Understanding License Compatibility and Compliance Risks & Processes in Free and Open Source Software

Dr. Catharina Maracke

Software Compliance Academy

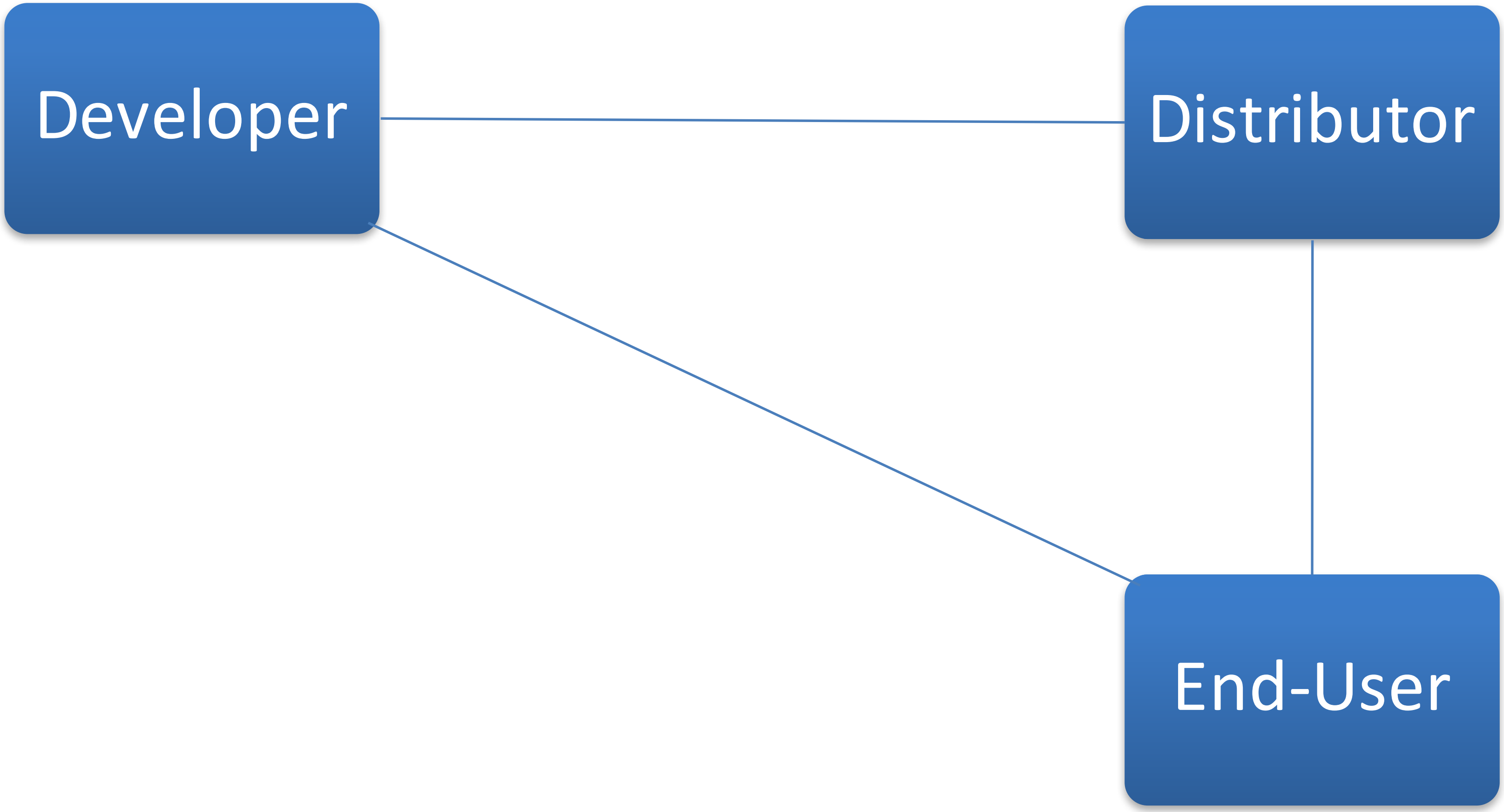
Agenda

1) Context: License Compatibility
2) Compliance Risks and Processes
3) OpenChain
4) Questions

Free and Open Source Software

- What is Free and Open Source Software?
- Four Freedoms!
- Definition?
  - Free Software http://www.gnu.org/philosophy/free-sw.en.html
  - Open Source Software https://opensource.org/osd-annotated

