Conformance in Questions

Context

The OpenChain Project builds trust in open source by making open source license compliance simpler and more consistent. The OpenChain Specification defines a core set of requirements every quality compliance program must satisfy. The OpenChain Curriculum provides the educational foundation for open source processes and solutions, whilst meeting a key requirement of the OpenChain Specification. OpenChain Conformance allows organizations to display their adherence to these requirements. The result is that open source license compliance becomes more predictable, understandable and efficient for participants of the software supply chain.

This document contains a series of questions to determine whether a company is OpenChain Conformant. If each of these questions can be answered with a "yes" then that company meets all the requirements of conformance to the OpenChain Specification version 1.2. If any of the questions are answered with a "no" then the company can clearly identify where additional investment is needed to improve the compliance process.

G1: Know Your FOSS Responsibilities

Section	Number	Spec Ref	Question Text
G1: Know Your FOSS Responsibilities	1.a	1.1, 1.1.1	Do you have a documented policy that governs FOSS license compliance of the Supplied Software distribution (e.g., via training, internal wiki, or other practical communication method)?
G1: Know Your FOSS Responsibilities	1.b	1.1	Is the policy internally communicated?
G1: Know Your FOSS Responsibilities	1.c	1.1.2	Do you have a documented procedure that communicates the existence of the FOSS policy to all Software Staff?
G1: Know Your FOSS Responsibilities	1.d	1.2, 1.2.1	Do you have FOSS training materials (e.g., slide decks or online course) covering the following topics?
G1: Know Your FOSS Responsibilities	1.d.i	1.2	- The FOSS policy and where to find it,
G1: Know Your FOSS Responsibilities	1.d.ii	1.2	- Basics of Intellectual Property law pertaining to FOSS and FOSS licenses,
G1: Know Your FOSS Responsibilities	1.d.iii	1.2	- FOSS licensing concepts (including the concepts of permissive and copyleft licenses),
G1: Know Your FOSS Responsibilities	1.d.iv	1.2	- FOSS project licensing models,
G1: Know Your FOSS Responsibilities	1.d.v	1.2	- Software Staff roles and responsibilities pertaining to FOSS compliance specifically and the FOSS policy in general,
G1: Know Your FOSS Responsibilities	1.d.vi	1.2	- Process for identifying, recording and/or tracking of FOSS components contained in Supplied Software?
G1: Know Your FOSS Responsibilities	1.e	1.2.2	Do you track the completion of the training for all Software Staff?
G1: Know Your FOSS Responsibilities	1.f	1.2, 1.2.3	Have 85% or more of the Software Staff completed a FOSS training within the last 24 months?
G1: Know Your FOSS Responsibilities	1.g	1.3	Do you have a process for reviewing the Identified Licenses to determine the obligations, restrictions and rights granted by each license?
G1: Know Your FOSS Responsibilities	1.h	1.3.1	Do you have a documented procedure to review and document the obligations, restrictions and rights granted by each license?

G2: Assign Responsibility for Achieving Compliance

Section	Number	Spec Ref	Question Text
G2: Assign Responsibility for Achieving Compliance	2.a	2.1, 2.2.1	Have you assigned individual(s) responsible for receiving external FOSS compliance inquiries ("FOSS Liaison")?
G2: Assign Responsibility for Achieving Compliance	2.b	2.1.1	Is the FOSS Liaison function publicly identified (e.g. via an email address and/or the Linux Foundation's Open Compliance Directory)?
G2: Assign Responsibility for Achieving Compliance	2.c	2.1.2, 2.2.3	Do you have a documented procedure that assigns responsibility for receiving FOSS compliance inquiries?
G2: Assign Responsibility for Achieving Compliance	2.d	2.2.1	Have you assigned a person, group or function responsible for managing internal FOSS compliance? The FOSS Compliance role and FOSS Liaison can be the same individual.
G2: Assign Responsibility for Achieving Compliance	2.e	2.2.2	Is legal expertise pertaining to FOSS compliance accessible to the FOSS Compliance Role (e.g., internal or external)?
G2: Assign Responsibility for Achieving Compliance	2.f	2.2.3	Have you assigned responsibilities to develop and maintain FOSS compliance policy and processes?
G2: Assign Responsibility for Achieving Compliance	2.g	2.1.2, 2.2.4	Do you have a documented procedure for handling review and remediation of non-compliant cases?

G3: Review and Approve FOSS Content

Section	Number	Spec Ref	Question Text
G3: Review and Approve FOSS Content	3.a	3.1.1	Do you have a documented procedure for identifying, tracking and archiving information about the collection of FOSS components from which a Supplied Software release is comprised?
G3: Review and Approve FOSS Content	3.b	3.1.2	Do you have FOSS component records for each Supplied Software release which demonstrates the documented procedure was properly followed?
G3: Review and Approve FOSS Content	3.c	3.2.1	Have you implemented a procedure that handles at least the following common FOSS license use cases for the FOSS components of each supplied Supplied Software release?
G3: Review and Approve FOSS Content	3.c.i	3.2	- distributed in binary form;
G3: Review and Approve FOSS Content	3.c.ii	3.2	- distributed in source form;
G3: Review and Approve FOSS Content	3.c.iii	3.2	- integrated with other FOSS such that it may trigger copyleft obligations;
G3: Review and Approve FOSS Content	3.c.iv	3.2	- contains modified FOSS;
G3: Review and Approve FOSS Content	3.c.v	3.2	- contains FOSS or other software under an incompatible license interacting with other components within the Supplied Software;
G3: Review and Approve FOSS Content	3.c.vi	3.2	- contains FOSS with attribution requirements.

G4: Deliver FOSS Content Documentation and Artifacts

Section	Number	Spec Ref	Question Text
G4: Deliver FOSS Content Documentation and Artifacts	4.a	4.1.1	Do you have a documented procedure that describes a process that ensures the Compliance Artifacts are distributed with Supplied Software as required by the Identified Licenses?
G4: Deliver FOSS Content Documentation and Artifacts	4.b	4.1.2	Do you archive copies of the Compliance Artifacts of the Supplied Software?
G4: Deliver FOSS Content Documentation and Artifacts	4.c	4.1.2	Can you easily retrieve the archived copies of the Compliance Artifacts of the Supplied Software?
G4: Deliver FOSS Content Documentation and Artifacts	4.d	4.1.2	Are the copies of the Compliance Artifacts archived for at least as long as the Supplied Software is offered or as required by the Identified Licenses (whichever is longer)?

G5: Understand FOSS Community Engagement

Section	Number	Spec Ref	Question Text
G5: Understand FOSS Community Engagement	5.a	5.1	Do you have a policy to explicitly permit or forbid contributions of your employees to FOSS projects on behalf of the organization?
G5: Understand FOSS Community Engagement	5.b	5.1.1	Do you have a documented FOSS contribution policy?
G5: Understand FOSS Community Engagement	5.c	5.1.2	Is your Software Staff aware of the existence of the FOSS Contribution Policy (e.g. via training, internal wiki, or other practical communication method)?
G5: Understand FOSS Community Engagement	5.d	5.2.1	Provided the FOSS contribution policy permits contributions, do you have a documented procedure that describes the FOSS contribution process?