**Openchain 適合仕様書**  
Version 1.0

**Contents**

[**はじめに** 3](#_Toc476563264)

[**用語の定義** 4](#_Toc476563265)

[**Requirements** 5](#_Toc476563266)

[G1: Know Your FOSS Responsibilities 5](#_Toc476563267)

[G2: Assign Responsibility for Achieving Compliance 6](#_Toc476563268)

[G3: Review and Approve FOSS Content 7](#_Toc476563269)

[G4: Deliver FOSS Content Documentation and Artifacts 8](#_Toc476563270)

[G5: Understand FOSS Community Engagement 9](#_Toc476563271)

[G6: Certify Adherence to OpenChain Requirements 10](#_Toc476563272)

# はじめに

OpenChain イニシアチブがスタートした2013年、この年ソフトウェア・サプライチェーンでオープンソースを活用していた実践者たちは、表面化してきている2つのパターンを観測していた：1) 成熟したオープンソース・コンプライアンスプログラムを持つ組織では、そのプロセスに意味ありげな類似性があったが； 2)一方でいまだ多くの組織においてソフトウェアのやり取りするためのプログラムは非先進的なものだった。後者では、ソフトウェアのやり取りに付随する、コンプライアンス関連生成物の一貫性や品質について信頼を喪失させる事態を引き起こし、. 結果として、サプライチェーンのそれぞれの段階において、上流側組織で既に実施したコンプライアンス業務を下流組織で再び実施されていた。

こういった背景から、標準的なプログラムの仕様というものを整備することができるかどうか検討する研究グループが形成された。これは、 i) 産業横断的に共有されるオープンソース・コンプライアンスに係る情報の品質と一貫性を促進し; ii)コンプライアンス作業の再実施に起因する、オープンソースに関連するトランザクションコストの低減することを見据えている。本研究グループは、ワーキンググループへと発展、のち2016年4月 、正式にThe Linux Foundationのコラボレーティブ・プロジェクトとして組織されることとなった。

OpenChain イニシアチブは以下のビジョンとミッションを有する：

* **ビジョン： フリー/オープンソース・ソフトウェア(FOSS)が、信頼でき一貫性のあるコンプライアンス情報とともに提供されるソフトウェア・サプライチェーンを実現すること**
* **ミッション: フリー/オープンソース・ソフトウェア(FOSS)の効果的マネジメントを実現するための 要件 をソフトウェア・サプライチェーンの参加者のために確立すること。こういった要件や関連する付随事項は、オープンに、ソフトウェア・サプライチェーン、オープンソース ・コミュニティやアカデミア（学術研究機関）の関係者それぞれがオープンに協働しながら開発を進めていく**

上記ビジョンとミッションに則り、本仕様書ではこれに適合するならばそのオープンソース・コンプライアンスプログラムは十分なレベルでの品質、一貫性と完全性を獲得している、その可能性を著しく高めてくれるであろう要件の一式を定義する。ただし、本要件のすべてを満たしていたとしてもそれが完全なコンプライアンスプログラムであることを保証するものではない。本要件は、そのプログラムがOpenChain に適合しているとみなすために満足していなければならない、ベースレベル（最低限）の要件セットを示したものである。本仕様書は、「どうやって(How）」や「いつ(When)」といった考慮ではなく、コンプライアンスプログラムの「何(What)」、「なぜ(Why)」の属性に焦点をあてている。また本仕様書は、さまざまな組織が自身のポリシーやプロセスが目的にベストフィットするよう仕立て上げられるよう、実用的なレベルでの柔軟性を確保している。

第2節では、仕様として全般で用いられる重要用語について定義していく。第3節では、仕様としての要件を示していく。それぞれに 一つ以上の「検証対象」が存在する。これらは提示された要件が満たされているかどうかを検討するために存在しなくてはならない、確証としての役割を担っている。すべての要件をそのプログラムが満たしている場合、それは仕様書1.0版における「 OpenChain 準拠(OpenChain Conforming)」とみなされる。

# 用語の定義

**分散型コンプライアンス生成物 －供給されたソフトウェアとともに特定されたライセンスが提供されることが求められる生成物一式であり以下を含んでいるもの：著作権表示（Copyright notice）、ライセンスのコピー、修正箇所の通知、帰属情報の通知、ソースコード、書面による提案など**

**FOSS (フリー/オープンソース・ソフトウェア) －オープンソース・イニシアティブ(OpenSource.org)によって発行されているオープンソース定義、もしくはフリーソフトウェア・ファウンデーションによって発行されているフリーソフトウェア定義に当てはまるライセンス、もしくはそれに類似した1つ以上のライセンスに従うソフトウェアのこと**

**FOSS 窓口担当－外部からのFOSSに係る問合せを受け付ける、指名された人のこと確認されたライセンス－適切な方法に則り確認ができたFOSSライセンスのこと**

**OpenChain準拠 －本仕様書のすべての要件を満たすプログラムのこと**

ソフトウェアスタッフ－提供されるソフトウェアを作り出し、コントリビュートし、もしくはそれを使えるようにするために責任を有しているあらゆる従業員や契約者のこと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 ww.spdx.org.

**Supplied Software** – software that an organization delivers to third parties (e.g., other organizations or individuals).

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

# Requirements

## G1: Know Your FOSS Responsibilities

**1.1 A written FOSS policy exists that governs FOSS license compliance of the Supplied Software distribution where, as a minimum, it must be internally communicated.**

**Verification Artifact(s):**

* 1.1.1 A documented FOSS policy exists.
* 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 requirements in other sections may.

