MOORCROFTS
CORPORATE LAW

Onboarding Process for [company] Limited

OPENCHAIN

Introduction

History

The OpenChain Project began in 2013 when a group of software supply chain open source practitioners observed two emerging patterns: 1) significant process similarities existed among organizations with mature open source compliance programs; and 2) there still remained a large number of organizations exchanging software with less developed programs. The latter observation resulted in a lack of trust in the consistency and quality of the compliance artifacts accompanying the software being exchanged. As a consequence, at each tier of the supply chain, downstream organizations were frequently redoing the compliance work already performed by other upstream organizations.

In October 2016, these concerns caused the Linux Foundation to launch OpenChain as a formally constituted collaborative project. The first iteration was the OpenChain Specification 1.0.

After beta testing between a small number of software companies, OpenChain 1.0 evolved into OpenChain 1.1, which was formally launched at the European Legal Network Conference in Barcelona in April 2017.

Subsequent to the launch, and consequent on positive response from many organisations with an interest in quality open source governance, the Linux Foundation is intent in increasing the profile and reach of the programme, through a strategy of outreach to both the FOSS community and prominent corporate consumers of FOSS, and instigating an international partner programme.

Moorcrofts has been involved in the development of OpenChain materials, and in August 2017 was appointed by the Linux Foundation to become one of 5 Pathfinder Partners worldwide (and the only one in the UK) to provide OpenChain professional services to its clients.

Evolution of OpenChain

OpenChain in its current form anticipates that the inputs (third party software components) and outputs (software products provided to customers) are all Open Source. In practice, the majority of software development activities consist of both open source and proprietary components, and it we anticipate that future iterations of OpenChain will address this issue. However, in the meantime, we have developed appropriate (and fairly minimal) extensions to OpenChain accordingly. The text in roman type in this document relates to the current OpenChain 1.1 specification, and text in *italic* relates to those elements covering the procurement and provision of software and SaaS services on a proprietary basis.

Applicability to [Company] Limited ("[Company]")

[Company] has engaged Moorcrofts to review its software compliance and licensing status, and to recommend changes appropriate to [Company]'s business. In common with many businesses providing software-based products, [Company] uses free and open source software, and combines it with internally-developed and externally sourced proprietary components, to develop software products which are, in the main, provided on a SaaS basis, but with some components made available by way of distribution.

OpenChain is currently the only formal compliance programme available covering Open Source, and given its high-profile backing from the Linux Foundation, as well as early adopters such as Qualcomm, Cisco, Siemens, ARM, HPE, Adobe and Western Digital Moorcrofts has recommended that [Company] seek OpenChain compliance as part of this process.

This document provides details of the criteria which apply to certification. As part of the process, Moorcrofts will work with [Company] to develop practices, policies and procedures compliant with the OpenChain specification, as extended by Moorcrofts to cover the procurement and supply of proprietary software as part of [Company]'s product, to ensure end-to-end compliance, irrespective of the type of software involved. The overall compliance achieved is intended to be a superset of the OpenChain Specification, drawing in best-practice from other aspects of software and services procurement.

Process

Stage 1

The first stage of the process is the knowledge acquisition phase, during which Moorcrofts works with [Company] to determine its business aims, culture and management structure, as well as acquiring the data necessary to begin the path to compliance. Although it provides the complete OpenChain specification, because compliance can be achieved in a number of ways, the precise route to compliance will depend upon the information gathered in stage 1. We regard culture as particularly important, as issues such as appetite for risk, attitude towards openness, whether software freedom is more important than maximizing the use of developed software, willingness to become involved with (or establish) free and open source project communities, and how those qualities are communicated to, and valued in, staff, are vital to ensure that the route to compliance and certification is deeply compatible with [Company]'s aims.

Stage 2

The second stage involves acquiring more detailed information, and is likely to require input from specific subject-matter experts from within [Company]. [In particular, this will involve an overview of possible analysis of actual coding working practices, review of structure of repos and the [CodeScanning] database, and review of specific documentation such as assignments, licences and EULAs.

It will be at this stage that the scope and aims are more clearly defined. For example, we will be recommending that the OpenChain Specification is extended to cover the use and provision of software on a proprietary basis (as set out elsewhere in this document). However, it may also be the case that specific client-facing issues are relevant, such as requests for certain forms or warranty and indemnity over provenance and IPR liability, and the scope of the engagement may be adjusted to deal with this (for example review of appropriate liability clauses within EULAs etc. to refer specifically to certification, of to permit the release of certain compliance materials under NDA).][We typically require access to [Company]'s repositories for this, and will set up a data room where relevant compliance materials such as policies and procedures can be uploaded].