FOSS Licensing Model

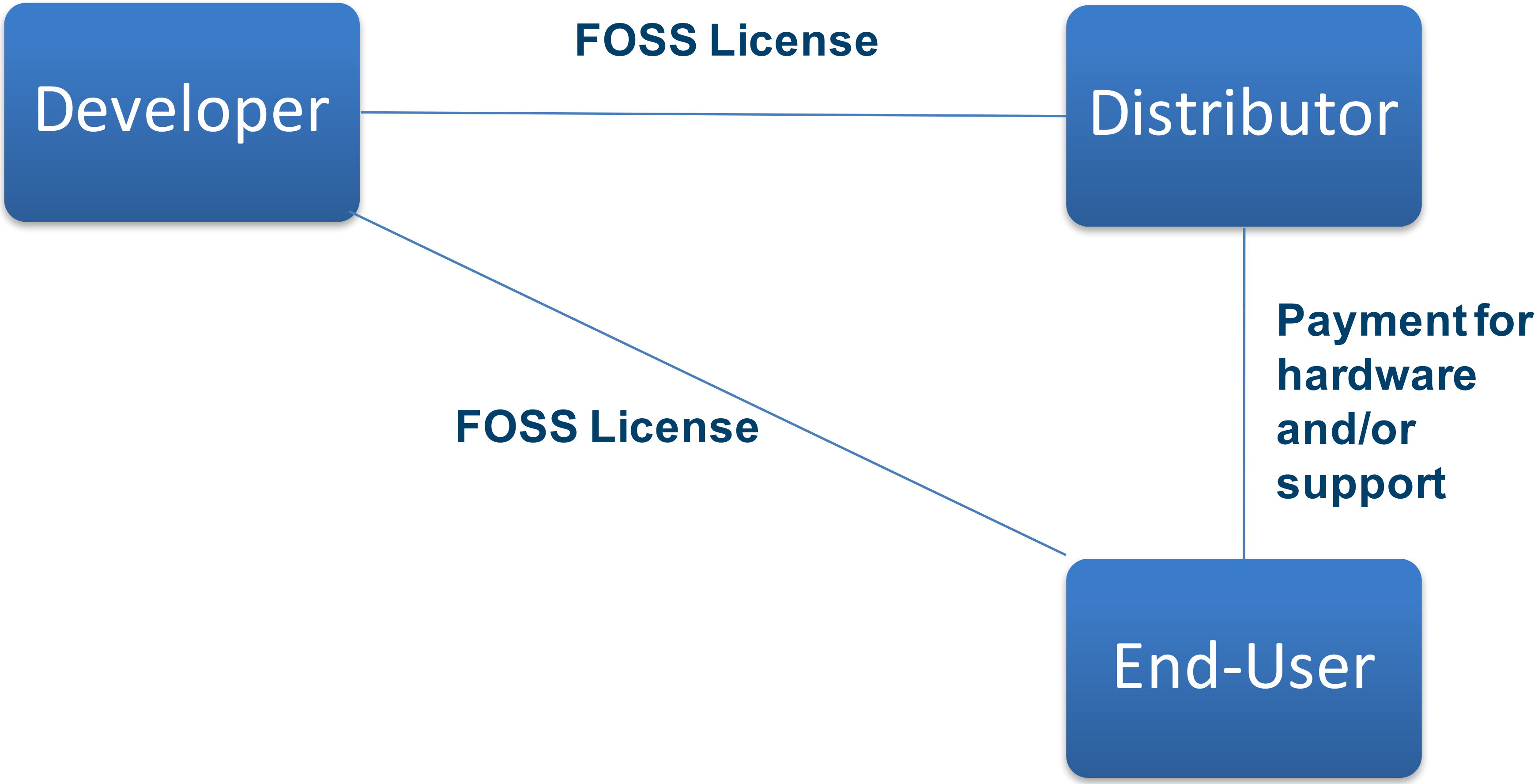


Developer

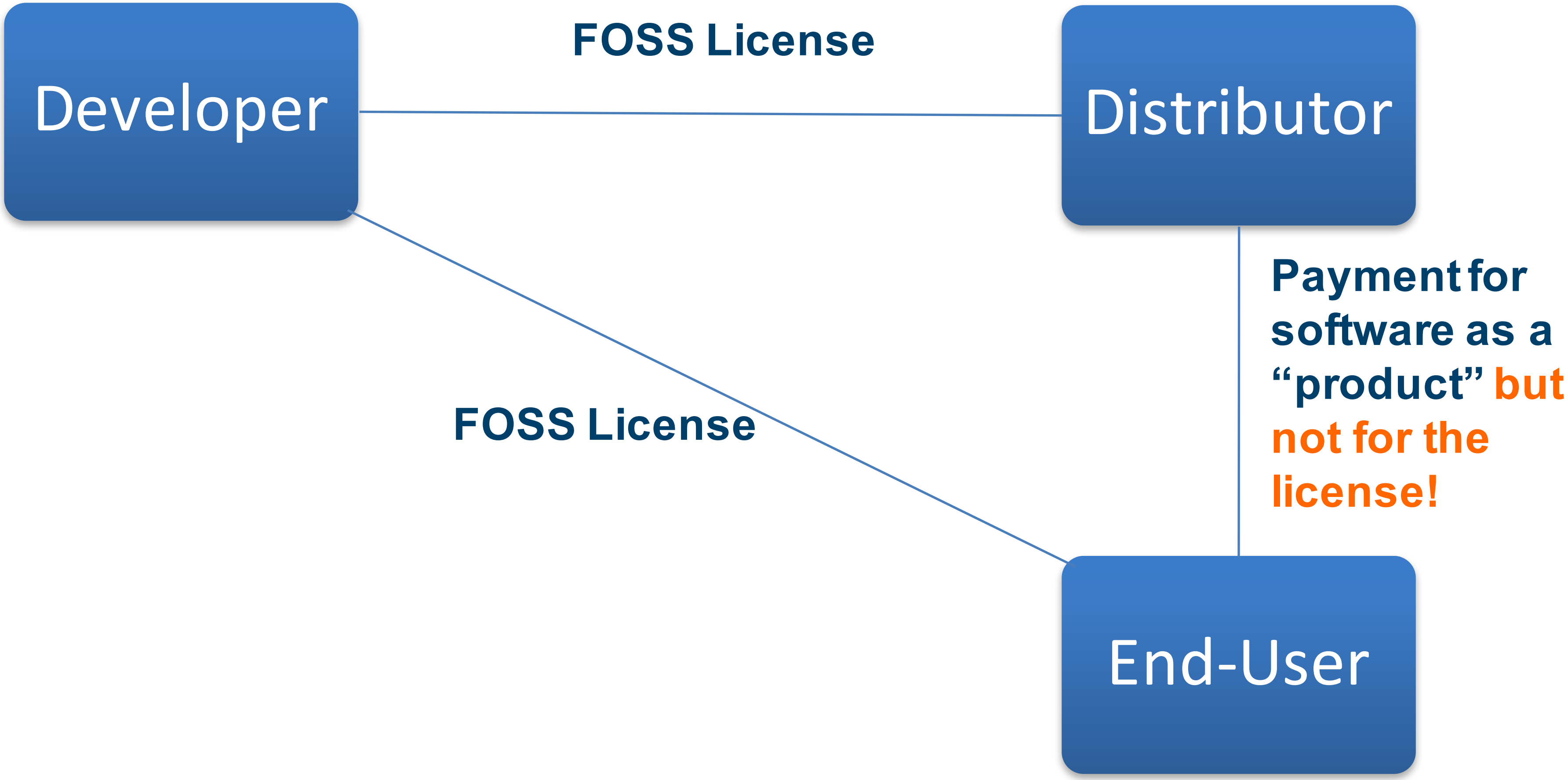
Distributor

End-User

FOSS Licensing Model



FOSS Licensing Model

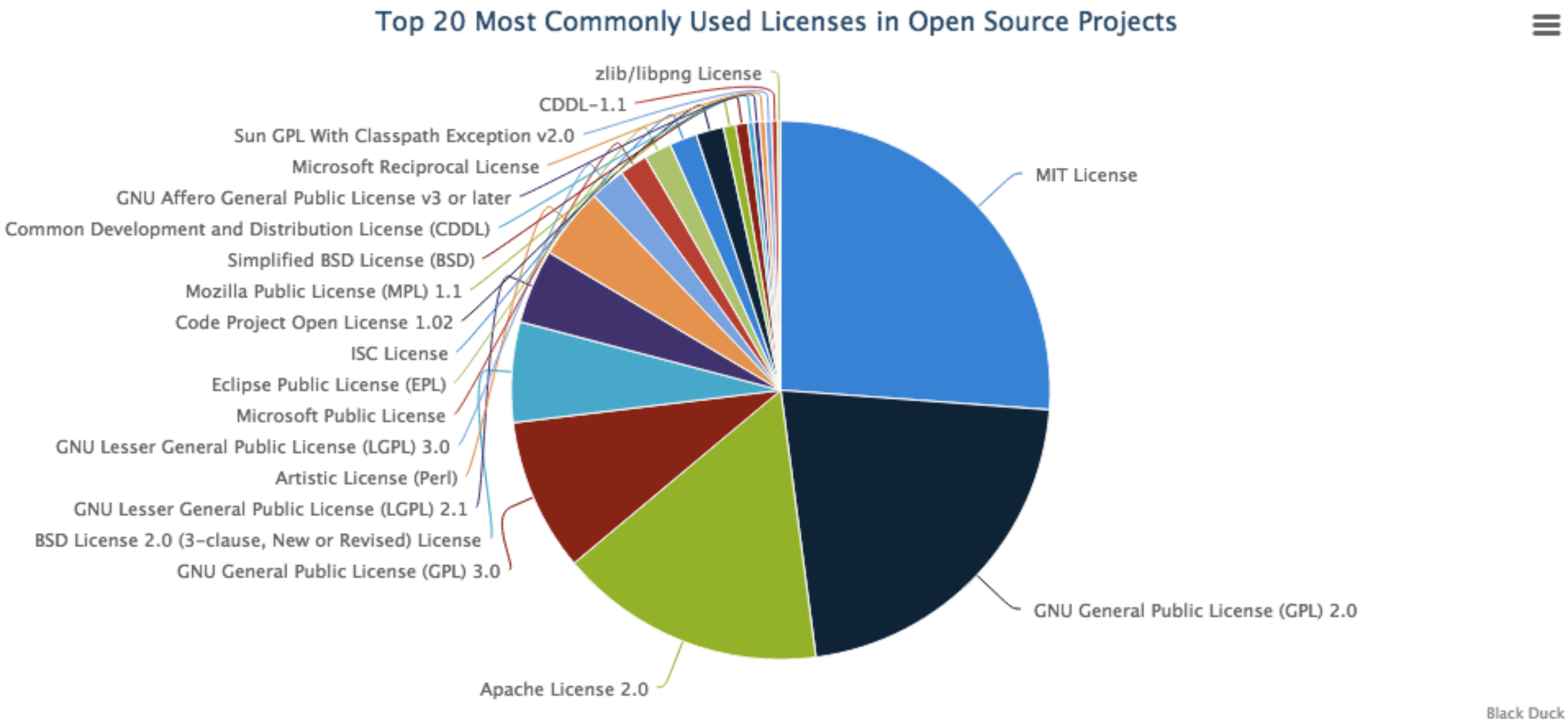


Developer
FOSS License
Distributor
Payment for software as a "product" but not for the license!
FOSS License
End-User

FOSS Licenses

- Different Free and Open Source Software licenses, e.g.
  - GPL
  - Apache
  - Mozilla Public License
  - BSD License
  - MIT License
  - …..
- Different versions, e.g.
  - GPL v. 2.0, GPL v. 3.0
  - Mozilla Public License v. 1, v. 1.1, v. 2

FOSS Licenses



https://www.blackducksoftware.com/top-20-open-source-licenses

License Categories

Strong Copyleft Licenses	Licenses with restricted Copyleft	Non-Copyleft (permissive) Licenses
GPL AGPL Eclipse Public License	LGPL Mozilla Public License Apple Public Source License	BSD License MIT License Apache License

Copyleft

„You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all parties under the terms of this license.“

Software Compliance

- Different Free and Open Source Software Licenses
  - Different license obligations!
  - Questions of interoperability!
- License violation?
  - Failure to observe license obligations
  - e.g. attribution, copyleft, etc.
- Legal Consequences?
  - Copyright infringement!
  - Legal action: Right holder's claims!
  - Management (personal) liability!

License Violation

- License violation?
- Legal consequences = Copyright infringement!
    - Sec. 97 et. seq. German Copyright Act
    - Example GPL v. 3: "*You may not propagate or modify a covered work except as expressly provided under this license. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License*
