OPENCHAIN

Introductory M&A Checklist

Version 1

Table of Contents

Context

The OpenChain Project builds trust in open source by making open source license compliance simpler and more consistent. The OpenChain Specification defines a core set of requirements every quality compliance program must satisfy. The OpenChain Curriculum provides the educational foundation for open source processes and solutions, whilst meeting a key requirement of the OpenChain Specification. OpenChain Conformance allows organizations to display their adherence to these requirements. The result is that open source license compliance becomes more predictable, understandable and efficient for participants of the software supply chain.

The goal of this checklist is to assist both the target and the acquirer with the OpenChain Specification being applied to Merger and Acquisition (M&A) activity. Using a checklist minimizes the time impact at deal closing time and helps the acquirer ensure the target has basic controls in place for conformance with open source licensing and security risks.

The checklist is divided in several parts depending on the business model of the target company. It contains a general section with topics to be checked by the acquiring company and subsection, focused on different business models of the target.

Checklist

1. Policies and Management

1.1 Does the target organization structure include a committee to create policies and review open source usage such an Open Source Review Board (OSRB) or an Open Source Programs Office (OSPO)? If yes:

- Please describe the regular operations of the committee (e.g. meeting frequency)
- Please describe the size of the committee as well as its composition (e.g. legal, product, ops)

1.2 Does the target organization have a formally documented open source usage policy? If yes:

- Is the policy communicated within the organization?
- Are the development teams trained on the basics of open source licensing?
- Does the policy cover the cases where open source technology is to be used within proprietary software, by copying or pasting or including dependencies?

1.3 Please describe the rejection and approval processes for requests for usage of third-party open source software within proprietary software.

2. Proprietary Software

2.1 Please describe the target's proprietary product or products

2.2 Please describe the distribution mechanisms (e.g. cloud, SaaS, hosted, on-prem, mobile, client side browser code)

2.3 Please list any known copyleft licensed (e.g. Affero GPL, GPL, LGPL, MPL) code used in proprietary software

2.4 Please list of any dual-licensed software that the target is using under a commercial license. (e.g. MySQL, Ghostscript)

2.5 Please list any source code modifications made to open source.

2.6 Please describe interaction of each element of open source with proprietary software (static or dynamic linking)

2.7 Please describe the usage of the following if any

- Export control and Cryptography
- Databases (e.g. MySQL or MongoDB)
- Web Services (e.g. AWS)
- Shipping containers or virtual machines: Provide details of Operating System and applications. (e.g. Docker, Linux)
- Any commercially licensed software
- Repository or package managers (e.g. maven, npm)

2.8 Are copyright headers maintained in proprietary source code?

2.9 Has any proprietary code been developed by third parties software suppliers/contractors outside the company?

3. Tooling

3.1 Is there any open source code scanner or similar tool deployed to detect, manage and enforce open source policies? If yes:

- Please provide name and version of the tool(s)
- Please describe the frequency of the scans (e.g., every build, once every major release)
- Please describe the process around detection and patching of open source related security vulnerabilities (e.g. OpenSSL, Struts2, Kubernetes)

4. Third-Party Open Source Software

4.1 Does Target contribute code or resources to any third-party open source projects, or has it ever done so? If yes:

- Please specify the projects and provide details of the contributions (licenses, websites and whether in code, resource or monetary)

4.2 Do any target employees hold positions on external open source projects, such as committers or project management committee? If so, please identify the project, employee, and position.

5. Open Source Claims

5.1 Please describe any claims of non-compliance made to the target, and any progress toward resolving them.

6. Document Request List

6.1 Please provide recent (less than 3 months old) Open Source Bill of Materials (BOM) or Open Source Disclosures listing all the open source used target's products

6.2 Please provide documents relating to open source usage, approval and rejection policies

6.3 Please provide any available third-party notices that may be displayed or distributed with target's products

6.4 Please identify any suppliers that provide open source as part of tangible inputs that are included in the target's products, such as chips or computers.

6.5 Please provide copies of any policies covering IP ownership and development by employees and contractors.

6.6 Please provide copies of any contracts with third parties/contractors for development of software, together with details of the software and licensing arrangement attaching to them.

6.7 Please confirm whether any third party sources of software produced or consumed by the target have been certified as OpenChain Conformant.