

Copyright © 2016-2017 Linux Foundation. Questo documento è distribuito con licenza Creative Commons Attribuzione 4.0 Internazionale (CC-BY 4.0) . Una copia della licenza è reperibile presso <https://creativecommons.org/licenses/by/4.0/>.

## Introduzione

L'OpenChain Initiative cominciò nel 2013 quando un gruppo di operatori impegnati nella filiera di approvvigionamento del software open source osservò l'insorgenza di due tendenze:

- esistevano significative similitudini tra organizzazioni con programmi maturi di conformità open source; e
- permaneva un ampio numero di organizzazioni che scambiavano software con programmi meno evoluti.

Dalla seconda osservazione scaturiva una mancanza di fiducia nella uniformità e qualità dei risultati in termini di conformità che si accompagnavano al software così scambiato. Come conseguenza, a ogni passaggio nella catena di fornitura, le organizzazioni a valle si trovavano frequentemente a compiere nuovamente gli sforzi di conformità già eseguiti da altre organizzazioni a monte.

Fu formato un gruppo di studio al fine di considerare se potesse essere creato un programma di specifiche standardizzate che

- facilitasse una più alta qualità e uniformità delle informazioni sulla conformità open source che si scambiavano all'interno dell'industria; e
- diminuisse gli elevati costi di transazione associati all'open source risultante dal rifacimento della conformità.

Il gruppo di studio evolvette in un gruppo di lavoro e, in aprile 2016 venne formalmente organizzato come un progetto collaborativo della Linux Foundation.

La Visione e la Missione dell'OpenChain Initiative sono le seguenti:

- Visione: una filiera di approvvigionamento dove il software libero/open source (FOSS) fosse trasmesso con informazioni sulla conformità affidabili e uniformi.
- Missione: stabilire requisiti per raggiungere una gestione efficiente del software libero/open source (FOSS) per i partecipanti alla filiera di approvvigionamento del software, in modo che tali requisiti e il relativo materiale di supporto siano sviluppati in modo collaborativo e aperto da rappresentanti della filiera di approvvigionamento del software, dalla comunità open source e dal mondo accademico.

In coerenza con la Visione e la Missione, queste specifiche definiscono un insieme di requisiti che, se rispettati, incrementerebbero significativamente la probabilità che un programma di conformità open source abbia raggiunto un sufficiente livello di qualità, uniformità e completezza; ciononostante, un programma che soddisfi tutte i requisiti delle specifiche non garantisce una piena conformità. I requisiti rappresentano un insieme di livello base (minimo) di requisiti che un programma deve rispettare per essere considerato essere conforme con OpenChain. Le specifiche si focalizzano sul "cosa" e sul "perché" di un programma di conformità, in contrapposizione a considerazioni sul "come" e sul "quando". Ciò assicura un livello pratico di flessibilità che permette a diverse organizzazioni di confezionare su misura le proprie procedure e processi per adattarsi meglio ai propri obiettivi.

Il Capitolo 2 introduce definizioni dei termini chiave usati all'interno delle specifiche. Il Capitolo 3 presenta i requisiti delle specifiche dove ciascuna ha una lista di uno o più Risultati Attesi. Essi rappresentano la prova che deve sussistere al fine di considerare un dato requisito soddisfatto. Se tutti i requisiti sono stati rispettati per un dato programma, esso viene considerato Conforme a OpenChain nel rispetto della versione 1.1 delle specifiche. I Risultati Attesi non sono pubblici, ma possono essere forniti sotto NDA o su richiesta confidenziale da parte di un'organizzazione [che si conforma a] OpenChain <!-- FIXME confrontarsi con Shane, che cavolo vuol dire questa parte qui, non è chiaro, manca "conforming" --> per validare la conformità.

## Definizioni

**FOSS (Free and Open Source Software)** : Software sottoposto a una o più licenze che rispettano la Open Source Definition, pubblicata dalla Open Source Initiative (OpenSource.org) o la Free Software Definition (pubblicata dalla Free Software Foundation) o licenze simili.

**Persona di Contatto FOSS**

Una persona designata a ricevere richieste di informazioni circa il FOSS.

**Licenze identificate**

Un insieme di licenze FOSS identificate a seguito dell'applicazione di un metodo appropriato di identificazione di tali licenze.

