Euroopan unionin osarahoittama KYMEN LAAKSON LIITTO

# Riskiarviointi opas

## 1 Mihin tarkoitukseen?

Tämän riskiarviointityökalun tarkoituksena on tukea sosiaali- ja terveysalan pienyrittäjiä riskiarvioinnin tekemisessä. Lainsäädäntö edellyttää riskiarviointia, mutta pienyrittäjille suunnattua käytännön tukea on saatavilla hyvin vähän. Tästä tarpeesta syntyi ajatus kehittää riskiarviointityökalu osana **CyberCare Kymi -hanketta**.

Tässä oppaassa esitellään tyypillisiä sosiaali- ja terveysalan riskejä – erityisesti pienyritysten näkökulmasta. Lisäksi selitetään, miten tietyt riskit voivat syntyä ja vaikuttaa toimintaan. Osa riskeistä on valmiiksi määritelty, eikä niitä voi poistaa – nämä ovat riskejä, jotka koskettavat jokaista verkkoyhteyksiä käyttävää sote-alan yritystä.

## 2 Miten se toimii?

Työkalu on jaettu kahdeksan riskipiireihin:

1. Toimitila
2. Liikkuva- / Etätyö
3. Tietoturva
4. Verkko
5. Sovellukset
6. Lääkinnälliset laitteet
7. Alihankintaketju
8. Muut Riskit

Työkalussa on riskejä, jotka ei voi muokata. Niitä riskejä löytyy jokaisessa yrityksessä, jossa käytetään internetti tavalla tai toisella. Muuttumattomien riskien alla on mahdollisuus lisätä omia yrityskohtaisia riskejä.

Riskit arvioidaan riskien vaikutuksen yritykselle ja kuinka todennäköisesti tämä riski isku yritykselle.

**Vaikutus x Todennäköisyys = Riski Yritykselle**

Asteikko on 1-5.

| Vaikutus | |
|---|---|
| 1 | Vähäinen |
| 2 | Kohtalainen |
| 3 | Merkittävä |
| 4 | Kriittinen |
| 5 | Erittäin kriittinen |

| Todennäköisyys | |
|---|---|
| 1 | Epätodennäköinen |
| 2 | Mahdollinen |
| 3 | Todennäköinen |
| 4 | Hyvin todennäköinen |
| 5 | Lähes varma |

# 3 Riskit

## 3.1 Mikä on riski?

**Riski** tarkoittaa mahdollisuutta, että jokin **haitallinen tapahtuma toteutuu** ja vaikuttaa yrityksen toimintaan negatiivisesti. Riski ei ole vielä tapahtunut vahinko, vaan **uhka, joka voi toteutua** – ja jos se toteutuu, siitä seuraa haittaa yritykselle, asiakkaille tai henkilöstölle.

Jokainen riski arvioidaan kahden kysymyksen kautta:

1. Kuinka todennäköistä on, että tämä tapahtuu?
2. Kuinka suuri vaikutus sillä olisi, jos se tapahtuisi?

Näiden perusteella lasketaan riskin taso:


## 3.2 Mitä pitää huomioida riskien arvioinnista?

Riskien arviointi ei ole aina yksinkertaista – erityisesti silloin, kun kyse on kyberuhkista tai muista harvinaisemmista tapahtumista, joita ei ole vielä itse kokenut.

Usein riskit tuntuvat vakavammilta ja konkreettisemmilta, jos vastaavaa on sattunut omassa lähipiirissä tai tuttavalle. Tällöin todennäköisyyttä arvioidaan helposti korkeammaksi kuin mitä se objektiivisesti olisi. Abstrakti riski muuttuu todelliseksi, kun se on tapahtunut jollekin tutulle.

Vaikutuksen arvioimiseen voi auttaa simuloimalla riskin toteutumista. Esimerkiksi, jos arvioit verkkoyhteyden merkitystä yrityksellesi, kokeile tehdä työpäivä ilman internetiä. Tai pohdi, mitä tapahtuisi, jos kiristyshaittaohjelma lamauttaisi kaikki laitteesi – miten se vaikuttaisi arjen toimintaan?

Sen sijaan todennäköisyyden arviointi on usein vaikeampaa. Arvio perustuu usein tunteeseen tai henkilökohtaisiin kokemuksiin. On tärkeää muistaa, että yksittäinen esimerkki ei kerro koko totuutta riskin todennäköisyydestä.

## 3.3 Toimitila

Tässä osiossa keskitytään yrityksen **toimitilojen fyysisiin riskeihin**. Nämä riskit voivat aiheuttaa käyttökatkoja, vaarantaa asiakasturvallisuuden tai estää koko toiminnan.

