien tunnistamiseen on hyödyntää omaa, kollegoiden ja alan asiantuntijoiden kokemusta toiminnan uhkista ja mahdollisuuksista. Tällöin kuitenkin tulee huomioida alttius omien kokemusten puolueellisuuteen, kuten taipuvaisuuteen puoltaa omia ennakkokäsityksiä tukevaa informaatiota. Äskettäin tapahtuneita tapauksia voidaan pitää todennäköisempiä, kun mitä ne tilastojen valossa ovat. Objektiivisuus on haaste.

Toinen lähtökohta riskien tunnistamiseen on kerätä tietoa aikaisemmin samassa tai vastaavassa toiminnassa toteutuneista riskeistä. Käyttökelpoinen aineisto kuvaa toiminnan menneitä ja nykyisiä olosuhteita, kuten toteutuneita uhkia ja hyödynnettyjä mahdollisuuksia, sekä ennusteita tulevista olosuhteista. Tietoa tulee hankkia paitsi oman toiminnan olosuhteista myös laajemmin toimialasta tai markkinoista, toimintaan liittyvästä teknologiasta, lainsäädännöstä, kansainvälisestä tilanteesta ja yhteiskunnan olosuhteista. Arvokasta aineistoa ovat case-kuvaukset, vahinkotilastot, yritysten vuosikertomukset, toimialan trendit ja historialliset ongelmat (JOHDA s. 110).

Riskien tunnistaminen toteutetaan usein ryhmätyönä esimerkiksi työpajassa, johon osallistuu useita henkilöitä yrityksestä sekä sen yhteistyökumppaneita ja mahdollisesti myös asiakkaita.

Yksi toteutus riskien tunnistamiseen on laatia käytettävissä olevan aineiston pohjalta skenaarioita sille, mitä omassa toiminnassa voisi tapahtua tarkasteltavana ajanjaksona. Aineistosta poimitaan tarkasteltavan toiminnan kannalta relevantit mahdolliset tapahtumat, kehityskulut, syyt ja ulkoiset tekijät sekä niiden toteutumisen todennäköisyys ja mahdolliset vaikutukset toimintaan. (VAHTI s. 30).

ISO 31010 -standardin mukaan riskien tunnistamiseen voidaan käyttää menetelmiä näkemysten keräämiseen. Tällaisia ovat mm. aivoriihi, Delfoi, haastattelut ja mielipidekyselyt. Lisäksi voidaan käyttää menetelmiä riskien lähteiden ja syiden sekä riskitekijöiden määrittämiseen. Esimerkkinä mainittakoon riskianalyttinen lähestymistapa ja juurisyyanalyysi. HAZOP-analyysi on puolestaan menetelmä fyysisten vaaratilanteiden lähteiden tunnistamiseen.

Dilemma on, että tietoa ei periaatteessa ole koskaan liikaa, mutta liian laajasta tietomäärästä voi olla vaikea tunnistaa olennaista tietoa oman toiminnan riskien kannalta. Tiedon jäsentämiseen ja tarkasteluun tulee käyttää sopivaa välinettä, kuten SWOT-analyysiä.

Riskien tunnistaminen on olennainen osa alkuvaiheessa laadittavaa riskikartoitusta. Riskien tunnistaminen ei kuitenkaan pääty tähän. Keskeisiä jatkotoimenpiteitä ovat säännöllinen riskien toteutumisen seuranta, uusien ja/tai muuttuneiden riskien tunnistaminen sekä olosuhteiden muutosten seuranta esimerkiksi ns. heikkojen signaalien kautta.

SWOT-analyysi

SWOT-analyysi on selkeä väline, jolla tunnistetaan esimerkiksi riskeihin liittyviä tapahtumia ja olosuhteita. SWOT-analyysillä tuotetaan nelikenttä, johon kirjataan tarkasteltavan toiminnan **nykyhetken vahvuudet ja heikkoudet** sekä **tulevaisuuden mahdollisuudet ja uhat**.

SWOT-analyysi voi kohdistua joko riskienhallinnassa tarkasteltavaan toimintaan kokonaisuutena tai rajatumminkin johonkin toiminnan osaan kuten tuotanto, markkinat tai digiympäristö. Alla olevan nelikenttä-kuvion keskellä on lueteltu joitain mahdollisia tarkastelun kohteita.

Sisäiset asiat	Ulkoiset asiat
S = Vahvuudet	O = Mahdollisuudet
Tarkastelun kohteet toiminnassa: <i>tuotanto, tuote, henkilöstötekijät, markkinat, maine, talous, lainsäädäntö/regulaatio, operatiivinen taso, strategia, digiympäristö</i>	
W = Heikkoudet	T = Uhat

[Avaa kuvan täysikokoinen versio.](#)

Nelikentän pohjalta toteutettavan riskien tunnistamisen voi aloittaa esimerkiksi seuraavilla kysymyksillä tarkastellen sekä negatiivisia että positiivisia seikkoja jokaisessa kentässä:

Vahvuudet

- mitkä tapahtumat heikentävät vahvuuksia toiminnassa?
- + mitkä tapahtumat luovat edellytyksiä vahvuuksien hyödyntämiselle toiminnassa?

Heikkoudet

- mitkä tapahtumat lisäävät heikkouksia?
- + mitkä tapahtumat lieventävät heikkouksia?

Mahdollisuudet

- mitkä tapahtumat heikentävät mahdollisuuksien hyödyntämistä toiminnassa?
- + mitkä tapahtumat vahvistavat toiminnan mahdollisuuksia?

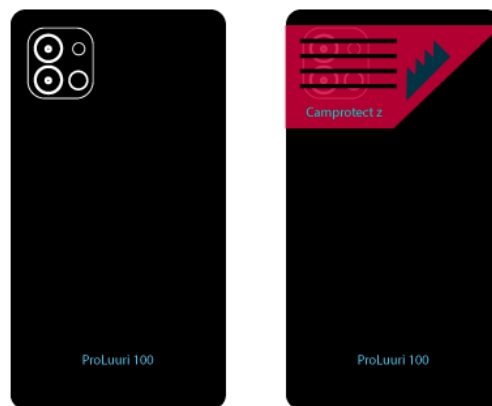
Uhat

- mitkä tapahtumat vahvistavat uhkien vaikutusta toimintaan?
- + mitkä tapahtumat lieventävät uhkien vaikutusta toimintaan?



Tapaus: Mullistava keksintö!

Kuvittele tilanne, jossa tuntemasi yritys on tehnyt mullistavan uuden keksinnön! Se on keksinyt uudenlaisen linssisuojan mobiililaitteiden kameroihin. Yritys pyytää sinulta neuvoa SWOT-analyysin tekemiseen keksinnölleen.



Tunnista seuraavat tilanteet sen mukaan, onko kyseessä *vahvuus*, *heikkous*, *mahdollisuus* vai *uhka*?

Vahvuus	Kukaan muu ei tee samanlaista linssisuoja.
Heikkous	Linssisuojan pystyy helposti kopioimaan, jos ei panosteta mallioikeuden suojan hakemiseen.
Mahdollisuus	Yhteistyö puhelinvalmistajien kanssa.
Uhka	Joku voi alkaa valmistamaan ja myymään samankaltaista linssisuojusta halvemmalla.

5.2 Riskianalyysi

Oppimistavoite: Tässä kappaleessa opit, miten suoritat riskianalyysin käyttäen menetelmiä kuten juurisyysanalyysi. Kappaleen lopussa on harjoitustehtävä juurisyysanalyysistä. Arvioitu ajankäyttö: 18 min.

Riskianalyysissä tarkastellaan käytettävissä olevan tiedon pohjalta epävarmuuden mahdollisia vaikutuksia tavoitteiden saavuttamiselle.

Analyyssissä tarkastellaan riskien syitä ja lähteitä, eri riskien keskinäistä riippuvuutta ja liittymäkohtia sekä riskien negatiivisia ja positiivisia seurauksia.

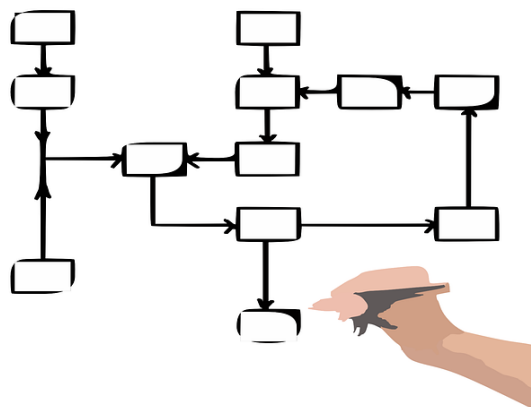
Riskianalyysin tarkoituksena on tukea kokonaisvaltaista käsitystä tarkasteltavaan toimintaan liittyvistä riskeistä ja niiden hallintamenetelmien valitsemista.

Hyökkääviin (eli offensiivisiin) lähestymistapoihin riskianalyysissä sisältyy tavoitellun voiton tasapainottaminen tappion riskiä vasten. Tässä lähestymistavassa ajatellaan, että mitä suurempi mahdollinen hyöty on, sitä halukkaampia ollaan ottamaan riskejä. (CORAS s. 3)

Puolustavissa (eli defensiivisissä) lähestymistavoissa riskianalyysi kohdistuu hallussa olevien resurssien suojelemiseen. Esimerkiksi suojaudutaan riskeiltä asiakastietojen vuotamisesta, jotta asiakkaita ei menetetä. (CORAS s. 3)

Riskianalyysissä tulee esille myös, kuinka **riskin elinkaari** huomioidaan riskinhallinnassa. Ajan kuluessa ja olosuhteiden vaihtuessa tapahtuman todennäköisyys, vaikuttavuus tavoiteisiin tai kohde, johon tapahtuma vaikuttaa, voivat muuttua (VAHTI s. 28).

ISO 31000 -standardin mukaan riskianalyysin yksityiskohtaisuus riippuu analyysin tarkoituksesta, analyysissä käytettävissä olevien tietojen saatavuudesta ja luotettavuudesta sekä saatavilla olevista resursseista. Esimerkkinä riskien tunnistamisen ja riskianalyysin osittaisesta limittäin menemisestä tarkastelemme **juurianalyysiä**. Se soveltuu ISO 31010 -standardin mukaan sekä riskien tunnistamiseen että riskianalyysin välineeksi.



Skenaario riskianalyysin välineenä

Skenaario on kuvaus toteutuneesta tai kuvitteellisesta tapahtumaketjusta, joka päättyi riskin toteutumiseen. Skenaarion kautta tarkastellaan syitä riskin toteutumiselle.

Riskeihin liittyviä tapahtumia tarkasteltaessa on mahdollista sekoittaa keskenään riski, riskin syy ja riskin seuraus (eli vaikutus tavoitteisiin).

Seuraavassa esimerkissä on tällainen tapahtumaketju: *olet ajamassa töihin, alkaa rankkasade, näkyvyys heikentyy ja ajat kolarin. Myöhästyt töistä.*

Tarkastellaan tätä tapahtumaketjua: mikä tapahtumista on riski, mikä on syy ja mikä seuraus?

1. Tunnistetaan tapahtuma, joka edistää toiminnan tavoitetta. Tavoitteenasi on saapua ajoissa työpaikalle.

2. Riski tunnistetaan tavoitetta vasten. Negatiivinen riski on tapahtuma, jonka vaikutus estää tavoitteen saavuttamisen. Toteutunut riski on tapahtuma, että jouduit kolariin työmatkalla. Tapahtuman vuoksi et ehtinyt työpaikalle ajoissa.

Kolariin joutuminen on tapahtuma, joka voi samalla olla riski myös monelle muulle tavoitteellesi. Jälkikäteen huomaat, että kolarin vuoksi et pääse suunnittelemaallesi lomamatkalle.

3. Tunnistetaan tapahtuma tai ilmiö, joka oli **välitön syy riskin toteutumiselle** eli kolariin joutumiselle. Tapahtumaketjun mukaan välitön syy oli, että näkyvyys huononi.

4. Tapahtumaketjusta voidaan tunnistaa myös **useita välillisiä syitä** riskin toteutumiselle. Välilliset syyt vaikuttivat välittömään syyn toteutumiseen. Välillisiä syitä olivat paitsi rankkasade myös se, että autosi pyyhkijänsulat olivat kuluneet.

Riskin toteutuminen on usein monen syyn summa. Kenties et olisi voinut ennaltaehkäistä välitöntä syytä etkä kaikkia välillisiä syitä. Kuitenkin ainakin yhteen välilliseen syyhyn olisit voinut vaikuttaa hankkimalla uudet pyyhkijät. Olisiko yksin se riittänyt estämään riskin toteutumisen?

Yllä kuvatun esimerkin kaltaisia skenaariota laatimalla voit hahmottaa toimintaasi vaikuttavia riskejä ja niiden syitä.

Kun analysoit skenaarion tapahtumia, älä sekoita toimintasi tavoitteita riskeihin, jotka vaikuttavat näihin tavoitteisiin: esimerkiksi sitä, pysykö projekti budjetissaan, siihen, että syyn Y seurauksena projektin budjetti ylittyy. Skenaariossa kuvattu tapahtuma, jolla on suora vaikutus tavoitteeseesi, on riski tälle tavoitteelle. Riski ei ole projektin budjetin ylittyminen, vaan budjettiin vaikuttavan syy Y:n toteutuminen.

Voit kuvata skenaarion tapahtumaketjun myös visuaalisesti tapahtumapuuna. Tähän sopiva työkalu on esimerkiksi CORAS.

Skenaariossa kuvatus tapahtumaketjun voit purkaa alla olevaan taulukkoon (joka pohjautuu lähteeseen JOHDA s. 103). Välilliset syyt luetellaan sen välittömän syyn kautta, johon ne liittyvät.

Riskin kuvaus	Välittömät syyt	Onko syy välttämätön riskin toteutumiselle?	Onko syy yksin riittävä riskin toteutumiselle?	Välilliset syyt
Ilmiö tai tapahtuma, joka suoraan vaikuttaa tavoitteeseen	Välitön syy 1	Kyllä / ei	Kyllä / ei	Välillinen syy 1.1
				Välillinen syy 1.2
	Välitön syy 2	Kyllä / ei	Kyllä / ei	Välillinen syy 2.1
				Välillinen syy 2.2
	jne.			jne.

[Avaa taulukon täysikokoinen versio.](#)

Riskin toteutumiseen vaikutetaan puuttumalla sen välittömiin syihin ja erityisesti niihin syihin, jotka ovat yksin riittäviä ja välttämättömiä riskin toteutumiselle.

Juurisyyanalyysi

Kun samaa ilmiötä tarkastellaan eri näkökulmista, saattaa näyttää löytyvän eri riskikategorioihin kuuluvia tai toisistaan erillisiä riskejä. Tällöin kannattaa selvittää, ovatko kyseessä oikeasti eri riskit vai onko toinen riski itse asiassa ensimmäisen riskin juurisyy. (JOHDA s. 83)

Tähän sopiva väline on juurisyyanalyysi (engl. Root Cause Analysis). Kyseessä on keino ongelmien aiheuttajien tunnistamiseen ja ratkaisun määrittelemiseen ongelman ehkäisemiseen. Se toimii riskienhallinnan välineenä, kun juurisyyanalyysin kautta voidaan tunnistaa riskien aiheuttajien välisiä riippuvuuksia. Analyysi voi auttaa tunnistamaan välillisiä riskejä, joita on usein vaikeampi tunnistaa kuin välittömiä riskejä. Riskihallittavaa tapahtuma tarkastellaan juurisyyanalyysissä ongelmana.

Juurisyyanalyysin lähtökohtana on oletus, että toiminnot/tapahtumat ovat kytköksissä toisiinsa. Toisin sanoen, ensimmäinen toiminta/tapahtuma käynnistää seuraavan ja tämä edelleen seuraavan, ja niin edespäin.

Juurisyyanalyysi aloitetaan viimeisestä tapahtumasta. Se on selvitettävä ongelma, kuten toteutuneena riskinä tarkasteltava kielteinen tapahtuma. Jäljittämällä toisiinsa ketjuuntuneita tapahtumia tai toimintoja taaksepäin ajassa selvitetään, mistä ongelma sai alkunsa eli mikä oli sen juurisyy.

Juurisyyanalyysin avulla ongelmalle löydetään yksi tai useampi aiheuttaja. Aiheuttajiin puuttumalla päästään poistamaan ongelman pohjimmaiset syyt.

Analyysillä voidaan myös selvittää, missä vaiheissa juurisyyistä liikkeelle lähteneet vaikutukset voimistuivat siten, että ilmenneen ongelman toteutuminen oli väistämätön. Toisin sanoen selvitetään, missä tapahtumaketjun vaiheessa olisi ollut mahdollista tehdä vielä korjaustoimenpiteitä.

