OPEN SOURCE
LEADERSHIP SUMMIT

INTRO TO SETTING UP A COMPLIANCE PROCESS IN YOUR ORGANIZATION

INDIRA BHATT, PRINCIPAL
GWYN FIRTH MURRAY, FOUNDER

THE LINUX FOUNDATION

Introductions | Indira Bhatt

Indira is currently an independent consultant, having worked previously as a manager in KPMG's San Francisco Advisory practice; with nearly 10 years of experience in the area of Free and Open Source Software (FOSS) due diligence. One of the original key members of the Palamida services team, over the years, Indira has led hundreds of OSS due diligence deals and helped various organizations successfully contribute code to the open source community. Indira is also a community representative for the Linux Foundations OpenChain Project and spearheaded the development of OpenChain's M&A checklist.

Introductions | Gwyn Murray

Gwyn Firth Murray, an “early adopter” in the legal community with respect to free and open source issues, is founder and principal of the Matau Legal Group. Matau Legal offers a broad range of commercial, licensing, and other legal services to both start-up and established companies in the high tech and biotech industries. Gwyn has worked as inside and outside counsel to computer hardware, computer software and pharmaceutical companies, including Apple, SGI, Alza Corporation, VA Linux Systems, and Kanisa, Inc. She has conducted her own law practice, dba Matau Legal Group, since 2002. Gwyn is a graduate of Stanford University Law School, and also holds an M.A. in Latin American Studies from Stanford University. She obtained her B.A. magna cum laude and with distinction in economics from Yale College.

Agenda

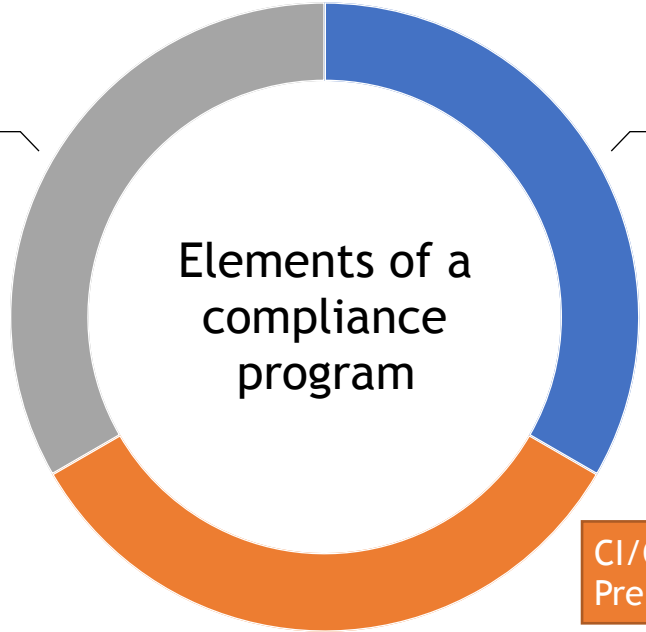
- Common issues and legal implications introduced by lack of an OSS compliance strategy
- Basic Components of setting up an OSS compliance program
- Compliance as seen in M&A
- Standards and first steps
- Q&A

- For an organization to use OSS effectively there needs to be a process around OSS intake, detection of licenses/ security issues, and remediation where action is necessary.
- Training of engineering / development teams is key.

Common Issues

- Lacking or inconsistent software intake process
- Lack of a mechanism for detection or tooling around OSS components
- License conflict and noncompliance
- Lack of ultimate project ownership and company wide governance policies (legal approval and rejection policies)
- Awareness around legal implications of these issues. . .

Elements of a compliance program



People

Developers
Legal
IT and OPS
Product Management
Sales, Support and Services

Process

Continuous scanning
Deep audits
Legal approval and rejection
Remediation
Governance framework and policies

Technology

CI/CD OSS Scan Tooling
Pre release Deep Scan OSS Audit Tooling

Basic steps to start creating a compliance program

- Management education and buy-in
- Gauging maturity by certification and checklists
- Defining developer education around OSS licensing. usage and modification
- Investing in OSS discovery tooling to create OSS bill of materials and notices across product lines
- Conducting legal reviews pre major release and defining the approval and rejection policies
- Gauging timelines for remediation and necessary patching

From the field: Compliance as seen in M&A

- Open Source code audits are performed as a standard
- Existing software bill of materials speed up deal closing
- Maturity around OSS usage or compliance processes is independent of company size
- Common issues found are improper use of components with strong copyleft or unknown licenses, unpatched security vulnerabilities, and ability to remediate quickly.

Standards

- Self certify with the OpenChain web app:
- https://www.openchainproject.org/conformance
- Use Checklists in and M&A non-M&A scenarios to gauge maturity:
- https://www.openchainproject.org/news/2019/01/16/openchain-ma-checklist-version-1-out-now
- Adopt SPDX standards: https://spdx.org/

Questions?
Thank you!

OPEN SOURCE
LEADERSHIP SUMMIT

Indira Bhatt
indira@tenthousandgiants.com
650-906-6042

Gwyn Firth Murray
gwyn@mataulegal.com
650-823-5864

THE LINUX FOUNDATION


OPEN SOURCE
LEADERSHIP SUMMIT
THE LINUX FOUNDATION