**Laitteiden rikkoutuminen**

Yrityksellä voi olla käytössä esimerkiksi tietokoneita, tulostimia, maksupäätteitä tai digitaalisia lukitusjärjestelmiä. Jos jokin näistä rikkoutuu, se voi aiheuttaa katkoksen asiakaspalveluun tai tietojen käsittelyyn.

Mieti: Onko varalaitteita saatavilla? Miten nopeasti laite saadaan korjattua tai vaihdettua?

**Laitteiden toimintahäiriöt**

Toimintahäiriö ei aina tarkoita, että laite hajoaa kokonaan – se voi myös hidastaa työtä, aiheuttaa virheitä tiedonkäsittelyssä tai estää järjestelmän käytön hetkellisesti.

Mieti: Miten työ sujuu, jos järjestelmä toimii hitaasti tai epävakaasti?

**Laitteiden väärinkäyttö**

Väärinkäyttö voi olla tahatonta (esim. asiakas koskee laitteeseen) tai tahallista (esim. ilkivalta tai työntekijän huolimattomuus). Tämä voi vaarantaa tietoturvan tai aiheuttaa vahinkoa laitteelle tai tiedoille.

Mieti: Onko laitteet sijoitettu niin, että asiattomat eivät pääse niihin käsiksi?

**Toimitilojen turvallisuus**

Tähän kuuluu muun muassa ovien lukitus, hälytysjärjestelmät, kulunvalvonta ja kameravalvonta. Jos toimitiloihin pääsee ulkopuolinen henkilö, voi seurauksena olla varkaus, tietovuoto tai muuta vahinkoa.

Mieti: Kuinka hyvin toimitila on suojattu ulkoisilta uhkilta? Onko esimerkiksi hälytysjärjestelmä käytössä?

**Muita toimitilaan liittyviä riskejä voivat olla:**

- **Sähkökatko**: Toiminta keskeytyy välittömästi, jos sähköt katkeavat.
- **Vesivahinko**: Voi tuhota laitteita, asiakirjoja tai aiheuttaa pitkäaikaisen käyttökatkon.
- **Ilkivalta**: Esimerkiksi ikkunoiden rikkominen tai tilojen sotkeminen.
- **Pääsyn estyminen toimitilaan**: Esimerkiksi tulipalo rakennuksessa tai viranomaismääräys (esim. sulku tai karanteeni).

## 3.4 Liikkuvatyö / Etätyö

Tässä osiossa keskitytään riskeihin, jotka liittyvät työn tekemiseen **toimiston ulkopuolella**. Tämä voi tarkoittaa esimerkiksi **kotikäyntejä asiakkaan luona**, **etätyötä kotoa käsin** tai vaikkapa **sähköpostien lukemista matkapuhelimella liikkeellä ollessa**.

Liikkuvassa työssä ja etätyössä riskit ovat erilaisia kuin toimistotyössä – erityisesti laitteiden, tiedon ja yhteyksien suojaaminen korostuu.

**Laitteiden katoaminen**

Kun työtä tehdään liikkuen, laitteita kuten kannettavia tietokoneita tai puhelimia kuljetetaan mukana. Ne voivat unohtua esimerkiksi asiakkaan luo, autoon tai kahvilaan.
Mieti: Voiko laitteen kadotessa joku muu päästä käsiksi tietoihin? Onko laite suojattu salasanalla ja lukituksella?

**Laitteiden varastaminen**

Laitteet ovat arvokkaita – sekä itse laitteena että niiden sisältämän tiedon vuoksi. Varastettu laite voi päätyä vääriin käsiin, ja tietoturva vaarantuu.
Mieti: Voiko laite tyhjentää etänä? Onko tietojen salaus käytössä?

**Internet-yhteyksien katkeaminen**

Etätyö vaatii verkkoyhteyksiä, mutta kotiverkot tai mobiilidata voivat olla epävakaita. Yhteyden katkeaminen kesken työn voi johtaa tietojen menetykseen tai asiakaspalvelun keskeytymiseen.
Mieti: Onko varayhteyttä tai offline-työskentelymahdollisuutta?

**Salakatselu (”shoulder surfing”)**

Kun työskennellään julkisissa tai avoimissa tiloissa, sivulliset voivat nähdä näytöllä näkyvät tiedot. Tämä on erityisen riskialtista, jos käsitellään asiakas- tai potilastietoja.
Mieti: Käytetäänkö näytönsuojaa? Työskennelläänkö vain yksityisissä tiloissa?