Ongelmien kategorisoinnit

Juurisyyanalyysissä ongelmaa analysoidaan monesta näkökulmista. Ongelman syitä voidaan etsiä esimerkiksi seuraavista luokista:

- **Fyysiset syyt:** aineelliset rikkoutumiset, kuten kulumisesta tai vahingosta johtuvat laiterikot.
- **Inhimilliset syyt:** ihmisten tekemät virheet tai asioiden tekemättä jättämiset; väärinymmärrykset ja virheelliset tulkinnat, jotka johtuvat osaamattomuudesta tai välinpitämättömyydestä; tahalliset tai rikolliset teot.
- **Organisatoriset syyt:** virheelliset tai puutteelliset käytännöt tai prosessit; puutteellinen johtaminen; puutteellisesti laaditut sopimukset.

Edellistä kategorisointia täydentää **”6M”-luettelo**, joka sisältää englanninkieliset käsitteet: Man, Machine, Methods, Measurements, Materials, Mother Nature, Management & Maintenance. Suomeksi käytetään esimerkiksi kategorioita:

- menetelmät, laitteet, hallinta, materiaalit, työvoima, raha.
- materiaalit, menetelmät ja prosessit, ympäristö, laitteet, henkilöt, mittaukset. (ISO 31010)

ISO 31010 -standardin mukaan juurisyyanalyysissä on mahdollista käyttää mitä tahansa kategorioiden joukkoa, joka sopii kuvaamaan analyysin kohteen olosuhteita.

Juurisyyanalyysin vaiheet

Juurisyyanalyysi etenee viiden vaiheen kautta seuraavasti:

1. **Ongelman ymmärtäminen:** järjestetään esim. aivoriihi, jossa haetaan vastauksia kysymyksiin ”mitä tapahtui?”, ”mikä meni vikaan?” tai ”miksi tapahtumalla oli toiminnalle kielteinen vaikutus?”
2. **Tietojen kerääminen** seikoista, joilla voi olla yhteys ongelman syntyyn, esimerkiksi ”kuinka kauan ongelma on ollut olemassa, ja mitkä ovat olleet sen vaikutukset?” Eri toimijoiden näkökulmat samaan ongelmaan voivat auttaa muita asianosaisia ymmärtämään ongelman uudella tavalla.
3. **Tietojen analysointi**, jolla poistetaan mahdollisuus, että jokin esitettävä johtopäätös onkin harhaanjohtava.

4. Juurisyiden selvittäminen sopivalla menetelmällä, esimerkiksi:

- a. "5 x Miksi?"
- b. Ruotokaavio-diagrammi eli syy-seuraus-analyysi

5. Ratkaisujen määrittelemine ja toteuttaminen ongelman juurisyyn poistamiseksi. Tätä kautta pienennetään tapahtuman todennäköisyyttä.

Esimerkki 5 x Miksi? -menetelmästä

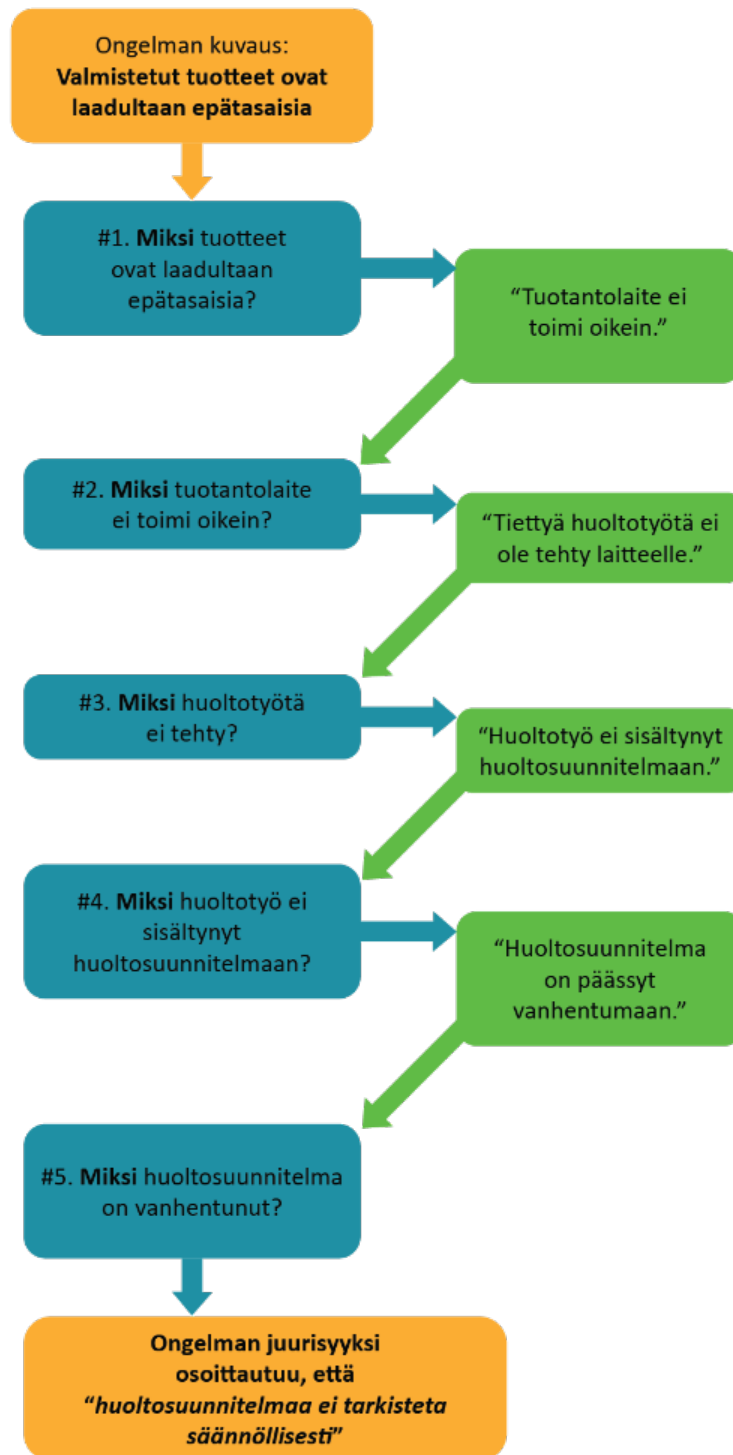
Tämän menetelmän kehitti alun perin Toyota Motor Company valmistusprosessiensa kehittämiseen. Tarkoituksena on ensin saada vastaus yhteen esitettyyn ongelmaan ja sitten lähteä syventämään ongelman syiden määrittelyä kysymällä joka vaiheessa "Miksi?". Lopulta, monesti viidennen "Miksi?"-kysymyksen jälkeen, päädytään ongelman juurisyihin.

On huomattava, että jokainen "Miksi?"-kysymys avaa vain yhden polun, jota etenemällä selviää vain yksi juurisy. Ensimmäinen "Miksi?"-kysymys voi mahdollisesti avata useita polkuja, joista jokainen johtaa eri juurisyihin. Tämän vuoksi ensimmäisen kysymyksen on kuvattava mahdollisimman täsmällisesti tarkasteltavaa ongelmaa.

Mikäli viimeisellä "Miksi?"-kysymyksellä ei saada vakuuttavaa vastausta ongelman juurisyystä, voidaan palata alkuun ja varioida vastausta ensimmäiseen "Miksi?"-kysymykseen.

"Miksi?"-kysymykset voivat johtaa esimerkiksi havaintoon, että fyysisenä syynä ilmenevä ongelma onkin juurisyiltään puute ohjeistuksessa.

Seuraavassa kaaviossa on esimerkki juurisyyn tunnistamisesta "5 x Miksi?"-menetelmällä:

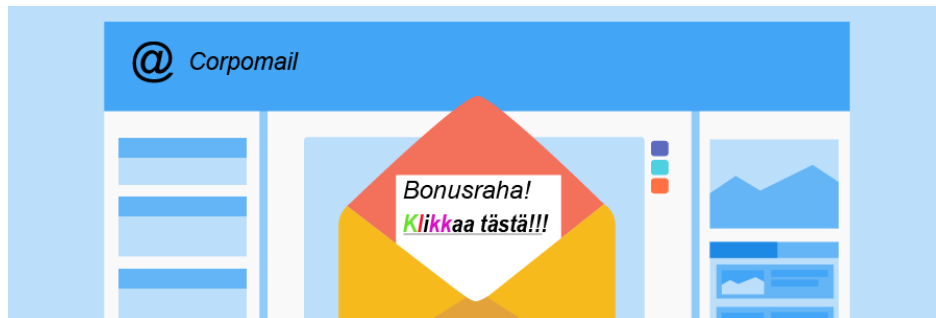


[Avaa kuvan täysikokoinen versio.](#)

Analyysin tulos esimerkissä: Tarkasteltu riski on, että valmistetut tuotteet voi olla epälaatuksia. Juurisyys toteutuneelle riskille on, että tuotantolaitteen huoltosuunnitelmaa ei tarkasteta säännöllisesti. Riski otetaan hallintaan yrityksessä esim. määrittelemällä, että huoltosuunnitelma pitää tarkistaa säännöllisin väliajoin ja että suoritettulle tarkistukselle tulee saada kuittaus esimieheltä.



Tapaus: Pankkitili tyhjennetty!



Huomaat kauhuksesi, että pankkitilisi on tyhjennetty! Muistelet luovuttaneesi pankkitietosi sähköpostitse sinua lähestyneelle asiakkaalle: hänen esihenkilönsä tarvitsi tietoja siirtääkseen tilillesi bonusrahaa palkkioksi hyvin tehdystä työstä. Rahat saadaksesi sinun tuli ainoastaan tunnistautua annetun linkin kautta. Nyt rahat ovat menneet, luvattua bonusrahaa ei kuulu ja epäiletkin tullesesi huijatuksi. Mietit syitä sille, miksi näin pääsi käymään.

Yhdistä seuraavassa kuhunkin juurisyyanalyysin vaiheeseen kuuluva pohdinta.

1. Ongelman ymmärtäminen. Mikä meni vikaan?	Luovutin pankkitietoni huijarille, joka vei rahani.
2. Tietojen kerääminen: millä kaikilla asioilla voi olla yhteys syntyneeseen ongelmaan?	Otan käyttöön roskapostisuodattimen. En enää klikkaa tuntemattomia linkkejä. Olen jatkossa tarkempi arkaluontoisten tietojen luovuttamisen suhteen.
3. Tietojen analysointi: Mitkä asiat todella liittyvät syntyneeseen ongelmaan?	Sähköposti näytti tulleen tutulta asiakkaalta ja linkin sivu näytti luotettavalta.
4. Juurisyiden selvittäminen esimerkiksi miksi-kysymysten avulla.	Miksi luovutin pankkitietoni? Koska luotin viestin lähettäjään. Miksi luotin häneen? Hän sanoi olevansa asiakkaani..
5. Ratkaisujen määritteleminen ja toteuttaminen: Poistetaan löydetty ongelmat ja pienennetään tapahtuman todennäköisyyttä.	Minulla ei ole käytössä roskapostisuodatinta. Klikkasin myös tuntematonta linkkiä sähköpostissa.

5.3 Riskien evaluointi

Oppimistavoite: Riskien merkittävyyden arviointi auttaa sinua tekemään päätöksiä tunnistettujen riskien käsittelyn tärkeysjärjestyksestä. Tässä kappaleessa opit myös laatimaan riskimatriisin. Kappaleen lopussa vastaat monivalintatehtäviin riskitason arvioimisesta liittyen erilaisiin digiriskeihin. Arvioitu ajankäyttö: 12 min.

Riskien merkittävyyden arviointi eli riskien evaluointi auttaa tekemään päätöksiä siitä, mitä tavoitteisiin vaikuttavia riskejä on tarpeen käsitellä ja missä tärkeysjärjestyksessä.

Konkreettinen keino arvioida useiden riskien keskinäistä merkittävyyttä on määrittää niille riskiluku. Tältä pohjalta arvioidut sekä toiminnan kannalta olennaiset riskit kirjataan riskimatriisiin.

Nettoriski lasketaan seuraavasti:

riskiluku = tapahtuman todennäköisyys * tapahtuman vaikutus

Tämä kaava on tullut esille jo aiemmin. Siihen palataan nyt tässä yhteydessä, sillä jotta riskiluku voidaan laskea, tulee **pisteyttää** jokaisen tapahtuman todennäköisyys ja sen vaikutuksen laajuus.

Pisteytyksen asteikko valitaan käsiteltävän kohteen eli sen mukaan, kuinka hienojakoinen arvio tarvitaan. Tasoja on oltava riittävästi, jotta kaikki tunnistetut tapahtumat voidaan priorisoida keskenään. Voidaan valita esimerkiksi kolmesta viiteen tasoa sekä tapahtuman todennäköisyydelle että sen vaikutukselle.

Todennäköisyyden ja vaikutuksen arviointi on subjektiivista, vaikka lähtökohtana olisi sama informaatio. Esimerkiksi todennäköisyysarvio ei välttämättä heijasta tapahtuman todellista todennäköisyyttä, koska arvio perustuu arvioijan tietämyksen tasoon. Tämän vuoksi on hyvä pyrkiä muodostamaan arvio useamman ihmisen näkemyksistä.

Todennäköisyyden arviointi

Tapahtuman todennäköisyyttä voidaan arvioida monella tavalla. Olennaista on, että tietyn toiminnan riskien arvioinnissa käytetään kauttaaltaan yhdenmukaista arviointia. Todennäköisyyden arvioinnin tarkoituksena on luoda pohja sille, että saadaan kaikki tunnistetut tapahtumat keskenään prioriteettijärjestykseen.

Seuraavassa on esimerkki analyysiasteikosta, jossa riskien arviointi tapahtuu neliportaisella asteikolla eli luvuilla 1–4 (JUDO s. 19):

1. **Epätodennäköinen** – tapahtuma toteutuu vain poikkeuksellisissa oloissa
2. **Mahdollinen** – tapahtuma saattaa toteutua joissakin olosuhteissa
3. **Todennäköinen** – odotetaan että tapahtuman toteutuminen on todennäköisempää, kun että se ei toteudu
4. **Lähes varma** – tapahtuma tai sitä vastaava "läheltä piti" -tilanne on toteutunut usein

aikaisemmin.

Tapahtuman toteutumisen todennäköisyyttä voidaan arvioida myös seuraavasti asteikolla 1–6):

- Tapahtuu kerran vuodessa (todennäköisyys: 1)
- Tapahtuu kerran vuosineljänneksessä (todennäköisyys: 2)
- Tapahtuu kerran kuukaudessa (todennäköisyys: 3)
- Tapahtuu kerran viikossa (todennäköisyys: 4)
- Tapahtuu kerran päivässä (todennäköisyys: 5)
- Tapahtuu useamman kerran päivässä (todennäköisyys: 6).

Todennäköisyyden arviointi voidaan suorittaa myös seuraavan kaltaisen taulukon pohjalta. Siinä on kaksi eri aikaulottuvuutta ja pisteytystä saman tapahtuman todennäköisyyden arvioinnille.

Tapahtuman todennäköisyys 3 kk sisällä	Tapahtuman pisteytys	Tapahtuman todennäköisyys 12 kk sisällä	Tapahtuman pisteytys
0–10%	1	0–10%	0
11–20%	3	11–20%	1
21–50%	5	21–50%	3
yli 50%	7	yli 50%	5

[Avaa taulukon täysikokoinen versio.](#)

On huomattava, että yksinkertaista keinoa laskea todennäköisyyttä ei pystytä läheskään aina tunnistamaan.

Digiriskejä arvioitaessa on hyvä huomioida, että monet haitalliset tapahtumat digiympäristössä, kuten sähköpostin ”spämmääminen” ja palvelunestohyökkäys, voidaan automatisoida niiden toteuttajan taholta. Näin ollen tapahtuman toteutuminen voi olla jatkuvaa.

Teoksen ”Johda riskejä” mukaan IT-riskeissä, eli IT-palveluiden tuottamisessa, hankinnassa ja hallinnoinnissa, ei ole tarkoituksenmukaista pyrkiä arvioimaan riskien aitoa todennäköisyyttä. Sen sijaan IT-riskien pisteytyksen kautta pitäisi saada tunnistettua kaikkein merkittävimmät riskit. (JOHDA s. 177)

Digiriskien priorisointi voidaan tehdä myös siltä pohjalta, miten riskien toteutuminen vaikuttaisi SLA (Service Level Agreement) -tasoihin. Ne on määritelty sopimuksissa asiakkaiden tai palveluntuottajan kanssa. (JOHDA s. 177)

Vaikutuksen arviointi

Toinen osa tapahtumien keskinäisestä priorisoinnista pohjautuu niiden vaikutuksiin suhteessa toiminnan tavoitteisiin.

Tapahtuman kielteinen vaikutus tavoitteisiin voidaan arvioida ja pisteyttää esimerkiksi seuraavanlaisella neliportaisella asteikolla:

Vaikutuksen arviointi	Vaikutuksen pisteytys
Vähäinen: tapahtuma aiheuttaa vähäistä haittaa tavoitteen saavuttamiselle.	0
Kohtalainen: tapahtuma viivästyttää tavoitteen saavuttamista; toimintaa ei tarvitse keskeyttää, mutta saatetaan joutua muuttamaan toiminnallisia suunnitelmia.	3
Merkittävä: tapahtuma vaikeuttaa tai hidastaa tavoitteen saavuttamista; toiminta joudutaan keskeyttämään.	7
Kriittinen: tapahtuma estää tavoitteen saavuttamisen; toiminta keskeytyy ja estyy pitkäksi ajaksi.	10

[Avaa taulukon täysikokoinen versio.](#)

Vastaavalla tavalla arvioidaan tunnistettujen tapahtumien myönteinen vaikutus tavoitteiden saavuttamiseen.

