OPENCHAIN

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.

1. Program Foundation

Section	Number	Spec Ref	Question Text
1. Program Foundation	1.a	1.1, 1.1.1	Do you have a documented policy that governs open source license compliance of the Supplied Software distribution (e.g., via training, internal wiki, or other practical communication method)?
1. Program Foundation	1.b	1.1.2	Do you have a documented procedure that communicates the existence of the open source policy to all Software Staff?
1. Program Foundation	1.c	1.2.1	Have you identified the roles and the corresponding responsibilities that affect the performance and effectiveness of the Program?
1. Program Foundation	1.d	1.2, 1.2.2	Have you identified and documented the competencies required for each role?
1. Program Foundation	1.e	1.2, 1.2.3	Have you documented evidence of assessed competence for each Program participant?
1. Program Foundation	1.f	1.3, 1.3.1	Do you have evidence documenting the awareness of your personnel of the following topics?
1. Program Foundation	1.f.i	1.3	- The open source policy and where to find it,
1. Program Foundation	1.f.ii	1.3	- The relevant open source objectives,
1. Program Foundation	1.f.iii	1.3	- The contributions expected to ensure the effectiveness of the Program,
1. Program Foundation	1.f.iv	1.3	- The implications of failing to follow the Program requirements,
1. Program Foundation	1.g	1.4	Do you have a process for determining the scope of your Program?
1. Program Foundation	1.h	1.4.1	Do you have a written statement that clearly defines the scope and limits of the Program?

Section	Number	Spec Ref	Question Text
1. Program Foundation	1.i	1.5	Do you have a process for reviewing open source license obligations, restrictions and rights?
1. Program Foundation	1.j	1.5.1	Do you have a documented procedure to review and document the obligations, restrictions and rights?

2. Relevant Tasks Defined and Supported

Section	Number	Spec Ref	Question Text
2. Relevant Tasks Defined and Supported	2.a	2.1, 2.2.1	Have you assigned individual(s) responsible for receiving external open source compliance inquiries ("Open Source Liaison")?
2. Relevant Tasks Defined and Supported	2.b	2.1.1	Is the Open Source Liaison function publicly identified (e.g. via an email address and/or the Linux Foundation's Open Compliance Directory)?
2. Relevant Tasks Defined and Supported	2.c	2.1.2	Do you have a documented procedure that assigns responsibility for receiving and responding to open source compliance inquiries?
2. Relevant Tasks Defined and Supported	2.d	2.2.1	Have you documented the persons, group or function supporting the Program role(s) identified?
2. Relevant Tasks Defined and Supported	2.e	2.2.2	Have the identified Program roles been properly staffed and has adequate funding provided.?
2. Relevant Tasks Defined and Supported	2.f	2.2.3	Is legal expertise pertaining to internal and external open source compliance identified?
2. Relevant Tasks Defined and Supported	2.g	2.2.4	Do you have a documented procedure assigning internal responsibilities for Open Source compliance.
2. Relevant Tasks Defined and Supported	2.h	2.2.5	Do you have a documented procedure for handling review and remediation of non-compliant cases?

3 Open Source Content Review and Approval

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

4. Compliance Artifact Creation and Delivery

Section	Number	Spec Ref	Question Text
4. Compliance Artifact Creation and Delivery	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?
4. Compliance Artifact Creation and Delivery	4.b	4.1.2	Do you archive copies of the Compliance Artifacts of the Supplied Software?
4. Compliance Artifact Creation and Delivery	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)?

5. Understand Open Source Community Engagement

Section	Number	Spec Ref	Question Text
5. Understand Open Source Community Engagement	5.a	5.1	Do you have a policy that governs contributions to open source projects on behalf of the organization?
5. Understand Open Source Community Engagement	5.b	5.1.2	Do you have a documented procedure that governs Open Source contributions?
5. Understand Open Source Community Engagement	5.c	5.1.3	Do you have a documented procedure that makes all Software Staff aware of the existence of the Open Source contribution policy?

6. Adherence to the Specification Requirements

Section	Number	Spec Ref	Question Text
6. Adherence to the Specification Requirements	6.a	6.1.1	Do you have documentation confirming that your Program meets all the requirements of this specification?
6. Adherence to the Specification Requirements	6.b	6.2.1	Do you have documentation confirming that your Program conformance was reviewed within the last 18 months?