**Huolimaton tiedon käsittely**

Etätyössä työntekijällä voi olla vähemmän valvontaa, ja tietojen käsittely saattaa muuttua huolettomammaksi. Esimerkiksi asiakastietoja voi jäädä avoimiksi näytölle tai niitä saatetaan käsitellä perheenjäsenten nähden.
Mieti: Onko ohjeistettu, missä ja miten tietoja saa käsitellä kodin ulkopuolella?

**Mobiililaitteiden turvallisuus**

Puhelimet ja tabletit ovat arkipäivää etätyössä, mutta niiden suojaaminen jää usein heikoksi. Esimerkiksi automaattinen näytön lukitus voi puuttua tai laitteen käyttöoikeuksia ei ole rajattu.
Mieti: Onko mobiililaitteissa salasanasuoja, automaattinen lukitus ja laitetunnistus? Voiko yritys hallita tai tyhjentää laitteen etänä?

## 3.5 Tietoturva

Tietoturva tarkoittaa kaikkea sitä, mikä liittyy **tiedon suojaamiseen**, olipa kyseessä asiakastiedot, potilastiedot tai yrityksen sisäiset asiakirjat. Pienessä sosiaali- ja terveysalan yrityksessä tietoturva ei aina ole järjestelmällisesti hallittua, mutta sen laiminlyönti voi aiheuttaa vakavia seurauksia – niin taloudellisia kuin maineeseen liittyviä.

Tässä osiossa käsitellään tietoturvaan liittyviä riskejä, jotka liittyvät työvälineisiin, tietoihin ja järjestelmien hallintaan.

**Luvaton pääsy työkoneisiin tai työvälineisiin**

Jos ulkopuolinen tai luvaton henkilö pääsee käsiksi työkoneeseen, esimerkiksi avoinna jätettyyn kannettavaan tai puhelimeen, tiedot voivat vaarantua.
Mieti: Lukkiutuuko laite automaattisesti, jos se jää hetkeksi ilman valvontaa?

**Tietovuoto**

Tietovuoto tarkoittaa, että luottamuksellista tietoa päätyy ulkopuolisten tietoon. Tämä voi tapahtua esimerkiksi sähköpostivirheen, laitevarkauden tai kyberhyökkäyksen kautta.
Mieti: Mitä tietoa yrityksessä käsitellään, ja miten se on suojattu?

**Työvälineiden turvallisuuden valvonnan puute**

Jos ei tiedetä, missä laitteet ovat, kuka niitä käyttää ja miten niitä käytetään, syntyy tietoturvariski.
Mieti: Onko jokaiselle laitteelle nimetty vastuu? Onko käyttölokeja?

**Tietojen menetys**

Tietoa voi kadota esimerkiksi vahingossa poistamisen, laitteen hajoamisen tai virustartunnan seurauksena.
Mieti: Onko varmuuskopiot olemassa – ja kuinka helposti ne saa palautettua?

**Varmuuskopioiden korruptoituminen**

Jos varmuuskopiot vahingoittuvat tai ovat viallisia, tietojen palautus ei onnistu silloin, kun sitä eniten tarvitaan.
Mieti: Testataanko varmuuskopiot säännöllisesti?

**Varmuuskopioiden testaamisen puute**

Varmuuskopioiden ottaminen ei yksin riitä – niiden toimivuus pitäisi testata ajoittain.
Mieti: Onko koskaan kokeiltu palauttaa tietoa varmuuskopiosta testimielessä?

**Heikot tietojenhallintakäytännöt**

Esimerkiksi, jos tiedot ovat sekalaisesti eri paikoissa tai jokainen työntekijä tallentaa tietoja eri tavalla, riskit kasvavat.
Mieti: Onko selkeät ohjeet, mihin ja miten tietoa tallennetaan?

**Tieto ei ole saatavilla**

Kyberturvallisuudessa puhutaan usein luottamuksellisuudesta, mutta saatavuus on yhtä tärkeä – tieto pitää olla käytettävissä silloin, kun sitä tarvitaan.
Mieti: Mitä tapahtuu, jos asiakastiedot eivät ole käytettävissä hoitotilanteessa?

**Heikko salasanapolitiikka**

Salasanat voivat olla liian yksinkertaisia, samoja käytetään useassa järjestelmässä tai niitä ei vaihdeta säännöllisesti. Salasanapolitiikalla määritellään esim. minkälainen salasana pitäisi käytä. Hyvä salasana on:

- Vähintään 15 merkkiä pitkään ja sisältää vähintään kaksi niistä kolmesta: pieniä ja isoja kirjaimia, numeroita ja erikoismerkkejä (välilyönti on erikoismerkki).