Riskimatriisi

Riskimatriisiin kautta käsitellään kaikkia toimintaan liittyviä riskejä kokonaisuutena. Jokaiselle matriisiin kirjatulle riskille määritellään riskiluku edellä kuvatulla tavalla. Riskiluvun pohjalta riskit priorisoidaan ja käytössä olevat resurssit voidaan kohdistaa merkittävimpien riskien hallitsemiseen.

Vaikutuksen laajuus Todennäköisyys	1 Vähäinen	2 Kohtalainen	3 Merkittävä	4 Kriittinen
	4 Lähes varma	Keskin- kertainen	Suuri	Kestämätön
3 Todennäköinen	Pieni	Keskin- kertainen	Suuri	Kestämätön
2 Mahdollinen	Minimaalinen	Keskin- kertainen	Keskin- kertainen	Suuri
1 Epätodennäköinen	Minimaalinen	Minimaalinen	Pieni	Keskin- kertainen

[Avaa kuvan täysikokoinen versio.](#)

Kuvassa on esimerkki riskimatriisin pohjasta, jossa riskiluku lasketaan kertomalla riskin vaikutus riskin todennäköisyydellä. Vaihtoehtoisesti matriisin toista ulottuvuutta, yleensä vaikutuksen laajuutta, voidaan painottaa esimerkiksi kaksinkertaistamalla sen arvo riskilukua laskettaessa.

Riskiluvut 1–16 on ryhmitetty viiteen riskitasoon, joiden sanallisten kuvausten tueksi käytetään värikoodausta. Näin saadaan muodostettua **indikaattoreita** (engl. Key Risk Indicators): kun arvio seurattavasta riskistä siirtyy tasolta seuraavalle, esim. keskinkertaisesta suureksi, ylittyy sen **huomioraja**. Edellisen esimerkin riskitasot on esitetty seuraavassa taulukossa.

Riskitaso (riskiluvut)	Vaadittavat toimenpiteet (esimerkiksi)
Minimaalinen (1–2)	Ei vaadi huomiota
Pieni (3–4)	..
Keskinkertainen (4–6)	..
Suuri (8–9)	..
Kestämätön (12–16)	Vaatii välitöntä huomiota

[Avaa taulukon täysikokoinen versio.](#)

Riskitasojen värikoodauksella nähdään nopeasti, mihin mahdollisiin tapahtumiin tulee kiinnittää huomioita ensimmäiseksi ja eniten. Samalla nähdään kokonaisuutena, mille riskitasoille kaikki toiminnalle tunnistetut riskit painottuvat. Esimerkiksi toiminta, jossa valtaosa tunnistetuista riskeistä arvioidaan kestävämmälle tasolle, kannattanee suunnitella uudelleen ennen toiminnan aloittamista.

Riskinsietokyky määritellään matriisin pohjalta: se on riskin suuruuden yläraja, johon asti ollaan valmiita sitoutumaan. Esimerkiksi matriisin punaisille alueille osuvia riskejä ei siedetä. **Riskinottohalu** on riskin määrän alaraja, jonka alittavat riskit ollaan valmiita ottamaan toiminnassa; esimerkiksi matriisin vihreille alueille sijoittuvat riskit.

Arvioinnin yhteydessä päätetään riskin mahdollisista täydennys- tai uudelleenarviointitarpeista. Mahdollinen päätös riskin merkittävyyden arvioinnille voi olla myös, että tiettyä riskiä ei oteta käsittelyyn, koska sen käsittely veisi resursseja muilta, merkittävämmäksi koetuilta riskeiltä. (JUDO s. 20)

Riskienhallintaprosessin seuraavassa vaiheessa matriisista riskit siirretään riskirekisteriin käsittelyä varten.

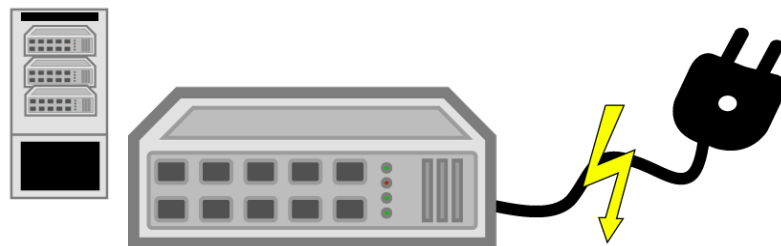
Dokumentoinnin tärkeys

On hyvä dokumentoida riskien arvioinnin perusteet, kuten se, mihin käytettävissä olleeseen tietoon ja tulkintoihin pohjautui tehty arvio kunkin tapahtuman todennäköisyydestä ja vaikutuksen laajuudesta. Näin arvioon voidaan myöhemmin palata riskien seurannan ja uudelleen arvioinnin yhteydessä.



Riskitasot

Arvioi alla esiteltyjä tapauksia riskimatriisin pohjalta. Laita tapaukset esitettyjen tietojen perusteella riskitasoltaan järjestykseen suurimmasta pienimpään.



Tapaus 1: Yrityksemme serverit tarvitsevat paljon sähköä. Jo viikon sähkökatko aiheuttaisi toiminnallemme kohtalaiset tappiot. Meillä on onneksi hyvät varavirtalähteet eikä ole todennäköistä, että sähköt olisivat näin pitkään poikki.



Tapaus 2: Erääseen IT-projektiin tehtiin todella iso rahallinen panostus. Sen epäonnistuminen aiheuttaisi toiminnallemme kriittiset, miljoonaluokan tappiot. Todennäköisyys epäonnistumiselle on 50/50.



Tapaus 3: Osastollamme on tällä hetkellä kova kiire. On 90% varmuudella todennäköistä, että projekti tulee myöhästymään ja joudumme maksamaan asiakkaallemme sopimussakkoa. Onneksi projekti on melko pieni ja sillä on vain vähäinen vaikutus toimintaamme.

Millä tapauksista on suurin riskitaso?

- ◇ Tapaus 1 (Viikon sähkökatko)
- ◇ Tapaus 2 (Iso rahallinen panostus)
- ◇ Tapaus 3 (Myöhästytävä projekti)

Millä tapauksella on keskinkertainen riskitaso?

- ◇ Tapaus 1 (Viikon sähkökatko)
- ◇ Tapaus 2 (Iso rahallinen panostus)
- ◇ Tapaus 3 (Myöhästynyt projekti)

Entä millä tapauksista on pienin riskitaso?

- ◇ Tapaus 1 (Viikon sähkökatko)
- ◇ Tapaus 2 (Iso rahallinen panostus)
- ◇ Tapaus 3 (Myöhästynyt projekti)

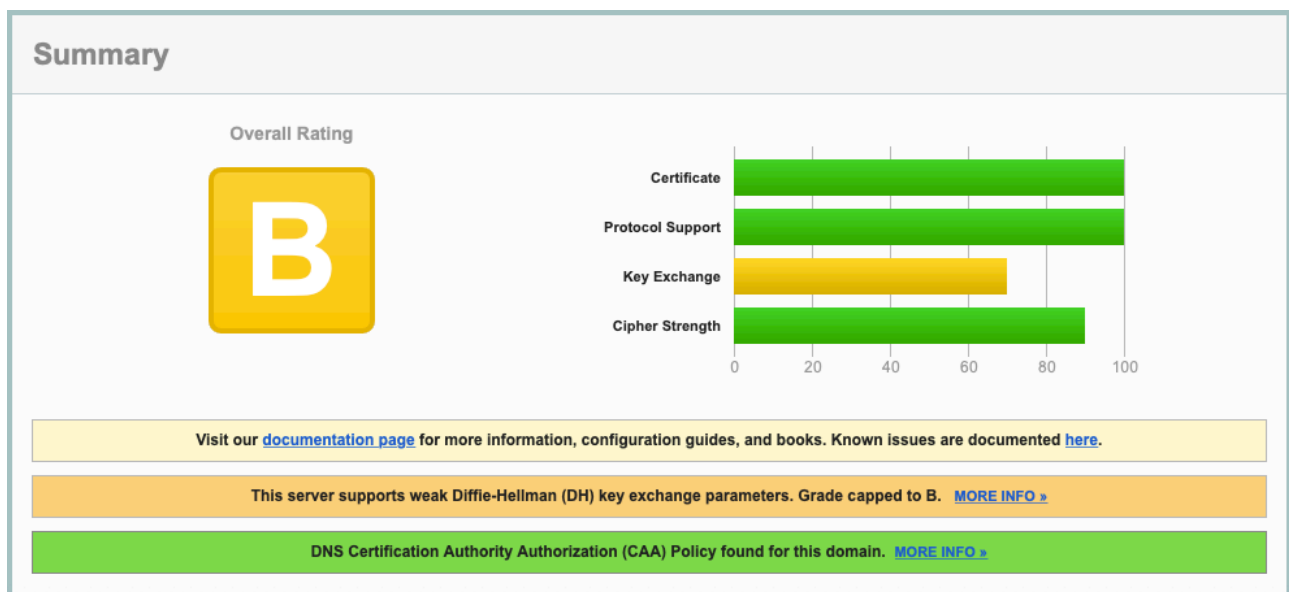
5.4 Digiriskien tunnistaminen yritystoiminnassa

Oppimistavoite: Tässä kappaleessa perehdyt matriisiin, jolla tunnistat erityisesti yritystoimintaan liittyviä digiriskejä. Täytät matriisin ohjeistuksen pohjalta. Arvioitu ajankäyttö: 30 min.

”Riskienhallinta on se, missä (muun muassa) turvallisuuden ja muun toiminnan pitäisi kohdata ja keskustella.” (VAHTI s. 13)

Digiriski voi periaatteessa olla mikä tahansa epävarmuus, jolla on vaikutusta asetettuihin tavoitteisiin digitaalisessa toimintaympäristössä. Digiriskejä voi siis olla lukuisia.

Internetissä yritys näkyy pitkälti sen verkkosivujen kautta. Yrityksen verkkosivujen mahdollisten haavoittuvuuksien tunnistamiseen on tarjolla maksuttomia verkkopalveluita, kuten [Qualysin ratkaisu](#), joka antaa yksityiskohtaisen teknisen arvion ohella selkeän yhteenvedon verkkopalvelun turvallisuudesta kuten kuvassa alla.



Mikäli analyysi osoittaa, että verkkopalvelun turvallisuudessa olisi parantamisen varaa, tulee parannuskohdat ottaa käsittelyyn esim. verkkosivujen palvelun tarjoajan kanssa. Asiakkaat voivat käyttää Qualysin kaltaisia ratkaisuja selvittäessään potentiaalisten yrityskumppaniensa tietoturvan tasoa sen pohjalta, miten turvallisuuteen on panostettu niiden julkisilla verkkosivuilla.

Skenaariot ja matriisi

Digiriskejä voidaan tunnistaa yrityksen digitoimintojen suojaamisen kautta. Aluksi luodaan skenaarioita vastaamalla kysymyksiin suojattavien kohteiden haavoittuvuuksista ja heikkouksista: *”Mitä meillä on digiympäristössä, mitä meillä tapahtuu digiympäristössä, mitä meihin voisi kohdistua digiympäristössä?”*. (VAHTI s. 30)

Skenaariosta poimitaan alla olevaan taulukkoon erilaisia yhdistelmiä:

- 1) jokaiselle suojattavalle/puolustettavalle kohteelle
- 2) jokaiselle mahdolliseksi tunnistetulle uhkalle kuten hyökkäykselle tai häiriölle.

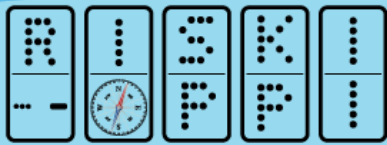
Lopuksi jokaiselle tarkastelun kohteena olevalle kohteen ja uhkan yhdistelmälle määritellään taulukkoon:

- 3) puolustuksen toteutus eli toimenpiteet hyökkäyksen/häiriön torjumiseen tai sen vaikutusten pienentämiseen.

Näin taulukkoon muodostettavan matriisin kautta läpikäydään järjestelmällisesti eri digiriskit eli kohteiden ja uhkien yhdistelmät (VAHTI s. 30). Matriisin kerätyt digiriskit viedään riskianalyysiin, jossa niitä tarkastellaan kokonaisuutena muiden tunnistettujen riskien kanssa.

TORJUNNAN NÄKÖKULMA: Suojattavat digitoiminnot HYÖKKÄYKSEN TAI HÄIRIÖN NÄKÖKULMA: Digitoimintoon kohdistuva uhka	VERKKO-KOMMUNIKAATIO Tietoliikennetekniikka, verkkoyhteydet, viestintä, kommunikaatio, kiinteä tai mobiili yhteys, toiminnon kannalta vaadittu minimi latenssi ja siirtokapasiteetti	TIETOVARANNOT Verkkosivusto, datan kerääminen, tiedostot, tietokannat ja tietovarastot	KÄSITTELY Ohjelmistot, tietojärjestelmät, pilvipalvelut ja tekoäly	AUTOMAATIO IoT, sensorit, robotiikka, etäkäyttö ja etävalvonta	VIRTUAALISUUS Virtuaalimallit, VR/MR/XR, virtuaaliläsnäolo, metaversumi
TEKNINEN HÄIRIÖ Käyttökeskeytys, yhteyskatkokset	1. Puolustuksen näkökulma 2. Ennakoitu hyökkäys tai häiriö 3. Puolustuksen toteutus	---			
TIETOTURVA Tietovarkaudet, teollisuusvakoilu, tietovuodot	---	---			
PALVELUNESTO Estohyökkäykset tietoliikennehäirintä					
TALOUSRIKOLLISUUS Kirstytys, petos, identiteettivarkaudet					
KYBERRIKOLLISUUS Virukset, hakkerointi					

Matriisi digiriskien tunnistamiseen. (VAHTI s. 30; RISKI-DIGI)



TEHTÄVÄ!

Lataa matriisi PDF-muodossa [tästä](#) ja täytä se oman organisaatiosi tilanteen pohjalta. Ota mielellään kollegoitasi mukaan taulukon täyttämiseen. Taulukon kautta arvio tilanteesta tulee päivittää säännöllisesti.



Kerro vielä, miten näiden asioiden oppiminen sujuu sinulta?

- ◇ Kaikki hyvin! Jatketaan.
- ◇ Haluan henkilökohtaista opastusta tähän aiheeseen

6.1 Riskien käsittely

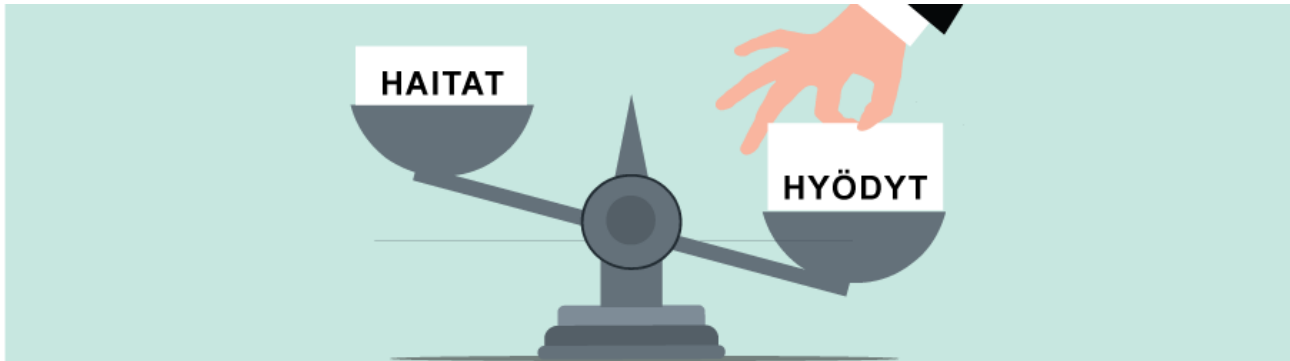
Oppimistavoite: Tässä kappaleessa opit, että riskien käsittelyyn kuuluu kaikki toimenpiteet, joilla riski muunnetaan hyväksyttävälle tasolle. Opit näitä keskeisiä käsittelytoimenpiteitä. Kappaleen lopussa testaat tietojasi tehtävissä, jotka käsittelevät jäännösriskejä parissa digitilanteessa. Arvioitu ajankäyttö: 10 min.

Riskien käsittely tarkoittaa sellaisten toimenpiteiden määrittelemistä, joilla tunnistettu riski muunnetaan hyväksyttävälle riskitasolle. Kun käsittely on tehty jokaiselle tunnistetulle riskille, voidaan toiminnassa edetä luottavaisemmin.