- Criminal and regulatory fine provisions, Sec. 106 et. seq. German Copyright Act

License Violation

- License violation?
- Legal consequences include:
  - Injunctive Relief
  - Removal / Recall
  - Right to Information
  - Damages and compensation
  - Reimbursement of costs
  - Source Code Release

Responsibility

- Compliance is a matter for the boss! Prominent case law includes:
  - Germany: Siemens, Volkswagen
  - US: In re Caremark International Inc.
  - Japan: Olympus, Daiwa Bank
- Management is responsible for a functioning compliance system
- Details and specific form of the compliance system depend on
  - Type, size, and organization of the company
  - Type of relevant laws and regulations
  - Geographical activities and representation
  - Grounds for suspicion / cases of non-compliance in the past

German (Stock) Corporation Act (AktG)

Art. 93 (Duty of Care and Responsibility of the Members of the Management Board)

(1) …….

(2) Members of the management board who violate their duties shall be jointly and severally liable to the company for any resulting damage. They shall bear the burden of proof in the event of a dispute as to whether or not they have employed the care of a diligent and conscientious manager.

German (Stock) Corporation Act

Art. 91 (Organization and Accounting)

(1) The management board shall ensure that the requisite books of account are maintained.

(2) The management board shall take suitable measures, in particular surveillance measures to ensure that developments threatening the continuation of the company are detected early.

