IAM

Efficient IP management in a market increasingly using open source

Eleftheria Stefanaki and Jimmy Ahlberg

17 May 2023

Shutterstock/klss

- Open source is often entangled with IP rights such as copyright, trade secrets, trademarks, and patents
- It crucial to identify open source components and subcomponents as well as the licences they carry
- The OpenChain Project is an international community of companies, dedicated to optimising compliance

Imagine finding out that 90% of the software in your products is not yours but only licensed in as third-party IP. As soon as you start reading the agreements, you realise some of them contain terms you are not familiar with or have never even heard of before, such as “source code”, “binary”, “object code”, and “system libraries”. Moreover, you cannot find basic contractual provisions such as “governing law” or “jurisdiction” in the agreements. These agreements (and there are hundreds of them) are all different, non-negotiable, ‘take-it-or-leave-it’ standard template licences.

After this unsettling discovery, your journey may look something like this: Firstly, you tell yourself that the above cannot be true (denial). Later on, you rightly become angry: “Surely someone must be responsible for this”. So, you take the elevator down to the software development team to read them the riot act (anger). Once there, you beg them – please! – stop bringing in all this third-party IP under these strange software licences (bargaining). If you are not outright laughed out of the room, they will reply that this is not going to happen if the company wants to continue to ship any products at all. You go back to your office, perhaps passing by the coffee machine, dejectedly thinking that “at least the coffee machine people do not have to deal with this issue” (depression). You would be wrong though, since the coffee machine uses the same kind of third-party IP under the same kind of licences as whatever product your company develops. Hopefully, you will eventually come out on the other side, realising that you must manage this strange third-party IP dependency. You just need to be smart about it and come up with the right tools, processes, and strategies to do so (acceptance)! We are here of course talking about open source, and you have just passed the five stages of - open source - grief.

The term ‘open source’ refers to software available under an **open source** licence, usually royalty free distribution, use and modification. Most of the applications that run in our smartphone or computer contain some **open source**. Even things we do not think about as being particularly “open”, such as our smart washing machines, our home automation systems, or for that matter, parts of the telecom infrastructure equipment handled by carriers, are built upon **open source** software. In **fact, we** guarantee that you are using open source software for reading this article right now.

Companies face major dependencies on third-party IP because of using **open source** in their products. The reason is that, regardless of the industry they are active in, there are few products or value chains that do not incorporate any software elements. For this reason, open source, more often than not, is entangled with IP rights such as copyright, trade secrets, trademarks, and patents.

Consequently, to succeed in the market, companies must address their **open source** dependency, not only from a technology, security and trade compliance perspectives, but also as an IP management issue. Surprisingly, few companies are well prepared for this.

Against this background, this article describes the significance of open source management in the context of IP management. We would like to introduce you to the **OpenChain Specification 2.1** (ISO/IEC 5230:2020) on **open source** licence compliance, and the benefits of implementing such a programme within the framework of your existing IP management.

Omnipresence of open source and subsequent risks

In its **2022 OSSRA report**, **Synopsis** found that, of the 2,409 **codebases** it audited for the purposes of the report, 97% contained open source. In the same report, it was revealed that among 17 industry sectors, such as energy and computer hardware, the presence of open source in their codebases was between 93% and 100%. **Due to the undeniable value and usefulness of open source solutions**, their uncontrollable diffusion raises concerns regarding security and licence compliance.

'Escaping' the use of ready-made **open source** components is neither possible nor desirable. To accomplish such an endeavour, a company would need to develop proprietary software solutions with the corresponding immense amount of time and money and no additional value. Meanwhile such a strategy would halt further innovation and market differentiation, since each company would dedicate disproportionate resources for developing software that already exists instead of striving for new and cutting-edge components.

Open source versus IP management: overlap and divergence

An all-encompassing IP management system needs to cover four important aspects: (i) risk management/compliance; (ii) housekeeping; (iii) education/training of employees; and (iv) external relations. An open source management programme deals with open source which is protected by copyright, making it an IP asset. The operation of an **open source** (IP) management programme should facilitate the productive use of **open source** solutions in the products and services of an organisation and – if intended – enable its participation and strategic contributions in **open source** communities. As a result, the organisation will fully capture the added value of the **open source** software used.