Riskien käsittely on resurssien kohdentamista: toiminnan tavoitteiden kannalta merkittävimmät riskit saavat suurimman huomion. Näin ollen riskien käsittely lähtee kunkin riskin arvon ja

merkittävyyden määrittelystä. Tarkasteltavan toiminnan kannalta arvokkaimpiin ja merkittävimpiin riskeihin kohdistetaan tarvittavat resurssit.

Riskin arvo



Jotta riski voidaan ottaa käsittelyyn, tulee riskille määritellä arvo. Se on laskelma siitä, mitä riskin käsittelyn mahdolliset vaihtoehdot tulevat kustantamaan rahana tai muuna resurssina. Lisäksi lasketaan kustannukset kaikkien riskien muodostamaan kokonaisuuden käsittelyyn.

On kaksi päätapaa tarkastella riskin arvoa (VAHTI s. 54):

1. Arvioidaan potentiaalisia menetyksiä riskin toteutuessa sekä arvioidaan mahdollisia etuja, joita riskien toteutuminen avaa.
2. Tarkastellaan riskin torjumiseen tarvittavien toimenpiteiden arvoa, kuten riskin siirtämiseen hankittavan vakuutuksen hintaa tai riskin seurantaan käytettävää henkilöresurssia.

Rahan sijaan riskin arvo voidaan määritellä muiden sellaisten resurssien kautta, joihin riski vaikuttaa.

Riskin merkittävyys

Edellä käsitelty riskimatriisi on väline, jolla pohjustetaan kunkin tunnistetun riskin merkittävyyden määrittely. Matriisissa riskitaso kullekin riskille saadaan kertomalla riskin vaikutus riskin todennäköisyydellä.

Riskin merkittävyys määrittyy riskitason pohjalta esimerkiksi seuraavasti (JUDO s. 20):

- Kriittinen riski, joka vaatii välittömiä toimenpiteitä (korkein riskitaso).
- Merkittävä riski, joka vaatii nopeita toimenpiteitä.
- Huomioitava riski.
- Seurattava riski (matala riskitaso).
- Jäännösriski, joka päätetään jättää hallintatoimien ulkopuolelle (yleensä matala riskitaso).
- Otettava riski, joka päätetään ottaa, jotta toiminnassa päästään etenemään (voi olla riskitasoltaan matala tai korkea).

Riskien merkittävyyttä arvioitaessa päätetään, mitä hallintatoimenpiteitä kunkin riskin suhteen tullaan tekemään, sekä arvioidaan esitetyn hallintatoimenpiteen toteutuksen prioriteettia, järjestystä, aikataulua ja tarvittavia resursseja.

Riskien määrittelyssä jokainen riski suhteutetaan toiminnalle asetettuihin tavoitteisiin sekä riskienhallintaan panostettaviin resursseihin. Tätä kautta määritellään raja-arvo sille, mitä riskissä voidaan sietää ja toisaalta mitä ei voida hyväksyä. Tämän huomiorajan ylittyessä reagoidaan suunnitellulla toimenpiteellä. (VAHTI s. 23–24)

Resursseja on harvoin käytettävissä lieventämään kaikkien riskien kielteisiä vaikutuksia. Jäännösriski tarkoittaa sitä osaa tunnistetusta riskistä, joka tietoisesti päätetään jättää hallintatoimien ulkopuolelle. Jäännösriski liittyy usein sellaiseen epävarmuuteen, joka ei edes olisi poistettavissa kohtuullisella kustannuksella tai toimenpiteellä. Jäännösriskiin voi myös sisältyä tunnistamaton riskin osaa, joka ilmenee vasta riskin toteutuessa. (VAHTI s. 55)

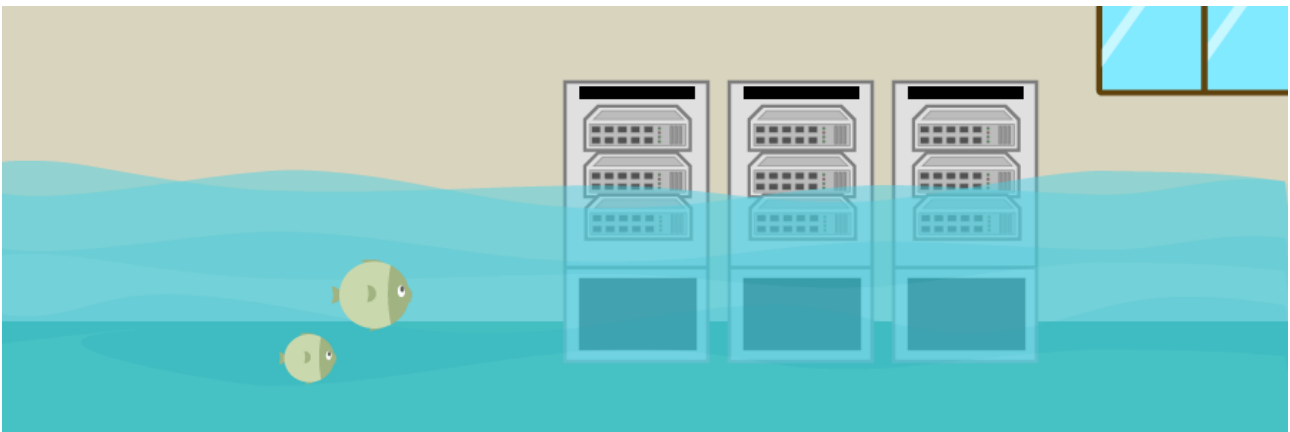


Mikä jää jäännösriskiksi?

Kuten edellä todettiin: *"Resursseja on harvoin käytettävissä lieventämään kaikkien riskien kielteisiä vaikutuksia. Jäännösriski tarkoittaa sitä osaa tunnistetusta riskistä, joka tietoisesti päätetään jättää hallintatoimien ulkopuolelle."*

Valitse seuraavista esimerkitapauksista jäännösriskiksi jäävä asia mahdollisissa digiriskitilanteissa.

Tapaus 1: Digiriskien siirtäminen vakuutuksella



Yritykselle tarjotaan vakuutusta, joka korvaa 2. kerroksessa, muiden toimisto- ja sosiaalitilojen yhteydessä sijaitsevalle **serverihuoneelle** mahdollisesti aiheutuvia vahinkoja. Vakuutus koostuu kolmesta osasta:

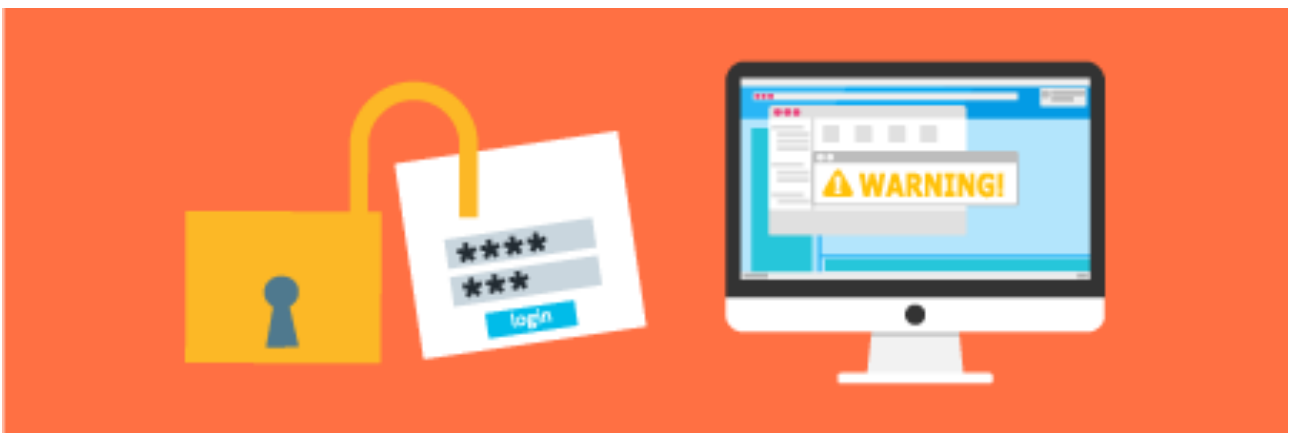
- a. Putkistovuodoista johtuvien vahinkojen turva
- b. Tulipalosta johtuvien vahinkojen turva
- c. Tulvavesi- ja muu luonnonilmiöiden turva

Kaikki yllä mainitut tilanteet huomioiva vakuutus tulisi kuitenkin erittäin kalliiksi. Hintaan saataisiin huomattava alennus jättämällä yksi turvavaihtoehdoista pois.

Mikä vakuutuksen osa voidaan tässä tapauksessa pudottaa jäännösriskinä pois?

- ◇ Putkistovuodoista johtuvien vahinkojen turva
- ◇ Tulipalosta johtuvien vahinkojen turva
- ◇ Tulvavesi- ja muu luonnonilmiöiden turva

Tapaus 2: Tietoturva



Yritys on huomionnut toiminnassaan tietoturvan tarkasti. Sen tietoturvaohjelmistot pidetään ajan tasalla ja henkilökuntaa koulutetaan aktiivisesti tunnistamaan työssään erilaisia tietoturvariskejä. Vaikka yritys on varautunut hyvin, on kaikkia uhkia vaikea poistaa kokonaan.

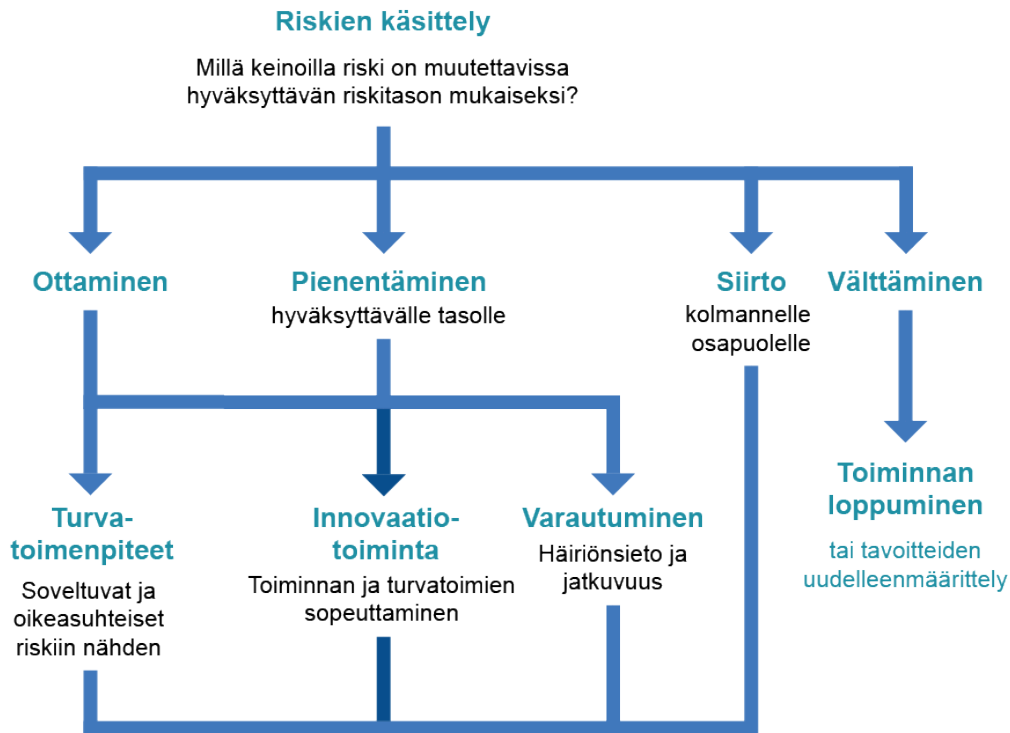
Mikä seuraavista tilanteista on todennäköisin jäännösriski?

- ◇ Yrityksen järjestelmiin kohdistuvat palvelunestohyökkäykset
- ◇ Henkilöstöön kohdistuvat tietojenkalasteluyritykset
- ◇ Tietokoneen hajoaminen ja tietojen menetys

6.2 Hallintatoimenpiteiden määrittäminen

Oppimistavoite: Tässä kappaleessa opit neljä riskienhallinnan toimenpiteiden periaatetta sekä kontrollin käsitteen. Kappaleen lopussa vastaat ”Puuttuva sana” -tehtävään digiriskin hallinnasta. Arvioitu ajankäyttö: 20 min.

Riskien käsittelyllä tarkoitetaan toimenpiteitä, joilla riski muutetaan hyväksyttävälle tasolle. Seuraavaksi esitellään tähän neljä erilaista toimenpidettä.



[Avaa kaavion täysikokoinen versio.](#) Kaaviossa esitetään yhteenveto riskienhallintatoimenpiteiden periaatteista pohjautuen OECD:n suositukseen (OECD s. 38).

Riskienhallintatoimenpiteet ovat **periaatteiltaan** seuraavat:

1) Riskiä **pienennetään**:

- a) **turvatoimenpiteillä**, joihin käytetyt resurssit ovat oikeasuhteiset riskiin merkittävyyteen nähden
- b) **innovaatiotoiminnalla** toiminnan ja turvatoimien sopeuttamisessa epävarmuuksiin
- c) **varautumisella**, jolloin varataan resursseja häiriönsiedon parantamiseen ja toiminnan jatkuvuuden varmistamiseen häiriötilanteissa.

2) Riski **siirretään** ulkopuoliselle taholle maksamalla hinta, jotta riskin toteutumisen kielteiseltä vaikutukselta välttyään omalta osalta. Käytännössä riski siirretään esimerkiksi ottamalla vakuutus

tai sopimuksella. Vakuutukset voivat olla vapaaehtoisia (kohdistuen henkilöön, omaisuuteen tai toimintaan) tai lakisääteisiä (esimerkiksi tapaturma- ja liikennevakuutukset) (JOHDA s. 146). Myös jonkin välineen vuokraaminen, sen ostamisen sijaan, on laitteeseen liittyvän riskin siirtämistä.

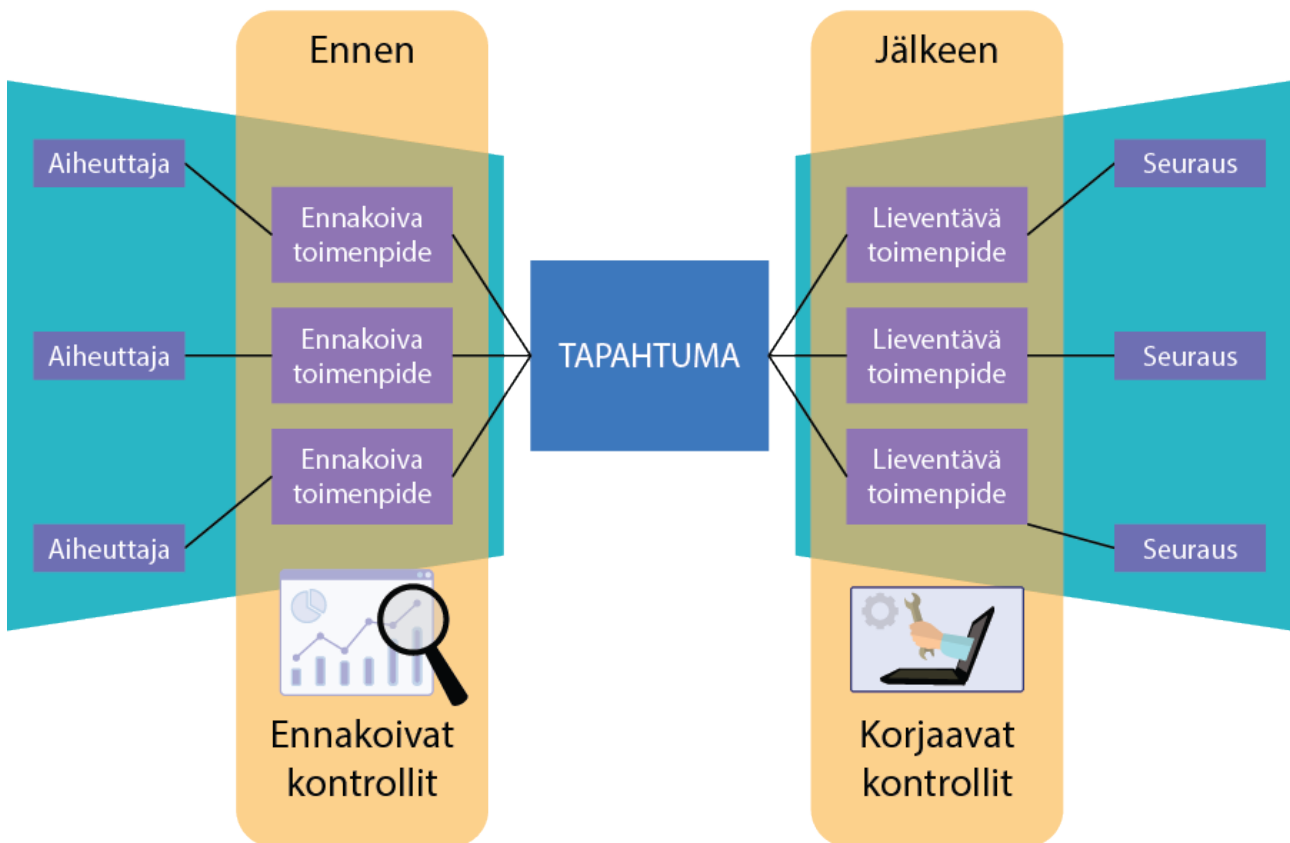
3) Riski päätetään **ottaa tai hyväksyä**, jolloin suunniteltu toiminta jatkuu riskistä tietoisena. Lisäksi, kuten kaaviossa kuvataan, voidaan otettavaakin riskiä pyrkiä pienentämään edellä mainituilla toimenpiteillä esimerkiksi pidemmällä aikavälillä.