German Act on Regulatory Offenses

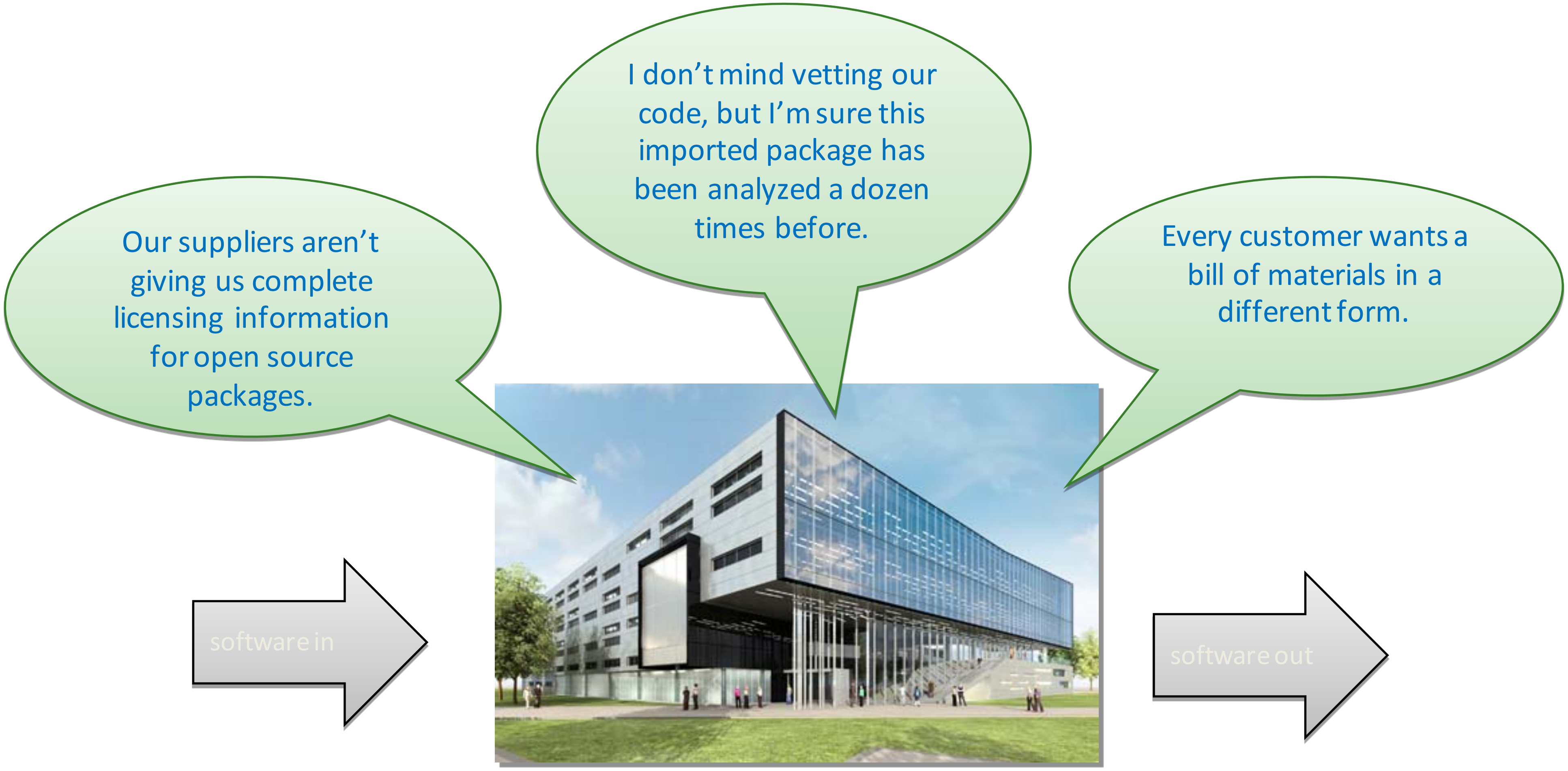
Sec. 130: Violation of Obligatory Supervision in Operations and Enterprises

(1) *Whoever, as the owner of an operation or undertaking, intentionally or negligently omits to take the supervisory measures required to prevent contraventions, within the operation or undertaking, of duties incumbent on the owner and the violation of which carries a criminal penalty or a regulatory fine, shall be deemed to have committed a regulatory offence in a case where such contravention has been committed as would have been prevented, or made much more difficult, if there had been proper supervision. The required supervisory measures shall also comprise appointment, careful selection and surveillance of supervisory personnel.*

(2) *.....*

(3) *Where the breach of duty carries a criminal penalty, the regulatory offence may carry a regulatory fine not exceeding one million….*

Software Compliance: Reality



Our suppliers aren't giving us complete licensing information for open source packages.

I don't mind vetting our code, but I'm sure this imported package has been analyzed a dozen times before.

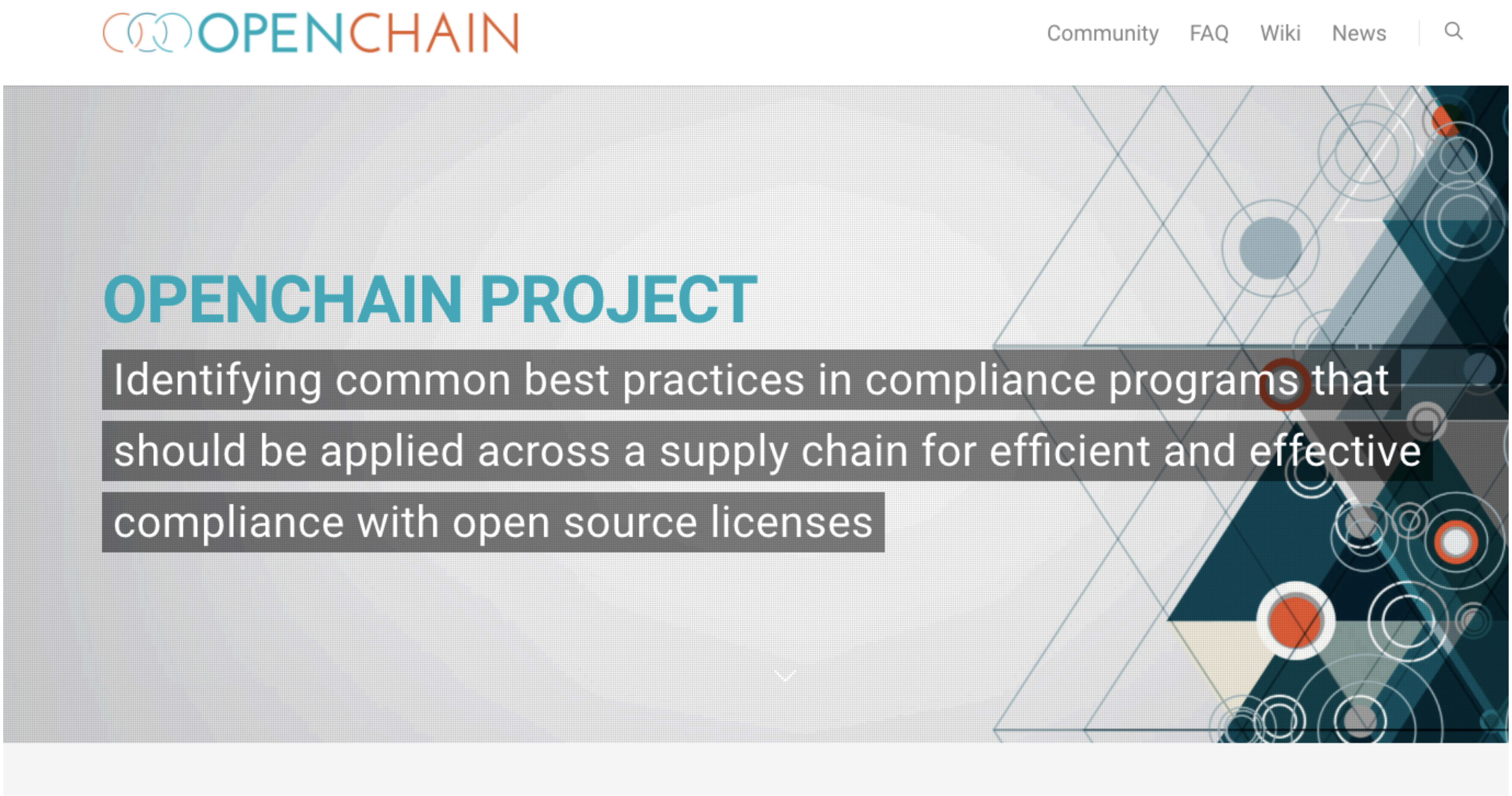
Every customer wants a bill of materials in a different form.

software in

software out

Software Compliance: Reality

- Current State of Software Compliance: High Transaction Costs
  - Process: Each company is re-creating essentially identical processes for open source compliance
  - Work Product: When code moves downstream, receiving company has to redo work, because
    - Can’t trust their results
    - Can’t assess their assumptions
    - Can’t share the data
    - Data not compatible – no standardized format available
- Standardization as one possible solution?