Open source is inherently different from any other form of IP-protected technology asset. That makes its management more challenging and, in some respects, more sophisticated. In an **open source** management programme, it is crucial to identify the open source components and subcomponents (dependencies) as well as the licences they carry. The **open source** user is expected to identify the rights and obligations corresponding to each licence and adhere to these.

Creating an **open source** management programme within each individual company from scratch can lead to complications in terms of scope, objectives and structure that each company might not be able to overcome. Following this individual approach, companies would not be able to perform a uniform assessment of their maturity and compliance level. However, the adoption of a standardised approach to **open source** management increases the likelihood of generating a consistent and qualitative result throughout the industry.

This is important when looking at the software supply ecosystem, where even "commercial" software contains **open source**. The benefits of consistent high-quality management programmes thus propagate in the entire software supply chain, meaning less time and resources wasted managing the consumed "commercial" software.

The OpenChain Specification on open source licence compliance

Responding to the challenge of bringing global industry solutions in the **open source** compliance realm, the **OpenChain Project** developed the OpenChain Specification. The OpenChain Project is an international community of companies, dedicated to optimising **open source** compliance and reinforcing trust in the open source supply chain. The OpenChain Specification has also been recognised as an ISO standard (**ISO/IEC 5230:2020**).

The development of this specification was the result of a collaborative initiative involving over 100 corporate contributors with the goal of creating a cross-industry standard on how to manage open source in an organisation. Consequently, the specification contains the minimum requirements considered essential in the industry for an organisation to establish and maintain a high-quality **open source** licence compliance programme.

The two main axis of the specification are documentation and awareness.

Firstly, the implementing companies are requested to produce the necessary documentation and to create documented procedures to form a fully-fledged open source compliance management system. As for raising awareness, the specification recognises the significance of critical employees being educated on open source and on the company's compliance management processes.

Additional pivotal action points of the OpenChain specification are:

- Identification of roles and responsibilities for the employees working with or being responsible for open source in the organisation;
- Establishment of procedures for review and management of the inbound and outbound software and the subsequent rights and obligations;
- Creation and management of a 'Software Bill of Materials' (**SBOM**);
- Setting up a process for preparation and distribution of the required compliance artifacts according to the identified licences; and
- Setting up review processes for **open source** to be contributed "**upstream**", ensuring that the contribution does not unintendedly impact the organisation's other IP rights, such as patents.

The OpenChain Project allows for self-certification (with commercial certifiers offering third-party certification as well). The specification functions as a tool that accommodates three major items: (1) gauging the maturity of **open source** software management within an organisation, (2) identifying potential weak points, and (3) pinpointing recommended actions for achieving the desired level of maturity.

On a larger scale, the specification aspires to set the industry's minimum requirements for **open source** compliance and management, accomplishing a certain level of trust between implementing organisations. Ultimately, the intention of the specification is to reduce the burden of compliance in the entire value chain.

The OpenChain Specification as a useful IP management tool

The omnipresent nature of **open source** creates complications both in terms of managing the software itself as well as managing the IP rights it is intertwined with. For this reason, the OpenChain specification offers an effective and industry-approved way of receiving and handling a variety of IP and technology assets.

As with all IP management implementations, a crucial point is to understand what IP is being used by the company (either owned by the company or by third parties) and securing adequate access and control thereto. The OpenChain specification contains useful check points on how to, in a consistent and risk-minimising way, bring third-party IP (in this case, in the form of open source) into an organisation.

Furthermore, the specification assists with a primary concern in IP management, ie, compliance with legal and contractual obligations for the purpose of avoiding potential legal risks. Its implementation helps mitigate risks related to inbound and outbound open source. The specification also provides the necessary safeguards and processes from the moment the code is introduced into the company and throughout the life cycle of the product in which this code is used.

A further complication in an **open source** setting is the - very real - risk of the organisation losing its "reputation" as a good **open source** citizen. Such an impact on its credibility is not a mere write-down of goodwill, but directly impacts an organisation in multiple ways. For example, it might be harder to recruit talent, obtain support from the **open source** community and, ultimately, get its technical contributions accepted into **open source** projects (meaning it cannot steer their direction).