4) Riski **vältetään** siten, että toimintaa ei käynnistetä alkuperäisen suunnitelman mukaisesti. Toiminnalle laaditaan uusi toteutustapa, jossa riskit ovat hyväksyttäviä tai poistettavissa eli riskeille tunnistetaan **poistoratkaisu**. Toiminnan uudelleensuunnittelun yhteydessä voidaan myös tavoitteet määritellä ainakin osittain uudelleen. Jos hyväksyttävää toteutustapaa ei löydetä, tulee harkita toiminnan lopettamista ainakin niiden riskien osalta, joille ei tunnisteta poistoratkaisua.

Jokaiselle tunnistetulle riskille pyritään valitsemaan vähintään yksi hallintatoimenpide näistä neljästä tyypistä. Vaihtoehtoisesti jokin riski voidaan jakaa osiin ja hallita sen osia erityyppisillä toimenpiteillä. Esimerkiksi yksi osa riskistä siirretään vakuutuksella ulkopuoliselle taholle ja toinen osa riskistä pienennetään sen seurantaan kohdistettavalla työpanoksella.

Kertaluonteiset toimenpiteet ja jatkuvat kontrollit

Hallintatoimenpiteitä voidaan asettaa kohdistumaan ennen tai jälkeen riskiksi tunnistetun tapahtuman. Aikaisemmin käsitelty **rusettianalyysi** on yksi menetelmä, jolla suunnitellaan hallintakeinoja riskiksi tunnistetun tapahtuman ympärille alla kuvatulla tavalla.

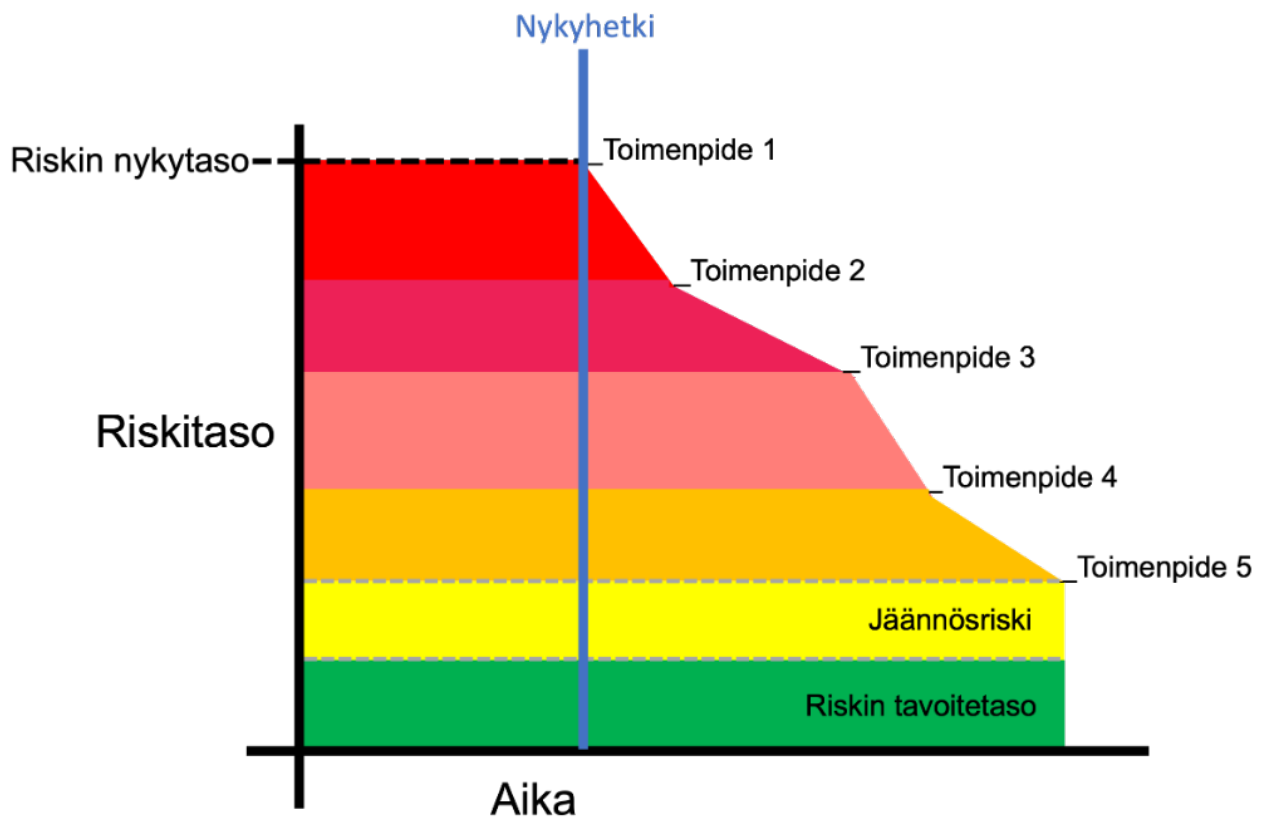


[Avaa kuvan täysikokoinen versio.](#)

Riskin aiheuttajat, kuten uhkat ja vaarat, luetellaan rusettikuvion vasemmalla puolella, eli ne sijoitetaan ennen tarkasteltavaa tapahtumaa.

Osalla riskienhallintatoimenpiteitä pienennetään riskin suuruutta ennen tapahtuman mahdollista toteutumista. Näillä toimenpiteillä pienennetään tapahtuman toteutumisen todennäköisyyttä ja/tai vähennetään tapahtuman kielteisiä vaikutuksia tavoitteisiin. Ennakoivat toimenpiteet pyritään kohdistamaan riskin juurisyihin (JOHDA s. 101).

Alla olevassa kaaviossa esitetään, miten sarjalla kertaluontoisia toimenpiteitä pienennetään riskitasoa. Tällainen kaavio toimii hallintatoimenpiteiden suunnitelman laatimisen pohjana. Kaaviolla voidaan esittää joko yksittäisen riskin tai useamman tunnistetun riskin yhdistelmän tasoon vaikuttaminen. Kun kaaviota käytetään suunnittelun välineenä, voidaan sen aika-akselille merkitä kalenterikuukausi ja toimenpiteen yhteyteen voidaan kirjata toimenpiteen toteuttamisen aiheuttamat kustannukset. Suunnitelmaa laadittaessa on myös huomioitava, millä tasolla on luottamus siihen, että suunnitellut toimenpiteet voidaan toteuttaa onnistuneesti ja että niillä saavutetaan tavoiteltu tulos riskin pienentämiseksi. (OPEN UNIVERSITY)



Kaaviossa visualisoidaan riskin taso ja sarja suunniteltuja toimenpiteitä, jotka ”vesiputous”-mallin mukaisesti pienentävät riskiä ajan myötä, kunnes toimenpiteillä saavutetaan hyväksytty riskitaso. Monesti toimenpiteiden jälkeen jää jäännösriskiä, joka hyväksytään ottaa. (OPEN UNIVERSITY)

Kontrolli on toistettava toimenpide, jonka kautta riski pidetään nykyisellä, hyväksytyksi katsotulla tasolla. Kontrollin toimiessa riski pysyy nykyisellä tasollaan, mutta kontrollin pettäessä voi riskin taso nousta. (OPEN UNIVERSITY)

Kontrollissa on kolme vaihetta:

1. **Tunnistaminen**: kontrolliin käytetään menetelmää, jolla tunnistetaan, että riskinä tarkasteltava tapahtuma on toteutumassa; esimerkiksi havaitaan, että riskin juurisyy on toteutunut
2. **Tulkinta**: kontrolliin käytetään menetelmää, jolla tulkitaan, että tunnistettu tapahtuma on aiheuttamassa riskin toteutumisen
3. **Toimenpide**: tulkinnan pohjalta suoritetaan ennalta määritelty toimenpide, jolla ehkäistään tapahtumasta seuraavan riskin toteutuminen tai lievennetään sen seurauksia. (OPEN UNIVERSITY)

Kontrolleja asetetaan hallitsemaan riskiä ennen ja jälkeen tarkasteltavan tapahtuman. Riskin aiheuttajille asetetaan ennakoivia kontrolleja eli toimenpiteitä, joilla aiheuttajan (tapahtuman) vaikutukset pyritään havaitsemaan, ehkäisemään tai korjaamaan (JOHDA s. 220).

Vastaavasti määritellään toimenpiteitä, joilla vaikutetaan tapahtuman jälkeisiin seurauksiin. Huomaa, että yllä esitettyssä rusettianalyyssissä riskiä tarkastellaan kielteisenä tapahtumana, jota hallitaan **lieventävillä toimenpiteillä** ja **korjaavilla kontrolleilla**. Yhtä lailla voidaan suunnitella

tapahtuman jälkeisiä toimenpiteitä, joilla tapahtuman seurauksista pyritään ottamaan hyöty irti tavoitteiden edistämiseksi.

Kertaluonteisen riskitasoa pienentävän toimenpiteen ja toistuvan kontrollin eron voi mieltää seuraavalla konkreettisella esimerkillä. Riskiksi tunnistetaan tulipalosta aiheutuva toiminnan keskeytyminen. Riskiä pienentävänä toimenpiteenä asennetaan palovaroitin toimitilaan. Ennakoivana kontrollina palovaroittimeen toimivuus testataan säännöllisesti. Korjaavaksi kontrolliksi laaditaan suunnitelma siitä, miten toimitaan, kun palovaroitin hälyttää.

Hallintatoimenpiteiden vertailu ja valinta

Jokaiselle riskille voidaan tunnistaa useita vaihtoehtoisia hallintakeinoja. Hallintatoimenpiteen valinta tehdään usein kustannus- ja hyötyanalyysin pohjalta (JOHDA s. 131). Analyysissä kustannuksia vasten punnittavia hyötyjä ovat myös muut tekijät kuin rahalliset tuotot tai saavutettavat säästöt.

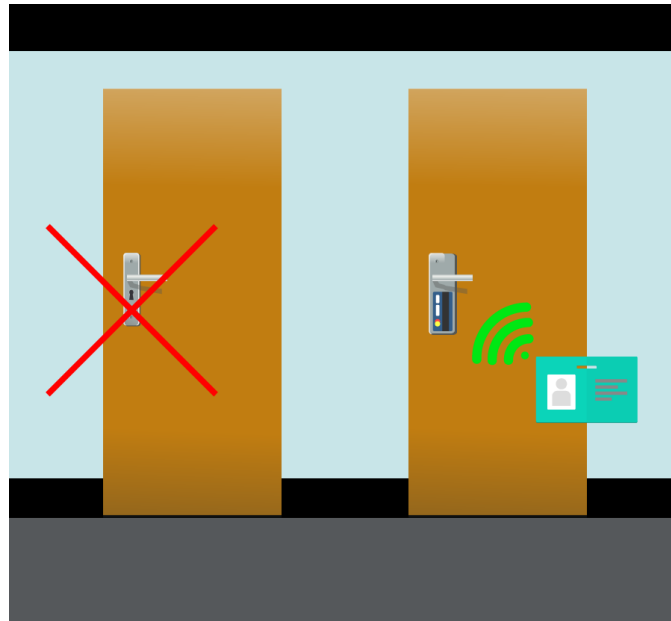
Sopivien toimenpiteiden valinta voidaan tehdä esimerkiksi oheisen taulukon pohjalta suoritettavan vertailun pohjalta (ROUNDS).

Kriteeri	Painokerroin (esim. 1x, 1,5x)	Arvo (esim. 1–10)		Painotettu arvo	
		Vaihtoehto 1: lyhyt kuvaus toimenpiteestä	Vaihtoehto 2: lyhyt kuvaus toimenpiteestä	Vaihtoehto 1: painotetut pisteet	Vaihtoehto 2: painotetut pisteet
Helpoin toteuttaa					
Nopein toteuttaa					
Edullisin toteuttaa					
Tehokkain					
Tuottaa nopeimmin tuloksia					
Vähiten sivuvaikutuksia					
Oma kriteeri					
				Yht.	Yht.

Vaihtoehtoisia toimenpiteitä arvioidaan esimerkiksi taulukon kuuden kriteerin kautta. Taulukkoa voi täydentää omilla kriteereillä. Mikäli jotain kriteereistä halutaan painottaa päätöksenteossa, annetaan sille suurempi kerroin kuin muille kriteereille. Jokainen vaihtoehto pisteytetään taulukon kriteerien pohjalta esimerkiksi asteikolla 1–10. Lopuksi lasketaan jokaisen kriteerin painotettu arvo sekä yhteispistemäärä jokaiselle vaihtoehdolle.



Tapaus: Digitalisoitu kulunvalvonta



Täydennä alla olevaan kertomukseen seuraavat riskienhallintatoimenpiteisiin liittyvät sanat: **pienentäminen**, **siirtäminen**, **hyväksyminen** ja **välttäminen**. Kirjoita sanat pienillä kirjaimilla. Voit vastata '-' ohittaaksesi kohdan.

Yrityksessä on otettu käyttöön digitalisoitu kulunvalvonta ja ovista pääsee sisään vain näyttämällä sähköistä tunnistekorttia ovilla sijaitseviin lukijoihin. Päätöksen taustalla oli lukkojen kalliin uudelleen sarjoittamisen avainten kadottua.

Kulunvalvontaa hoitaa valvontayritys, jolla on vakuutukset ongelmatilanteiden varalle. Tämä riskin ulkopuoliselle maksaa, mutta poistaa yhden työlään ongelman yritykseltä itseltään.

Kaikkia ovia ei pystytä siirtämään kulunvalvonnan piiriin, joten ne jäävät yrityksen omalle vastuulle. Tällaisia ovia on vain muutama, joten tilanteen on nähty perustelluksi.

Yrityksellä on erityinen tila tuotekehitykselle. Aiemmin kaikilla oli pääsy tilaan, mutta nyt on harkittu, ketkä pääsyä oikeasti tarvitsevat. Tämä riskin olisi onnistunut myös avaimilla, mutta sitä tultiin ajatelleeksi vasta tunnistekorttien käyttöönoton yhteydessä.

Yrityksessä on otettu käyttöön digitalisoitu kulunvalvonta ja ovista pääsee sisään vain näyttämällä sähköistä tunnistekorttia ovilla sijaitseviin lukijoihin. Päätöksen taustalla oli lukkojen kalliin uudelleen sarjoittamisen [REDACTED] avainten kadottua.

Kulunvalvontaa hoitaa valvontayritys, jolla on vakuutukset ongelmatilanteiden varalle. Tämä riskin [REDACTED] ulkopuoliselle maksaa, mutta poistaa yhden työlään ongelman yritykseltä itseltään.

Kaikkia ovia ei pystytä siirtämään kulunvalvonnan piiriin, joten ne jäävät yrityksen omalle vastuulle. Tällaisia ovia on vain muutama, joten tilanteen [REDACTED] on nähty perustelluksi.

Yrityksellä on erityinen tila tuotekehitykselle. Aiemmin kaikilla oli pääsy tilaan, mutta nyt on harkittu, ketkä pääsyä oikeasti tarvitsevat. Tämä riskin [REDACTED] olisi onnistunut myös avaimilla, mutta sitä tultiin ajatelleeksi vasta tunnistekorttien käyttöönoton yhteydessä.

6.3 Riskirekisteri hallintavälineenä

Oppimistavoite: tässä kappaleessa opit käyttämään riskirekisteriä riskien kirjaamiseen ja pohjaksi riskienhallintasuunnitelmalle. Lopuksi vastaat monivalintatehtävään riskirekisterin osista. Arvioitu ajankäyttö: 8 min.

Yleisenä välineenä riskienhallintaan käytetään **riskirekisteriä**. Se on yksinkertaisimmillaan taulukko, johon kirjataan tunnistetut riskit hallintaprosessin aikaisemmassa vaiheessa laaditusta riskimatriisista. Lisäksi kirjataan tiedot niihin kohdistettavista hallintatoimenpiteistä.

merkittävyyden värikoodaus

kriittinen merkittävä seurattava

	Riskin otsikko	Tapahtuman kuvaus	Tapahtuman vaikutuksen kuvaus	Riskin todennäköisyys	Riskin vaikutus	Riskin merkitys	Riskiін varautumisen kuvaus	Riskin omistaja	Riski toteutui
1	Projektihenkilöstön siirtyminen muihin tehtäviin	Määräaikaiset työsuhteet hankkeissa ja ohjelma-koordinaatiossa aiheuttavat riskin. Määräaikaiset henkilöt ryhtyvät hakeutumaan uusiin tehtäviin ohjelma-aikana.	Rekrytoinnit ja uusien henkilöiden perehdytys vie aikaa. Menetetään osaamista eikä tieto ja kokemus siirry.	4	5	20	Tiedon ja osaamisen siirto useammalle henkilölle. Päätötoimien valmistelu ja toteutus aloitetaan ajoissa.	N.N.	X
2	Suuri työkuorma	Liian paljon työtä suhteessa resursseihin.	Laatu kärsii ja tuloksia ei saada valmiiksi ajallaan. Aikataulut venyvät.	5	3	15	Tiimin jäsenet ottavat vastuun tekemisen priorisoinnista ja jaksamisen huolehtimisesta	L.L.	

