UNIVERSITY OF EASTERN FINLAND

Riskienhallinta

Tieto-/tietosuojariskejä ja niiden hallintaa

Koottu JUHTA/VAHTI –osoitusvelvollisuuden työpajamateriaalista

Mitä on riskienhallinta ja mikä on riski?

VAHTI 2/2017 ohje riskienhallintaan lainaus

Riskienhallinta on toiminto, jolla johdetaan ja ohjataan organisaation riskejä.

Riskienhallintapolitiikka sisältää organisaation päättämät, kuvaamat ja dokumentoimat riskienhallintaan liittyvät periaatteet ja tavoitteet.

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

Staattinen riski

- Riski kohdistuu **omaisuuteen**
- Omaisuudella on ominaisuuksia, jotka asettavat omaisuuden riskeille alttiiksi (haavoittuvuus)
- Omaisuus tai osa siitä voidaan menettää
- Omaisuuden suojaaminen voidaan optimoida riskien mukaisesti
- **Tieto on omaisuutta,** jonka arvoa ei usein ymmärretä

Dynaaminen riski

- Riski kohdistuu **tavoitteeseen**
- Tavoitteen saavuttamisen toteutuksessa voi tapahtua odottamattomia asioita
- Vaikutus voi olla pysyvä tai tilapäinen
- Suunnitelmaa voidaan parantaa etukäteen riskien perusteella
- **Tietojen käsittely, hallinta ja kehittäminen ovat (dynaamisia) tavoitteita**

Tietoriski

- **Riski kohdistuu tietoon tai tiedon olomuotoon kuten esim. paperiarkistoon tai tietojärjestelmään, jolla käsitellään tietoa**
- Tietoon ei ehkä pääse tai sen käsittely voi olla vaikeaa/hidasta. Tieto voi vuotaa tai se voidaan menettää. Tieto voi olla virheellistä tai ei ehkä jalostu toiminnan mukaan riittävän ketterästi.
- Paperiarkistoon ei ehkä pääse katsomaan tietoa. Se voi tuhoutua tulipalossa. Arkistoon voidaan jättää laittamatta tietoa tai laittaa väärää tietoa. Se voi mennä sekaisin eikä tietoa löydy.
- Tietojärjestelmä voi lakata toimimasta tai siihen ei pääse kirjautumaan. Tietojärjestelmä voi olla monimutkainen, vaikeasti käytettävä tai kankea. Tietojärjestelmä voi tuottaa virheellisiä tuloksia. Luottamuksellinen tieto voi vuotaa asiaankuulumattomille.
- Organisaation (digitaalinen) omaisuus ja tavoitteissa onnistuminen ovat riippuvaisia tiedosta ja tietojärjestelmistä.
- Tiedon varmentaminen ja suojaaminen voidaan optimoida riskien perusteella

Tietosuojariskien arviointi pohjautuu rekisterinpitäjän käsitykseen henkilötietojen käsittelystä

Tietoriskien tyypit

Riskityyppi	Tieto	Tietojärjestelmä
Pääsy (Access)	Tietoon pääsy on hankalaa tai hidasta. Tietoon ei pääse ollenkaan.	Tietojärjestelmään pääsy on hankalaa tai hidasta. Tietojärjestelmään ei pääse.
	Tieto vuotaa sivullisille.	Asiattomat pääsevät tietojärjestelmään.
Tarkkuus (Accuracy)	Tieto ei ole käyttökelpoista, koska se on virheellistä, puutteellista tai hävinnyt.	Tietojärjestelmä tuottaa virheellisiä tuloksia tai hävittää tiedon. Tieto tuhoutuu järjestelmässä.
Ketteryys (Agility)	Tieto ei jalostu. Tietoa ei pysty käyttämään kehitystarpeen mukaisesti.	Tietojärjestelmä ei kehity toiminnan kehityksen tahdissa.
Jatkuvuus (Availability)	Tieto ei ole käytettävissä.	Verkko ja/tai tietojärjestelmät eivät toimi.