Mieti: Onko salasanat riittävän vahvoja ja suojattuja? Onko käytössä kaksivaiheinen tunnistautuminen?

**Järjestelmien poikkeavaa käyttöä ei huomata**

Jos järjestelmässä tapahtuu jotain poikkeavaa (esim. yöllä kirjautuminen), sitä ei ehkä havaita, ellei ole valvontaa.
Mieti: Seurataanko, milloin ja kuka järjestelmiin kirjautuu?

**Lokitietojen puute tai saatavuuden puute**

Lokitiedot ovat tietoja siitä, mitä järjestelmässä on tapahtunut. Ilman niitä ei voi selvittää, kuka teki mitä ja milloin.
Mieti: Tallentuuko käyttö- ja tapahtumatiedot? Voiko niitä tarkistaa?

**Tietoturvan ja tietoverkon puutteet**

Esimerkiksi palomuurin puuttuminen, päivittämättömät ohjelmistot tai suojaamaton WiFi voivat avata ovia hyökkäyksille.
Mieti: Onko verkko ja laitteet suojattu nykyaikaisesti? Onko ohjelmistot ajan tasalla?

## 3.6 Verkko

Verkko eli internetyhteys ja sisäverkko ovat nykyään lähes kaikkien sosiaali- ja terveysalan yritysten toiminnan perusta. Verkon kautta siirretään asiakastietoja, pidetään yhteyttä, käytetään järjestelmiä ja tallennetaan tietoa pilvipalveluihin.

Verkkoon liittyvät riskit ovat usein näkymättömiä – ne eivät näy fyysisesti, mutta voivat lamauttaa koko toiminnan hetkessä. Siksi näihin riskeihin on tärkeää suhtautua vakavasti myös pienissä yrityksissä.

**Kiristyshaittaohjelmahyökkäys (ransomware)**

Tällaisessa hyökkäyksessä haittaohjelma salaa yrityksen tiedot ja vaatii lunnaita niiden vapauttamiseksi. Hyökkäys voi tulla esimerkiksi sähköpostin liitteen tai linkin kautta.
Mieti: Onko varmuuskopiot olemassa ja suojattu? Voiko toiminta jatkua ilman tietoja?

Yli 40% kaikista hyökkäyksistä sote-alan kohtaan ovat kiristyshaittaohjelmia.

**Phishing-hyökkäys (tietojen kalastelu)**

Yleinen hyökkäysmuoto, jossa huijataan työntekijä antamaan esimerkiksi käyttäjätunnukset ja salasanat väärennetyn sähköpostin tai verkkosivun kautta.
Mieti: Ovatko työntekijät saaneet koulutusta tai ohjeistusta tällaisiin tilanteisiin? Tiedätkö he mistä voisivat tarkista linkin?

**Luvaton pääsy yritysverkkoon**

**Jos yrityksen verkko on suojaamaton, esimerkiksi heikon palomuurin tai salasanapolitiikan vuoksi, ulkopuolinen voi päästä järjestelmiin.**
**Mieti: Onko palomuuri käytössä? Vaihdetaanko reitittimen salasanat säännöllisesti?**

**Henkilökohtaisten laitteiden käyttö yritysverkossa**

Työntekijät voivat käyttää omia puhelimia tai tietokoneita yrityksen verkossa, mikä voi tuoda mukanaan turvattomia ohjelmia tai viruksia.
Mieti: Onko sallittua käyttää omia laitteita työasioihin? Jos on, miten niiden turvallisuus varmistetaan?

**Vanhentuneet ohjelmistot**

Päivitykset sisältävät usein tärkeitä tietoturvaparannuksia. Vanhentuneet ohjelmat tai käyttöjärjestelmät ovat alttiita hyökkäyksille.
Mieti: Onko ohjelmistojen päivitykset automatisoitu? Kuka niistä vastaa?

**Haavoittuvuuksien hyväksikäyttö**

Jos järjestelmässä on tekninen heikkous (”haavoittuvuus”), hyökkääjät voivat käyttää sitä päästäkseen käsiksi tietoihin tai ohittamaan suojaukset.
Mieti: Onko käytössä vain tunnettuja ja luotettavia ohjelmia?

**Tietojen manipulointi**

Hyökkääjä tai huolimaton työntekijä voi muuttaa tietoa vahingossa tai tahallaan. Tämä voi johtaa esimerkiksi vääriin hoitopäätöksiin.
Mieti: Onko tiedon muokkaamiseen liittyvä toiminta valvottua ja lokitettu?