Tässä on kuvattu esimerkki yhdestä tavasta esittää riskirekisteri (lähde: www.vm.fi).

Riskirekisteri voidaan toteuttaa monella tavalla. Jo taulukkolaskentaohjelmalla ylläpidettävä taulukko voi toimia riskirekisterin pohjana. Riskirekisterien ylläpitämiseen on kehitetty monipuolisia ohjelmistoja, joita käydään tarkemmin läpi myöhemmässä moduulissa.

Riskirekisterin rakenteeseen sisältyy vähintään seuraavat osat eli sarakkeet:

1. riskin otsikko
2. riskinä tarkasteltavan tapahtuman kuvaus
3. tapahtuman vaikutuksen kuvaus suhteessa tavoitteisiin
4. värikoodattu riskin merkitys (tässä pohjautuen riskilukuun)
5. toimenpidesuunnitelma riskiin varautumisesta, kuten valittu hallintatoimenpide, riskin omistajan nimeäminen ja ohjeistus siitä, miten ilmoitukset riskihavainnoista tehdään.

Yksittäiset riskit listataan rekisteriin päällekkäin omille riveilleen.

Rekisteriin nimetty riskin omistaja vastaa riskin seurannasta ja hallintatoimenpiteiden toteuttamisesta ja lisäksi esimerkiksi siitä, että riskiin liittyviä hallintatoimenpiteitä kehitetään edelleen.

Riskirekisteriin voidaan lisäksi kirjata poikkeamat odotetusta, toteutuneet läheltä piti -tilanteet, riskitasoon vaikuttavat muutokset sekä muut riskiin liittyvät tapahtumat, kuten tunnistetut uudet uhkat tai avautuvat mahdollisuudet. Myös jokaisen seurattavan riskin huomiorajat voidaan kirjata rekisteriin.

Toiminnan edetessä riskirekisteriin merkitään, toteutuiko riski, missä olosuhteissa se toteutui ja millä vaikutuksilla. Olennaista onkin riskirekisterin jatkuva päivittäminen tilanteiden muuttuessa ja tiedon tarkentuessa.

Riskirekisteri toimii myös riskitiedon viestinnän välineenä yrityksen sisällä ja muille tahoille, joita asia koskettaa.

Riskienkäsittelysuunnitelma

Tehdyn arvioinnin pohjalta kokonaisuudelle laaditaan riskienkäsittelysuunnitelma eli kuvaus, joka sisältää kaikki kirjatut riskit ja niille tehtävät toimenpiteet, vastuiden jakamisen, käsittelyn aikataulut sekä raportoinnin ja seurannan vaatimukset. (JUDO s. 21) Suunnitelma voidaan laatia riskirekisterin pohjalta.

lhanteellisesti riskienkäsittelysuunnitelman laatiminen etenee rinnakkain toiminnan ja sen tavoitteiden suunnittelun kanssa. Suunnitelmaa laadittaessa korostuu se, että riskienhallintaan kuuluu resurssien tasapainottaminen. Kaikki käytössä olevat resurssit tuleekin määritellä osana riskienhallinnan taustatietoja. Riskienhallintaan panostettavat resurssit kuten henkilöstö ja varat ovat pois muista toiminnan käynnistämiseen ja ylläpitämiseen tarvittavista resursseista.



Tapaus: Virheellinen riskirekisteri

Alla on ote riskirekisteristä. Sarakkeet on merkitty A-G. Osaatko sanoa, missä solussa on sattunut virhe riskirekisterissä?

A	B	C	D	E	F	G
Riskin otsikko	Tapahtuman kuvaus	Tapahtuman vaikutuksen kuvaus	Riskin todennäköisyys	Riskin vaikutus	Riskin merkitys	Riskiін varautumisen kuvaus
Kyberhyökkäys yrityksen kriittisiin järjestelmiin	Muuttunut maailmantilanne on lisännyt kyberhyökkäyksiä erityisesti kriittiseen infraan kohdistuen	Toiminnalle keskeistä tietoa menetetään. Menetetään kyky operoida täydellä teholla	3	4	5	Tiedon säännöllinen varmuuskopiointi, tietojärjestelmien tietoturvapäivitykset, henkilöstökoulutus

[Avaa taulukon täysikokoinen versio.](#)

- ◇ A (Riskin otsikko)
- ◇ B (Tapahtuman kuvaus)
- ◇ C (Tapahtuman vaikutuksen kuvaus)
- ◇ D (Riskin todennäköisyys)
- ◇ E (Riskin vaikutus)
- ◇ F (Riskin merkitys)
- ◇ G (Riskin varautumisen kuvaus)

7.1 Riskienhallintaprosessi toiminnan tukena

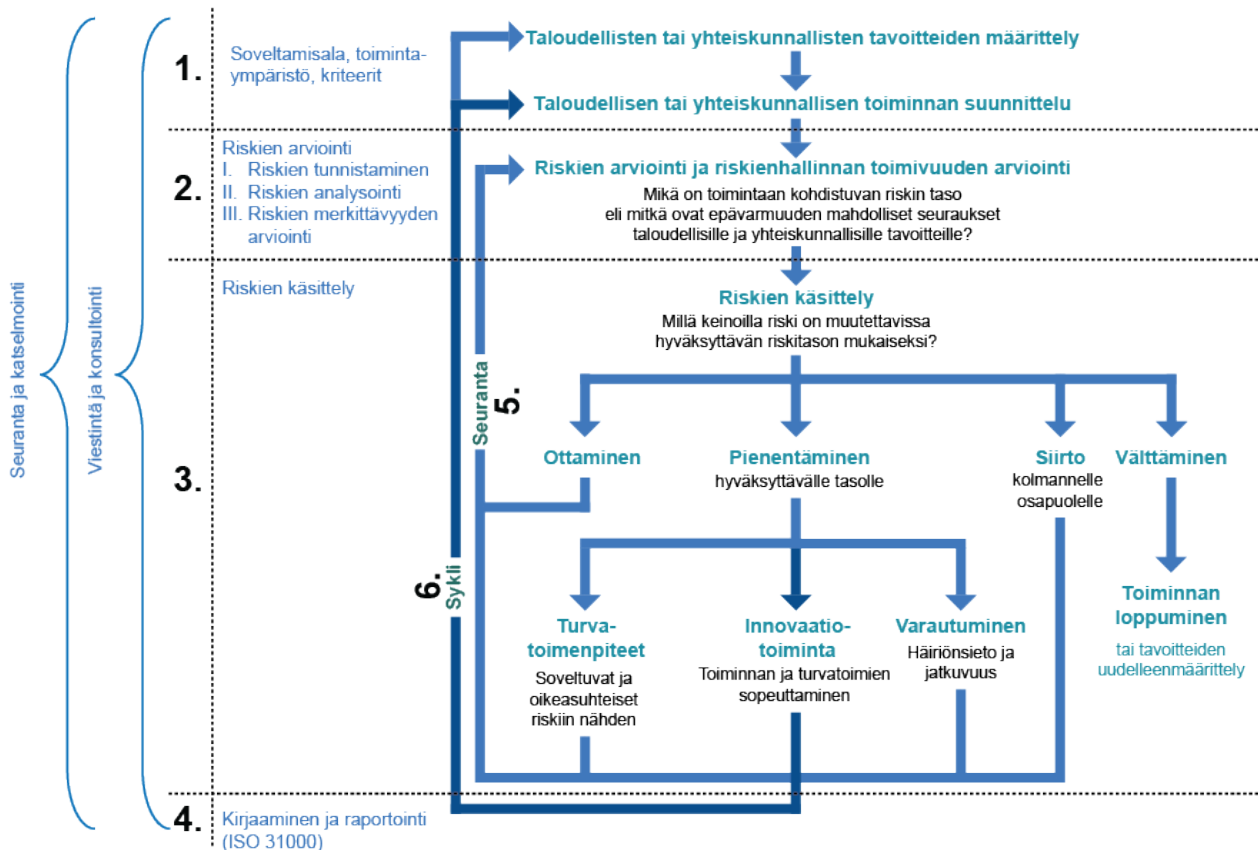
Oppimistavoite: kertaat tähän asti oppimasi riskienhallintaprosessin vaiheet ja miten käytät sitä kokonaisuutena. Tehtävissä kappaleen lopussa arvioit riskienhallintaprosessia oman toimintasi kannalta. Arvioitu ajankäyttö: 12 min.

Riskienhallinta etenee rinnakkain muun toiminnan kanssa ja sillä turvataan asetettujen tavoitteiden saavuttaminen.

Riskienhallinta on monivaiheinen prosessi, jossa jokainen vaihe tuottaa syötettä seuraaville

vaiheille. Vaiheet tulee ajoittaa siten, että ne osuvat oikeisiin jaksoihin toiminnassa. Toiminnan tulisi siis olla siinä vaiheessa, että on kertynyt riittävästi tietoa toimenpiteiden täsmentämiseksi ja ne osataan toteuttaa oikealla hetkellä.

Alla olevassa kaaviossa on esitetty käytäntölähtöinen riskienhallinnan prosessi. Sen keskeiset vaiheet on jo käsitelty. Nyt yhteenvedona tarkastelemme prosessia kokonaisuutena ja sitä, miten riskienhallinta täsmentyy prosessin aikana kertyvän uuden tiedon ja olosuhteiden muutosten myötä. Kaaviossa esitetty **riskienhallinnan kuusivaiheinen prosessiesittely** tarkemmin alla.



[Avaa kaavion täysikokoinen versio.](#) Kaaviossa esitetään riskienhallinnan prosessi pohjautuen OECD:n suositukseen. Kaavion vasemmalle puolelle on merkitty vastaavat riskienhallinnan vaiheet sen mukaan, miten ne on nimetty ISO 31000 -standardissa.

VAIHE 1: Määritellään tavoitteet toiminnalle, johon liittyviä riskejä halutaan hallita. Käynnistettävä toiminta suunnitellaan tavoitteiden pohjalta, ja toimintaan kohdistuvat epävarmuudet otetaan käsittelyyn.

Tavoitteita vasten määritellään joukko taustatietoja tarkasteltavasta toiminnasta, kuten käytössä olevat resurssit, tehtävien väliset kytkökset, aikataulut sekä toimintaan osallistuvien henkilöiden kokemus riskienhallinnasta. Osana taustatietoja voidaan kuvata myös tietoja toimialasta, markkinoista, yleisistä trendeistä jne. Tämä tehdään siinä laajuudessa kuin on olennaisia tavoitteiden ja niihin liittyvien epävarmuuksien määrittelemisen kannalta.

Eryteisesti digitaalisen toimintaympäristön taustatietoja ovat mm. digitaalisten palveluiden

vaatimusten kehitys, esimerkiksi viranomaismääräykset ja laajemmin digitaalisten teknologioiden kehitys omalla toimialalla.

VAIHE 2: Riskien arviointi, joka sisältää kolme vaihetta:

- I. **Riskien tunnistaminen** eri menetelmiä hyödyntäen, esim. SWOT-analyysi.
- II. **Riskianalyysi**, jolla tuotetaan perusta päätöksille siitä, mitkä tunnistetuista riskeistä otetaan käsittelyyn.
- III. **Riskin arviointi** ja priorisointi.

Erityisesti digiriskien arviointiin arvokasta informaatiota on ajankohtainen kyberuhkatieto. Suomen olosuhteista mainio lähde on: <https://www.kyberturvallisuuskeskus.fi/fi/>.

VAIHE 3: Riskien käsittelyssä päätetään, millä toimenpiteillä jokainen riski muutetaan hyväksyttävälle riskitasolle niin, että suunniteltu toiminta voidaan aloittaa tai sitä kannattaa jatkaa. Edellä tehty riskien priorisointi pohjustaa hallintatoimenpiteiden valitsemista. Hallintatoimenpiteitä on neljän periaatteen mukaisia:

- I. Riskin **pienentäminen**
- II. Riskin **siirto**
- III. Riskin **välttäminen**
- IV. Riskin **ottaminen**.

- Vaihtoehtoinen toteutustapa riskien käsittelylle on jakaa toimenpiteet kahteen kategoriaan seuraavasti:
- **1) riskien kontrollointi** (periaatteina riskin pienentäminen, siirto ja välttäminen, kuten edellä);
- **2) riskien rahoitus jakautuen siirtämiseen** (vaihtoehtoina esim. a) vastuista vapautuminen; b) vakuutus sopimukset) **ja riskin omalla vastuulla pitämiseen** (vaihtoehtoina esim. a) suuri omavastuu; b) korvausrahasto; c) captive-yhtiö). (SUOMINEN s. 99) Captive-yhtiöllä tarkoitetaan käytännössä suuren yrityksen omistamaa 'vakuutusyhtiötä', joka vakuuttaa yksinomaan omistajansa riskejä.

Riskinkantokyvyllä viitataan yksilön tai yrityksen kykyyn toimia riskin toteutuessa.

Riskinkantokyvyllä määritetään **rajat, joiden puitteissa yksilö tai organisaatio voi ottaa riskejä toiminnassaan**. Rajat liittyvät resursseihin, kuten rahaan, aikaan ja osaamiseen. Rajoja voidaan tarkastella myös maineen tai hyvinvoinnin näkökulmasta. Harvalla organisaatiolla on käytettävissään niin paljon resursseja, että sen riskinkantokyky olisi täydellinen.

Erityisesti **jäännösriskeistä päätettäessä** on keskeistä määrittää, minkälaisista riskeistä on kysymys. Muutoin riskien yhdistelmät uhkaavat toiminnan mahdollisuuksia tai koko organisaation olemassaoloa. (VAHTI s. 55–56)

VAIHE 4: Riskienhallinta ei toteudu organisaatiossa, mikäli riskienhallinnasta ja sen tuottamasta tiedosta ei olla tietoisia. **Viestintä** ja riskeistä raportointi onkin nähtävä keskeisenä osana riskienhallinnan prosessia sen eri vaiheissa. (VAHTI s. 13)

Asiakkaille ja yhteistyökumppaneille on tärkeää kertoa, miten riskit on otettu haltuun toiminnassa. Läpinäkyvyys on osa toiminnan vastuullisuutta. Esimerkiksi välitön raportointi yritetystä tietomurrosta toimii varoituksena muille alan toimijoille. Läpinäkyvyys mahdollistaa riskienhallintaan kohdistettujen toimenpiteiden arvioinnin organisaation sisällä ja sen sidosryhmille siten, että **tietojen jakaminen ei itsessään tuota merkittäviä riskejä**. (VAHTI s. 37) Julkisesti ei kannata kertoa yksityiskohtaisesti esimerkiksi käytössä olevia tietotietoturvaratkaisuja, ettei niihin aleta etsimään haavoittuvuuksia.

VAIHE 5: Riskienhallintaan kuuluu jatkuva **seuranta ja uudelleenmäärittely**. Tällöin tarkastellaan sitä, miten uhkat ja mahdollisuudet toteutuvat toiminnan edetessä, miten käytössä olevat hallintatoimenpiteet toimivat tai eivät toimi ja miten ne edistävät tai estävät asetettujen tavoitteiden saavuttamista.

Riskien seurantaan liittyy riskiin kohdistuvien muutostekijöiden havainnointi. Niitä ovat riskien riippuvuudet, kerrannaisvaikutukset ja kehittyminen.

VAIHE 6: Olennaista riskienhallinnan prosessissa on **sykli**, jossa palataan jonkin ajan jälkeen takaisin toiminnan suunnitteluun sekä ehkä tavoitteidenkin uudelleentarkasteluun. Tämä tapahtuu muun muassa tähänastisen toiminnan aikana kertyneen tiedon ja mahdollisesti muuttuneiden olosuhteiden valossa. Prosessi jatkuu aiemmin tunnistettujen riskien uudelleenarvioinnilla ja uusien riskien tunnistamisella.

Toiminnan tavoitteita tulee tarkastella uudelleen, mikäli suunnitellulle toiminnalle ei riskianalyysin mukaan saavuteta hyväksyttävää riskitasoa, jonka puitteissa toiminta kannattaisi käynnistää.