Stage 3

The third stage involves the creation of a detailed report setting out the current compliance status, with detailed recommendations as to next steps. After consideration and discussion of the content of the report, [Company] and Moorcrofts will agree a compliance programme based on the recommendations set out in the report.

Stage 4

Stage 4 involves implementation of the recommendations, with the involvement of Moorcrofts as agreed. This may include drafting of appropriate policies and procedures, assisting with practical aspects of implementation, providing training (on either a direct-training or train-the-trainer basis) and assisting in establishing and documenting procedures, as well as additional work agreed within the scope for Stage 2. It may also involve updating existing documentation (such as client terms and conditions and SaaS service agreements, third party supply agreements, such as hosting agreements, development agreements, subcontractor agreements and testing and quality control services agreements).

Stage 5

Stage 5 involves an audit of the processes and procedures as implemented in Stage 4 against the Open Chain Specification. Where there are non-compliances, Moorcrofts will work with [Company] to address them. This may also involve input from third party experts (for example, to check that firmware loaded into shipped devices corresponds with the source made available).

The key deliverable is a letter of advice, which may be made available to third parties, certifying that [Company] has achieved compliance with the OpenChain Specification 1.1. **(Important: nothing requires [Company] to obtain such a letter of advice before describing itself as compliant: it is open to [Company] to assess its own level of compliance against the OpenChain criteria at any time, and if it is satisfied it has met the criteria, to describe itself as having achieved self-certified compliance.)**

Stage 6

Moorcrofts will (if requested by [Company]) make itself available to address licensing queries as they arise from time to time, and also to regularly test compliance with the Specification, and renew the advice letter (if requested) from time to time, in the light of updates to the OpenChain Specification or the adoption of additional modules.

Section 1: Vision and Mission

The Vision and Mission of the OpenChain Project are as follows:

> Vision:
>
> A software supply chain where a set of specified *software products consisting of or incorporating* free/open source software (FOSS) is delivered with trustworthy and consistent compliance information.
>
> Mission:
>
> Establish requirements to achieve effective management of *software components including* free/open source software (FOSS) for software supply chain participants, such that the requirements and associated collateral are developed collaboratively and openly by representatives from the software supply chain, open source community, and academia.

In accordance with the Vision and Mission, this specification defines a set of requirements that if met, would significantly increase the probability that an open source compliance program had achieved a sufficient level of quality, consistency and completeness; although a program that satisfies all the specification requirements does not guarantee full compliance. The requirements represent a base level (minimum) set of requirements a program must satisfy to be considered OpenChain Conforming. The specification focuses on the “what” and “why” qualities of a compliance program as opposed to the “how” and “when” considerations. This ensures a practical level of flexibility that enables different organizations to tailor their policies and processes to best fit their objectives.

Section 2 introduces definitions of key terms used throughout the specification.

Section 3 presents the specification requirements where each one has a list of one or more Verification Artifacts. They represent the evidence that must exist in order for a given requirement to be considered satisfied. If all the requirements have been met for a given program, it would be considered OpenChain Conforming in accordance with version 1.1 of the specification. Verification Artifacts are not intended to be public, but could be provided under NDA or upon private request from the OpenChain organization to validate conformance.

Section 2: Definitions

FOSS (Free and Open Source Software) - software available under a license which meets the Open Source Definition published by the Open Source Initiative (OpenSource.org) and/or the Free Software Definition (or ‘four freedoms’) published by the Free Software Foundation, and which is used (and, where applicable distributed, under such license).

FOSS Liaison - a designated person who is assigned to receive external FOSS inquiries.

FOSS Policy *- a policy detailing the processes, procedures and rules applicable to the selection, acquisition, incorporation, documentation, testing, deployment and licensing of Supplied Software, where the Supplied Software consists of or includes an element of FOSS (and which may therefore consist, in addition to FOSS, of Proprietary Software and software developed internally).*

Identified Licenses - a set of FOSS *and Proprietary Software* licenses identified as a result of following an appropriate method of identifying such licenses.

OpenChain Conforming - a program that satisfies all the requirements of this specification.

