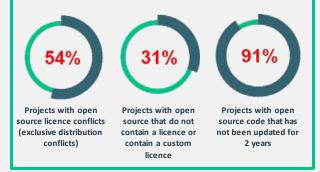
Your Pocket Roadmap:

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.



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, legal liability become Trojan horses of liability, which could lead to loss of valuable IP and opportunities for bad actors.

workflows by building

in process gates with

required statuses and

other code checks.

Implement an Open Source monitoring process and quidelines on the usage of Open

Source.

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.

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

 Ignoring potential license 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.

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

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

 Particular in the case of procuring software or components that will be material to a product, it is crucial to understand OSS exposure before commercialization of that product.



IP: Is your organization proactive or reactive in their OSS Automate compliance 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 before a need arises. If you only consider about this topic just before a transaction, it can be too late to address any issues, and it might give the impression that your company lacks sophistication. IIP:Build aniterative OSSprocess intoproductdevelopmentcycle.

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

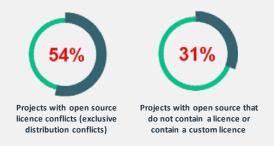
© Taylor Wessing 2023

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.



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, legal liability become Trojan horses of liability, which could lead to loss of valuable IP and opportunities for bad actors.

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

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.

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

 Ignoring potential license 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.

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

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

 Particular in the case of procuring software or components that will be material to a product, it is crucial to understand OSS exposure before commercialization of that product.



Is your organization proactive or reactive in their OSS

Automate compliance approach?

workflows by building in process gates with required statuses and other code checks. Always be aware of where and how the organization is utilizing

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 before a need arises. If you only consider about this topic just before a transaction, it can be too late to address any issues, and it might give the impression that your company lacks sophistication. IIP:Build aniterative OSSprocess intoproductdevelopmentcycle.

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

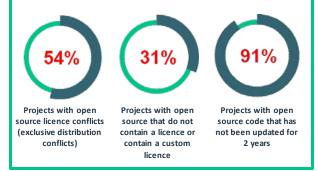
© Taylor Wessing 2023

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 2023 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.



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, legal liability become Trojan horses of liability, which could lead to loss of valuable IP and opportunities for bad actors.

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

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.

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

 Ignoring potential license 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.

workflows by building

in process gates with

required statuses and

other code checks.

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

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

 Particular in the case of procuring software or components that will be material to a product, it is crucial to understand OSS exposure before commercialization of that product.



TIP: Is your organization proactive or reactive in their OSS Automate compliance 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 before a need arises. If you only consider about this topic just before a transaction, it can be too late to address any issues, and it might give the impression that your company lacks sophistication. IIP:Build aniterative OSSprocess intoproductdevelopmentcycle.

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

© Taylor Wessing 2023