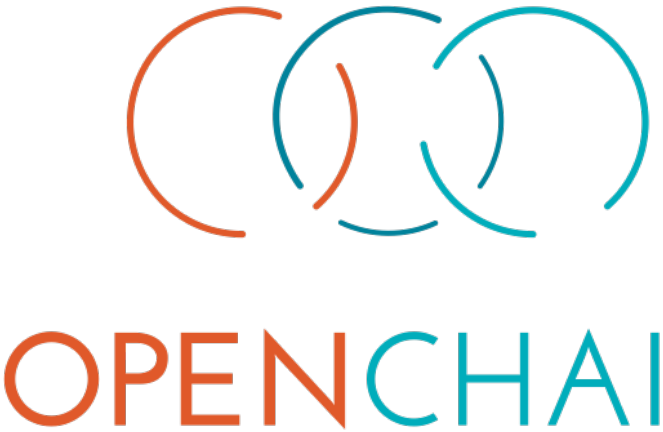


The OpenChain PlayBooks

Small Company

Non-Prescriptive Examples of
OpenChain ISO/IEC 5230:2020 implementation

Version 1

Introduction

The OpenChain PlayBooks are intended to help you understand the types of decisions made by managers in companies adopting OpenChain ISO/IEC 5230:2020. We cover examples of the decision-process in small, medium and large companies. Our examples are based on companies (a) in the technology industry, (b) in the middle of the supply chain and (c) shipping physical products containing software.

This may sound specific. However, the intention is to provide a thinking-tool for your company. Whether you are in the technology, finance, cloud, infrastructure or automotive industry (or any other), you will face similar challenges and solutions. The same applies whether you are in the middle of the supply chain or at its end, and whether you are shipping hardware or software. Our chosen examples cover a lot of ground.

There may be situations where you would like more examples for more specific industries. This is where the OpenChain Project community comes in. 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

Finally, this PlayBook contains an appendix with all the questions you need to answer to become OpenChain ISO/IEC 5230:2020 conformant. If you can answer all of these questions with “yes,” you have a conformant program. If you answer some of the questions with “no,” you know where to invest resources.

Small Company

Challenge Definition

1. We are a company that buys existing small-factor ARM boards that run Linux, and resell them in a custom housing, running an IoT edge application developed by us, built on Open Source components. Our challenge is to make this Open Source compliant and list all the used packages and licenses.

Our Challenge

- **Our customers now require us to provide a disclosure document of open source license compliance for our IoT product. We have limited staff, limited time and limited resources to address this issue, and several people are doing more than one job inside the company. Our approach needs to realistically reflect this.**

Current Situation

We currently have engineering resources using open source but no dedicated open source team or open source program. We are aware that certain key material is probably needed to ensure we manage open source effectively:

1. A **policy** (see Appendix 2) that encapsulates the company's strategy towards open source use.
2. A **process** or processes (see Appendix 3) to ensure the relevant teams understand the policy.
3. A **training** program (see Appendix 4) to ensure we can execute the policy.

We have

1. No formal/documented processes - our developers work well together and "know" the application well enough. Our CI/CD pipeline is automated, and its infrastructure-as-code configuration is effectively our process documentation.
2. No in-house legal staff. Our management team have contacts with local firms for accounting / employment / trademark law and other areas. No contact for open source compliance law yet.
3. No formal training material.
4. **No open source policy has been adopted yet, and we do not necessarily have the know how**
5. **No governance structures has been established yet**

The People Involved

Engineering and management staff (other personnel may be involved too).

Personas

The Senior Engineer

She has been working in this field for ten years and has been with this company for five years. She is experienced in developing proprietary software and has experience in using open source. While not an expert in open source licensing (or general licensing), she has basic knowledge regarding the obligations of key open source licenses and how they impact hardware distribution. This said, she is using “community knowledge” instead of deep personal expertise in the matter.

The Management Representative

They have been with this company for four years. Previously they were with a competing company for seven years. They have deep experience in product management but have largely relied on members of their teams or departments to deal with the details of software development and legal matters. They are aware that open source process management may need changing their level of involvement or adjustments in previously successful processes.