Proprietary Software *– software available under a licence which does not meet either the Open Source Definition published by the Open Source Initiative (OpenSource.org) or the Free Software Definition (or four freedoms) published by the Free Software Foundation, and which is used (and, where applicable distributed, under such licence). ‘Proprietary Software’ includes both software available under paid-for licensing terms as well as software which is in some ways similar to FOSS, but is not fully compliant with the relevant licences (such as standards licences, shareware licenses or non-commercial and other restricted field-of-use licences).*

Software Staff - any employee or contractor that defines, contributes to or has responsibility for preparing Supplied Software. Depending on the organization, that may include (but is not limited to) software developers, release engineers, quality engineers, product marketing and product management.

SPDX or Software Package Data Exchange - the format standard created by the SPDX Working Group for exchanging license and copyright information for a given software package. A description of the SPDX specification can be found at www.spdx.org.

Supplied Software - software that an organization delivers to third parties (e.g., other organizations or individuals) *whether that software is supplied by means of* *distribution, or whether the functionality is made available by other means, for example through SaaS service provision*.

Verification Artifacts - evidence that must exist in order for a given requirement to be considered satisfied.

Section 3: Requirements

1 Know Your FOSS Responsibilities

1.1 A written FOSS policy exists that governs FOSS license compliance of the Supplied Software distribution. The policy must be internally communicated.

Verification Artifact(s):

1.1.1	A documented FOSS policy exists.	Please provide a copy of any FOSS policy. In the absence of any existing policy, Moorcrofts will provide an appropriate draft.
1.1.2	A documented procedure exists that makes all Software Staff aware of the existence of the FOSS policy (e.g., via training, internal wiki, or other practical communication method). Rationale: Ensure steps were taken to create, record and make Software Staff aware of the existence of a FOSS policy. Although no requirements are provided here on what should be included in the policy, other sections may impose requirements on the policy.	Please provide a copy of any procedure covering training and awareness. In the absence of any existing policy, Moorcrofts will provide an appropriate draft.

Rationale: Ensure steps were taken to create, record and make Software Staff aware of the existence of a FOSS policy. Although no requirements are provided here on what should be included in the policy, other sections may impose requirements on the policy.

1.2 Mandatory FOSS training for all Software Staff

The training, at a minimum, covers the following topics:

- The FOSS policy and where to find a copy;
- Basics of Intellectual Property law pertaining to FOSS, *Proprietary Software* and FOSS *and Proprietary Software* licenses;
- FOSS licensing concepts (including the concepts of permissive and copyleft licenses);
- *Licensing concepts applicable to Proprietary Software, including royalty payments and typical restrictions applicable to Proprietary Software Licenses (field of use, sub-licensing, per-user licensing, site licensing and geographical restrictions);*

- FOSS project licensing models (including SaaS);
- *Proprietary Software licensing models (including SaaS);*
- Software Staff roles and responsibilities pertaining to FOSS *and Proprietary Software* compliance specifically and the FOSS policy in general; and
- Process for identifying, recording and/or tracking of FOSS *and Proprietary Software* components contained in Supplied Software.

Software Staff must have completed FOSS training within the last 24 months to be considered current. A test may be used to allow Software Staff to satisfy the training requirement.

Verification Artifact(s):

1.2.1	FOSS training materials covering the above topics exists (e.g., slide decks, online course, or other training materials).	Please provide a copy of any such materials. In the absence of any existing materials, Moorcrofts will provide an appropriate draft.
1.2.2	Method of tracking the completion of the training for all Software Staff, including any verification that the training has been understood.	Please provide a copy of any procedure covering the tracking of training and assessment. In the absence of any existing procedure, Moorcrofts will provide an appropriate draft.
1.2.3	At least 85% of the Software Staff are current, at any given time.	Please provide details of the mechanisms by which the threshold is checked and maintained.

Rationale: Ensure the Software Staff have recently attended FOSS *and Proprietary Software* training and that a core set of relevant topics is covered (however, a typical training program would likely be more comprehensive than that required here).

1.3 A process exists for reviewing the Identified Licenses to determine the obligations, restrictions and rights granted by each license.

Verification Artifact(s):

1.3.1	A documented procedure exists to review and document the obligations, restrictions and rights granted by each Identified License governing the Supplied Software.	Please provide a copy of any such procedure. In the absence of any existing procedure, Moorcrofts will provide an appropriate draft.