Tietosuojariskit

Tietosuojariskit rekisteröidylle (=rekisteröidyn oikeudet tai vapaudet vaarantuvat tietoriskien vuoksi)

- Henkilötieto ei ole saatavilla organisaation virkamiehelle, henkilötiedon käsittelijälle ja/tai rekisteröidylle (asiakas, kansalainen, kumppani, työntekijä)
- Henkilötieto vuotaa organisaation sisällä tai ulkopuolelle sivullisille
- Henkilötieto on virheellinen, vanhentunut, puutteellinen tai hävinnyt
- Mihinkään henkilötietoon ei pääse laajan tietojärjestelmähäiriön vuoksi

Tietosuojatoiminnan riskit (=rekisteröidyn oikeudet tai vapaudet vaarantuvat tietosuojakyvykkyyden puutteen tai heikkouden vuoksi)

- Henkilötiedon käsittely ilman laissa määriteltyä perustetta (ml. asiakkaan suostumus)
- Henkilötietojen käsittely muussa kuin alkuperäisessä, määritellyssä käyttötarkoituksessa
- Rekisteröidyn oikeuksia ei pystytä toteuttamaan (esim. tietojen käsittelyn rajoittaminen)
- Henkilötietojen käsittely ei ole hallittua (esim. organisaation tai toimittajan toiminta on puutteellista tai virheellistä – ohjeistuksen, seurannan tai toimittajahallinnan/sopimuksien puutteet)

Tietosuojariskejä

Tietoriski	Operatiivinen vaikutus yksikön toiminnalle	Vaikutus koko organisaatiolle	Tietosuojariski rekisteröidylle	Vaikutuksia rekisteröidylle
Henkilötieto ei ole saatavilla virkamiehelle, henkilötiedon käsittelijälle ja/tai rekisteröidylle (asiakas, työntekijä)	Valmistelu ja päätöksenteko viivästyy, määräajan ylitys, työajan hukkaaminen	Tuottavuuden lasku, maineen menetys, korjauskustannukset, oikeudenmenetykset, korvausvastuut ja sakot	Pääsy omiin tietoihin estyy, viivästynyt päätös tai toiminta, oikeuksien ja/tai vapauksien menetys	Potilaan hoitotoimenpiteiden viivästyminen, velkajärjestelyn viivästyminen ja taloudelliset menetykset
Henkilötieto vuotaa sisällä tai ulkopuolelle	Ilmoitusvelvollisuus valvontaviranomaiselle ja rekisteröidyille	Maineen menetys, korjauskustannukset, korvausvastuut ja sakot	Salassa pidettävien henkilötietojen luottamuksellisuuden menetys, syrjintä, vapauksien ja/tai oikeuksien menetys	Henkilön arkaluontoiset talous- tai terveystiedot tulevat yleiseen tietoon
Henkilötieto on virheellinen, vanhentunut, puutteellinen, hävinnyt tai tuhoutunut	Virheellinen päätös (jos ei huomata) tai toiminta, käsittelyä rajoitettava (jos huomataan) ja määräajan ylitys	Maineen menetys, korjauskustannukset, korvausvastuut ja sakot	Virheellinen tai viivästynyt päätös tai toiminta, oikeuksien ja/tai vapauksien menetys	Opiskelijan koulutuspaikka jää saamatta virheellisten todistusmerkintöjen vuoksi tai oppilas jätetään vaaralliseen paikkaan
Mihinkään henkilötietoon ei pääse (laaja verkko tai tietojärjestelmähäiriö)	Päätöksenteko viivästyy, määräajan ylitys, työajan hukkaaminen ja henkilöstön turhautuminen	Tuottavuuden lasku, maineen menetys, korjauskustannukset, korvausvastuut ja sakot	Pääsy omiin tietoihin estyy, viivästynyt päätös tai toiminta, oikeuksien ja/tai vapauksien menetys	Henkilöstön palkanmaksun viivästyminen