**Tietojen väärinkäyttö ja luvaton käyttö**

Tätä voi tapahtua sekä ulkopuolelta että sisäisesti. Esimerkiksi työntekijä voi katsoa asiakastietoja, joihin hänellä ei ole oikeutta.
Mieti: Onko jokaiselle käyttäjälle rajattu pääsy vain omiin työtehtäviin tarvittaviin tietoihin?

**Salattavan tiedon paljastuminen**

Jos arkaluonteista tietoa siirretään ilman salausta (esim. sähköpostilla), se voi paljastua kolmansille osapuolille.
Mieti: Käytetäänkö salattua sähköpostia ja suojattuja yhteyksiä?

**Yksityisyyden loukkaus**

Potilaan tai asiakkaan tietojen käsittely ilman lupaa tai tarpeetonta tietojen katselua voi rikkoa tietosuojalakia ja vahingoittaa yrityksen mainetta.
Mieti: Onko henkilöstöllä selkeä käsitys siitä, mitä tietoja saa käsitellä ja milloin?

**Haittaohjelmien pääsy työasemille ja verkkolaitteisiin**

Jos virustorjunta tai palomuuri puuttuu tai ei toimi, haittaohjelma voi päästä laitteisiin ja levitä verkon kautta koko yritykseen.
Mieti: Onko virustorjunta ajan tasalla kaikissa laitteissa? Onko automaattinen skannaus käytössä?

## 3.7 Sovellukset

Yhä useampi pienyritys käyttää verkkopohjaisia sovelluksia ja pilvipalveluita jokapäiväisessä työssään. Esimerkiksi asiakastietoja käsitellään sähköisissä järjestelmissä, viestintä tapahtuu sähköpostilla tai etävastaanotoilla, ja tiedostoja säilytetään pilvessä.

Sovellukset tuovat mukanaan helppoutta ja liikkuvuutta – mutta samalla ne luovat uusia riskejä, erityisesti kun käsitellään arkaluonteisia potilas- tai asiakastietoja.

**Hyökkäykset verkkosovelluksiin**

Verkkosovelluksia (esim. ajanvarausjärjestelmät tai asiakastietokannat) voidaan yrittää murtaa tai häiritä. Heikosti suojatut järjestelmät voivat olla hyökkäyksen kohteena.
Mieti: Onko käyttämäsi sovellus turvallinen ja luotettavan toimijan tarjoama? Saako se säännöllisiä päivityksiä?

**Arkaluonteisten tietojen jakaminen pilvipalvelussa**

Etävastaanottojen, sähköpostien tai yhteisten tiedostojen kautta saatetaan jakaa esimerkiksi terveystietoja. Jos suojaus on puutteellinen, tiedot voivat päätyä vääriin käsiin.
Mieti: Käytetäänkö salattuja yhteyksiä? Onko selvää, kuka saa nähdä ja käsitellä tietoa?

**Tietojen menetys pilvipalveluissa**

Pilvessä oleva tieto voi kadota esimerkiksi teknisen vian, inhimillisen virheen tai palveluntarjoajan ongelmien vuoksi.
Mieti: Onko tärkeistä tiedoista olemassa varmuuskopioita? Säilytetäänkö niitä myös muualla kuin pilvessä?

**Riittämätön pääsynhallinta pilvipalvelussa**

Jos kaikilla käyttäjillä on samat oikeudet, kuka tahansa voi vahingossa (tai tahallaan) poistaa, muokata tai jakaa tietoa.
Mieti: Onko käyttäjäoikeudet määritelty oikein? Onko pääsy vain niillä, joilla siihen on tarve?

## 3.8 Lääkinnälliset laitteet

Lääkinnälliset laitteet ovat keskeisessä roolissa sosiaali- ja terveysalan toiminnassa. Niiden kautta voidaan mitata, seurata ja hoitaa potilaita, mutta ne voivat myös olla tietoturva- ja potilasturvallisuusriskien lähteitä. Koska laitteet kytkeytyvät usein verkkoon ja tallentavat tai siirtävät potilastietoa, on niiden suojaaminen erityisen tärkeää.

Tässä osiossa käsitellään lääkinnällisiin laitteisiin liittyviä riskejä, jotka voivat vaarantaa sekä tietoturvaa että asiakasturvallisuutta.

**Luvaton pääsy fyysisesti**
Jos ulkopuolinen henkilö pääsee käsiksi lääkinnälliseen laitteeseen paikan päällä, hän voi muuttaa asetuksia, varastaa tietoa tai aiheuttaa toimintahäiriön.
Mieti: Missä laitteet sijaitsevat? Onko pääsy niihin rajattu vain valtuutetuille henkilöille?