OPENCHAIN PROJECT

Identifying common best practices in compliance programs that should be applied across a supply chain for efficient and effective compliance with open source licenses

OpenChain

- OpenChain = new layer of trust in the FOSS ecosystem
- ISO 9000/9001-like conformity assessment standard
- Identify and consolidate common best practices in today's compliance programs to:
  - ✓increase efficiency and effectiveness
  - ✓increase transparency
  - ✓build trust
- Provide a reference model for the management of open source software within an organization based upon:
  - ✓reliable internal processes
  - ✓educated personal

OPENCHAIN

OpenChain

- Supply chain reference model including 6 Goals (G):
  - Know your FOSS responsibilities
  - Assign Responsibility for Achieving Compliance
  - Review and Approve FOSS Content
  - Deliver FOSS Content Documentation and Artifacts
  - Understand FOSS Community Engagement
  - Certify Adherence to OpenChain Requirements
- Each goal is defined by supporting practices (SP)
- Work and process is documented and discussed (CC0):
  - https://www.openchainproject.org/
  - https://wiki.linuxfoundation.org/openchain/start

OpenChain

Vision: A software supply chain where free/open source software (FOSS) is delivered with trusted and consistent compliance information.

Mission: Establish requirements to achieve effective management of free/open source software (FOSS) for software supply chain participants, such that the requirements and associated collateral are developed collaboratively and openly by representatives from the software supply chain, open source community, and academia.

OPENCHAIN

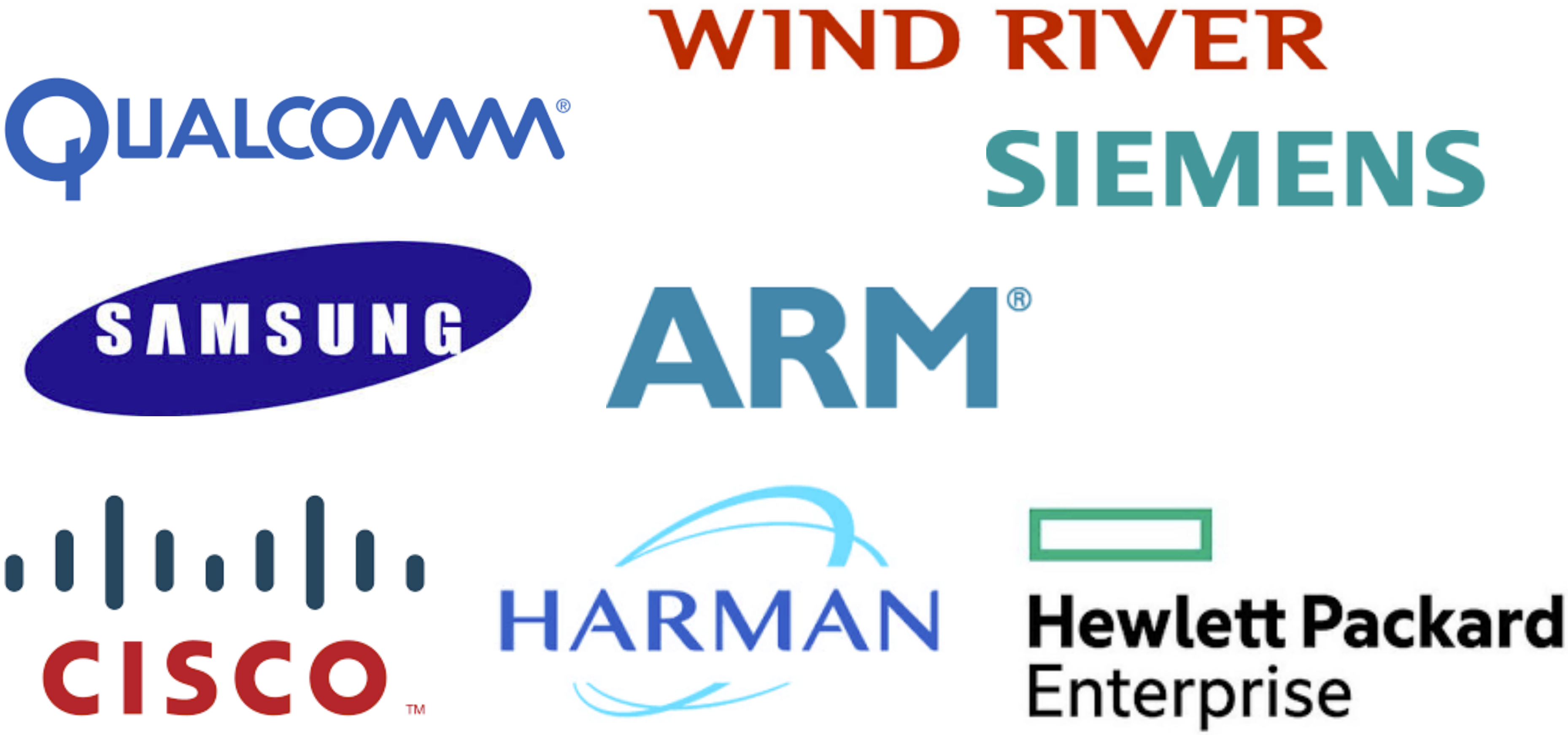
OpenChain: Work Groups

Specification: Version 1.0 launched and available via the OpenChain website. Comments and questions welcome!

Curriculum: Designed to help organizations meet the training and process requirements of the OpenChain specification. Details at https://wiki.linuxfoundation.org/openchain/curriculum

Conformance Check: Designed to assess an organization’s status of conformance with a specific version of the specification

Who is involved?



Self-Certification

- Gives an internal (biased?) view and assessment
- What requirements have to be satisfied for an organization to claim their process is OpenChain certified?
- Minimum Verification Artifacts – *current status of discussion!*
- Automated checklist?
- What happens in case of false statement?
  - Enforcement?
  - Future direction of the project?

Third-Party Certification

gives an external (independent) view and assessment – and documents the status of the relevant compliance system at a specific time!

internally

- helps identify issues and take necessary corrective action at an early stage
- if periodically done, shows internal development of compliance system and status

externally

- helps reporting to external partners and parties (business partners, shareholders, regulators)
- in case of a dispute, can serve as evidence of an appropriate compliance system!

