



# Avointa lähdekoodia koskevat toimintaperiaatteet ja riskienhallinta



Antto Oksanen  
Associate, on secondment



Sami Rintala  
Partner

Avoin lähdekoodi on monella tapaa erinomainen menetelmä tuottaa ja kehittää ohjelmistoja. On kuitenkin muistettava, ettei sen käyttö ole koskaan riskitöntä ja usein ilmaisista komponenteista huolimatta, sen käyttöön liittyy kustannuksia.

Oikein implementoituna avoimen lähdekoodin avulla on kuitenkin mahdollista saavuttaa kilpailuetua sekä helpottaa tuotekehitystyötä merkittävästi. Jos avoimen lähdekoodin yrityskäytön ydinkysymyksiin kiinnitetään asianmukaisesti huomiota, voidaan avoimen lähdekoodin tarjoamista lukuisista eduista myös nauttia – pitäen samalla avoimeen lähdekoodiin liittyvät oikeudelliset ja kaupalliset riskit kurissa. Yrityskäytön kannalta on tärkeää olla tietoinen käytettävistä lisensseistä sekä huolehtia lisenssiehtojen noudattamisesta ja avoimen lähdekoodin oikeanlaisesta teknisestä integraatiosta muuhun koodiin.

Tässä artikkelissa keskitymme avoimeen lähdekoodiin liittyvään riskienhallintaan ja listaamme vinkit open source policy -toimintaperiaatteiden laatimiseksi. Avoimen lähdekoodin ohjelmistojen käyttöön liittyvistä eduista ja haasteista sekä avoimen lähdekoodin lisensseistä voit lukea tarkemmin aikaisemmasta artikkelistamme "[Avoin lähdekoodi – edut ja haitat](#)".

## Keinoja avoimeen lähdekoodiin liittyvään riskienhallintaan

Uhkakuvat omisteisten ohjelmistojen muuttumisesta tahdonvastaisesti avoimiksi voivat täysin aiheellisesti aiheuttaa yrityksissä huolta. Yrityksessä saatetaan myös pohtia vaikkapa komponenttien elinkaaren merkitystä ohjelmistokehitykseen tai koodissa olevan tietoturva-aukon muodostaman riskitilanteen ratkaisua.

Riskienhallintaan on onneksi olemassa keinoja, kuten soveltuvien lisenssien valinta, lisenssiehtojen kartoitus ja noudattaminen sekä kattavien avoimen lähdekoodin toimintaperiaatteiden laatiminen ja ylläpito.

### 1. Tietoturvariskit

On tärkeää kartoittaa ohjelmistokomponenttien haavoittuvuudet ja ymmärtää, mitä ne ovat. Haavoittuvat komponentit voivat altistaa yrityksen erilaisille kyberhyökkäyksille ja tietomurroille. Tästä syystä on olennaista seurata avoimen lähdekoodin komponenttien turvallisuutta ja varmistaa, että niihin liittyvät tietoturvakorjaukset päivitetään säännöllisesti.

### 2. Oikeudelliset riskit

Avoimen lähdekoodin lisenssit eivät ole keskenään samanlaisia, joten niiden suomat oikeudet ja velvollisuudet vaihtelevat merkittävästi. On kriittistä ymmärtää, mitkä lisenssit ovat käytössä ja vastaavatko ne ohjelmiston suunniteltua käyttöä. Copyleft-ehdot, kuten GPL-lisenssi, voivat edellyttää johdannaisteosten lähdekoodin julkaisua, mutta kaikissa tilanteissa tämä ei ole tarpeellista. Esimerkiksi, tietyissä erityistilanteissa GPL-lisenssi ei velvoita paljastamaan lähdekoodia, ja nämä poikkeukset yritysten on syytä selvittää erikseen. On myös tärkeää noudattaa lisenssiehtoja poistamatta lisenssitekstejä tai tekijänoikeusilmoituksia.

### 3. Operatiiviset riskit

Ohjelmiston tekninen toteutus vaikuttaa merkittävästi avoimen lähdekoodin komponenttien käyttöön, jolloin on suositeltavaa esimerkiksi ratkaista ajoissa mahdolliset kysymykset erilaisten komponenttien linkityksestä muuhun koodiin. On myös tärkeää seurata käytettävien koodiversioiden ikää ja arvioida niiden soveltuvuutta kokonaisuuteen. Käytettäessä valmiiksi käyttökelpoisia komponentteja, jotka voidaan integroida muuhun kokonaisuuteen ilman merkittäviä muutoksia, voidaan usein vähentää riskiä lähdekoodin julkaisovelvoitteista. Esimerkiksi käytettäessä tiettyä komponenttia sellaisenaan ilman muokkausta, ei synny johdannaistyötä, joka laukaisisi julkaisovelvoitteen.