**Luvaton pääsy verkossa**
Laitteet voivat olla yhteydessä verkkoon esimerkiksi etäseurantaa varten. Jos verkkoyhteys ei ole riittävästi suojattu, hyökkääjä voi päästä käsiksi laitteen toimintoihin.
Mieti: Onko laitteet suojattu palomuurilla ja salatuilla yhteyksillä? Päivitetäänkö ohjelmistot säännöllisesti?

**Tietojen vuotaminen laitteen kautta**
Jos laite tallentaa tai välittää potilas- tai asiakastietoja, ne voivat vuotaa ulkopuolisille esimerkiksi hyökkäyksen, virheellisen käytön tai puutteellisen salauksen vuoksi.
Mieti: Onko tiedonsiirto aina salattu? Kuka voi käyttää laitteen keräämää tietoa?

**Avoimet portit**
Jos laitteen verkkoyhteyksissä on avoimia portteja, ne voivat tarjota helpon väylän hyökkääjille.
Mieti: Onko portit suljettu tai rajattu vain tarpeellisiin toimintoihin?

**Toimintahäiriöt**
Laitteen ohjelmistovirheet, häiriöt tai väärinkäyttö voivat estää sen toiminnan kriittisellä hetkellä.
Mieti: Onko olemassa varalaite tai suunnitelma, jos laite ei toimi?

**Yhteensopivuusongelmat muiden järjestelmien kanssa**
Jos laite ei toimi yhteen muiden järjestelmien kanssa, voi syntyä virheitä tietojen siirrossa tai hoitoprosessissa.
Mieti: Onko laite testattu ja hyväksytty käytettäväksi nykyisten järjestelmien kanssa?

**Asiakasturvallisuuden vaarantuminen**
Lääkinnällisen laitteen väärä toiminta tai väärinkäyttö voi johtaa suoraan potilaan hoidon vaarantumiseen.
Mieti: Onko henkilöstöllä riittävä koulutus laitteen käyttöön? Seurataanko laitteen toimivuutta säännöllisesti?

**Etähyökkäyksille alttius**
Etäkäyttö tuo mukanaan hyötyjä, mutta myös riskejä – laitteeseen voidaan yrittää murtautua mistä tahansa.
Mieti: Onko etäyhteyksissä käytössä kaksivaiheinen tunnistautuminen? Onko käytössä vain turvallisia etäkäyttökanavia?

## 3.9 Alihankintaketju

Jokaisella yrityksellä on alihankkijoita – myös kaikkein pienimmillä. Alihankkijoita voivat olla esimerkiksi ohjelmistojen toimittajat kuten Microsoft tai Google, tulostin- ja IT-laitetoimittajat, kirjanpitopalvelut, pilvipalveluntarjoajat, siivouspalvelut tai jopa verkkoyhteyden tarjoaja.

Yrityksen vastuulla on varmistaa, että myös nämä ulkopuoliset toimijat käsittelevät tietoja turvallisesti.

Lain mukaan yritys on vastuussa alihankkijoiden henkilötietojen käsittelystä. Jos esimerkiksi alihankkijan järjestelmästä tapahtuu tietovuoto, vastuu kuuluu myös toimeksiantajalle yritykselle. Siksi pelkkä yleinen sopimus ei riitä – on tärkeää kysyä:

- Miten alihankkija suojaa tietoja?
- Kuka käsittelee tietoja ja missä?
- Voidaanko tietoturvaa auditoida tai tarkistaa?

Hyvin laadittu ja tietoturvaa huomioiva sopimus on osa riskienhallintaa – ja samalla osoitus vastuullisesta toiminnasta asiakkaiden ja viranomaisten suuntaan.

**Alihankkijan virheellinen käsittely ja säilytys henkilötiedoista**

Jos alihankkija ei käsittele tietoja turvallisesti – esimerkiksi tallentaa ne suojaamattomalle laitteelle tai siirtää niitä ilman salattua yhteyttä – yritys on silti vastuussa seurauksista.
Mieti: Onko sopimuksessa selkeästi sovittu, miten henkilötietoja saa käsitellä ja säilyttää?

**Sopimusten rikkomukset**

Jos alihankkija toimii vastoin sovittua – esimerkiksi säilyttää tietoja pidempään kuin sallittu tai käyttää niitä muihin tarkoituksiin – kyseessä on sopimusrikkomus.
Mieti: Tarkistetaanko säännöllisesti, että sopimusehtoja noudatetaan? Onko rikkomuksiin määritelty seuraukset?