**1.2 Mandatory FOSS training for all Software Staff exists such that:**

* **The training, as a minimum, covers the following topics:**
* **The FOSS policy and where to find a copy;**
* **Basics of IP law pertaining to FOSS and FOSS licenses;**
* **FOSS licensing concepts (including the concepts of permissive and copyleft licenses);**
* **FOSS project licensing models;**
* **Software Staff roles and responsibilities pertaining to FOSS compliance specifically and the FOSS policy in general; and**
* **Process for identifying, recording and/or tracking of FOSS 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 course materials covering the above topics exists (e.g., slide decks, online course, or other training materials).
* 1.2.2 Method of tracking the completion of the course for all Software Staff.
* 1.2.3 At least 85% of all Software Staff are current, as per definition in above section.

**Rationale:**

Ensure the Software Staff have recently attended FOSS training and that a core set of relevant FOSS topics are covered. The intent is to ensure a core base level set of topics are covered but a typical training program would likely be more comprehensive than what is required here.

## G2: 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 means of contacting the FOSS Liaison by way of electronic communication.**

**Verification Artifact(s):**

* 2.1.1 FOSS Liaison function is publicly identified (e.g., via an email address and/or the Linux Foundation’s Open Compliance Directory).
* 2.1.2 A documented procedure exists that assigns responsibility for receiving FOSS compliance inquiries.

**Rationale:**

Ensure there is a reasonable way for third parties to contact the organization with regard to

FOSS compliance inquiries.

**2.2 Identify Internal FOSS Compliance Role(s).**

* **Assign** i**ndividual(s) responsible for managing internal FOSS compliance. The FOSS Compliance role and the FOSS Liaison can 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**
* **Escalation p**ath is available for resolution of FOSS compliance issues.

**Verification Artifact(s):**

* 2.2.1 Name of persons, group or function in FOSS Compliance role(s) identified.
* 2.2.2 Identify source of legal expertise available to FOSS Compliance role(s).
* 2.2.3 A documented procedure exists that assigns responsibilities for FOSS compliance.
* 2.2.4 A documented procedure exists that identifies an escalation path for issue resolution.

**Rationale:**

Ensure certain FOSS responsibilities have been effectively assigned. OpenChain Conformance Specification 1.0

## G3: Review and Approve FOSS Content

**3.1 A process exists for identifying, tracking and archiving a list of all FOSS components (and their respective Identified Licenses) from which Supplied Software is comprised.**

**Verification Artifact(s):**

* 3.1.1 A documented procedure exists used to identify, track, and archive a list of FOSS components and their Identified Licenses from which the Supplied Software is comprised.

**Rationale:**

To ensure a process exists for identifying and listing all FOSS components used to construct the Supplied Software. This inventory must exist to support the systematic review of each component’s license terms to understand their respective distribution obligations and restrictions applicable to the Supplied Software. The recorded inventory also serves as evidence that the process was followed.

**3.2 The FOSS program must be capable of handling typical FOSS use cases encountered by Software Staff for Supplied Software, which may include the following use cases - when parts of the Supplied Software (note that the below list is neither exhaustive, nor may all of the below use cases apply depending on the organization):**

* **are distributed in binary form**
* **are distributed in source form**
* **are integrated with other FOSS such that it may trigger copyleft obligations**
* **contains modified FOSS**
* **contains FOSS or other software under an incompatible license interacting with other**
* **components within the Supplied Software**
* **contains FOSS with attribution requirements**

**Verification Artifact(s):**

* 3.2.1 A process has been implemented that is capable of addressing the typical FOSS use
* cases encountered by Software Staff for Supplied Software.

**Rationale:**

To cause the FOSS program to be sufficiently robust to address that organization’s typical use cases as a result of that organization’s business practices.

## G4: Deliver FOSS Content Documentation and Artifacts

**4.1 Prepare the following Distributed Compliance Artifacts to accompany the Supplied Software as required by the corresponding Identified Licenses which might include (but is not limited to) the required:**

* **copyright notices**
* **copies of Identified Licenses**
* **modification notifications**
* **attribution notices**
* **prominent notices**
* **source code**
* **required build instructions and scripts**
* **written offers**

**Verification Artifact(s):**

* 4.1.1 A documented procedure exists describing a process that ensures the Distributed Compliance Artifacts be distributed with Supplied Software as required by the Identified Licenses.
* 4.1.2 Copies of the Distributed Compliance Artifacts of the Supplied Software are archived and easily retrievable (e.g., legal notices, source code, SPDX documents), 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).

**Rationale:**

Ensure the complete collection of compliance artifacts accompany the Supplied Software as required by the Identified Licenses that govern the Supplied Software.

## G5: Understand FOSS Community Engagement

**5.1 A written policy exists that governs contributions to publicly accessible FOSS projects by employees on behalf of the organization where, as a minimum, it must be internally communicated.**

**Verification Artifact(s):**

* 5.1.1 A documented FOSS contribution policy exists;
* 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).

**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 Provided the FOSS contribution policy permits such contributions, a process exists for confirming contributions adhere to the FOSS contribution policy, which might include (but is not limited to) the following considerations:**

* legal approval for license considerations
* business rationale or approval
* technical review of code to be contributed
* community engagement and interaction, including a project’s Code of Conduct or equivalent
* adherence to project-specific contribution requirements

**Verification Artifact(s):**

* 5.2.1 Provided the FOSS contribution policy permits contributions, a documented procedure exists that describes the FOSS contribution process.

**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 specific situation it is understood that no process may exist and this requirement would nevertheless be met.

## G6: Certify Adherence to OpenChain Requirements

**6.1 In order for an organization to be OpenChain certified, it must affirm that it has a FOSS program that meets the criteria described in this OpenChain Conformance Specification version 1.0.**

**Verification Artifact(s):**

* 6.1.1 The organization affirms that a program exists that meets all the requirements of this OpenChain Conformance Specification version 1.0.

**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.