OPENCHAIN

OpenChain 規範書
1.1 版

內容

This is an official translation from the OpenChain Project. It has been translated from the original English text. In the event there is confusion between this translation and the English version, The English text shall take precedence.

本文爲 OpenChain 專案的正式翻譯。其由原始英文文本翻譯而來。當本翻譯與英文版本混淆，英文文本應優先。

1) 簡介

OpenChain 促進會始於 2013 年，當時一群軟體供應鏈開源執事人員觀察到兩個新興型態：1) 於具有成熟開源合規方案組織間重要程序的相似性；以及 2) 仍然有大量的組織採較低度發展的方案來交換軟體。後一觀察現象導致伴隨軟體交換的合規稽證在一致性和質量上缺乏信任。因此，在供應鏈的每一層，下游組織經常重做上游組織已經執行過的合規工作。

一個研究團隊被成立來考量是否可以創建一份標準方案規範書，以：i) 促進產業間共享的開源合規資訊有更佳的質量及一致性；和 ii) 降低與開源合規工程重覆施行有關的高交易成本。該研究團隊發展爲一個工作團隊，並於 2016 年 4 月，正式編組爲 Linux Foundation 下的協作專案。
OpenChain 促進會的願景和任務如下：

- **願景：** 一個傳遞自由開源軟體 (free/open source software, FOSS) 時附隨可靠和一致合規資訊的軟體供應鏈。

- **任務：** 爲軟體供應鏈參與者制定可達到 FOSS 有效管理的要件，並使來自軟體供應鏈、開源社群，以及學術界的代表們，能開放且協力地發展本要件及相關附屬文件。

依據願景和任務，本規範書定義了一系列的要件，儘管一個滿足所有規範書要件的方案並不能保證完整合規；然當要件被滿足時，將大爲增加開源合規方案達到充足質量、一致性，及完整性等級的可能性。這些要件呈現一個方案被視爲遵循 OpenChain 所必須滿足的基礎等級（最小）要求。相較於「如何」及「何時」的考量，本規範書聚焦於合規方案「什麼」及「爲什麼」的特性。這確保了實際操作的靈活度，使不同的組織能定製他們的政策及程序以適切符合他們的目標。

第二章介紹貫穿本規範書所使用關鍵用語的定義。第三章介紹規範書要件，每個要件都有一個或多個審核稽證的列表。爲了讓給定的要件被視爲滿足，它們代表必須存在的證據。倘若給定方案的所有要件都達到，該方案將根據 OpenChain 規範書 1.1 版被視爲遵循 OpenChain。審核稽證並非被指定公開，然得以在保密協議下或應 OpenChain 組織的私下要求來提供以驗證一致性。

2) 定義

FOSS（自由開源軟體） - 軟體程式依據一個或多個授權條款，該條款符合開放源碼促進會 (OpenSource.org) 發布之開放源碼定義 (Open Source Definition) 或自由軟體基金會發布之自由軟體定義 (Free Software Definition) 或類似條款。

FOSS 聯繫人-被指派接收外部 FOSS 垂詢的指定人員。

確認條款 - 依循適當方法而確認的一組 FOSS 授權條款。

遵循 OpenChain - 滿足本規範書所有要件的方案

軟體工作人員 - 任何對提供軟體進行範圍界定、貢獻，或負責準備的雇員或承包商。依據組織，可能包括（但不限於）軟體開發人員，發布工程師，品管工程師，產品行銷以及產品管理。

SPDX 或軟體套件資料交換 - 由 SPDX 工作團隊爲給定軟體套件創建用以交換授權與著作權資訊的標準格式。有關 SPDX 規範的說明，可見 www.spdx.org。

提供軟體 - 組織向第三方交付的軟體。

審核稽證 - 爲了使給定要件被視爲滿足，所必須存在的證據。

3) 要件

G1：了解你的自由開源軟體責任

1.1 **存在一份成文的 FOSS 政策書，用於管理提供軟體散布時的 FOSS 授權合規。**該政策必須於內部傳達。

審核稽證：

- ☐ 1.1.1A 存在一份被列冊的 FOSS 政策書。
- ☐ 1.1.2A 存在一份被列冊的流程，使得所有的軟體工作人員知悉 FOSS 政策書的存在。（例如，透過教育訓練，內部共筆，或其他實際可行的傳達方式。）