Huolellisella suunnittelulla ja riskienhallinnalla voidaan hyödyntää avoimen lähdekoodin tarjoamia etuja samalla minimoiden siihen liittyvät riskit.

## Yrityksen avointa lähdekoodia koskevat open source policy -toimintaperiaatteet

Nykyään lienee pikemminkin sääntö kuin poikkeus, että ohjelmistokehitystä tekeville yrityksillä on olemassa avoimen lähdekoodin suhteen noudatettavia toimintaperiaatteita. Organisaatioiden avoimen lähdekoodin riskejä on helpompi hallita, kun avoimen lähdekoodin parissa työskentelevät ovat tietoisia yhteisistä pelisäännöistä. Periaatteet voivat koskea esimerkiksi tiettyjen lisenssien välttämistä tai sitä, kuka tekee lopulliset päätökset komponenttien käyttöönnotosta.

Hyvin hoidettu avoin lähdekoodi ja selkeät talon sisäiset pelisäännöt sen käytöstä, ns. open source policy, ovat keskeinen osa yrityksen avoimen lähdekoodin käyttöä koskevaa riskienhallintaa.

**Yritysten open source policyn laatimista helpottavia kysymyksiä ovat esimerkiksi:**

Sisäinen työnjako eri tahojen välillä

- Ketkä tekevät avointa lähdekoodia koskevia päätöksiä?
- Miten kommunikaatio, vastuukysymykset ja tehtävienjako yrityksen koodaajien ja juristien välillä toteutetaan avointa lähdekoodia koskevissa kysymyksissä?
- Kenellä on vastuu avoimen lähdekoodin käyttöä koskevasta ”kokonaiskuvasta”?

Käytössä olevat avoimen lähdekoodin lisenssit

- Onko organisaatiolla lista käytettävistä lisensseistä kokonaiskuvan ylläpitämiseksi, ottaen erityisesti huomioon vahvan copyleftin lisenssit?
- Onko organisaation listaan sisällytetty eri lisenssien keskeisimmät velvoitteet?

Avoimen lähdekoodin sallitut käyttötapaukset

- Milloin avointa lähdekoodia on sallittua hyödyntää ja milloin sen käyttö on ehdottomasti kielletty?

Lisenssiehtojen noudattaminen

- Kuinka organisaatioissa varmistetaan lisenssien vaatimuksenmukaisuus (compliance)?

Ohjeistukset yrityksen käyttämän skannaustyökalun käyttöä koskien

- Etenkin käytettäessä suuria määriä avoimen lähdekoodin komponentteja, on tavallista käyttää erilaisia skannaustyökaluja lisenssityyppien ja tekstien löytämiseksi koodipaketeista

Työntekijän avoimen lähdekoodin käyttö työtehtävien ulkopuolella

- Onko työntekijöille viestitty selkeästi, että yrityksen omaa koodia ei saa käyttää työntekijöiden vapaa-ajan projekteissa?

## Yrityksen muistilista

Yritysten on tärkeää kartoittaa ohjelmistokomponenttien haavoittuvuudet, ymmärtää eri lisenssien ehdot ja seurata käytettävien koodiversioiden ikää ja soveltuvuutta. Näin voidaan hallita riskejä ja varmistaa, että avoimen lähdekoodin komponentit eivät aiheuta turvallisuusuhkia, oikeudellisia ongelmia tai toiminnallisia haasteita.

Hyvin laaditut avoimen lähdekoodin toimintaperiaatteet auttavat hallitsemaan riskejä tehokkaasti. Periaatteet määrittelevät esimerkiksi tiettyjen lisenssien välttämisen, päätöksentekijät ja vastuukysymykset. Selkeät sisäiset pelisäännöt ja työnjako parantavat organisaation kykyä hyödyntää avointa lähdekoodia turvallisesti ja tehokkaasti.

Mikäli yrityksessä ei ole kattavaa tuntemusta aiheesta, harkitse asiantuntijoiden apua avoimen lähdekoodin toimintaperiaatteiden laatimisessa, lisenssivalinnassa ja lisenssiehtojen analysoinnissa. Asiantuntijat voivat auttaa minimoimaan avoimeen lähdekoodiin liittyviä riskejä ja varmistaa, että organisaatiot noudattavat kaikkia tarvittavia lisenssiehtoja.

Avustamme mielellämme asiakkaitamme open source -liitännäisissä kysymyksissä, mukaan lukien mahdollisissa tulkintakysymyksissä ja open source -toimintaperiaatteiden laatimisessa. Yritysten globaalina neuvonantajana meillä on runsaasti kokemusta avoimen lähdekoodin riskienhallinnasta ja siihen liittyvistä oikeudellisista kysymyksistä.

*Ota yhteyttä, niin voimme yhdessä etsiä ratkaisut avoimeen lähdekoodiin liittyviin kysymyksiinne.*

---

Services

Intellectual Property and Technology

---