**Alihankkijan pääsy väärään tietoon**

Jos alihankkijalla on pääsy järjestelmiin, voi olla riski, että he näkevät tietoja, jotka eivät kuulu heille. Esimerkiksi tukipalvelu voi päästä potilastietoihin tarpeettomasti.
Mieti: Onko pääsyoikeudet rajattu tiukasti? Onko lokitietoja siitä, kuka katsoo mitäkin?

**Tiedon väärinkäyttö tai manipulointi alihankkijan puolelta**

Pahimmassa tapauksessa alihankkija tai sen työntekijä käyttää tietoa väärin – joko vahingossa tai tahallisesti. Tietoja voidaan muokata, vuotaa tai käyttää sopimattomiin tarkoituksiin.
Mieti: Onko alihankkijalla salassapitosopimus? Ovatko heidän työntekijänsä koulutettu tietoturvaan?

## 3.10 Muut riskit

Kaikki riskit eivät liity teknologiaan tai tietoturvaan. Sote-alan työssä kohdataan päivittäin monenlaisia tilanteita, joissa **turvallisuus**, **työhyvinvointi** ja **asiakastilanteiden hallinta** ovat keskiössä. Tässä osiossa käsitellään muita riskejä, jotka eivät sovi aiempiin kategorioihin, mutta joita **ei saa unohtaa** – erityisesti asiakastyötä tekevässä ympäristössä.

**Sisäiset uhat (henkilöstö)**

Työntekijä voi vahingossa tai tahallisesti aiheuttaa riskejä. Esimerkiksi huolimattomuus, epäasiallinen käytös tai väärä tiedonkäsittely voi vaarantaa asiakasturvallisuuden tai yrityksen maineen.
Mieti: Onko henkilöstölle annettu riittävä perehdytys, vastuut ja toimintamallit poikkeustilanteisiin?

**Työuupumus (henkilöstö, johto, asiakkaat, yhteistyökumppanit)**

Pitkittynyt kuormitus vaikuttaa työkykyyn, tarkkaavaisuuteen ja virheiden riskiin. Uupunut työntekijä voi toimia epähuomiossa väärin tai laiminlyödä ohjeita.
Mieti: Seurataanko työkuormitusta? Onko käytössä keinoja palautumiseen ja tukeen?

**Ulkoiset uhat (asiakkaat, omaiset, sidosryhmät)**

Yrityksen ulkopuolelta tulevat ihmiset voivat aiheuttaa uhkia – esimerkiksi aggressiivinen asiakas, painostava omainen tai yhteistyökumppanin väärinkäsitys.
Mieti: Onko henkilöstö koulutettu kohtaamaan vaikeita tilanteita? Onko hätätoimintamalli selvä?

**Muita riskejä, jotka voisivat koskea yrityksenne:**

Sote-ala sisältää myös fyysisen työn ja altistumisen riskejä, jotka voivat aiheuttaa vakavia tapaturmia tai sairastumisia.

**Työntekijöihin kohdistuva henkinen ja fyysinen väkivalta**

Erityisesti asiakaskohtaamisissa voi esiintyä väkivaltaa tai uhkaavia tilanteita.
Mieti: Onko väkivaltatilanteisiin varauduttu? Tiedetäänkö, miten niissä toimitaan?

**Sähköisku / Palovammat**

Sähkölaitteiden käyttöön liittyy riskejä – esimerkiksi rikkoutunut johto tai viallinen laite voi aiheuttaa sähköiskun tai palovamman.
Mieti: Onko laitteet tarkastettu ja kunnossa? Onko henkilökunta tietoinen turvallisista käyttötavoista?

**Neulanpisto**

Esimerkiksi rokotuksia tai injektioita annettaessa on riski neulanpistosta, mikä voi altistaa taudinaiheuttajille.
Mieti: Onko pistovälineiden hävittämiseen selkeät ohjeet ja välineet?

**Siivousaineet / Kemikaalit**

Puhdistusaineet ja desinfiointikemikaalit voivat aiheuttaa ihoärsytystä, hengitystieoireita tai vaaratilanteita, jos niitä käsitellään väärin.
Mieti: Säilytetäänkö aineet lukitussa tilassa? Onko käyttöohjeet ja suojavälineet käytössä?

**Bakteerit / Virukset / Infektiot**

Sote-työssä ollaan usein lähikontaktissa asiakkaisiin, mikä altistaa infektioille.
Mieti: Käytetäänkö asianmukaisia suojaimia? Noudatetaanko hygieniakäytäntöjä johdonmukaisesti?