Yhteenveto

Teoksessa ”Johda riskejä” ehdotetaan, että lähtökohta hallintakeinoja valittaessa on **ensisijaisesti pienentää negatiivisen riskin toteutumisen todennäköisyyttä omilla toimenpiteillä**. Vasta kun on tehty kaikki mahdollinen omien toimenpiteiden suunnittelun osalta, harkitaan jäljellä olevan riskin siirtämistä. (JOHDA s. 190)

Liian laajasta riskien siirrosta aiheutuvat kustannukset voivat tehdä toiminnasta taloudellisesti kannattamatonta. Erään arvion mukaan liiketoimintaan kytkeytyvistä riskeistä vain noin kolmannes voidaan siirtää vakuuttamalla, jolloin valtaosa eli jopa 65–75 prosenttia riskeistä on luonteeltaan aineettomia ja haastavampia hallita (RAUTANEN).

Jos riskin todennäköisyyden pienentäminen osoittautuu liian kalliiksi saavutettavan hyödyn kannalta, tulee panostaa etukäteissuunnitelmaan mitä tehdään, mikäli riski toteutuu (JOHDA s. 131).

Edes kriittisiksi tunnistettujen riskien täydellinen rajoittaminen ei välttämättä ole optimaalinen tavoite riskienhallinnalle. Teoksessa ”Johda riskejä” esitetään, että tavoitteena tulisi olla tasapainoinen riskienhallinta yrityksen riskikantokyvyn puitteissa (JOHDA s. 131).

Riskienhallintaan kuuluu, että **tietty määrä epävarmuutta jää** edelleen osaksi toimintaa, mutta epävarmuus on **tehty siedettäväksi** käyttöön otetuilla hallintatoimenpiteillä.



Vastaa seuraavaksi, **mikä tai mitkä riskienhallintaprosessin vaiheista on mielestäsi hankalin tai suuritöisin toteuttaa?**

- ◇ Vaihe 1 Toiminnan tavoitteiden määrittely
- ◇ Vaihe 2 Riskien arviointi
- ◇ Vaihe 3 Riskien käsittely
- ◇ Vaihe 4 Viestintä ja raportointi
- ◇ Vaihe 5 Seuranta ja uudelleenmäärittely
- ◇ Vaihe 6 Toiminnan tarkastelu uudelleen tiedon karttuessa / olosuhteiden muuttuessa.



Kerro vielä tarkemmin, **miksi valitsemasi vaiheet ovat mielestäsi hankalia tai suuritöisimpiä digiriskien hallinnassa?**

7.2 Osallistu riskienhallintaan organisaatiossasi

Oppimistavoite: hahmotat, miksi on tärkeää, että riskienhallintaan osallistuvat kaikki yrityksessä ja että riskienhallintakulttuurin rakentuminen on keskeistä. Kappaleen lopussa vastaat avoimeen tehtävään digiriskien hallinnan nykytilanteesta. Arvioitu ajankäyttö: 12 min + lisätehtävä.

”Ainoa vaihtoehto riskienhallinnalle on kriisinhallinta - ja kriisien hallinta on paljon kalliimpaa, aikaakuluttavampaa ja nöyryyttävämpää.” (James Lam, *Enterprise Risk Management*)

Organisaatiossa, kuten yrityksessä, on riskienhallinnan tavoitteena tukea ennakoivaa johtamista. Riskienhallintaan tulee osallistua kaikki organisaation tasot. Riskienhallinta organisaatiossa lähtee koko organisaation tai sen osan tekemisen ja tavoitteiden määrittelystä. Se, mitä tunnistetaan riskiksi tai digiriskiksi, muodostuu organisaation tai sen osan tavoitteiden ja vaatimusten pohjalta. Esimerkiksi tietohallintayksiköllä on lakisääteisen tehtävän kautta määrittäviä vaatimuksia

riskienhallintaan. (VAHTI s. 50)

Toimintaan vaikuttavat riskit ja suunnitelmat niiden käsittelemiseksi muodostavat organisaation riskisalkun. Riskisalkussa riskit esitetään yleensä riskiarvojen suuruusjärjestyksessä. Vastuu riskisalkun sisällöstä tulisi jakaa organisaation osien kesken. Organisaation osien tulisi olla tietoisia riskeistään, niiden jäännösosista sekä riskinkantokyvystään ja näihin vaikuttavista tekijöistä (VAHTI s. 54).

Riskienhallintakulttuurin rakentaminen

Kirjassa ”Johda riskejä” esitetään kolme käytännön vinkkiä riskienhallintakulttuurin vahvistamiseksi organisaatiossa (JOHDA s. 88–89):

1. **Näkyvät artefaktit:** esimerkiksi kulunvalvonta fyysisiin ja digitaalisiin tiloihin.
2. **Ääneen sanotut ja dokumentoidut periaatteet:** esimerkiksi johdon kannanotot organisaation tahtotilasta riskienhallintaan. Kirjatut periaatteet ja ohjeet on oltava kaikkien organisaation jäsenten helposti saatavilla.
3. **Ääneen sanomattomat yksilölliset käsitykset:** kunkin organisaation jäsenen omakohtainen käsitys siitä, miten riskienhallinnassa tulisi toimia, esimerkiksi silloin, kun dokumentoitu ohjeistus ei täsmälleen kuvaa käsillä olevaa tilannetta. Riskienhallinnallinen toimintatapa on usein hyvin käytännönlähteistä ja maalaisjärkistä toimintaa. Organisaation riskienhallintakulttuuri vahvistuu, kun yksilölliset käsitteet saadaan ohjattua linjaan organisaatiolle määritettyjen tavoitteiden kanssa.

Digiriskien hallinta rakentaa laajempaa digiturvallisuutta toiminnassa. Digitaalisessa toimintaympäristössä luodaan turvallisuuden kulttuuria kannustamalla kaikkia toimijoita tuomaan esiin havaitsemiaan epäkohtia siten, että niihin pystytään puuttumaan. Palautteen antaminen on mielekästä, kun nähdään, että siitä seuraa konkreettisia toimenpiteitä. Jo pelkästään viesti siitä, että palaute on huomioitu voi riittää motivoimaan. Riskienhallintakulttuurin rakentuminen alkaa tällaisista pienistä toimista, joilla muokataan organisaation jäsenten asennoitumista. (VAHTI s. 13)

Ihminen tarvitsee muistutuksia mahdollista uhista. Myös organisaatiot, joihin riskienhallinnan kulttuuri on jo vakiintunut, tarvitsevat muistutuksia uusiutumiseen ja jähmettymisen välttämiseen. Uhkat muuttuvat, joten organisaation sisällä tarvitaan ajantasaista viestintää, kuten kannustimia, muistutuksia, perusteluita, päivitettyjä ohjeita ja varoituksia. (VAHTI s. 13)

Riskienhallinnan periaatteet

ISO 31000 -standardissa riskienhallinnan kokonaisvaltainen viitekehys rakentuu kolmesta osasta: periaatteet, puitteet ja prosessi. Näistä jälkimmäinen, eli riskienhallinnan prosessi, onkin jo tullut esiteltyä tässä aineistossa. Sekä prosessi että puitteet rakentuvat periaatteiden pohjalle.

Keskeisiä **periaatteita** digiriskien hallinnan kannalta ovat mm. seuraavat (ISO 31000):

- ytimessä on, että riskienhallinta luo toiminnalle lisäarvoa ja säilyttää sen

- riskienhallinta on olennainen osa kaikkia organisaation prosesseja
- riskienhallinnan lähtökohtana on epävarmuuden huomioiminen toiminnassa
- riskienhallinta on osa päätöksentekoa
- riskienhallinta pohjautuu parhaaseen saatavilla olevaan tietoon
- riskienhallinta toteutetaan organisaation tarpeiden mukaan
- riskienhallinta tukee organisaation jatkuvaa kehittämistä.

Periaatteet ja puitteet määrittävät riskienhallinnan prosessia organisaatiossa. Organisaation asettamat riskienhallinnan periaatteet ovat perustana riskienhallinnan puitteille. **Puitteissa** määritellään riskienhallinnan valtuudet ja sitoutuminen (eli ketkä organisaatiossa ovat vastuussa mistäkin); puitteiden suunnittelu; sekä puitteiden seuranta, katselmointi ja kehittäminen. (ISO 31000)



Riskienhallinnan kokonaisvaltaisuus

Käsitteellä **Enterprise Risk Management (ERM)** korostetaan riskienhallinnan kokonaisvaltaisuutta, jota toteutetaan yrityksen kaikissa toiminnoissa. Riskienhallinnan perustan ja suunnan luovat yrityksen arvot ja strategia. Riskienhallinnan toiminta ja tavoitteet määritellään yrityksen riskienhallintapolitiikassa, periaatteissa ja toimintaohjeissa. Esimerkiksi digiriskien hallinnalle olennainen periaate on, että yrityksessä pyritään aina ottamaan oppia tapahtuneista vahingoista, poikkeamista ja läheltä-piti -tilanteista. (JOHDA s. 46-47)

Kokonaisvaltainen riskienhallinta painottaa seuraavia elementtejä (JOHDA s. 47):

1. **Tunnistetaan tapahtumia**, joilla toteutuessaan on vaikutusta yritykseen:
 - **kielteisesti** eli tapahtumat, jotka toteutuessaan estävät arvon muodostumisen tai heikentävät jo luotua arvoa;
 - **myönteisesti** eli tapahtumat, jotka toteutuessaan kumoavat kielteisiä vaikutuksia tai mahdollistavat edistää tavoitteiden saavuttamista.
2. Mahdollisuudet kanavoidaan tavoitteenasetteluun. Laaditaan suunnitelmat mahdollisiin tilaisuuksiin tарттumisesta (nk. **strategiakytkestä**).

3. Riskienhallintaan osallistuu yrityksen koko organisaatio (nk. **organisatorinen kokonaisvaltaisuus**).
4. Riskienhallinta kattaa sekä negatiiviset että positiiviset epävarmuudet, jotka vaikuttavat yrityksen toiminnan tavoitteisiin (nk. **substanssin kokonaisvaltaisuus**).

COSO ERM on yrityksen sisäisen valvonnan lähtökohdista ja sisäisen valvonnan riskienhallinnan tarpeisiin laadittu, erityisesti yrityksissä käytössä oleva riskienhallinnan malli.

ERM on laaja kokonaisuus, johon voit perehtyä lisää omien tarpeidesi pohjalta. Lue lisää: [COSO ERM yhteenveto](#) (lisätehtävä: 10 min)

Riskienhallinta yhteistyökumppaneiden kanssa

Yrityksen riskienhallinnan tulee kattaa myös yhteistyökumppaneiden, kuten alihankkijoiden, toiminnan kautta koko toimitusketjun. Toimitusketjun kartoituksen välineenä toimivat visuaaliset kartat, joilla tuodaan esille toimitusketjun rakenne, toimijoiden väliset riippuvuudet sekä vastuunvaihdot, jotka saattavat sisältää riskejä. Kartoitusta varten tehtävän tiedonkeruun menetelmiä ovat toimitusketjun osien arviointikyselyt tai vierailut kumppaneiden toimipisteisiin. Paikan päällä selvitetään ovatko alihankkijan alihankkijalla riskienhallinnan asiat oikeasti kunnossa vai onko osa riskeistä haluttu haudata.

Yhteistyö on olennaista riskienhallinnassa digitaalisessa toimintaympäristössä, jossa koko kentän hahmottaminen omatoimisesti on vaikeaa. Paitsi asiakkaiden ja yhteistyökumppaneiden myös kilpailijoiden kesken on varauduttava tiedonvaihtoon, sillä digiympäristön uhkat voivat levitä nopeasti haittamaan koko toimialaa. (VAHTI s. 38)

Vastuun jakaminen

Riskienkäsittelysuunnitelma on siis keskeinen väline riskienhallinnan jalkauttamiseen yrityksen organisaatiossa. Kaikkien organisaatioiden jäsenten ei kuitenkaan kuulu olla vastuussa kaikista riskienhallintaan liittyvistä toimenpiteistä.

Riskienkäsittelysuunnitelmassa vastuuhenkilöiden nimeämiseen voidaan käyttää **RACI-mallia** seuraavasti:

Responsible = Vastuullinen: kuka suorittaa päätetyn toimenpiteen riskin hallintaan.

Accountable = Vastuussa: kuka tekee päätöksen toimenpiteestä ja valvoo että tehtävä suoritetaan.

Consulted = Konsultoitava: kenen kanssa neuvotellaan päätöksestä, esimerkiksi pyydetään ohjeita.

Informed = Tiedotettava: keille tiedotetaan päätöksestä tai tehtävän suorittamisesta.



Kerro alla omin sanoin, mitkä asiat ovat mielestäsi tällä hetkellä yrityksiin liittyvän digitaalisen riskienhallinnan suurimpia ongelmakohtia?

Pohdi samalla, mitkä asiat puolestaan ovat näkemyksesi mukaan hyvin hoidettuja asioita digitaaliseen riskienhallintaan liittyen?

8.1 Uhkan kääntäminen mahdollisuudeksi

Oppimistavoite: Tässä kappaleessa opit keinoja, joilla voit kääntää riskissä olevan uhan mahdollisuudeksi, kuten uudeksi liiketoiminnaksi. Kappaleen lopussa vastaat tehtävään nelikenttäajattelusta mahdollisuuksien tunnistamisen. Arvioitu ajankäyttö: 15 min + lisätehtävä.

Epävarmuus voi siis olla toiminnalle paitsi uhka, myös mahdollisuus.

Yksi lähestymistapa riskienhallintaan onkin **pyrkimys muuttaa uhkia mahdollisuuksiksi ja vaikutuksiltaan positiivisiksi lopputuloksiksi**. Tällä lähestymistavalla, eli riskienhallintaprosessin yhtenä periaatteena olevalla **innovaatiotoiminnalla**, voidaan kehittää uutta toimintaa tai sopeuttaa käynnissä olevia aktiviteetteja. (VAHTI s. 60; OECD s. 54–55)

Arvokas kysymys kuuluukin, miten uhka käännetään mahdollisuudeksi? Kärjistetysti voidaan esittää, että yhden toimijan uhka on mahdollisuus toiselle toimijalle: ratkaisua, jolla omassa toiminnassa torjutaan jokin uhka, voidaan tarjota toisille toimijoille.

Tarkastellaan lopuksi riskienhallintaprosessien vaiheiden kautta uhkan kääntämistä mahdollisuudeksi.

1. Pohjustus tavoitteiden määrittelyssä

Uhkan kääntämistä mahdollisuudeksi pohjustetaan selvittämällä tavoitteiden määrittelyn yhteydessä, missä rajoissa tavoitteita tai toimintaa on valmiuksia muuttaa. Jatkuva poukkoilu tavoitteiden kanssa ei ole kannattavaa. Mahdollisesti kannattaa asettaa muutama kiinteä tavoite ja muutama joustava tavoite, jotka tukevat kiinteitä tavoitteita. Palaa siis kappaleen 4 yhteydessä laatimaasi taulukkoon tavoitteidesi määrittelyistä.

2. Mahdollisuuksien tunnistaminen SWOT-analyysillä

Kappaleessa 5.1 esitellyn SWOT-analyysin nelikentän pohjalta tarkastellaan toimintaan liittyviä negatiivisia seikkoja, joita ovat sisäiset heikkoudet ja ulkoiset uhkat, sekä positiivisia seikkoja, joita ovat sisäiset vahvuudet ja ulkoiset mahdollisuudet.

Sisäiset asiat S = Vahvuudet - Mitkä tapahtumat heikentävät vahvuuksia toiminnassa? + Mitkä tapahtumat luovat edellytyksiä vahvuuksien hyödyntämiselle toiminnassa?	Ulkoiset asiat O = Mahdollisuudet - Mitkä tapahtumat heikentävät mahdollisuuksien hyödyntämistä toiminnassa? + Mitkä tapahtumat vahvistavat toiminnan mahdollisuuksia?
Tarkasteltava toiminta ja tavoitteet	
W = Heikkoudet - Mitkä tapahtumat lisäävät heikkouksia? + Mitkä tapahtumat lieventävät heikkouksia?	T = Uhkat - Mitkä tapahtumat vahvistavat uhkien vaikutusta toimintaan? + Mitkä tapahtumat lieventävät uhkien vaikutusta toimintaan?

[Avaa taulukon täysikokoinen versio.](#)

Etsitään toimia, joilla kääntää SWOT-analyysillä tunnistetut negatiiviset seikat, kuten tapahtumat, positiivisiksi omassa toiminnassa. Toisin sanoen tarkastellaan SWOT-nelikentässä miinusmerkkisiä kysymyksiä:

- Mitkä tapahtumat heikentävät vahvuuksia toiminnassa?
- Mitkä tapahtumat lisäävät heikkouksia?
- Mitkä tapahtumat heikentävät mahdollisuuksien hyödyntämistä toiminnassa?
- Mitkä tapahtumat vahvistavat uhkien vaikutusta toimintaan?

Näillä kysymyksillä lähestyttävillä riskienhallintakeinoilla, varsinkin **ennakoivilla, riskien laajentumista estävillä tai lieventävillä toimenpiteillä**, voidaan muodostaa tunnistettuihin tapahtumiin ydinajatus. Sen avulla uhkat käännetään mahdollisuuksiksi omassa toiminnassa.

Riskienhallintakeinojen mahdollistajat etsitään nelikenttään kirjatusta positiivisista seikoista.

