Self-Certification Questionnaire

The Simple Way To Check
OpenChain ISO/IEC 5230:2020 Conformance

Revision 1
2021-11-26

Introduction

OpenChain ISO/IEC 5230:2020 is the International Standard for open source license compliance. It is simple, effective and suitable for companies of all sizes in all markets. This standard is openly developed by a vibrant user community and freely available to all. It is supported by extensive reference material and official service provider partners.

You can adopt OpenChain ISO/IEC 5230:2020 by self-certification in your own time or working with a service provider for independent assessment or third-party certification. Our recommended path is self-certification and we provide this questionnaire to support this with a series of "yes" or "no" questions.

We have a lot of resources to support you if you need assistance. You can join our mailing lists, our webinars, our group calls and our regional work groups to discuss challenges with your peers and in your native language. You can get started here:
https://www.openchainproject.org/community

As part of our online support you can also self-certify using our web app for free here:
https://certification.openchainproject.org/
We have a video discussing online self-certification here:
https://www.youtube.com/watch?v=lVM4RH8RRl0
Online self-certification is the same as this questionnaire. It is just another option.

Finally, if you want direct support from the project you can email info@openchainproject.org with questions. We provide support for free. The OpenChain Project is funded by our Platinum Members and is designed to help support the global supply chain transition to more effective and efficient open source license compliance.

Our Platinum Members

The Self-Certification Questionnaire

Section 1: Program foundation

- Do you have a documented policy governing the open source license compliance of the Supplied Software?
- Do you have a documented procedure to communicate the existence of the open source policy to all Software Staff
- Have you identified the roles and responsibilities that affect the performance and effectiveness of the Program?
- Have you identified and documented the competencies required for each role?
- Have you documented the assessed competence for each Program participant?

  Have you documented the awareness of your Program participants on the following topics?
  - The open source policy and where to find it;
  - Relevant open source objectives;
  - Contributions expected to ensure the effectiveness of the Program;
  - The implications of failing to follow the Program requirements.

- Do you have a process for determining the scope of your Program?
- Do you have a written statement clearly defining the scope and limits of the Program?
- Do you have a documented procedure to review and document open source license obligations, restrictions and rights?

Section 2: Relevant tasks defined and supported

- Have you assigned individual(s) responsibility for receiving external open source compliance inquiries?
- Is the external open source compliance contact publicly identified (e.g. via an email address or the Linux Foundation Open Compliance Directory)?
- Do you have a documented procedure for receiving and responding to open source compliance inquiries?
- Have you documented the persons, group or function supporting the Program role(s) identified?
- Have the identified Program roles been properly staffed and adequately funded?
- Has legal expertise to address internal and external open source compliance been identified?
- Do you have a documented procedure assigning internal responsibilities for open source compliance?
- Do you have a documented procedure for handling review and remediation of non-compliant cases?

Section 3: Open source content review and approval

- Do you have a documented procedure for identifying, tracking and archiving information about the open source components in a Supplied Software release?
- Do you have open source component records for the Supplied Software which demonstrate the documented procedure was properly followed?

    Do you have a documented procedure that covers these common open source license use cases for open source components in the Supplied Software?
    - Distribution in binary form;
    - Distribution in source form;
    - Integration with other open source that may trigger additional obligations;
    - Containing modified open source;
    - Containing open source or other software under incompatible licenses for interaction with other components in the Supplied Software;
    - Containing open source with attribution requirements.

Section 4: Compliance artifact creation and delivery

- 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?
- Do you have a documented procedure for archiving copies of Compliance Artifacts for the Supplied Software?
- Are the Compliance Artifacts archived at least as long as the Supplied Software is offered and as required by the Identified Licenses?

Section 5: Understanding open source community engagements

- Do you have a policy for contribution to open source projects on behalf of the organization?
- Do you have a documented procedure governing open source contributions?
- Do you have a documented procedure for making all Software Staff aware of the open source contribution policy?

Section 6: Adherence to the specification requirements

- Do you have documentation confirming that your Program meets all the requirements of this specification?
- Do you have documentation confirming that your Program conformance was reviewed within the last 18 months?