Planning Our Strategy

1. We will use OpenChain ISO/IEC 5230:2020 to guide our strategy. We will analyze our current internal operations and compare them against OpenChain ISO/IEC 5230:2020 to identify gaps.
2. We can make use of OpenChain Project recommended open source development and awareness training content/reference materials.
3. We can make use of community support and mentorship via the OpenChain Project community and other project communities. The best place to get started is here: https://www.openchainproject.org/get-started/participate

Executing Our Plan

Step 1

Form a virtual Open Source Program Office (OSPO), consisting of the Engineering and the Management Representative. Identify any other key figures who need (or want) to be involved, such as people from legal, procurement or sales. The goal of this step is to establish a virtual OSPO that will be responsible for completing the activity.

Step 2

Members of the virtual OSPO and other stakeholders decide an initial proposed scope for the program - in our case the software delivered in the IoT product. The goal of this step is to set the parameters for what the new OSPO will do.

Step 3

Members of the OSPO draft a written open source policy based on their understanding of the company's current operations and requirements. The goal of this step is to allow discovery of the current perspectives and potential solutions.

Step 4

Members of the OSPO compare the draft policy against the OpenChain self-certification questionnaire and identify any gaps between the policy and the ISO/IEC standard for open source license compliance. The goal of this step is to make sure the policy allows for a quality open source compliance program.

Step 5

Members of the OSPO create a plan to implement the policy in the company and socialize the adoption method and timescale within the company. The goal of this step is to prepare to apply the solution in production.

Step 6

Members of the OSPO apply the new company policy, including adoption of OpenChain ISO/IEC 5230:2020 via the self-certification questionnaire. The goal of this step is to execute company policy.

Step 7

Members of the OSPO establish processes to monitor open source packages and components, store the results of this monitoring and have a way to share the records of these results through Software Bill of Materials (SBOM). The goal of this step is to provide verification of the policy being implemented.

Notes

1. While going through the steps above we needed to make decisions about complexity of discussions, policy and processes.
2. Using examples from the OpenChain Project community we focused our decisions on the concept of Minimal Viable Product (MVP). We chose the simplest, shortest approach to addressing every challenge.
3. This allows us to get started quickly but does not prevent us from iterating and improving over time.
4. This offered the best balance of cost and benefit in managing open source processes.
5. For example, when it came to policy, we used the shortest policy possible based on existing reference material. In our case, we did this based on example policies provided by the OpenChain Project.
6. When it came to using an SBOM, we decided to use SPDX Lite. This was designed to help smaller suppliers get started with industry-standard SBOMs without using large amounts of company time.

7. When it came to using automation, we decided to engage with the OpenChain Reference Tooling Work Group to learn how to get started with minimal cost.
8. Our default stance was to seek help from the OpenChain Project community when we needed to work out the best way to approach these challenges. Learning from our peers was cheaper, faster and more effective than trying to solve things alone.

Periodic assessment

The OSPO schedules a review of the program every 18 months to ensure it maintains conformance with OpenChain ISO/IEC 5230:2020. This also meets one of the requirements of the standard.

The OSPO also schedules a review of current company processes every six months to help ensure everything is optimized. This review is based on, for example, reports from individual project managers about how **quick** and **effective** current processes are, and which current processes are **causing challenges** for the teams.

Appendix 1 - Self-Certification Questionnaire

Commented [1]: There are some comments about the self-certification and other appendices below. These will be addressed in editing cycles outside of the playbooks due to being sourced elsewhere in the OpenChain Project ecosystem.

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?

Commented [2]: I have to admit I find it a bit weird to require a process for determining scope. I realise this is how it's written in other OpenChain documents. I think this should be process/mechanism for reviewing and modifying scope.

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 internal and external open source compliance inquiries?
- Have you identified and documented the persons, group or function supporting the Program role(s)?
- 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?

Commented [3]: I suspect this is where barriers many come up (and its a bit late in this onboarding!). What if the company has some issues that are expensive/time consuming to address but are very low risk? Better to not be conformant to OpenChain?

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?