Rationale: To ensure a process exists for reviewing and identifying the license obligations for each Identified License for the various use cases.

2 Assign Responsibility for Achieving Compliance

2.1 Identify FOSS Liaison Function ("FOSS Liaison").

Assign individual(s) responsible for receiving external FOSS inquiries; FOSS Liaison must make commercially reasonable efforts to respond to FOSS compliance inquiries as appropriate; and publicly identify a means by which one can contact the FOSS Liaison.

Verification Artifact(s):

2.1.1	FOSS Liaison function is publicly identified (e.g., via a published contact email address, or the Linux Foundation's Open Compliance Directory).	Please provide details of where the liaison function is identified.
2.1.2	An internal documented procedure exists that assigns responsibility for receiving FOSS compliance inquiries.	Please provide a copy of any procedure covering the handling of FOSS compliance enquiries. In the absence of any existing procedure, Moorcrofts will provide an appropriate draft.

Rationale: *Ensure there is a reasonable way for third parties to contact the organization with regard to FOSS compliance inquiries and that this responsibility has been effectively assigned.*

2.2 Identify Internal FOSS Compliance Role(s).

- Assign individual(s) responsible for managing internal FOSS compliance. The FOSS Compliance role and the FOSS Liaison may be the same individual.
- FOSS compliance management activity is sufficiently resourced:
- Time to perform the role has been allocated; and
- Commercially reasonable budget has been allocated.
- Assign responsibilities to develop and maintain FOSS compliance policy and processes;
- Legal expertise pertaining to FOSS compliance is accessible to the FOSS Compliance role (e.g., could be internal or external); and
- A process exists for the resolution of FOSS compliance issues.

There may be quasi-FOSS compliance issues that arise in relation to certain sorts of licence – for example, compliance with standards. It would be anticipated that the FOSS compliance role would cover these issues as well, as further documented, depending on the specifics of the software acquired, and the relevant out-licences.

Two separate compliance modules (standards and patents) are being developed to address this point.

Verification Artifact(s):

2.2.1	Name of persons, group or function in FOSS Compliance role(s) internally identified.	Please provide details of the relevant individuals of groups.
2.2.2	Identify source of legal expertise available to FOSS Compliance role(s) which could be internal or external	Moorcrofts is happy to be identified as the relevant source of legal expertise.
2.2.3	A documented procedure exists that assigns internal responsibilities for FOSS compliance	Please provide a copy of the relevant procedure. Moorcrofts is happy to provide a suitable draft if required.
2.2.4	A documented procedure exists for handling the review and remediation of noncompliant cases.	Please provide a copy of the relevant procedure. Moorcrofts is happy to provide a suitable draft if required.

Rationale: *Ensure certain FOSS responsibilities have been effectively assigned.*

3 Review and Approve FOSS *and Proprietary Software* Content

3.1 A process exists for creating and managing a FOSS *and Proprietary Software* component bill of materials which includes each component (and its Identified Licenses) in a Supplied Software release.

Verification Artifact(s):

3.1.1	A documented procedure exists for identifying, tracking and archiving information about the collection of FOSS components from which a Supplied Software release is comprised.	Please provide a copy of the relevant procedure. Moorcrofts is happy to provide a suitable draft if required.
3.1.2	FOSS component records exist for each Supplied Software release which demonstrates the documented procedure was properly followed.	Please provide a copy of the relevant procedure. Moorcrofts is happy to provide a suitable draft if required.

Rationale: To ensure a process exists for creating and managing a bill of materials covering components (FOSS *and Proprietary Software*) used to construct the Supplied

Software. A bill of materials is needed to support the systematic review of each component's license terms to understand the obligations and restrictions as it applies to the distribution of the Supplied Software.

3.2 The FOSS management program must be capable of handling common FOSS *and Proprietary Software* license use cases encountered by Software Staff for Supplied Software, which may include the following use cases (note that the list is neither exhaustive, nor may all of the use cases apply):

- distributed in binary form;
- distributed in source form;
- integrated with other FOSS such that it may trigger copyleft obligations;
- *provided on a Software as a Service basis, or other basis where the functionality of the software is made available without the software being distributed;*
- contains modified FOSS *or Proprietary Software*;
- contains FOSS or other software under an incompatible license interacting with other components within the Supplied Software; and/or
- contains FOSS *or Proprietary Software* with attribution requirements or requirements involving the provision of other notices or documentation (e.g. a copy of the relevant licence).