Tietoriskien vaikutuksia

Vaikutusalue	Pääsy		Tarkkuus	Ketteryys	Jatkuvuus
	Ei pääse	Vuotaa			
Toimintaan	Toiminto, palvelu tai prosessi pysähtyy ja ihmiset turhautuvat, koska ihmiset eivät voi tehdä töitään, koska eivät pääse tietoon tai tietojärjestelmään.	Ylimääräistä kiireellistä työtä ja sanktioita, jos tieto vuotaa sivullisille.	Toimintapäätökset, toiminto, palvelu tai prosessi tuottaa vääriä tuloksia, koska ei ole tietoa tai ihmisten toiminta perustuu puutteelliseen tai virheelliseen tietoon tai virheellisesti toimivaan järjestelmään.	Toiminto, palvelu tai prosessi ei saavuta kehitystavoitteita eikä kehity, koska tieto ei jalostu tai tietojärjestelmä ei kehity toiminnan tarpeiden mukaisesti.	Toiminto, palvelu tai prosessi pysähtyy ja ihmiset turhautuvat, koska ihmiset eivät voi tehdä töitään, koska tietojärjestelmät eivät toimi.
Asiakkaalle	• Huonoa tai hidasta palvelua. • Turhautumista ja ylimääräistä vaivaa asian edistämiseksi. • Taloudellisia menetyksiä. • Tilapäinen/pysyvä terveyshaitta tai hengen menetys.	• Luonnollisen henkilön oikeuksien ja vapauksien menetys. • Turhautumista ja ylimääräistä vaivaa asian korjaamiseksi. • Taloudellisia menetyksiä.	• Virheellinen päätös asiassa virheellisen palvelun johdosta. • Luonnollisen henkilön oikeuksien ja vapauksien menetys. • Turhautumista ja ylimääräistä vaivaa asian korjaamiseksi. • Taloudellisia menetyksiä. • Tilapäinen/pysyvä terveyshaitta tai hengen menetys.	• Huonoa palvelua. • Turhautumista ja ylimääräistä vaivaa.	• Huonoa tai hidasta palvelua. • Turhautumista ja ylimääräistä vaivaa asian edistämiseksi. • Taloudellisia menetyksiä. • Tilapäinen/pysyvä terveyshaitta tai hengen menetys.
Organisaatiolle	Lain mukaisten velvollisuuksien laiminlyönti tai virkavirhe	• Lain noudattamatta jättämisestä sanktioita • Valvontaviranomaisen tarkkailun alaiseksi.	Virkavirhe väärästä päätöksestä	• Organisaatio ei saavuta strategisia ja jatkuvan kehittämisen tavoitteita. • Tuottavuuden kasvutavoitteiden menetys	Lain mukaisten velvollisuuksien laiminlyönti tai virkavirhe
	• Tuottavuuden hävikkiä työpanoksen menettämisestä sekä ylimääräisiä kustannuksia kiireellisestä korjaamisesta. • Negatiivista julkisuutta, maineen menetystä ja asukaspakoa. • Valituksia, oikeustapauksia ja korvauksia.				