Fundraising and Investment

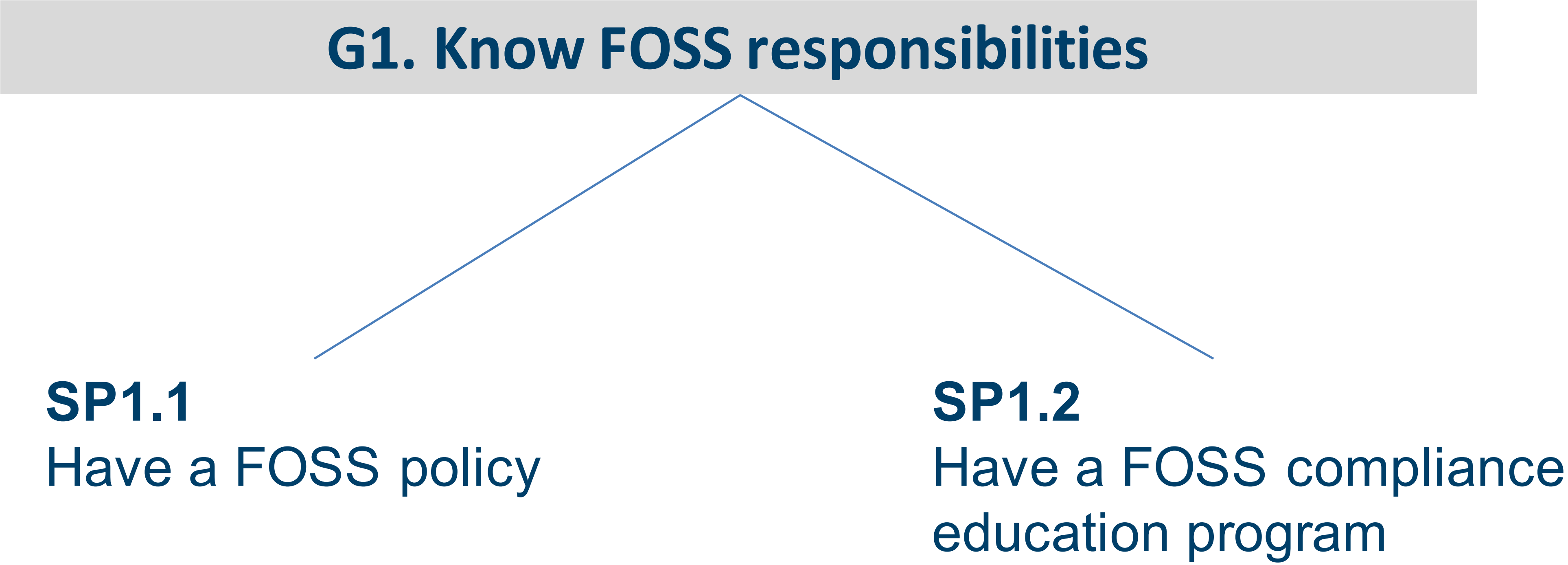
- Company and business assessment and valuation
- IP Portfolio?
  - Value in IP
  - Value in products built on top of it
- Due Diligence
  - Which licenses?
  - Compliance with license obligation?
  - Documentation / Certification?
  - What is the price for license violation (non-compliance)?
- Compliance is important!

Summary

- Different FOSS licenses raise questions of compatibility
- Understanding different FOSS licenses is important
  - Risk Management / Liability
  - Compliance
- OpenChain is a standard for governance, monitoring, and compliance across the software development lifecycle that provides a benchmark against which companies can measure their supplier.
- For questions, please contact cmaracke@scompliance.com

Appendix I

OPENCHAIN

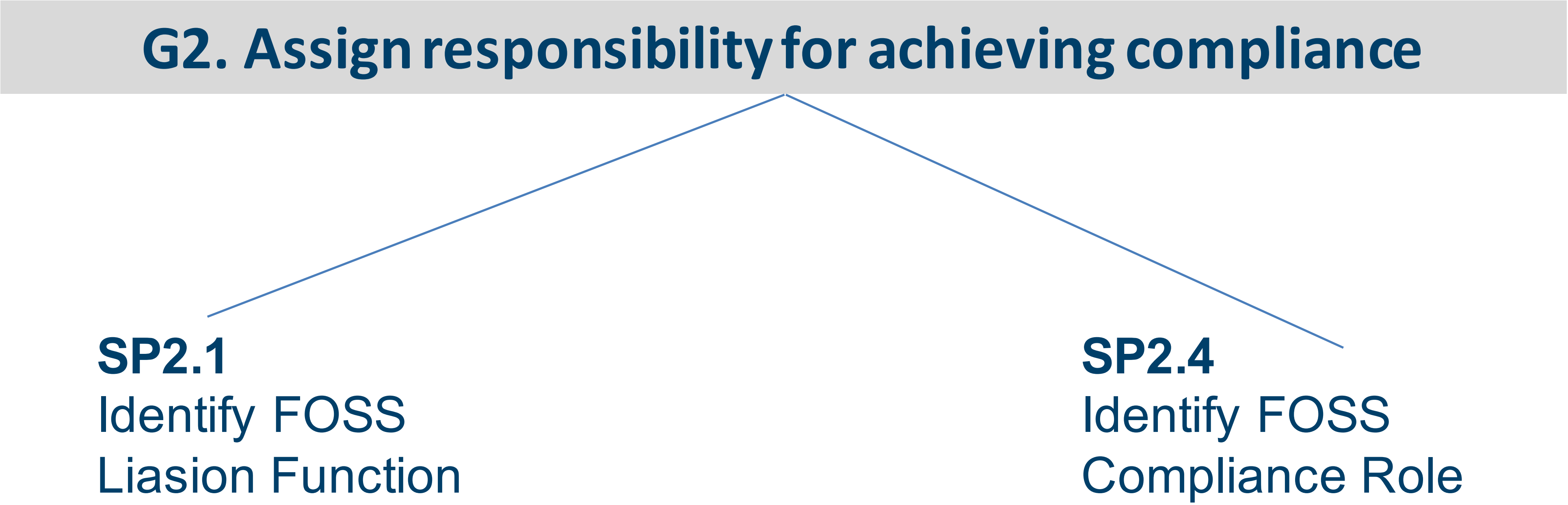


G1. Know FOSS responsibilities

SP1.1
Have a FOSS policy

SP1.2
Have a FOSS compliance education program

OPENCHAIN



G2. Assign responsibility for achieving compliance

SP2.1
Identify FOSS
Liasion Function

SP2.4
Identify FOSS
Compliance Role

OPENCHAIN

G3. Review and Approve FOSS Content

SP3.1
Have a FOSS review procedure that identifies, tracks and archives a list of all FOSS components and their respective identified licenses from which supplied software is comprised