Verification Artifact(s):

3.2.1	A procedure has been implemented that handles the common FOSS license use cases for the FOSS components of each Supplied Software release.	Please provide a copy of the relevant procedure. In the absence of any existing procedure, Moorcrofts will provide an appropriate draft.

Rationale: *To ensure the program is sufficiently robust to handle an organization's common FOSS license use cases. That a procedure exists to support this activity and that the procedure is followed*

4 Deliver FOSS Content Documentation and Artifacts

4.1 Prepare the set of artifacts representing the output of the FOSS management program for each Supplied Software release. This set is referred to as the Compliance Artifacts which may include (but are not limited to) one or more of the following: source code, attribution notices, copyright notices, copy of licenses, modification notifications, written offers, SPDX documents and so forth.

Verification Artifact(s):

4.1.1	A documented procedure exists that ensures the	Please provide a copy of the relevant

	Compliance Artifacts are prepared and distributed with Supplied Software release as required by the Identified Licenses.	procedure. In the absence of any existing procedure, Moorcrofts will provide an appropriate draft.
4.1.2	Copies of the Compliance Artifacts of the Supplied Software release are archived and easily retrievable, and the archive is planned to exist for at least as long as the Supplied Software is offered or as required by the Identified Licenses (whichever is longer).	Please provide details of the means by which the compliance Artifacts are archived and made retrievable.

Rationale: Ensure the complete collection of Compliance Artifacts accompany the Supplied Software as required by the Identified Licenses that govern the Supplied Software along with other reports created as part of the FOSS review process.

5 Understand FOSS Community Engagement

5.1 A written policy exists that governs contributions to FOSS *(or similar)* projects by the organization. The policy must be internally communicated.

Verification Artifact(s):

5.1.1	A documented FOSS contribution policy exists;	Please provide a copy of the relevant policy. In the absence of any existing policy, Moorcrofts will provide an appropriate draft.
5.1.2	A documented procedure exists that makes all Software Staff aware of the existence of the FOSS contribution policy (e.g., via training, internal wiki, or other practical communication method).	Please provide a copy of the relevant procedure. In the absence of any existing procedure, Moorcrofts will provide an appropriate draft.

Rationale: *Ensure an organization has given reasonable consideration to developing a policy with respect to publicly contributing to FOSS. The FOSS contribution policy can be made a part of the overall FOSS policy of an organization or be its own separate policy. In the situation where contributions are not permitted at all, a policy should exist making that position clear.*

5.2 If an organization permits contributions to FOSS projects then a process must exist that implements the FOSS contribution policy outlined in Section 5.1.

Verification Artifact(s):

5.2.1	Provided the FOSS contribution policy permits contributions, a documented procedure exists that governs FOSS contributions.	Please provide a copy of the relevant policy. In the absence of any existing policy, Moorcrofts will provide an appropriate draft.

Rationale: Ensure an organization has a documented process for how the organization publicly contributes FOSS. A policy may exist such that contributions are not permitted at all. In that situation it is understood that no procedure may exist and this requirement would nevertheless be met.

6 Certify Adherence to OpenChain Requirements

6.1 In order for an organization to be OpenChain certified, it must affirm that it has a FOSS management program that meets the criteria described in this OpenChain Specification version 1.1.

Verification Artifact(s):

6.1.1	The organization affirms that a FOSS management program exists that meets all the requirements of this OpenChain Specification version 1.1	Moorcrofts will prepare an appropriate form of affirmation once compliance has been achieved.

Rationale: To ensure that if an organization declares that it has a program that is OpenChain Conforming, that such program has met all the requirements of this specification. The mere meeting of a subset of these requirements would not be considered sufficient to warrant a program be OpenChain certified.

6.2 Conformance with this version of the specification will last 18 months from the date conformance validation was achieved. Conformance validation requirements can be found on the OpenChain project's website.

Verification Artifact(s):

6.2.1	The organization affirms that a FOSS management program exists that meets all the requirements of this OpenChain Specification version 1.1 within the past 18 months of achieving conformance validation.	Moorcrofts will prepare an appropriate form of affirmation once compliance has been achieved.

Rationale: It is important for the organization to remains current with the specification if they want to assert program conformance overtime. This requirement ensures that the program's supporting processes and controls do not erode if they want to continue to assert conformance with the specification over time.