Esimerkkejä riskien todennäkyysluokista

Luokka	No	VAHTI ohje	Esimerkkejä	
			Historiatieto tarkasteluvälillä	Olemassa olevan kontrollin tehokkuus
Lähes varma	4	Tapahtuma toteutuu tai on toteutunut usein ja on tapahtunut useita ”läheltä piti”-tilanteita.	Tilastojen mukaan riskitapahtuma on toistunut useaan kertaan tiheämmin kuin tarkasteluvälillä.	Heikko tai olematon kontrolli.
Todennäköinen	3	Tapahtuman tiedetään tai odotetaan toteutuvan mitä suurimmalla todennäköisyydellä.	Riskitapahtuma on toteutunut monissa aikaisemmissa kausissa.	Kontrollia hallitaan mutta se on vain osittain tehoava.
Mahdollinen	2	Tapahtuma saattaa toteutua joissakin olosuhteissa tai tapauksissa. Tapahtuma on toteutunut joskus omassa organisaatiossa tai muualla.	Riskitapahtumasta on olemassa aikaisempi historiatieto.	Kattavaa kontrollia arvioidaan ja tehokkuutta testataan.
Epätodennäköinen	1	Tapahtuma toteutuu vain poikkeuksellisissa oloissa. Mahdollisuus toteutumiseen on tällöin enimmäkseen teoreettinen. Esimerkiksi silloin, kun riskin ei tiedetä aikaisemmin toteutuneen.	Riskitapahtumasta ei ole historiatietoa.	Kontrolli on optimoitu sekä jatkuvassa kehityksessä ja/tai systemaattisessa tehokkuuden arvioinnissa/ testauksessa.

Esimerkkejä riskien vaikutusluokista

Seuraukset	No	VAHTI ohjeen esimerkki vaikutusluokista
Kriittinen	4	• Riskin toteutuminen estää tai keskeyttää kokonaan esimerkiksi toiminnan kannalta tärkeän strategisen tavoitteen saavuttamisen tai jonkin organisaation tuottaman kriittisen prosessin tai palvelun. • Toteutumisesta voi seurata suurta vahinkoa tai kustannuksia myös muille. • Seuraus tai tapahtuma, jonka vuoksi toiminta joudutaan keskeyttämään ja se estyy pitkähköksi ajaksi. • Tapahtumasta voi aiheutua merkittäviä kustannuksia organisaation tai valtionhallinnon näkökulmasta katsottuna. • ~~Suuren ihmisjoukon~~ Ihmisten terveys tai henki vaarantuu ja sillä voi olla vaikutusta laajalti koko yhteiskunnan toimintaan. • Organisaation maine tai asema kansallisissa ja/tai Suomen maine kansainvälisissä yhteyksissä vaarantuu.
Merkittävä	3	• Riskin toteutuminen vaikeuttaa, hidastaa tai muutoin vaarantaa merkittävällä tavalla tärkeän tavoitteen saavuttamisen. • Toteutuminen voi aiheuttaa merkittävää vahinkoa tai kustannuksia. • Seuraus tai tapahtuma, jonka vuoksi toiminta joudutaan keskeyttämään, tai tapahtuman seurauksena aiheutuu vähäistä suurempia kustannuksia. • Tapahtumasta voi aiheutua myös omaisuuden rikkoontumista. • ~~Yksittäisten ihmisten terveys tai henki voi vaarantua.~~ • Organisaation maine luotettavana toimijana heikentyy merkittävästi.
Kohtalainen	2	• Riskin toteutuminen viivästyttää tai heikentää selvästi mahdollisuuksia saavuttaa yhtä tai useampia tavoitteista. • Seuraus tai tapahtuma, jonka vuoksi ei tarvitse keskeyttää toimintaa, mutta saatetaan joutua muuttamaan toiminnallisia suunnitelmia. • Tapahtumasta voi aiheutua vähäisiä kustannuksia. • Maine luotettavana toimijana vaarantuu.
Vähäinen	1	• Riskin toteutumisesta voi aiheutua vähäistä haittaa tavoitteen saavuttamiselle. • Toteutumisella on vähäinen vaikutus organisaation toimintaan.

