OPENCHAIN

The OpenChain PlayBooks

Medium 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 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.

Medium Company

Challenge Definition

The situation is that we need to ship a motherboard for an embedded system. It contains the Linux kernel. Our company faces one or more of three common organizational challenges:

1. Our engineers wish to use open source. This bottom-up approach requires persuading top management open source is the most effective way to accomplish goals.
2. Our customers may require us to be license compliant. This is the inverse of the first challenge and requires top management to "sell" the idea to project teams.
3. Our partners or investors require the company to have solid open source licensing approaches to obtain or continue investment. This is another top-down situation.

Our Challenge

- **Our customers may require us to be license compliant.**

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

We have

1. A policy that includes a "permitted list" of projects we are comfortable with and a "denied list" of licenses we are not comfortable with.
2. Some processes focused on engineering teams using the policy.
3. A recurring training program for engineers known to be working on open source.

The People Involved

Senior engineering, legal and management staff.

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 Legal Expert

He has been working in the field of software licensing for eight years and has always worked at this company. He is experienced in other areas of law too, particularly related to trademarks. He has limited experience in open source licensing and has relied on the engineering department to understand market norms. He has spent some time reading open source licenses, interpreting them and seeking to reconcile his interpretation with online resources. The match has not always been perfect.

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

We will use the OpenChain self-certification questionnaire as a way to check our current status versus the status required for OpenChain ISO/IEC 5230:2020 self-certification. This involves understanding the:

1. Current policy for managing decisions around open source (and other) software.
2. Current processes being used for managing open source (and other) software.
3. Current records showing the usage of this software over the previous year.

Executing Our Plan

Step 1

A virtual open source program office (OSPO) is established with one senior engineer, one legal expert and one management representative. Initial tasks are split between the team members as follows:

1. The senior engineer checks the engineer department’s current policy, processes and records for managing open source (and other) software. She has permission to approach individual project managers to conduct this assessment.
2. The legal expert checks the legal department’s current policy, processes and records for managing open source (and other) software. He has permission to approach individual legal managers to conduct this assessment.
3. The management representative checks what policy and guidance is possessed in the executive team for managing open source (and other) software. They have permission to approach individual executives to conduct this assessment.

Step 2

The virtual OSPO has a meeting to review the results of Step 1. The goals are:

1. To see if each department has policy, processes and records regarding open source (and other) software.
2. To see if the existing policy, processes and records from each department match each other or are compatible with each other.
3. To make a combined report showing how consistent the policy, processes and records are in the company.

Step 3

If the results of Step 2 show that existing processes are consistent throughout the company then the OSPO activity can process to Step 4. If the existing processes are not consistent throughout the company, the OSPO prepares an initial advisory to management to align processes using OpenChain ISO/IEC 5230:2020. When permission is granted they proceed to Step 4.

Step 4

The senior engineer obtains the OpenChain ISO/IEC 5230:2020 self-certification questionnaire (See Appendix 1) and distributes it to other members of the OSPO. They hold a round-table meeting and:

1. The senior engineer checks the engineer department's current policy, processes and records for alignment with the OpenChain ISO/IEC 5230:2020 self-certification questionnaire.
2. The legal expert checks the legal department's current policy, processes and records for alignment with the OpenChain ISO/IEC 5230:2020 self-certification questionnaire.
3. The management representative checks what policy and guidance is possessed in the executive team for alignment with the OpenChain ISO/IEC 5230:2020 self-certification questionnaire.
4. They share findings in an active manner to create a list of suggestions for:
    a. Aligning all the processes across departments with OpenChain ISO/IEC 5230:2020.
    b. And doing this using the OpenChain ISO/IEC 5230:2020 self-certification questionnaire.

Step 5

The OSPO prepares a report outlining to management how to align processes using OpenChain ISO/IEC 5230:2020. When the OSPO receives permission from management to proceed according to the recommendations from the report they proceed to write:

1. A document for the engineering department explaining what policy, processes and training needs to be undertaken and a timeline for implementation.
2. A document for the legal department explaining what policy, processes and training needs to be undertaken and a timeline for implementation.
3. A document for the management team explaining what policy, processes and training needs to be undertaken and a timeline for implementation.

NOTE: It is recommended that these documents be as short and as simple as possible. Unless the company already has sophisticated processes in place the company can build the compliance program over time. It is far better to have something basic that can be implemented soon rather than something perfect that will take too long to implement.

Step 6

The OSPO holds meetings during the midpoint and the endpoint of the timelines for implementation in each department. The goals are:

1. To support and encourage each department in the execution of the plan with the combined experience of the OSPO members.
2. To keep the management team informed of progress and to adjust timescales as necessary to ensure success.

Reviewing Our Results

When each department reports their activity is complete, the OSPO has a special workshop to review the results against OpenChain ISO/IEC 5230:2020 self-certification questionnaire.

1. If the results match the questionnaire the OSPO team members create a report to management explaining that self-certification conformance is complete.
2. If the results do not match the questionnaire the OSPO team members return to Step 6 and help the relevant department complete their work.

Periodic Reassessment

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 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

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 internal and external 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?