理由說明：

確保 FOSS 政策書被創建、紀錄，並使軟體工作人員知悉其存在的步驟被執行。雖然什麼應該要被包括到政策書裡在此並未被提出，然其他章節可能會施加要求。

1.2 存在對所有軟體工作人員必須性的 FOSS 教育訓練，使得：

- **該教育訓練，至少包括以下主題：**
  - **FOSS 政策書及至何處取得副本；**
  - **涉及 FOSS 及 FOSS 授權條款的智慧財產法律基礎知識；**
  - **FOSS 授權概念（包括寬鬆式及 copyleft 授權的概念）；**
  - **FOSS 專案授權模式；**
  - **軟體工作人員的角色及其與具體 FOSS 合規及一般 FOSS 政策相關的責任；及**
  - **於提供軟體裡確認，紀錄和／或追蹤 FOSS 元件的程序。**
- **軟體工作人員必須在過去 24 個月內完成 FOSS 教育訓練（方被視爲當期）。得使用測驗方式許可軟體工作人員滿足此一教育訓練的要求。**

審核稽證：

- ☐ 1.2.1 存在涵蓋上述各主題的 FOSS 教育訓練素材（例如，投影片、線上課程，或其他教育訓練素材）。
- ☐ 1.2.2 追蹤所有軟體工作人員完成教育訓練的方法。
- ☐ 1.2.3 根據上述定義，至少 85% 的軟體工作人員是當期的。

理由說明：

確保軟體工作人員參與了近期的 FOSS 教育訓練，且一組核心的 FOSS 相關主題被包含其內。此目的是爲了確保核心基礎層面的主題得到涵蓋，然典型的教育訓練方案可能比此處的要求更爲全面。

1.3 存在審查確認條款的程序，以確定每個授權條款授與的權利，其義務性要求及限制。

審核稽證：

- 1.3.1 存在一份被列冊的流程，使每個管理提供軟體之確認條款，其授與的權利，義務性要求及限制得被審查與紀錄。

理由說明：

確保在各種使用案例裡，用於審查及確認每一個確認條款授權義務性要求的程序存在。

G2：分擔責任以達到合規

2.1 確認 FOSS 聯繫人的職責

- **指派人員負責接收外部的 FOSS 垂詢；**
- **FOSS 聯繫人必須盡其商業上合理的努力以合宜地回應 FOSS 合規垂詢；及**
- **公開地確認一個他人能夠連絡到 FOSS 聯繫人的途徑。**

審核稽證：

☐ 2.1.1 FOSS 聯繫人的職責是公開地確認（例如，透過一個已公布的連絡電郵地址，或透過 Linux Foundation 的開源合規聯繫目錄）。

☐ 2.1.2 存在一份被內部列冊的流程，以分配接收 FOSS 合規垂詢的責任。

理由說明：

確定第三方就 FOSS 合規垂詢有合理的管道能連絡組織，並且此責任已被有效率地分派。

2.2 確認內部 FOSS 合規內部的角色分配

- **指派人員負責管理內部的 FOSS 合規。此一 FOSS 合規角色與 FOSS 聯繫人可能爲同一人員。**
- **FOSS 合規管理活動得到充份資源：**
  - **履行該角色的時間已被分配；及**
  - **商業上合理的預算已被分配。**
- **分派開發及維護 FOSS 合規政策與程序的責任；**
- **與 FOSS 合規有關的法律專家可爲 FOSS 合規角色接觸諮詢（例如，可爲內部或外部專家）；及**
- **存在一套解決 FOSS 合規爭議的程序。**

審核稽證：

☐ 2.2.1 FOSS 合規角色分配的人員姓名，團體或職責在內部被確認。

☐ 2.2.2 確認內部或外部法律專家的源頭資訊能被 FOSS 合規角色獲得。

☐ 2.2.3 存在一份被列冊的流程，以分派 FOSS 合規的內部責任。

☐ 2.2.4 存在一份被列冊的流程，以處理不合規案例的審查與補正。

理由說明：

確定相當程度 FOSS 責任分擔已被有效率的分派。

G3：審查及核準自由開源軟體內容

3.1 存在一個程序用於建立與管理 FOSS 元件素材清單，該清單包含所發布提供軟體裡每一個元件及其確認條款。

審核稽證：

- 3.1.1 存在一份被列冊的流程，以確認，追蹤，及將構成所發布提供軟體的 FOSS 元件集合資訊建檔保存。
- 3.1.2 每個發布的提供軟體皆存在 FOSS 元件的紀錄，以證明該列冊流程被合宜的遵循。

理由說明：

爲確定建立與管理 FOSS 元件素材清單，以構成提供軟體的程序存在。一份支持系統性審查每一個元件授權條款的素材清單是必要的，以理解當它適用於提供軟體的散布時，義務性要求及限制爲何。