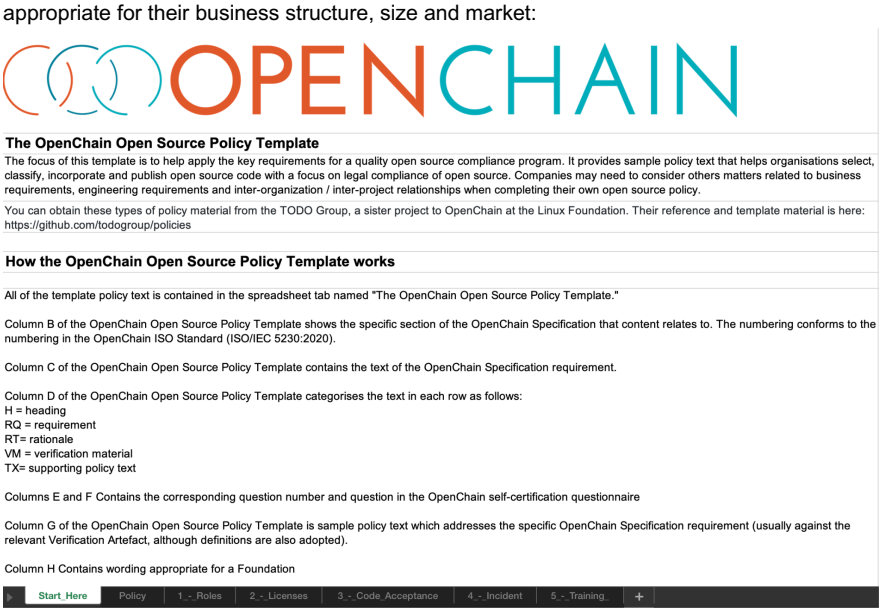
Section 6: Adherence to the specification requirements

- 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?

Appendix 2 - Policy Reference Material

Commented [4]: It would be great if someone could create a .doc or markdown version containing the "generic policy text" only as the spreadsheet looks a bit complex.

The OpenChain Project maintains a policy template to help companies create a policy appropriate for their business structure, size and market:



The OpenChain Open Source Policy Template

The focus of this template is to help apply the key requirements for a quality open source compliance program. It provides sample policy text that helps organisations select, classify, incorporate and publish open source code with a focus on legal compliance of open source. Companies may need to consider others matters related to business requirements, engineering requirements and inter-organization / inter-project relationships when completing their own open source policy.

You can obtain these types of policy material from the TODO Group, a sister project to OpenChain at the Linux Foundation. Their reference and template material is here: https://github.com/todogroup/policies

How the OpenChain Open Source Policy Template works

All of the template policy text is contained in the spreadsheet tab named "The OpenChain Open Source Policy Template."

Column B of the OpenChain Open Source Policy Template shows the specific section of the OpenChain Specification that content relates to. The numbering conforms to the numbering in the OpenChain ISO Standard (ISO/IEC 5230:2020).

Column C of the OpenChain Open Source Policy Template contains the text of the OpenChain Specification requirement.

Column D of the OpenChain Open Source Policy Template categorises the text in each row as follows:
H = heading
RQ = requirement
RT= rationale
VM = verification material
TX= supporting policy text

Columns E and F Contains the corresponding question number and question in the OpenChain self-certification questionnaire

Column G of the OpenChain Open Source Policy Template is sample policy text which addresses the specific OpenChain Specification requirement (usually against the relevant Verification Artefact, although definitions are also adopted).

Column H Contains wording appropriate for a Foundation

Start_Here | Policy | 1_-_Roles | 2_-_Licenses | 3_-_Code_Acceptance | 4_-_Incident | 5_-_Training_ | +

You can get it from this link:
https://github.com/OpenChain-Project/Reference-Material/tree/master/Open-Source-Policy/Official/2.1/en

Appendix 3 - Process Reference Material

There is a large amount of example process material available through the OpenChain Project reference library:
https://github.com/OpenChain-Project/Reference-Material

For example, there are various checklists:
https://github.com/OpenChain-Project/Reference-Material/tree/master/Checklists/Official

There are also flowcharts showing some compliance workflows:
https://github.com/OpenChain-Project/Reference-Material/tree/master/Flowcharts/Official/2.0/en

Because of the wealth of options regarding open source license compliance process management, the material cited above is intended for reference in inspiration rather than to be prescriptive.

Appendix 4 - Training Reference Material

There are various approaches to training (slides, online course, etc), and different companies have different requirements. However, we have a few suggested resources to get you started.

Firstly, there are reference training slides and reference automation slides available from the OpenChain Project:

https://github.com/OpenChain-Project/Reference-Material/tree/master/Training-Slides/Official/2.1/en

Secondly, the OpenChain Project and LF Training have released two courses with completion badges on the LF Training platform: