**Spécifications OpenChain**

Version 1.1

**Contents**

[1) Introduction 3](#_Toc480843023)

[2) Définitions 4](#_Toc480843024)

[3) Exigences 5](#_Toc480843025)

[G1: Know Your FOSS Responsibilities 5](#_Toc480843026)

[G2: Assign Responsibility for Achieving Compliance 7](#_Toc480843027)

[G3: Review and Approve FOSS Content 8](#_Toc480843028)

[G4: Deliver FOSS Content Documentation and Artifacts 9](#_Toc480843029)

[G5: Understand FOSS Community Engagement 10](#_Toc480843030)

[G6: Certify Adherence to OpenChain Requirements 11](#_Toc480843031)

[Appendix I: Language Translations 12](#_Toc480843032)

Copyright © 2016-2017 Linux Foundation. This document is licensed under the Creative Commons Attribution 4.0 International (CC-BY 4.0) license. A copy of the license can be found at <https://creativecommons.org/licenses/by/4.0/>.

# Introduction

L’Initiative OpenChain a débuté en 2013 quand un groupe de professionnels de l'open source a observé deux tendances émergentes : 1) des similarités significatives existent entre les processus d'organisations ayant un programme de conformité open source mâture ; et 2) il existe encore un grand nombre d’organisations échangeant du logiciel ayant des programmes moins développés. Cette dernière observation a entrainé un manque de confiance dans la cohérence et la qualité des livrables de conformité accompagnant le logiciel échangé. En conséquence, à chaque maillon de la chaîne de fournisseurs, les organisations avales refaisaient régulièrement le travail de conformité déjà réalisé par les organisations amonts.

Un groupe d’étude fût formé pour évaluer si une spécification d’un programme standard pourrait être créée qui permettrait de : i) faciliter une meilleure qualité et cohérence des informations de conformité open source partagées au travers de l’industrie ; et ii) diminuer les coûts importants associés à l’open source résultant de la nécessité de revoir la conformité. Le groupe d’étude a évolué en un groupe de travail, et en avril 2016, organisé formellement en tant que projet collaboratif de la Fondation Linux.

La Vision et la Mission de l’initiative OpenChain sont les suivantes :

* **Vision : Une chaîne de fournisseur de logiciel dans laquelle le logciel libre et/ou open source est fourni avec des informations de conformité fiables et cohérentes.**
* **Mission: Etablir les exigences pour atteindre une gestion efficace des logiciels libre et/ou open source pour les participants de la chaîne de fournisseurs de logiciel, afin que les exigences et garanties associées soient développées collaborativement et ouvertement par les représentants de la chaîne de fournisseurs de logiciel, la communauté open source, et le monde universitaire.**

En accord avec la Vision et la Mission, cette spécification définit un jeu d’exigences qui, si satisfaites, améliorera significativement la probabilité qu’un programme de conformité open source ait achevé un niveau suffisant de qualité, cohérence et complétude ; bien qu’un programme qui satisfasse toutes les exigences de la spécification ne garantisse pas une conformité complète. Les exigences représentent un jeu d’exigences de base (minimum) qu’un programme doit satisfaire pour être considéré Conforme à OpenChain. La spécification se concentre sur les qualités des ‘quoi’ et ‘pourquoi’ d’un programme de conformité et non aux considérations des ‘comment’ et ‘quand’. Ceci assure un niveau --réaliste-- de flexibilité qui permet aux différentes organisations d’adapter leurs politiques et processus pour mieux atteindre leurs objectifs.

La section 2 introduit les définitions et termes clés utilisés tout au long de la spécification. La section 3 présentes les exigences de la spécification avec pour chacune une liste d’un ou plusieurs --Artéfacts-- de Vérification. Ils représentent la preuve qui doit exister pour considérer une exigence donnée satisfaite. Si toutes les exigences ont été satisfaites pour un programme donné, il sera considéré Conforme à OpenChain en accord avec la version 1.1 de cette spécification. Les Artéfacts de Vérification ne sont pas destinés à être publics, mais pourraient être fournis sous --Accord de Confidentialité-- ou sur demande privée de l'organisation OpenChain pour valider la conformité.

