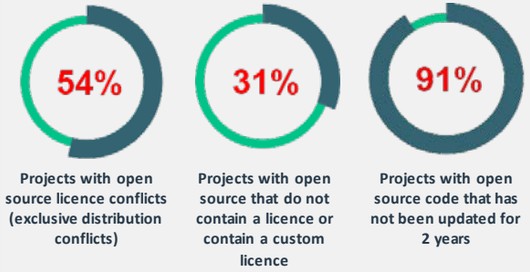
Your guide to OSS and the pitfalls to avoid

Your Pocket Roadmap:

TaylorWessing

Key Facts

- **Open Source Software** (**OSS**) saves your business time and money, enables interoperability of product platforms, and developers love it.
- ⚠ The Open Source Security and Risk Analysis Report shows **97%** of audited code contains open source.
- OSS used improperly it can be financially and operationally devastating.
- Some OSS can be restrictive and contain viral effects (Copyleft) which at their worst can lead to substantial damage to a company's goodwill and loss of IP rights held in your own software solution.



Projects with open source licence conflicts (exclusive distribution conflicts)

Projects with open source that do not contain a licence or contain a custom licence

Projects with open source code that has not been updated for 2 years

1

Is there OSS in your Product?

- Up to 70% of new software projects or software integrated into physical products depend on open source code. If your company is not monitoring your open source usage, you risk a range of legal liability, which could lead to loss of valuable IP and opportunities for bad actors.

TIP:
Implement an Open Source monitoring process and guidelines on the usage of Open Source.

2

Is there an approval process to help developers introduce new OSS?

- To keep up with the volume of OSS code and help maintain company policies while using OSS, work with your legal team to create an official approval process for contributing to OSS projects and using OSS in your projects.

3

Do you incorporate OSS Due Diligence into Vendor/Component Selection Process?

- Particularly when procuring software or components that will be material to a product, it is crucial to understand OSS exposure before commercialization of that product.

TIP:
When evaluating vendors, consider the company's OSS strategy as well as potential legal risks.

4

Can you easily audit dependencies, licences and other important information for the use of OSS?

- Ignoring potential licence risks only leads to future licensing issues. Although everything appears to be in order on the surface, investigating potential dependency issues is just as important as sanitized code.

TIP:
Automate compliance workflows by building in process gates with required statuses and other code checks.

5

Is your organization proactive or reactive in their OSS approach?

- Always be aware of where and how the organization is utilizing OSS, provide proactive guidance prior to OSS use, and conduct regular audits as part of proper IT hygiene. If you only consider this just before a transaction, it can be too late to address any issues.

TIP:
Build an iterative OSS process into product development cycle.

Do you have any questions?

Please do get in touch.

Mag. Erik Steiner
Senior Associate, Vienna
T: +43 1 716 55 0
E: e.steiner@taylorwessing.com

© Taylor Wessing 2023
This publication is not intended to constitute legal advice. Taylor Wessing entities operate under one brand but are legally distinct, either being or affiliated to a member of Taylor Wessing Verein. Taylor Wessing Verein does not itself provide services. Further information can be found on our regulatory page at www.taylorwessing.com/regulatory.