3.2 FOSS 管理方案必須能夠處理軟體工作人員提供軟體時，一般會碰到的使用案例，可能包括下列使用案例（注意本列表並未詳盡，亦可能不適用於所有的使用案例）：

- **以二進位執行檔形式散布；**
- **以源碼形式散布；**
- **與其他 FOSS 整合而可能觸發 copyleft 義務性要求；**
- **內含修改過的 FOSS；**
- **內含 FOSS 或其他軟體，是採與提供軟體裡其他互動元件不相容的授權條款；及／或**
- **內含 FOSS 帶有姓名標示的要求。**

審核稽證：

- 3.2.1 爲發布提供軟體裡的 FOSS 元件，一套能處理一般 FOSS 授權使用案例的流程已被實施。

理由說明：

確定該方案能充份堅實地處理組織常見的 FOSS 授權使用案例。存在一個支持這個活動的流程，且該流程被遵循。

G4：傳遞自由開源軟體內容文件及檔案集

4.1 **爲每個提供軟體準備一組代表其 FOSS 管理方案產出的檔案集。此被指稱的檔案集可能包括（但不限於）以下一個或多個：源碼，姓名標示聲明，著作權聲明，授權條款副本，修改註記，提供源碼的書面文件 (written offers)，SPDX 文件及其他。**

審核稽證：

- 4.1.1 存在一份被列冊的流程，以確定合規檔案集有依確認條款的要求，而與提供軟體發布時一同被準備及散布。

- 4.1.2 提供軟體發布時的合規檔案集副本被建檔保存並可輕易取回，且此保存檔規劃至少在提供軟體提供期間，或是依照確認條款的要求期間會存在（以較長者爲準）。

理由說明：

確定合規檔案集的完整集合，有依管理提供軟體之確認條款的要求，併與提供軟體及其他報告，被作爲 FOSS 審查程序的一部份。

G5：理解自由開源軟體社群參與

5.1 存在一份成文的政策書，以管理組織對 FOSS 專案的貢獻。該政策必須於內部傳達。

審核稽證：

- 5.1.1 存在一份被列冊的 FOSS 貢獻政策書；
- 5.1.2 存在一份被列冊的流程，使得所有的軟體工作人員知悉 FOSS 貢獻政策書的存在。（例如，透過教育訓練，內部共筆，或其他實際可行的傳達方式。）

理由說明：

確定一個組織對發展政策以公開貢獻 FOSS 已作了合理的考量。此 FOSS 貢獻政策可作爲組織整體 FOSS 政策的一部份，或作爲其獨立政策。當貢獻完全不被允許的情況下，一個明確表達此立場的政策也應該存在。

5.2 若組織允許貢獻 FOSS 專案，則實施 5.1 節描述的 FOSS 貢獻政策書之程序必須存在。

審核稽證：

- 5.2.1 倘若 FOSS 貢獻政策書允許貢獻，存在一份被列冊的流程以管理 FOSS 貢獻。

理由說明：

確定對組織如何公開貢獻 FOSS 有列冊的程序。若是貢獻完全不被允許，該政策書仍可存在。在這種狀況下，沒有流程存在是可理解的，且雖然如此本要件仍可被視爲達到。

G6：依循 OpenChain 要件進行認證

6.1 爲了使組織獲得 OpenChain 認證，該組織必須證實其 FOSS 管理方案達到 OpenChain 規範書 1.1 版描述的標準。

審核稽證：

- 6.1.1 該組織證實其 FOSS 管理方案存在，且達到本 OpenChain 規範書 1.1 版的所有要件。

理由說明：

要確定一個組織是否如其宣稱擁有方案是遵循 OpenChain 的，該方案要達到本規範書的所有要件。僅是達到這些要件的一小部份，該方案將不會被認爲足以保證得到 OpenChain 認證。

6.2 從一致性完成認證日開始，對此版本規範書的一致性狀態將會維持 18 個月。一致性認證的要件能在 OpenChain 專案網站上找到。

審核稽證：

- 6.2.1 組織證實其 FOSS 管理方案存在，達到本 OpenChain 規範書 1.1 版的所有要件，且在過去 18 個月內完成一致性認證。

理由說明：

若一個組織想長時間宣稱方案具一致性，那與當期規範書保持一致是很重要的。如果他們想要持續宣稱與此規範書具一致性的話，此一要件得確定方案的支持程序及控制不會逐步喪失。

附錄 I：語言翻譯

爲了便利全球採用，我們歡迎將本規範書翻譯成多種語言的努力。由於 OpenChain 採開源專案方式運作，翻譯亦由那些願意貢獻他們時間與專業的人士推動，依照 CC 姓名標示 4.0 授權與本專案的翻譯政策來進行。本政策的細節及現有翻譯能在 OpenChain 專案規範書網頁上找到。