A guide to the OpenChain specification

The OpenChain Specification spells out multiple requirements and action points that eventually aim to ensure the much-needed evaluation of the consumed open source and the conformance with the respective licences. As we keep returning to in this article, it is key to understand what is being introduced as well as where, how and by whom it is being used within the organisation. Only then, it is possible to guarantee compliance with third-party IP, track vulnerabilities, and make sure that open source is introduced and consumed in accordance with the organisation's policies.

The main outline of the specification is the following:

- **What do you need?** Identification of an organisation's **open source** responsibilities (Section 3.1);
- **Who do you need?** Resources and responsibilities assignment for **open source** compliance (Section 3.2);
- **What should they do?** Review and approval of inbound **open source** content (Section 3.3);
- **How do you show it?** Compliance artifacts (Section 3.4);
- **How do you manage contributions?** (Section 3.5); and

- **Are you compliant?** Adherence to the specification requirements (Section 3.6).

We will now provide a brief description of the main requirements and examine in more detail how they assist in reducing potential risks and how they translate to a quality IP management programme.

Open source compliance and IP management

1. **Risk management – Compliance**

Risk management and compliance in the context of **open source** appear to be two sides of the same coin; on the one hand, organisations manage the risk of losing their own IP rights while, on the other hand, avoid infringing third-party IP by breaching the obligations set by each open source licence that covers each open source component. Risks can be averted, and legal obligations can be safely and confidently met when a company adopts a comprehensive **open source** management programme.

The first 'order of business' is to consider and document the organisation's **open source** policy entailing high-level 'do's and don'ts' concerning open source consumption and contribution in an organisation as well as general directions on the same topics. Establishing and making available an **open source** policy (Section 3.1.1) is the first step towards a successful open source compliance management programme.

Through official written processes regarding the response to internal or external licence compliance queries (Section 3.2.1) and through the articulation of the rights and obligations of the identified licences (Section 3.1.5), the organisation guarantees compliance therewith as well as full exploitation of its IP. It is of great importance to make sure that a business complies with its licensing obligations without 'infecting' its own intangible assets. The 'infection' of an organisation's intangible assets refers to the inadvertently granting of royalty-free licences of its IP (eg, copyright on proprietary code or patented inventions) due to the use of open source licensed code. For example, the establishment of SBOMs (Section 3.3.1) allows the organisation to have a clear overview of the **open source** components it is introducing and using.

Relatedly, an **open source** management programme pays special attention to the **open source** contribution policy of each organisation and the need for eg, developers participating in open source projects to be fully aware of the dos and don'ts when it comes to contributing code upstream (Section 3.5.1). By following this policy, no IP rights of the company should be jeopardised from said contributions.

Another crucial element of this specification is the maintenance of **open source** 'hygiene' within an organisation. This implies having procedures in place, so that when code is introduced, it is additionally scanned to ensure that the software components are adequately secure. Such procedures have the beneficial side effect of being particularly useful for vulnerability management of the inbound software which occurs in a consistent and detailed manner throughout the product life cycle.

2. **Housekeeping – Innovation management**

Besides being an appropriate IP risk management tool, the OpenChain Specification provides a comprehensive baseline for housekeeping within an organisation. The specification requirements introduce processes that function as checks and balances between different departments for the harmonious and effective management of **open source** solutions. Special emphasis is given to the establishment of multi-layered, automated procedures for coping with a variety of challenges potentially encountered in the use of open source. One example is the establishment of procedures for handling the review and remediation of cases where compliance issues exist regarding certain open source obligations (Section 3.2.2.5).

For the purpose of continuity, consistency and reliability, these procedures are requested to be documented and, often, available to the organisation's employees. As a result, the employees can speak 'the same language' and have a common understanding when it comes to open source via the homogenous and well-established processes within the company.

'Running a tight ship' in terms of **open source** is imperative for the achievement of compliance targets and for a long-term, holistically higher performance within an organisation. Along the same lines, during an M&A process, the due diligence could be facilitated and the parties benefitted by an efficient **open source** management programme.

What is more, housekeeping is tightly related to innovation management for organisations that heavily rely on ground-breaking technologies for releasing products and generating revenue. The procedures previously discussed in the context of **open source** compliance management result in the creation of a log that contains all the **open source** components and related IP brought in and used by the organisation. Consequently, the organisation can direct its R&D efforts accordingly as well as manage any commercial contracts involving software.

