OPENCHAIN

Conformance in Questions

Context

The OpenChain Project builds trust in open source by making license compliance simpler and more consistent. It maintains the OpenChain Specification to define a core set of requirements every quality compliance program must satisfy. 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 has an OpenChain Conformant program. 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 2.1 (functionally identical to ISO/IEC DIS 5230:2020(e)). 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 governing the open source license compliance of the Supplied Software?
1. Program foundation	1.b	1.1, 1.1.2	Do you have a documented procedure to communicate the existence of the open source policy to all Software Staff
1. Program foundation	1.c	1.2, 1.2.1	Have you identified the roles and 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 the assessed competence for each Program participant?
1. Program foundation	1.f	1.3, 1.3.1	Have you documented the awareness of your Program participants on 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	- Relevant open source objectives;
1. Program foundation	1.f.iii	1.3	- 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, 1.4.1	Do you have a process for determining the scope of your Program?
1. Program foundation	1.h	1.4, 1.4.1	Do you have a written statement clearly defining the scope and limits of the Program?
1. Program foundation	1.i	1.5, 1.5.1	Do you have a documented procedure to review and document open source license 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) responsibility for receiving external open source compliance inquiries?
2. Relevant tasks defined and supported	2.b	2.1, 2.1.1	Is the external open source compliance contact publicly identified (e.g. via an email address or the Linux Foundation Open Compliance Directory)?
2. Relevant tasks defined and supported	2.c	2.1, 2.1.2	Do you have a documented procedure for receiving and responding to open source compliance inquiries?
2. Relevant tasks defined and supported	2.d	2.1, 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	2.1, 2.2.2	Have the identified Program roles been properly staffed and adequately funded?
2. Relevant tasks defined and supported	2.f	2.1, 2.2.3	Has legal expertise to address internal and external open source compliance been identified?
2. Relevant tasks defined and supported	2.g	2.1, 2.2.4	Do you have a documented procedure assigning internal responsibilities for open source compliance?
2. Relevant tasks defined and supported	2.h	2.1, 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, 3.1.1	Do you have a documented procedure for identifying, tracking and archiving information about the open source components in a Supplied Software release?
3 Open source content review and approval	3.b	3.1, 3.1.2	Do you have open source component records for the Supplied Software which demonstrate the documented procedure was properly followed?
3 Open source content review and approval	3.c	3.2, 3.2.1	Do you have a documented procedure that covers these common open source license use cases for open source components in the Supplied Software?
3 Open source content review and approval	3.c.i	3.2, 3.2.1	- Distribution in binary form;
3 Open source content review and approval	3.c.ii	3.2, 3.2.1	- Distribution in source form;
3 Open source content review and approval	3.c.iii	3.2, 3.2.1	- Integration with other open source that may trigger additional obligations;
3 Open source content review and approval	3.c.iv	3.2, 3.2.1	- Containing modified open source;
3 Open source content review and approval	3.c.v	3.2, 3.2.1	- Containing open source or other software under incompatible licenses for interaction with other components in the Supplied Software;
3 Open source content review and approval	3.c.vi	3.2, 3.2.1	- Containing 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, 4.1.1	Do you have a documented procedure describing the process for ensuring the Compliance Artifacts are distributed with Supplied Software as required by the Identified Licenses?
4. Compliance artifact creation and delivery	4.b	4.1, 4.1.2	Do you have a documented procedure for archiving copies of Compliance Artifacts for the Supplied Software?
4. Compliance artifact creation and delivery	4.c	4.1, 4.1.2	Are the Compliance Artifacts archived at least as long as the Supplied Software is offered and as required by the Identified Licenses?

5. Understanding open source community engagements

Section	Number	Spec Ref	Question Text
5. Understanding open source community engagements	5.a	5.1, 5.1.1	Do you have a policy for contribution to open source projects on behalf of the organization?
5. Understanding open source community engagements	5.b	5.1, 5.1.2	Do you have a documented procedure governing open source contributions?
5. Understanding open source community engagements	5.c	5.1, 5.1.3	Do you have a documented procedure for making all Software Staff aware 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, 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, 6.2.1	Do you have documentation confirming that your Program conformance was reviewed within the last 18 months?