Riskinsietokyky ja riskinottohalu

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

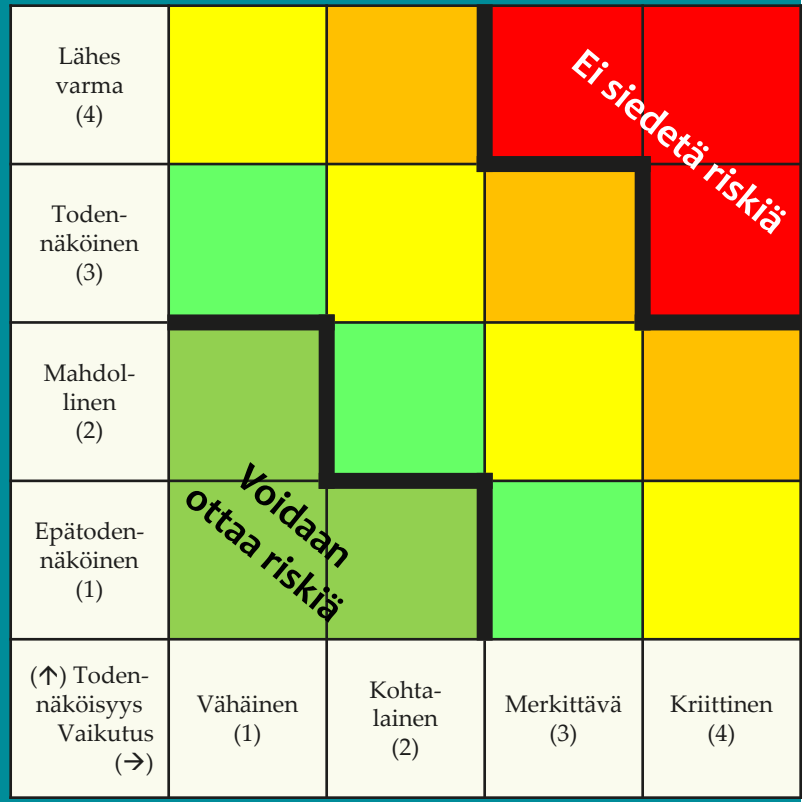
Riskinsietokyky on riskin suuruuden yläraja, johon asti organisaatio on valmis sitoutumaan riskien määrittelyn jälkeen.

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

Riskinottohalu on riskin määrän alaraja, jonka alittavat riskit organisaatio on valmis ottamaan pyrkiessään asettamiinsa tavoitteisiin.

Esimerkiksi

- **Organisaatio ei siedä** pysyvän vamman tai kuoleman aiheuttavaa riskiä tai vaikutus ylittää 25% vuositalousarviosta, korjauskustannukset tuplaavat palvelun vuosikulut, toiminta pysähtyy yli viikoksi, 20% asiakkaista menettää luottamuksen tai riski voi aiheuttaa vakavan pitkäaikainen maineen menetyksen
- **Voimme ottaa riskiä, jos** menetys on maksimissaan 3% vuositalousarviosta, korjauskustannukset eivät ylitä 10% palvelun vuosikuluista, toiminta hidastuminen on vähäistä ja väliaikaista maksimissaan viikon ajan tai vakuutus kattaa 80% riskin vaikutuksista



Tietosuojariskien kartta (esimerkki)

1 Henkilötieto voi olla virheellistä, vanhentunutta tai tuhoutunut

Vääriä johtopäätöksiä ja päätöksiä. Asiakkaalle virheellisiä toimenpiteitä. Asiakas kärsii vahinkoja (tulevaisuus, terveys, talous) tai joutua hengenvaaraan. Organisaation korvausvelvollisuus. Organisaation maine voi kärsiä. Luottamus organisaation palveluihin laskee tai menetetään. Organisaation toiminnot kärsivät. Pitkällä tähtäimellä odotettu toimintojen tehokkuuden ja tuottavuuden kasvu jää toteutumatta.

2 Henkilötieto ei jalostu (joustavuus) toiminnan kehityksen mukana

Manuaaliset työt jatkuvat. Toimintaa ei voi kehittää tarpeen mukaan. Pitkällä tähtäimellä odotettu toimintojen asiakastyytyväisyyden, tehokkuuden ja tuottavuuden kasvu jää toteutumatta.