**Conforme a OpenChain** : un programma che soddisfi tutti i requisiti di questa specifica.

**Staff del Software**

un dipendente o un appaltatore che definisce, contribuisce a o ha responsabilità circa la preparazione di Software fornito. A seconda dell'organizzazione, ciò potrebbe includere (ma non si limita a) sviluppatori software, specialisti del rilascio, responsabili della qualità, responsabili del marketing di prodotto, responsabili di prodotto.

SPDX o Software Package Data Exchange : il formato standard creato dall' SPDX Working Group per lo scambio di informazioni di licenza e copyright circa un determinato pacchetto software. Una descrizione delle specifiche SPDX può essere reperita a <http://www.spdx.org> <!--  
FIXME segnalare che gli URL vanno sempre identificati con il protocollo! -->

Software Fornito : software che un'organizzazione fornisce a terze parti (per esempio, a un'altra organizzazione o a un'altra persona)

Risultati Attesi : prove che debbono esistere al fine di considerare soddisfatto un determinato requisito.

## Requisiti

### ## G1: Conosci le tue responsabilità in materia di FOSS

1. Esiste una policy FOSS interna, la quale regola il rispetto delle licenze FOSS nella distribuzione del Software Fornito. La Policy deve essere comunicata internamente.

Risultati Attesi

- 1.1.1 Esistenza di una policy FOSS scritta
- 1.1.2 Esistenza di Una procedura documentata che renda tutto lo Staff del Software informato dell'esistenza di una policy FOSS (per esempio, tramite formazione, un wiki interno, ovvero altri metodi di comunicazione).

Razionale

Assicurare che siano stati intrapresi passi nella direzione di creare, registrare e rendere lo Staff del Software informato dell'esistenza di una policy FOSS. Sebbene qui non sono forniti requisiti su cosa debba essere incluso in tale policy, altre sezioni potrebbero imporre requisiti sulla policy.

Esiste un aggiornamento FOSS obbligatorio per tutto lo Staff del Software, tale per cui:

<!-- FIXME: inserire la numerazione -->

- Il training, come minimo, copre le seguenti aree:
  - La policy FOSS e dove reperire una copia;
  - Fondamenti del diritto della proprietà industriale attinente al FOSS e alle licenze FOSS;
  - I concetti del licensing FOSS (inclusi i concetti di licenze permissive e copyleft);
  - I modelli di licenza del FOSS;
  - Ruoli e responsabilità dello Staff Software riguardo specificamente alla conformità FOSS e in generale alla policy FOSS; e
  - Processi per identificare, registrare e/o tenere traccia di componenti FOSS contenuti nel Software Fornito.
- Lo Staff Software deve aver completato un aggiornamento FOSS nei 24 mesi (per essere considerato aggiornato). Un test può essere impiegato per consentire allo Staff Software di soddisfare il requisito di aggiornamento.

Risultati Attesi

- Esiste materiale di aggiornamento FOSS che copre le aree di cui sopra (per esempio, set di slide, corsi online o altro materiale di aggiornamento).
- Un metodo per tenere traccia del completamento dell'aggiornamento per tutto lo Staff Software.
- Almeno l'85% dello Staff Software è aggiornato, come da definizioni nel capitolo precedente.

Razionale

Assicurare che lo Staff Software abbia recentemente partecipato a un aggiornamento FOSS e che un insieme fondamentale di argomenti FOSS siano stati affrontati. L'intento è di assicurare che un livello di base fondamentale di argomenti siano stati affrontati, ma un programma di aggiornamento tipico sarebbe verosimilmente più ampio di quanto qui è richiesto.

Esiste un processo per esaminare le Licenze Identificate per determinare le obbligazioni, le restrizioni e i diritti conferiti da ciascuna licenza.

## Risultati Attesi

- Esistenza di una procedura documentata per la revisione e la documentazione delle obbligazioni, delle restrizioni e dei diritti conferiti da ciascuna Licenza Identificata che regoli il Software Fornito.

## Razionale

Assicurare l'esistenza di una procedura documentata per la revisione e la documentazione delle obbligazioni, delle restrizioni e dei diritti conferiti da ciascuna Licenza Identificata per le varie ipotesi d'uso.

## Assegna responsabilità per raggiungere la conformità

### Identifica le Funzioni di coordinamento esterno del FOSS ("Persona di Contatto FOSS")

- Nomina i soggetti responsabili per ricevere domande esterne sul FOSS;
- Le Persone di Contatto FOSS devono intraprendere sforzi commercialmente ragionevoli per rispondere appropriatamente alle richieste circa la conformità FOSS; e
- Identificare pubblicamente un mezzo tramite il quale si possa contattare il Contatto FOSS.