Esimerkki 1: vähäriskiseksi suunnittelu

Digitaalisessa toimintaympäristössä uutta liiketoimintaa avaa **vähäriskiseksi suunnittelu**. Tällä tarkoitetaan prosessia, jossa tuotteelle, palvelulle tai prosessille suunnitellaan toteutustapa, jossa tietyt sille ominaiset riskit on otettu luotettavasti haltuun.

Vähäriskisessä suunnittelussa huomioidaan asiakkaalle negatiiviset riskit, kuten tietosuojariskit (tavoitteena *privacy by design*) tai turvallisuusriskit (tavoitteena *safety by design* tai *security by design*). Tuotteen vähäriskiseksi suunniteltu toiminnallisuus nostetaan esiin kilpailuetuna. (VAHTI s. 61)

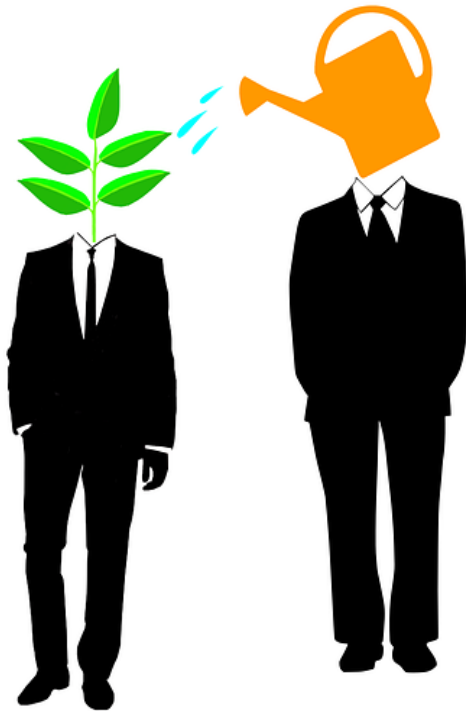
Esimerkki 2: riskilähtöinen innovointi

Riskilähtöinen innovointi tarkoittaa, että tuotetta tarjoava yritys ottaa vastuulleen osan niistä kielteisistä riskeistä, jotka kohdistuvat asiakkaaseen tuotteen käytön aikana. Riskien siirtäminen pois asiakkaalta huomioidaan tuotteen hinnassa. Asiakas maksaa yritykselle tuotteen käytöstä ("pay for performance") ehkä enemmän kuin kilpailijoille, kun tuote toimii sovitun laisesti. Jos jokin riski toteutuu ja tuotteen suorituskyky heikkenee, maksaakin asiakas vähemmän. Asiakas ei omista tuotetta. Riskilähtöinen innovointi mahdollistaa liiketoimintamallien uudistamisen silloin, kun tuotteen käyttöön liittyville riskeille voidaan määritellä hinta esimerkiksi suorituskykyyn perustuen. Riskilähtöinen innovointi voi olla erottuva kilpailutekijä tai sillä voidaan edistää uuden teknologian myyntiä, kun asiakkaan ei tarvitse kantaa kaikkia riskejä teknologian soveltuvuuden selvittämisessä. (GIROTRA 2011)

Esimerkiksi riskilähtöisestä innovoinnista voidaan nostaa yritys Netafim, joka on kehittänyt uudenlaisen kastelujärjestelmän viljelmille. Aluksi järjestelmät eivät kuitenkaan menneet kaupaksi, sillä viljelijät suhtautuivat skeptisesti kastelujärjestelmän väitettyihin hyötyihin, kuten satojen parantumiseen. Järjestelmän soveltuvuuteen omaan käyttöön liittyi epävarmuuksia (engl. "information risk"), jotka aiheuttivat viljelijöille korkean kynnyksen kastelujärjestelmän hankkimiseen.

Tilanne muuttui, kun Netafim vaihtoi liiketoimintamallia ja alkoi myydä viljelijöille kastelukaluston sijaan palvelua viljelyn tehostamiseksi. **Uusi liiketoimintamalli** siis oli, että **viljelijät maksoivat kastelujärjestelmän käytöstä toteutuneiden satojen perusteella** (eli periaatteella "pay for performance"). (GIROTRA 2014)

Uusi liiketoimintamalli ratkaisi sen haasteen, ettei viljelijöillä ei ollut aiempaa tietoa teknologian suorituskyvystä heidän viljelmillään, mikä puolestaan johti epävarmuuteen ja haluttomuuteen investoida uuteen järjestelmään. Uudella liiketoimintamallilla **Netafim siirsi vastuulleen riskiä** siitä, ettei kastelujärjestelmän suorituskyky olisikaan vastannut asiakkaan odotuksia. (GIROTRA 2014)



Netafinin asiantuntemus viljelyn riskeistä ja kyky optimoida erikseen jokaiselle asiakkaalleen kastelujärjestelmä parhaimpaan suorituskyykyyn mahdollisti uuden liiketoimintamallin toteuttamisen. Tämän vuoksi yritys katsoi voivansa tarjota asiakkailleen suojaa uuden teknologian käyttöön liittyviltä riskeiltä uudella, taloudellisesti kannattavalla liiketoimintamallilla.

Tällä liiketoimintamallilla Netafim **hajautti tuotteen suorituskyykyyn liittyvän riskin** useiden asiakkaiden kesken. Jos jonkin asiakkaan sadon laatu heikkeni, yritys ei välttämättä laskuttanut asiakasta ollenkaan satokautena. Tämä antoi yritykselle dataa heikon sadon syistä, jolloin kastelujärjestelmää voitiin parantaa antamaan jatkossa parhaan suorituskyykyyn asiakkaalle. Sadon epäonnistuminen on riski, ja sen seuraamukset jaetaan konkreettisesti asiakkaan kanssa (engl. "incentive-alignment risk").

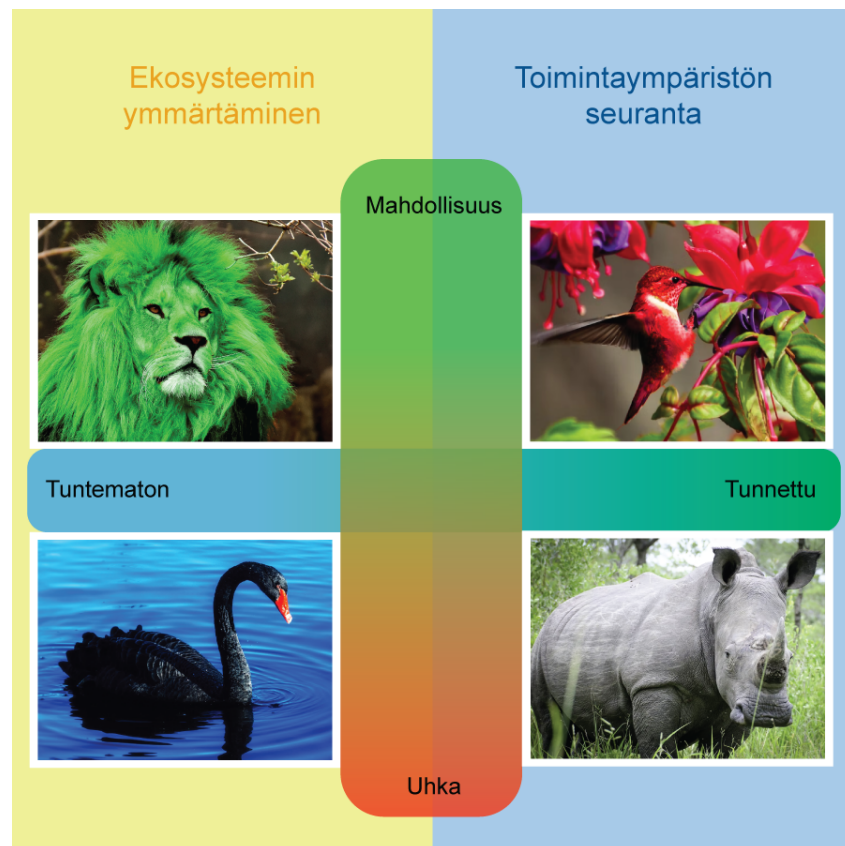
Liiketoimintamallin uudistaminen riskilähtöisellä innovoinnilla käynnistyy tunnistamalla yrityksen omat riskit ja asiakkaiden riskit nykyisessä tuotteessa ja liiketoimintamallissa. Riskit voivat liittyä esimerkiksi puutteelliseen tietoon tuotteesta tai asiakkaan mielestä itselleen kohdistuvasta kohtuuttomasta riskistä tuotteen käyttöönottamisesta. Uudessa liiketoimintamallissa huomioidaan, millä ehdoilla asiakkaalle kohdistuvat riskit voidaan kannattavalla tavalla siirtää yrityksen vastuulle, jotta hankinta ei esty. Netafinin tapauksessa, yritys onnistui laajentamaan markkinaosuuttaan.

Uuden liiketoimintamallin kehittäminen riskilähtöisellä innovoinnilla edellyttää tuotteen pilotointia muutaman asiakkaan kanssa sopivan hinnoittelun ja sopimusehtojen tunnistamiseksi, sekä riskin jakamista korostavan markkinointistrategian laatimiseksi. (GIROTRA 2014)

3. Nelikenttäajattelu mahdollisuuksien tunnistamiseen

Kun riski käsitteellistetään tapahtumaksi, joka voi olla tunnettu tai tuntematon, sekä uhka tai mahdollisuus, voidaan muodostaa alla kuvattu nelikenttä.

Nelikentän ulottuvuuksien kuvaamiseen on esityksissä käytetty eläinmetaforia. Toisin sanoen, eläimeen liitetyillä ominaisuuksilla kuvataan riskin ominaisuuksia. Tämä havainnollistava yhteenveto pohjautuu konsultointiyritys Arterin asiantuntijan esitykseen. Vastaavia ja määrittelyiltään erilaisiakin eläinmetaforia on kuvattu muissa riskienhallinnan esityksissä.



[Avaa kuvan täysikokoinen versio.](#)

Kuvattuun nelikenttään on mahdollisuuksien tunnistamiseksi liitetty **ulottuvuus ekosysteemi-toimintaympäristö** siten, että **tuntemattomat mahdollisuudet** löytyvät ekosysteemin ymmärtämisestä ja **tunnetut mahdollisuudet** nousevat (liike)toimintaympäristön jatkuvasta seurannasta. (ARTER)

Mietitään seuraavassa eläimiin liitettyjä ominaisuuksia ja niiden kautta riskin ulottuvuuksia sekä sitä, miten uhka voidaan kääntää mahdollisuudeksi.

Musta joutsen edustaa tuntematonta uhkaa. Sillä viitataan kielteiseen tapahtumaan, jota ei pystytä ennakoimaan. Sillä on toteutuessaan suuri vaikutus, ja jälkikäteen tarkasteltuna se näyttäytyy ilmeiseltä uhkalta. Mustan joutsenen käsite pohjautuu Nassim Talebin teokseen. Esimerkkejä toteutuneista musta joutsen -ilmiöistä ovat finanssikriisit vuosina 1987 ja 2008. Covid-19 voidaan myös käsittää musta joutsen -tapahtumaksi, sillä vaikka riski globaalille viruspandemialle on ollut tunnistettu uhka, olivat Covid-19-pandemian globaalit vaikutukset paljon

odotettua laajemmat.

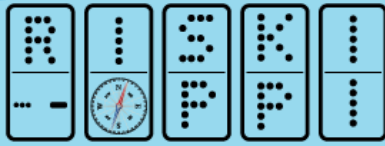
Harmaa sarvikuono edustaa nelikentässä tunnettua uhkaa, joka on toteutuessaan merkittävä, mutta jonka ennakoimiseksi tai lieventämiseksi ei tehdä riittäviä toimenpiteitä. Se pohjautuu Michele Wuckerin esitykseen. Harmaa sarvikuono on tapahtuma, joka toteutuessaan pahimmassa tapauksessa jyrää oman toiminnan alleen, ellei tämän riskin ennakoimiseen tai lieventämiseen tehdä toimenpiteitä. Tunnettu uhka pelätään ottaa käsittelyyn, edes puheenaiheeksi, tai sen hallinnan kustannuksia ei haluta ajatella. Harmaat sarvikuonot voivat olla sekä sisäisiä että ulkoisia uhkia. Sisäinen digiriski, joka tunnistetaan harmaaksi sarvikuonoksi, on esimerkiksi tilanne, jossa jättäydytään yhden järjestelmätoimittajan varaan, luottaen järjestelmän toiminnan jatkumiseen häiriöttä. Luonnonkatastrofien toteutumiseen ulkoisina riskeinä ei voida vaikuttaa omalla toiminnalla, mutta riskienhallinnalla voidaan pyrkiä lieventämään katastrofin vaikutusta omiin tavoitteisiin. Voidaan myös esittää, että Covid-19 olikin harmaa sarvikuono -ilmiö. Vaikka uhka globaalista viruspandemiasta on ollut tunnettu, niin Covid-19 -tapauksessa ei oltu tehty riittäviä toimenpiteitä viruksen leviämisen ennakoimiseksi, ja tämän myötä maailmanlaajuisen poikkeustilan lieventämiseksi.

Punainen kolibri edustaa tunnettua mahdollisuutta, joka voi olla merkittävä. Mahdollisuus ei kuitenkaan edellytä varautumista tai siihen on vaikea tarttua uuden liiketoiminnan luomiseksi. Tällaisten mahdollisuuksien tunnistaminen edellyttää toimintaympäristön perusteellista seurantaa ja tiedon keräämistä ympäristön ilmiöistä. Esimerkkejä toteutuneista punainen kolibri -ilmiöistä ovat siirtymä perusmobiilipuhelimista älypuhelmiin ja itsepalvelukassojen tuominen myymälöihin.

Vihreä leijona edustaa tuntematonta mahdollisuutta. Eläinmaailmassa ei nykytiedon mukaan tunneta vihreänväristä leijonaa. Se on mm. alkemiasta tuttu metafora, joka symboloi alkemian prosessien lopputulosta eli kultaa. Esimerkkejä vihreästä leijonasta ovat Internetin leviäminen kaiken kansan käyttöön 1990-luvulla sekä netin mahdollistamat jakamistalouden palvelut, kuten Airbnb ja Uber. Vihreiden leijonien kaltaisten liiketoimintamahdollisuuksien tunnistaminen edellyttää ymmärrystä siitä laajemmasta ekosysteemistä, jossa toimitaan. Käsitys siitä, miten asiakkaat käyttävät tuotteita, täsmentää näkemystä mahdollisuuksista ja uhkista ekosysteemissä. Mahdollisuudet nousevat siitä, että tilaus- ja toimitusketjut ymmärretään alusta loppuun, sekä käsitetään ketjujen kokonaisvaikutukset taloudellisesti, ympäristönäkökulmasta sekä turvallisuus- ja vastuullisuusnäkökulmasta. (ARTER)

Lisätehtävä: tulevaisuusajattelun kehittäminen

Tulevaisuusajattelun kehittäminen vahvistaa riskienhallinnan taitoja. Sitran julkaisema **Tulevaisuuden tekijän työkalupakki** tarjoaa välineitä, joilla kehittää kykyä kartoittaa erilaisia mahdollisia tulevaisuuksia. Perehdy aiheeseen tarkemmin [täällä](#). **Megatrendit 2023** eli visio tulevaisuuteen vaikuttavista kehityskuluista on koottuna [tällä sivulla](#).

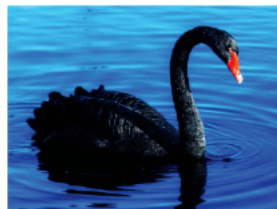


TEHTÄVÄ!

Yhdistä eläinmetafora siihen liitetyn riskin ominaisuuksia osuvammin kuvaavaan määritelmään.



Kuvaa mahdollisuutta "loihdia", oikealla toiminnalla, jotain arvokasta epävarmuudesta.



Sen olemassaolo kiistettiin uskomuksen tai paremman tiedon puutteessa.



On nopea liikkeissään ja täten kuvaa mahdollisuutta, joka on vaikea saada kiinni.



Tunnettu, sekä tietyissä olosuhteissa, todellinen uhka olemassaololle.

Lähteet ja palautekysely

Lähteet



Lähdeluettelo on koottu [tälle sivulle](#).

Palautekysely



Lopuksi pyydämme, että vastaat palautekyselyn kolmeen kysymykseen:



Kysymys 1. Moduulin alussa kysyimme, mitä oppimistavoitteita sinulla on. Kuinka hyvin pääsit moduuli 1:n aikana näihin tavoitteisiisi?



Kysymys 2. Miten moduulin aineisto lisäsi osaamistasi riskien hallintaan?



Kysymys 3. Mitä aiheista liittyen digiriskien hallintaan haluaisit oppia lisää? Vai koetko jo saaneesi tarvittavat tiedot? Entä haluatko antaa muuta palautetta Kompassi-hankeryhmälle?

Halutessasi voit palata tämän aineiston pariin myös myöhemmin. Jos haluat edelleen laajentaa osaamistasi, perehdy Riskioppi-ympäristön [Moduuleihin 2&3](#)!