3 Tärkeä henkilötieto ei ole saatavilla, kun sitä tarvitsee

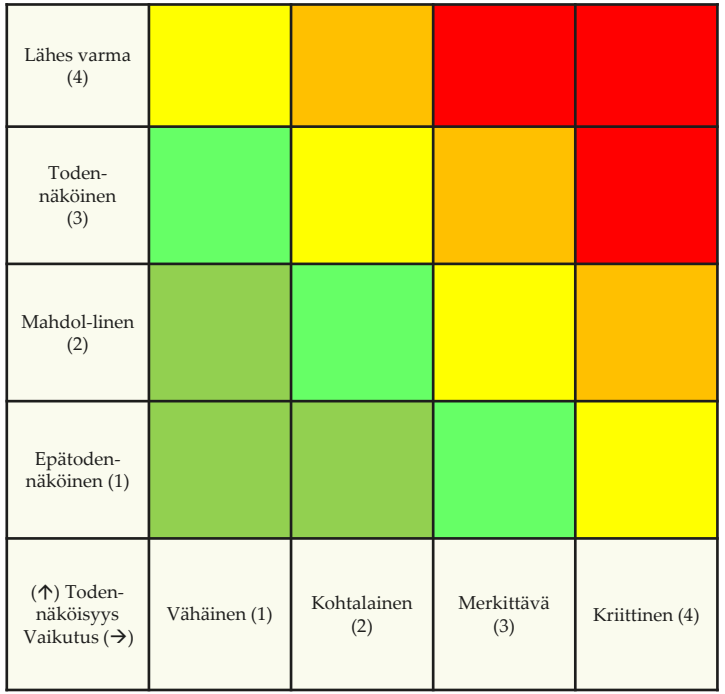
Työt hidastuvat tai estyvät toiminnoissa ja vääriä päätöksiä vanhoilla tiedoilla. Asiakkaalle vääriä toimenpiteitä. Asiakkaat eivät voi asioida. Asiakas kärsii vahinkoja (terveys, talous) tai joutuu hengenvaaraan. Organisaatio voi joutua korvausvelvolliseksi. Maine kärsii kolauksen. Luottamus palveluihin laskee.

4 Arkaluontoinen henkilötieto vuotaa sivullisille

Suuri ylimääräinen työ asian selvittämiseksi ja korjaamiseksi. Työtä menee tuottamattomaan asiaan. Asiakas kärsii henkisiä ja taloudellisia vahinkoja sekä menettää luottamuksen palveluihin. Mikäli tapaus saa laajasti julkisuutta, maine kärsii ison kolauksen, joka vaikuttaa pitkään organisaation kanssa.

5 Laaja odottamaton katkos tietojärjestelmien käytössä

Työt estyvät laajasti toimialoilla. Toiminta estyy. Asiakkaat eivät saa palvelua. Asiakkaat eivät voi asioida ja kärsivät vahinkoja (mahdollisuuden menetys tai terveydellinen tai taloudellinen menetys) tai joutuvat hengenvaaraan. Organisaatio kärsii mittavia taloudellisia vahinkoja ja joutuu korvausvelvolliseksi. Laaja toimintahäiriö saa helposti laajasti julkisuutta ja organisaation kärsii ison kolauksen sekä vaikuttaa pitkään asioinnissa organisaation kanssa. Luottamus palveluihin kärsii.



Itsearvioiti

Tiedän tietäväni Osaanko antaa vastuullisten tehdä työnsä ja ohjata/sparrata vain tarvittaessa? Riskinotto luonnostaan. ”Tähän suuntaan”	**Tiedän tietämättömyyteni** Ymmärränkö tukeutua asiantuntijaan? Miten tunnistan asiantuntijan, että hän tietää / osaa? Hallittu riskinottaminen. ”Faktojen pohjalta”.
En tiedä tietäväni Miten kehittää itsetuntemusta ja rohkeutta? Miten tunnistaa osaaminen/tietämys? Riskiä kartetaan tai minimoidaan. ”Varman päälle”.	**En tiedä tietämättömyyttäni** Miten kehittää itsetuntemusta ja nöyryyttä? Mistä tunnistaa ettei oikeasti tiedä? Hallitsematon riskinottaminen. ”Rinta rottingilla”.