## Risultati Attesi

- Identificazione pubblica della funzione di Contatto FOSS (per esempio, tramite un indirizzo email pubblicizzato, o la Open Compliance Directory della Linux Foundation).
- Esistenza di una procedura interna documentata che assegna le responsabilità per ricevere richieste circa la conformità FOSS.

## Razionale

Assicurare che vi sia un modo ragionevole per i terzi di contattare l'organizzazione per domande circa la conformità FOSS e che questa responsabilità sia stata effettivamente assegnata.

### Identifica i ruoli interni di conformità FOSS

- Nomina i soggetti responsabili per gestire la conformità FOSS interna. Il ruolo circa la conformità FOSS interna e il ruolo di Contatto FOSS possono coesistere nella stessa persona.
- L'attività di gestione della conformità FOSS è dotata di sufficienti risorse:
  - Il tempo per svolgere le funzioni del ruolo è stato allocato; e
  - Un budget commercialmente ragionevole è stato assegnato.
- Assegna responsabilità di sviluppare e manutenere le policy e i processi FOSS;
- Competenze legali circa la conformità FOSS sono accessibili ai ruoli di conformità FOSS (potrebbero essere risorse interne o esterne); e
- Esiste un processo per la risoluzione di questioni di conformità FOSS.

## Risultati Attesi

- I nomi delle persone, gruppi o funzioni nei ruoli di conformità FOSS identificati internamente.
- L'identificazione di risorse di competenza legale disponibili alle funzioni di conformità FOSS, che possono essere interne o esterne.
- Esistenza di una procedura identificata per assegnare responsabilità interne per la conformità FOSS.
- Esistenza di una procedura documentata per gestire la revisione di casi di mancata conformità e porvi rimedio.

## Razionale

Assicurare che le responsabilità FOSS siano effettivamente assegnate.

<span id="\_Toc480843028"

## class="anchor">G3: Verifica e Approva il Contenuto FOSS

3.1 Esiste un processo per creare e gestire una lista di materiali per il componente FOSS G3 che include ciascun componente (e le sue Licenze Identificate) in una versione del Software Fornito.

## Risultati Attesi:

- 3.1.1 Esiste una procedura per identificare, tracciare e archiviare informazione sulla collezione di componenti FOSS dai quali è

composta una versione del Software Fornito.

- 3.1.2 Esistono registrazioni dei componenti FOSS per ciascuna versione del Software Fornito che dimostrano che la procedura documentata è stata seguita correttamente.

#### Razionale

Garantire che esista un processo per creare e gestire una lista dei materiali per il componente FOSS utilizzata per costruire il Software Fornito. Una lista dei materiali è necessaria per supportare la revisione sistematica dei termini di licenza di ciascun componente per comprendere gli obblighi e le restrizioni applicabili alla distribuzione del Software Fornito.

Il programma di gestione del FOSS deve essere in grado di gestire i casi comuni d'uso di licenza FOSS incontrati dallo Staff del Software per il Software Fornito, che possono includere i seguenti casi d'uso (si noti che l'elenco non è esaustivo e non si applicano tutti i casi d'uso):

- distribuito in formato binario;
- distribuito in formato sorgente;
  - integrato con altro FOSS che può attivare degli obblighi copyleft; - contiene FOSS modificato; - contiene FOSS o altro software con una licenza incompatibile che interagisce con altri componenti del Software Fornito; e/o
  - contiene FOSS con requisiti di attribuzione.

#### Risultati Attesi

- 3.2.1 È stata implementata una procedura che gestisce i casi comuni d'uso di licenza FOSS per i componenti FOSS di ciascuna versione del Software Fornito.

#### Razionale

Assicurare che il programma è sufficientemente robusto per gestire > i casi comuni d'uso di licenza FOSS per un'organizzazione. Che esiste > una procedura per supportare quest'attività e che la procedura è seguita. >

## G4: Consegna la Documentazione e i Materiali del Contenuto FOSS

4.1 Preparare l'insieme di materiali che rappresentano il risultato del programma di gestione del FOSS per ogni versione del Software Fornito. Questo insieme è definito come Materiali di Conformità che possono includere (ma Non sono limitati a) uno o più dei seguenti: codice sorgente, dichiarazione di attribuzione, dichiarazione sul copyright, copia delle licenze, notifiche di modifica, offerte scritte, documenti SPDX e così via.