# Définitions

**FOSS (Free and Open Source Software, logiciel libre et/ou open source) - logiciel soulmis à une ou plusieurs licences qui respecte l'Open Source Definition publiée par l'Open Source Initiative (OpenSource.org) ou la Free Software Definition (publiée par la Free Software Foundation) ou licence similaire.**

**Contact FOSS - une personne chargée de recevoir les demandes externes de renseignement sur les FOSS**.

**Licences Identifiées - un ensemble de licences FOSS identifiées comme résultat d'une méthode appropriée d'identification de telles licences.**

**Conforme à OpenChain - un programme qui satisfait toutes les exigences de cette spécification.**

**Equipe Logiciel - tout employé ou consultant qui** définit, contribue à, ou est responsable de préparer, le Logiciel Fourni. En fonction des organisations, ceci peut inclure (mais n'est pas limité à) les développeurs logiciel, les ingénieurs de version, les ingénieurs qualité, les responsables produit et marketing produit.

**SPDX ou Software Package Data Exchange (Echange de Données de Paquet Logiciel) - le format standard créé par le Groupe de Travail SPDX pour les informations de licence et de droits d'auteur pour un paquet logiciel donné. Une description de la spécification SPDX peut être trouvée sur le site www.spdx.org.**

**Logiciel Fourni - logiciel qu'une organisation fournit à des tierces parties (i.e., personnes morales et/ou physiques).**

**Points de Vérification - preuve qui doit exister pour qu'une exigence puisse être considérée comme satisfaite.**

# Exigences

## G1: Connaître vos responsabilités vis à vis des FOSS

* 1. **Il existe une politique formelle relative aux FOSS qui régit la conformité aux licences FOSS pour la distribution du Logiciel Fourni. La politique doit être communiquée en interne.**

**Point(s) de vérification** :

* 1.1.1 Il existe une politique documentée relative aux FOSS.
* 1.1.2 Il existe une procédure documentée informant l'Equipe Logiciel de l'existence d'une politique FOSS (par exemple, via formation, wiki interne, ou autre moyen de communication).

**Raison**:

S'assurer que l'Equipe Logiciel ait été informée de l'existence d'une politique FOSS. Bien qu'aucune exigence ne soit fournie ici sur ce que la politique devrait contenir, d'autres sections peuvent définir des exigences sur son contenu.

* 1. **Il existe une formation sur le FOSS, obligatoire pour l"Equipe Logiciel, qui :**
* **Au minimum, couvre les sujets suivants :**
  + **La politique FOSS et où en trouver une copie ;**
  + **Les bases de la Propriété Intellectuelle en relation avec le FOSS et les licences FOSS ;**
  + **Les concepts de licences FOSS (y compris les concept de licence permissive et copyleft) ;**
  + **Les modèles de licences de projet FOSS ;**
  + **Les rôles et responsabilités de l'Equipe Logiciel vis-à-vis de la politique FOSS en général et de la conformité FOSS en particulier ; et**
  + **Les processus pour identifier, enregistrer et tracer les composants FOSS contenus dans le Logiciel Fourni.**
* **L'Equipe Logiciel doit avoir reçu cette formation FOSS dans les derniers 24 mois (pour être considérée valide). Un test peut être utilisé pour permettre à l'Equipe Logiciel de satisfaire cette exigence de formation.**

**Point(s) de vérification :**

* 1.2.1 Il existe un support de formation au FOSS couvrant les sujets mentionnés ci-dessus (par exemple, diapositives de présentation, cours en ligne, ou autre support de formation).
* 1.2.2 Méthode de suivi de la participation à la formation par l'Equipe Logiciel.
* 1.2.3 Au moins 85% de l'Equipe Logiciel a une formation au FOSS valide, telle que défini ci-dessus.

**Raison**:

S'assurer que l'Equipe Logiciel a récemment participé à la formation FOSS et qu'un ensemble clé des sujets liés au FOSS est couvert. L'intention est d'assurer qu'un ensemble clé de sujets de base est couvert mais qu'un programme typique de formation serait succeptible d'être plus complet que ce qui est réquit ici.

* 1. **Il existe un processus pour revoir les Licences Identifiées pour déterminer leurs obligations, restrictions et droits accordés par chacune des licences.**

**Point(s) de vérification :**

* 1.3.1 Il existe une procédure documentée pour revoir et renseigner les obligations, restrictions et droits accordés par chacune des Licences Identifiées gouvernant le Logiciel Fourni.