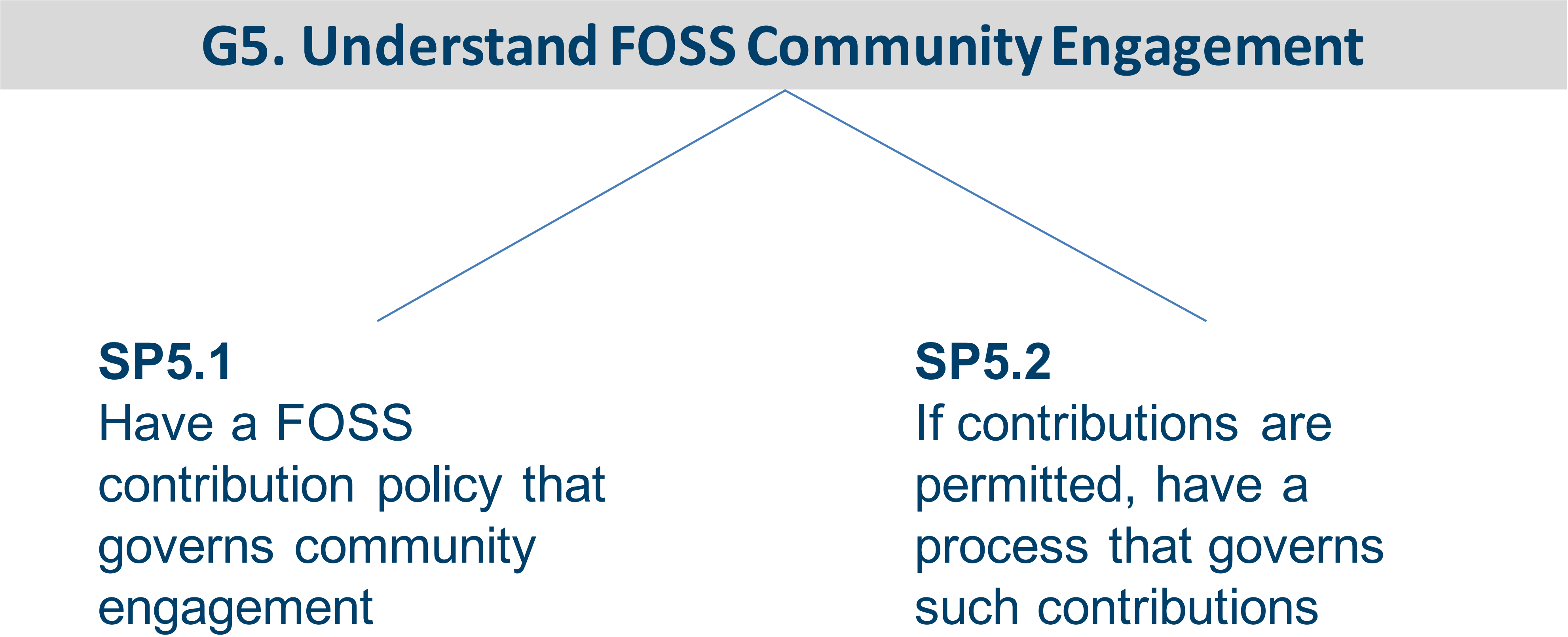
SP3.2
The FOSS review procedure must address the typical use cases that apply to that particular business

G4. Deliver FOSS Content Documentation and Artifacts

Prepare the following distributed compliance artifacts to accompany the supplied software as required by the corresponding identified licenses, including but not limited to:

- Copyright Notices
- Copies of Identified Licenses
- Modification Notifications
- Attribution Notices
- Prominent Notices
- Source Code Required Build Instructions and Scripts
- Written Offers

OPENCHAIN



G5. Understand FOSS Community Engagement

SP5.1
Have a FOSS contribution policy that governs community engagement

SP5.2
If contributions are permitted, have a process that governs such contributions

OPENCHAIN

G6. Certify Adherence to OpenChain Requirements

Affirm that your FOSS management program meets the criteria described in the OpenChain Conformance Specification (may require the completion of a checklist available at the OpenChain website)

Questions?

Thank You!

cmaracke@scompliance.com

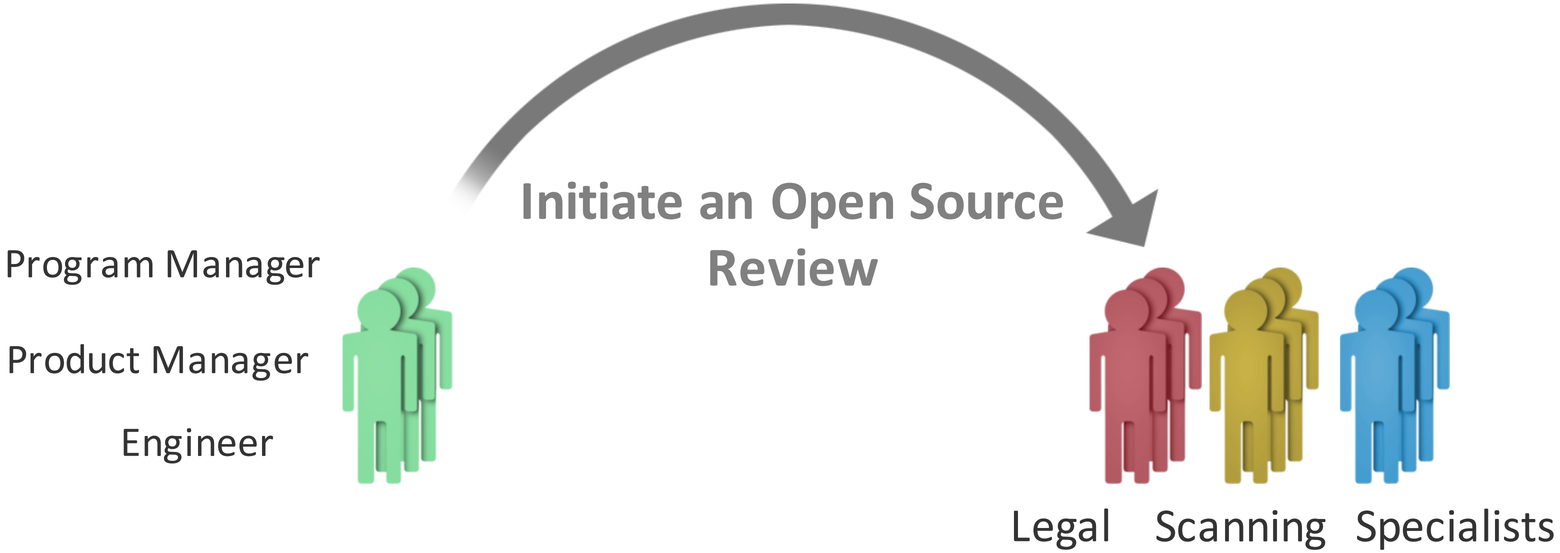
Appendix II

Thoughts and Materials

Further Thoughts

- Future Compliance Systems – Objectives and Goals?
  - Understanding different FOSS license obligations
  - Organizational aspects: Documentation and processes
  - Legal aspects: Analysis of license obligations, compatibility
  - Maintenance and Training
- What is the price?
  - What is the price for a sophisticated compliance system?
  - What is the price for license violation (non-compliance)
- How can we build an ecosystem of trust?
  - License enforcement?
  - Compliance!