# 4 Miten tulkin tulokset?

Riskin suuruus lasketaan kertomalla **riskin todennäköisyys** ja **vaikutus** keskenään:

**Vaikutus × Todennäköisyys = Riskitaso**

Tämän arvioinnin jälkeen saatu tulos sijoitetaan **riskimatriisiin**, joka auttaa hahmottamaan, kuinka merkittävä riski on yrityksen toiminnan kannalta.

| Todennäkköisyys / Vaikutus | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **1** | 1 | 2 | 3 | 4 | 5 |
| **2** | 2 | 4 | 6 | 8 | 10 |
| **3** | 3 | 6 | 9 | 12 | 15 |
| **4** | 4 | 8 | 12 | 16 | 20 |
| **5** | 5 | 10 | 15 | 20 | 25 |

| Väri | Riski |
|---|---|
| | Vähäpätöinen riski |
| | Vähäinen riski |
| | Kohtalainen riski |
| | Korkea riski |
| | Merkittävä riski |

**Miten ylläpitää riskiarviota jatkossa?**

Riskiarviointi ei ole kertaluonteinen tehtävä. **Kyberturvallisuusuhat ja toimintaympäristö muuttuvat jatkuvasti**, ja siksi myös riskiarviota täytyy päivittää säännöllisesti.

# 5 Mitä tehdään riskiarvioinnin jälkeen?

Riskiarvioinnin tekeminen ei ole päätepiste, vaan **alku tietoiselle riskienhallinnalle**. Kun yritys on tunnistanut omat riskinsä ja arvioinut niiden vaikutuksen ja todennäköisyyden, seuraava askel on **toiminta**.

## 5.1 Mieti, miten riskiä voi pienentää (riskien lieventäminen)

Jokaiseen riskiin tulisi pohtia ainakin yksi keino, jolla:

- riskiä voidaan kokonaan poistaa,
- sen todennäköisyyttä voidaan pienentää, tai
- sen vaikutusta voidaan rajoittaa, jos se toteutuu.

Esimerkkejä riskien lieventämisestä:

- **Tietovuotoriski?** → Käyttöönotetaan vahvemmat salasanakäytännöt ja kaksivaiheinen tunnistautuminen.
- **Laitehajoamisen riski?** → Hankitaan varalaitteita tai huoltosopimus.
- **Verkkokatkon riski?** → Otetaan käyttöön varayhteys mobiiliverkon kautta.

Tärkeää: Mitä suurempi riski (esim. punaisella alueella riskimatriisissa), sitä **nopeammin ja määrätietoisemmin siihen tulisi reagoida.**

## 5.2 Kirjaa ja seuraa toimenpiteet

Kaikki suunnitellut toimet on hyvä dokumentoida – mitä tehdään, kuka tekee ja mihin mennessä. Tämä helpottaa vastuunjakoa ja varmistaa, että asiat todella etenevät.

Voit esimerkiksi luoda **toimenpidelistan**, jossa näkyy:

- Riski
- Suunniteltu toimenpide
- Vastuuhenkilö
- Takaraja
- Tila (tehty / kesken / ei aloitettu)

## 5.3 Päivitä riskiarvio vuosittain

Riskiarvio ei ole kertaluonteinen tehtävä. Maailma muuttuu, teknologia kehittyy, asiakkaiden tarpeet muuttuvat – ja **yrityksen riskit muuttuvat siinä mukana**.

Siksi: **Riskiarviointi tulisi tehdä vähintään kerran vuodessa.**

Lisäksi se kannattaa päivittää aina, kun:

- yrityksen toiminta muuttuu (uusi palvelu, uusi järjestelmä),
- tulee uusia lakeja tai suosituksia,
- sattuu poikkeama (esim. tietovuoto tai palvelukatko).

Riskiarvion päivittämisestä voi tehdä vuosittaisen rutiinin, esimerkiksi osana vuoden alun tai tilikauden suunnittelua.

## 5.4 Ota henkilöstö mukaan

Riskienhallinta ei ole vain yrittäjän vastuulla – jokainen työntekijä on osa turvallista toimintaa.

- Jaa arvioinnin tulokset tiimille, keskustele niistä, ja kerro miksi tietyt käytännöt muuttuvat.

- Koulutus ja avoin keskustelu lisäävät sitoutumista ja ehkäisevät virheitä.

## 5.5 Osoita vastuullisuutta asiakkaille ja viranomaisille

Hyvin tehty ja ajantasainen riskiarvio osoittaa:

- vastuullisuutta,
- asiakastietojen kunnioitusta,
- ja sitoutumista turvalliseen toimintaan.

Jos joudut selvittämään poikkeamaa tai tarkastusta, dokumentoitu riskiarvio ja siihen liittyvät toimet osoittavat, että yritys on toiminut huolellisesti.