#### Risultati Attesi

- 4.1.1 Esiste una procedura documentata che assicura che i Materiali di Conformità vengono preparati e distribuiti con la versione del Software Fornito come richiesto dalle Licenze Identificate.
  - 4.1.2 Copie dei Materiali di Conformità della versione del Software Fornito sono archiviate e facilmente recuperabili, ed è previsto che l'archivio esista almeno fino a quando il Software Fornito viene offerto o è richiesto dalle Licenze Identificate (a seconda di quale sia il termine più lungo).

#### Razionale

Assicurare che la collezione completa dei Prodotti di Conformità accompagni il Software Fornito come richiesto dalle Licenze Identificate che disciplinano il Software Fornito insieme alle altre relazioni create nel quadro del processo di revisione FOSS.

### G5: Comprendere il Coinvolgimento della Comunità FOSS

5.1 Esiste una politica scritta che regola i contributi ai progetti FOSS da parte dell'organizzazione. La politica deve essere comunicata internamente.

#### Risultati Attesi

- 5.1.1 Esiste una politica documentata di contributo FOSS;
- 5.1.2 Esiste una procedura documentata che rende tutto il Personale Software consapevole dell'esistenza della politica di contributo FOSS (per esempio, mediante formazione, un wiki interno, altri metodi pratici di comunicazione).

## Razionale

Assicurarsi che un'organizzazione abbia dato ragionevole considerazione allo sviluppo di una politica per contribuire pubblicamente al FOSS. La politica di contributo FOSS può far parte della politica globale FOSS di un'organizzazione o può essere una politica specifica. Nella situazione in cui i contributi non sono consentiti del tutto, dovrebbe esistere una politica che renda chiara questa posizione.

5.2 Se un'organizzazione consente i contributi ai progetti FOSS allora deve esistere un processo che implementi la politica di contributo FOSS prevista nel capitolo 5.1.

## Risultati Attesi

- 5.2.1 Se la politica di contributo FOSS consente di contribuire, esiste una procedura documentata che disciplina i contributi FOSS.

## Razionale

Assicurarsi che un'organizzazione abbia un processo documentato riguardo come > l'organizzazione contribuisce pubblicamente FOSS. Può esistere una politica > tale per cui i contributi non sono consentiti del tutto. In questa situazione è > chiaro che una procedura può non esistere e questo requisito sarebbe > comunque soddisfatto. G6:

## Certificare l'Adesione ai Requisiti OpenChain

6.1 Affinché un'organizzazione sia certificata OpenChain, deve dichiarare di disporre di un programma di gestione FOSS che soddisfa i criteri descritti in questa versione 1.1 della Specifica OpenChain.

Prodotto(i) di Verifica:

- 6.1.1 L'organizzazione dichiara che esiste un programma di gestione FOSS che soddisfa tutti i requisiti di questa Specifica OpenChain versione 1.1.

## Razionale

>

Per garantire che se un'organizzazione dichiara di avere un programma che è Conforme ad OpenChain, tale programma ha soddisfatto tutti i requisiti di questa specifica. La semplice conformità ad un sottoinsieme di tali requisiti non sarebbe considerata sufficiente per garantire che un programma sia certificato OpenChain.

\*\*6.2 La conformità con questa versione della specifica durerà 18 mesi dalla data di ottenimento della convalida della conformità. I requisiti di convalida possono essere trovati sul sito web del progetto OpenChain. \*\*

Prodotto(i) di Verifica:

- 6.2.1 L'organizzazione afferma che esiste un programma di gestione FOSS che soddisfa tutti i requisiti di questa Specifica OpenChain versione 1.1 negli ultimi 18 mesi di ottenimento della convalida di conformità.

## Razionale

È importante che l'organizzazione rimanga aggiornata con la specifica se vuole affermare la conformità del programma nel tempo. Questo requisito assicura che i processi e i controlli che supportano il programma non sono erosi se vogliono continuare ad assicurare la conformità alle specifiche nel tempo.

## Appendice I: Traduzioni =====

Per facilitare l'adozione globale, accogliamo con piacere gli sforzi per tradurre la specifica in più lingue. Poiché OpenChain funziona come un progetto open source le traduzioni sono guidate da coloro che vogliono contribuire con il loro tempo e le loro competenze per eseguire le traduzioni secondo i termini della licenza CC-BY 4.0 e secondo la politica di traduzione del progetto. I dettagli della politica e le traduzioni disponibili si trovano nella [pagina web della specifica](#) del Progetto OpenChain.