OPENCHAIN

10-01-2018

OpenChain Workgroup - The Linux Foundation

Antitrust Policy Notice

- Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

- Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

Onboarding Team

- Feedback from Vancouver conference = OpenChain promoters need answers and guidance for a range of questions
- Organized common questions posted to our promoters along the Path to Conformance
- Some questions need content sourced from other workteams
- Output
  - Additional FAQs for other workteams
  - New Onboarding materials

Path to Conformance:
1) Awareness of Open Source Compliance

- Open Source risks and obligations
  - What is the engineering, business and legal perspective on open source risks/obligations?
  - What risks are specific to export and security?
  - What open source issues arise in a supply chain?
  - What are social and PR risks?
  - How do we explain when ask about dollar-value risks?
  - How to deal with open source requests from community/enforcers?
- Why should my organization comply with Open Source obligations?
  - Is it only risk avoidance?
  - Benefits of community participation?
  - What are hidden costs of non-compliance?

Path to Conformance:
2) Awareness of Compliance Obligations (know what to do)

- What is OpenChain?
  - What are the benefits of OpenChain conformance?
  - What are the benefits of membership?
  - What problems does this solve?
- What are key elements of conformance (bill of materials, etc.)? I.e. what is the TLDR version of the spec (maybe something similar to CC description for licenses)
- Involvement in OpenChain
  - What are the costs of conformance?
  - What are the costs of the spec?
  - Free spec, self-certify… what's the catch? What's the value?
- How does conformance impact my business relationships?
  - Can anyone require conformance? (e.g. customers)
  - Why require partner organizations to conform?
- Are there downsides or risks of OpenChain conformance?

Path to Conformance:
3) Support to Implementing Conformance Processes

- Implementing OpenChain-conformant processes
  - How do I implement processes to reach OpenChain conformance?
  - How have others implemented processes?
- How do partner projects fit into conformance?
- Assessing current compliance status
  - What are my Open Source risks? How do assess risks within my organization?
  - How to do current assessment of processes? Where are my gaps?
- Implementing conformance processes
  - How to I prioritize implementing risk assessment and conformance processes?
  - Are there OpenChain reference implementations?
  - Can open source be tracked along with other third party software (commercial software)?
  - What are the details required for conformance (e.g., format of disclosures, public contacts, dealing with community requests/enforcement)?
  - What level of process is “good enough”?

Path to Conformance:
3) Support to Implementing Conformance Processes

- Operational questions
  - What happens when mistakes happen?
  - How do mergers affect my processes?
  - How to deal with enforcement?
  - How to deal with open source requests from community/enforcers?

Path to Conformance:
4) Support to Obtain OpenChain Conformance

- How do I obtain status as OpenChain conformant?
- How can I publicize conformance?
- Terminology – what does certification/conformance/compliance mean?
- Operational questions
  - Do I conform to a certain OpenChain specification version? What if the version changes?
  - Scope of conformance issue – help me understand if only part or my whole organization needs to be conformant?
  - How do mergers or mistakes impact conformance status?

Training Requirement

1.1 Competence

The organization shall:

a) Identify the roles and the corresponding responsibilities of those roles that affects the performance and effectiveness of the FOSS compliance program;
b) Determine the necessary competence of person(s) fulfilling each role
c) Ensure that these persons are competent on the basis of appropriate education, training, or experience;
d) Where applicable, take actions to acquire the necessary competence
e) Retain appropriate documented information as evidence of competence

1.2 Awareness

The organization shall ensure that persons doing work are aware of:

a) The FOSS policy;
b) Relevant FOSS objectives;
c) Their contribution to the effectiveness of the FOSS compliance program;
d) The implications of not conforming with the FOSS compliance program requirements;

Organization Scope

ISO 9001:2015 Spec

- Ensures higher quality product deliverables
- Certifies a product Quality Management System (QMS) [program]
- Does not prescribe the scope the QMS governs
- Organization is required to define document scope

OpenChain Spec

- Ensures higher quality compliance artifacts for software deliverables
- Certifies a Open Source compliance program
- ???

Thoughts?

Questions?