**Raison**:

S'assurer qu'il existe un processus pour revoir et identifer les obligations des licences pour les cas d'usage donnés pour chaque Licence Identifiée.

## G2: Attribuer les responsabilités pour atteindre la conformité

**2.1 Identifiez un rôle de Correspondant FOSS("Correspondant FOSS").**

* **Attribuez à une ou plusieurs personne la responsabilité de traiter les demandes FOSS externes ;**
* **Le correspondant FOSS doit s'appliquer, dans une limite raisonable d'un point de vue commercial, à traiter correctement les demandes de conformité FOSS ; et**
* **Indiquez publiquement un moyen simple de joindre le correspondant FOSS.**

**Point(s) de vérification** :

* 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).
* 2.1.2 An internal documented procedure exists that assigns responsibility for receiving FOSS compliance inquiries.

**Raison**:

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.**

**Point(s) de vérification** :

* 2.2.1 Name of persons, group or function in FOSS Compliance role(s) internally identified.
* 2.2.2 Identify source of legal expertise available to FOSS Compliance role(s) which could be internal or external.
* 2.2.3 A documented procedure exists that assigns internal responsibilities for FOSS compliance.
* 2.2.4 A documented procedure exists for handling the review and remediation of non-compliant cases.

**Raison**:

Ensure certain FOSS responsibilities have been effectively assigned.

## G3: Review and Approve FOSS Content

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

**Point(s) de vérification :**

* 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.
* 3.1.2 FOSS component records exist for each Supplied Software release which demonstrates the documented procedure was properly followed.

**Raison**:

To ensure a process exists for creating and managing a FOSS component bill of materials 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 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;**
* **contains modified FOSS;**
* **contains FOSS or other software under an incompatible license interacting with other components within the Supplied Software; and/or**
* **contains FOSS with attribution requirements.**

**Point(s) de vérification** :

* 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.

**Raison**:

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.

## G4: Fourniture des Documentations et Livrables FOSS

**4.1         Préparer l'ensemble des livrables qui représente la sortie du programme de gestion des FOSS pour chacune des versions du Logiciel Fourni. Cet ensemble correspond aux Livrables de Conformité qui peuvent inclure (mais ne sont pas limités à) un ou plusieurs des items suivants : code source, notices d'attribution, notices de droits d'auteur, copie des licences, notifications de modifications, offres écrites, documents SPDX et ainsi de suite.**

**Point(s) de vérification :**

* 4.1.1 Il existe une procédure documentée qui assure que les Livrables de Conformité sont préparés et distribués avec les versions du Logiciel Fourni comme requis par les Licences Identifiées.
* 4.1.2 Des copies des Livrables de Conformité de la version du Logiciel Fourni sont archivées et facilement accessibles, et une archive est plannifiée pour être disponible tant que le Logiciel Fourni est offert ou que ceci est requis par les Licences Identifiées (le plus long des deux).

**Raison**:

S'assurer qu'une collection complète des Livrables de Conformité ainsi que les rapports créés dans le cadre du processus de revue des FOSS accompagnent le Logiciel Fourni comme requis par les Licences Identifiées qui gouvernent le Logiciel Fourni.

## G5: Understand FOSS Community Engagement

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

**Point(s) de vérification** :

* 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).

**Raison**:

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.**

**Point(s) de vérification :**

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

**Raison**:

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.

## 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 management program that meets the criteria described in this OpenChain Specification version 1.1.**

**Point(s) de vérification** :

* + - 6.1.1 The organization affirms that a FOSS management program exists that meets all the requirements of this OpenChain Specification version 1.1.

**Raison**:

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.**

**Point(s) de vérification :**

* + - 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.

**Raison**:

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 overtime.

# Appendix I: Language Translations

To facilitate global adoption we welcome efforts to translate the specification into multiple languages. Because OpenChain functions as an open source project translations are driven by those willing to contribute their time and expertise to perform translations under the terms of the CC-BY 4.0 license and the project’s translation policy. The details of the policy and available translations can be found on the OpenChain project [specification webpage](https://wiki.linuxfoundation.org/openchain/spec-translations).