Compliance Process: Example



Program Manager

Product Manager

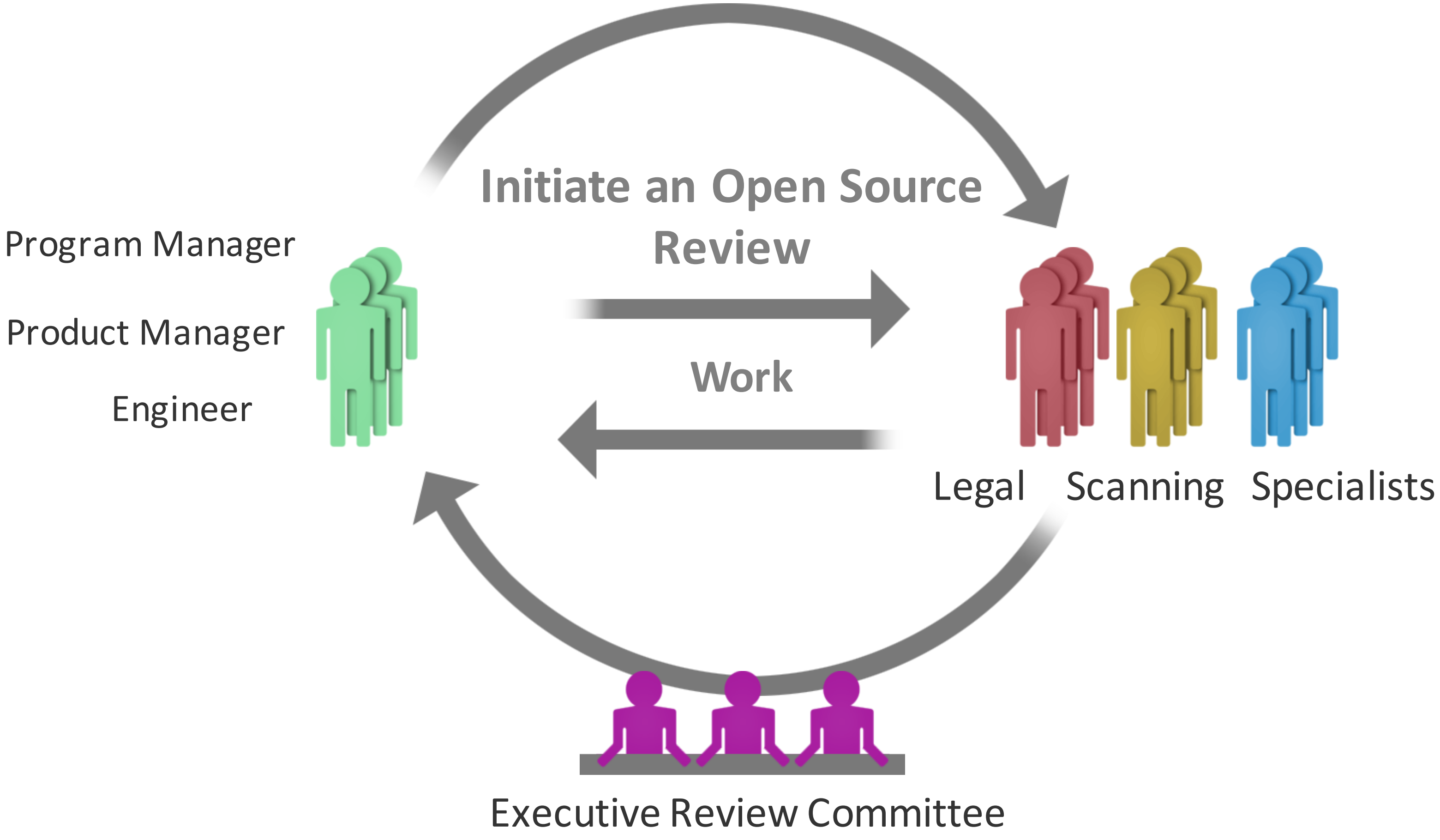
Engineer

Initiate an Open Source Review

Legal Scanning Specialists

What is it?
How do you want to use it?
Who gets it and how?

Compliance Process: Example



Initiate an Open Source Review

Work

Program Manager

Product Manager

Engineer

Legal Scanning Specialists

Executive Review Committee

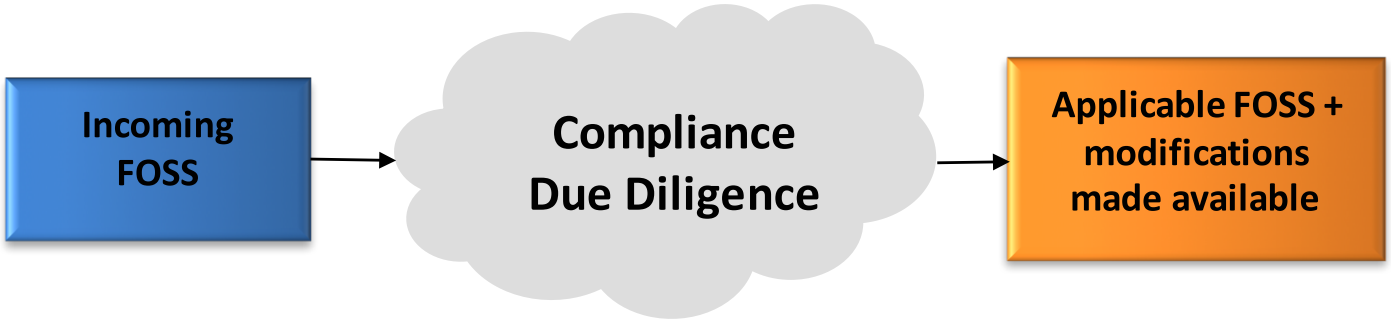
Introduction

- Compliance management consists of a set of actions that controls the intake and distribution of FOSS used in commercial products.

- The result of compliance due diligence is an identification of all FOSS used in the product and a plan to meet the FOSS license obligations.

Compliance End-to-End Process

- Compliance management activities provide a record of diligence with regard to the usage of FOSS and provide appropriate compliance records demonstrating the diligence process and allowing you to build a product map identifying all the software components of the product and their origin from an authorship and license perspective.



Links and Materials

- Copyelft and GPL Tutorial: https://copyleft.org/guide/
- SFLC Compliance Guide: https://www.softwarefreedom.org/resources/2014/SFLC-Guide_to_GPL_Compliance_2d_ed.html
- FSF FAQ: https://www.gnu.org/licenses/gpl-faq.en.html
- OpenChain FAQ: https://www.openchainproject.org/faq
- OpenChain Wiki: https://wiki.linuxfoundation.org/openchain/start

Contact

Software Compliance Academy

http://www.scompliance.com/

Office: office@scompliance.com

Dr. Catharina Maracke: cmaracke@scompliance.com