OPENCHAIN

OPENCHAIN 規範書

版本 2.0

在開源裡建立信任以構建軟體解決方案

內容

此為 OpenChain 專案的官方翻譯，譯自原英文文本。當本譯文與英文版本產生混淆時，以英文版本優先。

1) 簡介

此份規範定義開源授權合規方案主要要件以確保其品質。目的是為了提供建立信任的基準讓組織間能夠交換由開源軟體組成的軟體解決方案。規範一致性確保了方案設計目的是為每個軟體解決方案生成所需的合規稽證（即法律聲明，原始碼等等)。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「為什麼」的特性。這能確保實際操作的靈活度，使不同的組織能選擇他們的政策及進程以適切符合他們的規模，目標以及範圍。舉例來說，OpenChain 一致性方案可以涵蓋單個產品線或整個組織。

此簡介提供相關訊息給所有潛在用戶。第二章定義貫穿本規範書所使用的關鍵術語。第三章定義方案實現一致性必須滿足的要件。此要件必須包含一個或一個以上審核稽證(亦即紀錄) 以確保能滿足要件。審核稽證不需要公開，雖然組織可能會根據保密協議（NDA）選擇將其提供給他人。

此規範是作為一項開放式計畫所開發而成，其中收到了來自 150 個以上貢獻者的回饋資訊。通過查看規範郵件列表和常見問題 (FAQs)，可以了解其歷史沿革。

2) 定義

"合規稽證" - 一組檔案集合代表交付軟體的輸出方案。其中可以包括（但不限於）以下中的一個或多個：原始碼，姓名標示聲明，著作權聲明，授權條款副本，修改註記，提供原始碼的書面文件(written offers)，開放原始碼元件物料清單以及 SPDX 文件。

"確認條款" - 一組經過適當方法來識別構成軟體的開源組件之開源軟體授權。

"OpenChain 一致性" - 滿足本規範書所有要件的方案。

"開源軟體" - 軟體程式依據一個或多個授權條款，該條款符合開放原始碼促進會 (OpenSource.org) 發布之開放原始碼定義 (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。

" **方案**" – 一套用來管理組織內開源授權合規行為的政策，流程和人員。

"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" - 此標準格式由 Linux 基金會下 SPDX (Software Package Data Exchange) 工作小組所設計，其目的是為了交換授權與著作權資訊於給定軟體套件。有關 SPDX 規範的說明，可見 www.spdx.org。

"交付軟體" - 組織向第三方交付的軟體。（例如，其他組織或個人）。

"審核資料" - 證明滿足給定要件的資料.

3) 要件

1.0 方案基礎

1.1 政策

具備一份成文且經過內部溝通的開源政策書，此政策書用於管理交付軟體散布時的開源合規授權。

審核資料:

- ☐ 1.1.1 具備一份開源政策書文件.
- ☐ 1.1.2 具備一份流程文件，使得所有的軟體工作人員知悉開源政策書的存在。（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 :

確保開源政策書撰寫、紀錄，並使軟體工作人員意識到開源策略之存在。雖然在此並未提出什麼應該要被包括到政策書裡，然而其他章節可能會增添要求。

1.2 能力

組織需要:

- **確認和方案執行以及效益之相關角色以及其相對應之職責;**
- **決定每個角色對應人員都具備必要能力**
- **確保這些人員透過適當的教育，培訓和/或經驗的基礎上能夠勝任職務;**
- **如有需要，採取行動以獲得必要的能力; 以及**
- **保留合適文件資訊以作為證明這些能力的證據。**

審核資料:

- ☐ 1.2.1 **具備一份說明文件，敘述方案中不同參與者的角色以及相對應之責任。**
- ☐ 1.2.2 **具備一份確認文件來敘述每個角色的能力。**
- ☐ 1.2.3 **具備一份證明文件評估每個方案參與者的能力。**

理由說明 :

確保履行方案職責的參與者已經取得足夠能力來履行其各自的角色和職責。

1.3 意識

組織應確保方案參與者了解:

a) 開源政策書;
b) 開源相關目標;
c) 參與者對於方案效益的貢獻; 以及
d) 未能遵守方案要件之影響。

審核資料:

- 1.3.1 具備一份證明文件評估每個方案人員對於方案目標，方案貢獻以及未能遵守方案要件之影響意識。

理由說明 :

確保方案人員對本方案中各自的角色和職責有足夠的意識。

1.4 方案範圍

不同的方案可能由不同層次範圍所管轄。例如，方案可以管理單一產品線系列，整個部門或整個組織。每一個方案須聲明其方案之指定範圍。

審核資料:

- 1.4.1 具備書面陳述來定義本方案的確切範圍和限制。

理由說明:

彈性化的構建方案以符合組織範圍需求。有些組織可以選擇維護特定產品線系列的方案，而其他組織則可以實行一個方案來管理整個組織內的交付軟體。

1.5 授權義務

具備審查確認條款的流程，以確定每個授權條款授與的權利，其義務性要求及限制。

審核資料:

- 1.5.1 具備一份流程文件，每個確認條款都須經過此流程進行審查與紀錄，以確認其授與的權利，義務性要求及限制。

理由說明:

確保具備一個確認條款授權義務性要求的流程，此流程可應用於組織內可能遇到的各種使用案例 (如要件 3.2 中所定義)。

2.0 定義並支持相關任務

2.1 接觸

維護一個有效回應來自外部開源查詢的流程。公開確認一個方法讓第三方可以進行開源合規性查詢。

審核資料:

- ☐ 2.1.1 具備公開可見的方法以允許任何第三方進行開源授權合規性查詢 (例如，透過一個公開的連絡電郵地址，或透過 Linux Foundation 的開源合規聯繫目錄)。
- ☐ 2.1.2 具備一個內部流程文件來描述如何回應第三方開源授權合規性查詢。

理由說明:

確保組織具備一個合理的方法，能夠聯絡以及有效回應來自第三方開源授權合規性查詢。

2.2 資源有效化

確認以及方案資源任務:

- **分配當責以確保能夠成功執行方案任務。**
- **方案任務具備充份資源:**
- **已配置履行該任務所需時間；及**
- **已配置充足的資金。**
- **具備一個用於審查和更新策略和支持任務的流程;**
- **需要指導的人可與開源合規有關的法律專家進行接觸；及**
- **具備一個解決開源合規爭議的流程。**

審核資料:

- ☐ 2.2.1 具備一份文件來記錄方案角色中確切人員，團體或職責之確切名稱。
- ☐ 2.2.2 確切安排人員於方案角色中，並提供充足的資金。
- ☐ 2.2.3 確認擁有內部或外部法律專業知識以解決開源授權合規事項。
- ☐ 2.2.4 具備一份流程文件來描述如何分派內部開源合規之職責。
- ☐ 2.2.5 具備一份流程文件來描述如何審核以及修正不合規之事例。

理由說明 :

確保：i）方案責任得到有效支持和充分資源 以及 ii）定期更新策略和支持流程，以最佳化的方式來適應並實踐開源合規性之變化。

3.0 審查及核準開源內容

3.1 物料清單

具備一個流程用來建立以及管理物料清單，該清單包含交付軟體中每一個開源元件 (以及確認授權條款)。

審核資料:

- ☐ 3.1.1 具備一份流程文件來描述如何確認，追蹤，審查，核準和歸檔有關交付軟體中的開源元件集合。
- ☐ 3.1.2 每個交付軟體皆需具備開源元件紀錄，以證明該流程文件被合宜的遵循。

理由說明:

確保具備一個流程能夠建立以及管理交付軟體中的開源元件物料清單。物料清單用來支持系統面審查以及批准每個組件的授權條款以瞭解散布交付軟體中所需之義務以及限制。

3.2 授權條款合規

此方案必須能夠管理軟體工作人員在處理交付軟體上，時常會碰到的開源授權條款使用案例，其中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;**
- **以原始碼形式散布；**
- **與其他開放原始碼整合而可能觸發 copyleft 義務性要求；**
- **內含修改過的開放原始碼;**
- **內含開放原始碼或其他軟體，其中與交付軟體裡其他互動元件不相容的授權條款；及／或**
- **內含開放原始碼帶有姓名標示的要求。**

審核資料:

- ☐ 3.2.1 具備一份流程文件來描述如何在交付軟體的開放原始碼元件中處理常見開放原始碼授權使用案例。

理由說明:

具備一個程序來遵循確保該方案能充份堅實地處理組織中常見的開源授權使用案例。

4.0 建立並交付產出合規稽證

4.1 合規稽證

具備一個流程來建立交付軟體中的合規稽證集。

審核資料:

- 4.1.1 具備一份流程文件來描述發布交付軟體時需一同準備以及發布合規稽證之程序，此合規稽證需滿足確認條款之要求。

- 4.1.2 具備一份流程文件來描述交付軟體中合規稽證的副本歸檔程序 - 此檔案從最後遞交交付軟體後至少需存在一段合理的時間; 或者根據確認條款中的要求(以較長者為準)。此外也具備證明該程序已被正確遵循的記錄。

理由說明 :

確保在商業面上盡一切合理努力，根據確認條款來準備交付軟體中的合規稽證。

5.0 理解開源社群參與

5.1 貢獻

如果一個組織考量對開源專案貢獻

- **具備書面政策書來管理對開源專案的貢獻;**
- **此政策書必須經過內部溝通; 以及**
- **具備一個流程來實行此政策**

審核資料:

若一個組織允許對開源項目進行貢獻，則必須存在以下內容:

- 5.1.1 具備一份開源貢獻政策書;
- 5.1.2 具備一份文件來描述管理開源貢獻的程序; 以及
- 5.1.3 具備一份文件來描述如何讓所有軟體工作人員知悉開源貢獻政策書存在的程序(例如，透過教育訓練，內部共筆，或其他實際可行的傳達方式)。

Rationale:

確保一個組織允許對開源項目進行貢獻時，已給予合理的考慮以進行開源貢獻政策書發展以及實行。開源貢獻政策書可成為整體開源政策的一部分，也可以作為自己獨立的政策。

6.0 遵守規範要件

6.1 一致性

組織必須確認方案滿足本規範中提出的要件，才能確認該方案已符合 OpenChain 一致性。

審核資料:

- 6.1.1 具備一份文件以確認要件 1.4 中提到的方案已滿足本規範書的所有要件。

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，該方案要達到本規範書的所有要件。若僅是達到這些要件的一部份則是不夠的。

6.2 持續期間

從一致性完成認證日開始，對此版本規範書的一致性狀態需要維持至少 18 個月。可以在 OpenChain 專案網站上找到一致性認證的註冊程序。

審核資料:

- 6.2.1 在獲得一致性驗證開始的 18 個月內，需具備一份文件以確認方案已滿足本規範書的所有要件(版本 2.0)。

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同步是很重要的。如果他們想要持續宣稱方案與此規範書具一致性的話，此一要件得以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

為了促進全球採用，我們歡迎將本規範書致力於翻譯成多種語言。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。