3. **Education**

To optimise risk management and housekeeping, it is beneficial to provide the employees with the tools needed to appreciate the benefits and complexities of open source. For this reason, education and awareness are at the forefront for the OpenChain Specification (Sections 3.1.1.1, 3.1.2.3, 3.1.3.1 and 3.5.1.3). An organisation should guarantee that its employees working with open source are competent for their role and are aware of what is expected from them. In addition, all relevant employees should have the fundamental level of knowledge around internal processes to be in sync and collaborate seamlessly.

For this reason, it is critical to provide training to the professionals within the company on the importance of open source as well as on the policies and procedures covering its management. A key point of emphasis is that developers need to be conscious of the **open source** policy and **open source** contribution policy of their organisation in order to make informed executive and/or technical decisions.

4. **External relations - Contributions**

Considering the increasing influence of **open source** solutions across industries, higher business performance means capitalising on the incremental value of open source. This can only occur in a secure environment that acknowledges its relevance. The implementation of OpenChain Specification views **open source** management in an integrated manner. Namely, it focuses on compliance and consumption, without neglecting the need to contribute back to **open source** projects (Section 3.5).

Being involved in **open source** communities is not a priority for many organisations, since it does not fit all business models. On the other hand, an organised and target-oriented participation can produce short- and long-term benefits for **open source** users. Firstly, they can actively engage in the 'give and take' of the community in terms of **code** development, **bug fixes**, support and, secondly, get the opportunity to have a say in future **open source** projects. Therefore, instead of simply consuming software components for their products and services, implementers of OpenChain might optionally elect to give back to **open source** communities and enhance the value of open source for their business.

Apart from the need to map out an advisory open source contribution policy (Section 3.5.1.1), conformance with the OpenChain Specification means that an organisation must establish a documented procedure to advise developers regarding corporate approaches to contributing to **open source** projects and to guide them through the contribution process (Section 3.5.1.2). Such procedure also needs to be communicated to all relevant employees (Section 3.5.1.3).

Finally, the implementation of OpenChain could be advantageous in the macro level, since it might act as a springboard for cultivating the **open source** culture within the company. The possibility to further educate employees on the intricacies of open source will benefit the immediate operations and, gradually, the overall large-scale strategic targets of the company. On an industry-level, the more the organisations implement this standard, the closer the industry will get to healthier **open source** management. Following the objective set out in the specification itself, the establishment of a robust **open source** licence compliance management system plays a seminal role in building trust between organisations across different industries.

Conclusion

In the era of 5G, "softwareisation" and "smartification", the all-connected world overflows with new and innovative products and services. Therefore, the need for a robust IP management system is imminent. In this respect, IP management is equally important when dealing with software, in the form of **open source** compliance management.

This is where the OpenChain Specification comes along. By implementing this specification, you might not be able to answer the question of which **Linux kernel** distribution is best for your embedded products; that decision will remain in the domain of the Chief Technology Officer of your company (CTO). But, you can rest assured that:

- legal risks are minimised;
- the relevant stakeholders have the right training and the right resources;
- compliance is done systematically; and
- the organisation has increased visibility into security issues that may arise, facilitated through the identification of any third-party IP used.

Should engineers wish to contribute **bug fixes** or new features upstream, there are processes within the organisation to address this. It is all about putting processes in place that guarantees fewer risks and less friction down the line.

Due to these evident advantages of **open source** management, the OpenChain Specification has so far been adopted by **many companies of different sizes and from different industries**, including large multinational companies such in various industries such as Automotive, Telecommunications, IT, Healthcare, and Fintech.

Perhaps, it is time for your organisation to take the plunge, get ahead of the curve and include **open source** management as part of their IP management practices as well. This way you can make both IP and open source management boring – but safe.

The views expressed in this article are those of the authors and do not necessarily reflect the opinions of Ericsson.

Eleftheria Stefanaki

Author | Senior IPR and Open Source Researcher

Ericsson

Jimmy Ahlberg

Author | Open Source Policy Director

Ericsson and chair of the OpenChain Projects Governing Board