# 開放原始碼
# 良善治理
# 手冊

作者群：OSPO 聯盟與良善治理倡議 (GGI) 參與者
版本：v1.2
日期：2025 年 03 月 10 日

# Contents

# 1 簡介

本文件介紹了一套方法論，用以在組織內實施開放原始碼軟體的專業化管理。內文說明如何正確且公平地使用開放原始碼軟體，保障企業免受技術、法律及智慧財產權相關風險的威脅，並使開放原始碼的優勢最大化。無論組織在上述議題的處理上處於何種階段，本文件均提供您指引與思路，協助您在開源領域取得進展並邁向成功。

## 1.1 內文

大多數大型終端使用者和系統整合商已經在其資訊系統或產品與服務部門中採用自由及開放原始碼軟體（FOSS）。開放原始碼合規已成為一個日益受到重視的議題，許多大型企業已設立合規管理專員的職位。然而，儘管整頓公司內部的開源供應鏈（即合規的目標所在）是基礎，使用者也**必須**回饋開源社群，並為開源生態系統的永續性做出貢獻。我們認為，開源治理涵蓋整個生態系統，包括與在地社群互動、培養與開源軟體供應商及服務專家的良好合作關係。這些舉措將開源合規推向新的層次，而這正是**良善**開源治理的核心所在。

此倡議並不僅止於合規與責任的範疇，重點在於提升終端使用者（通常是軟體開發者）及系統整合商的社群意識，並在歐洲的開放原始碼生態系統中建立互利共贏的合作關係。

《開源軟體良善治理手冊》協助各類型的組織——包括大中小型企業、市政府、大專院校、協會等——透過協調人員、流程、技術與策略，使開放原始碼所帶來的效益最大化。而在如何充分發揮開放原始碼優勢方面，特別是在歐洲，各方仍處在學習與創新的階段，還沒有人能完全掌握自己在該領域的技術發展現狀中的實際定位。

此倡議旨在協助各類型的組織透過以下方式實現上述目標：

- 一份條理清晰的**行動**目錄，為開放原始碼軟體的專業化管理提供實施路線圖。
- 一套用於定義、監控、報告及溝通進度的**管理工具**。
- 一條**清晰且實用的改進路徑**，透過小幅且可負擔的步驟來降低風險、教育人員、調整流程，並強化組織內外的溝通。
- 一系列關於開源授權、最佳實務案例、培訓以及生態系參與的**指引**與**精選參考資料**，以借助開源意識與文化，鞏固內部知識，並擴展組織領導力。

本指引的編寫考量了以下需求：

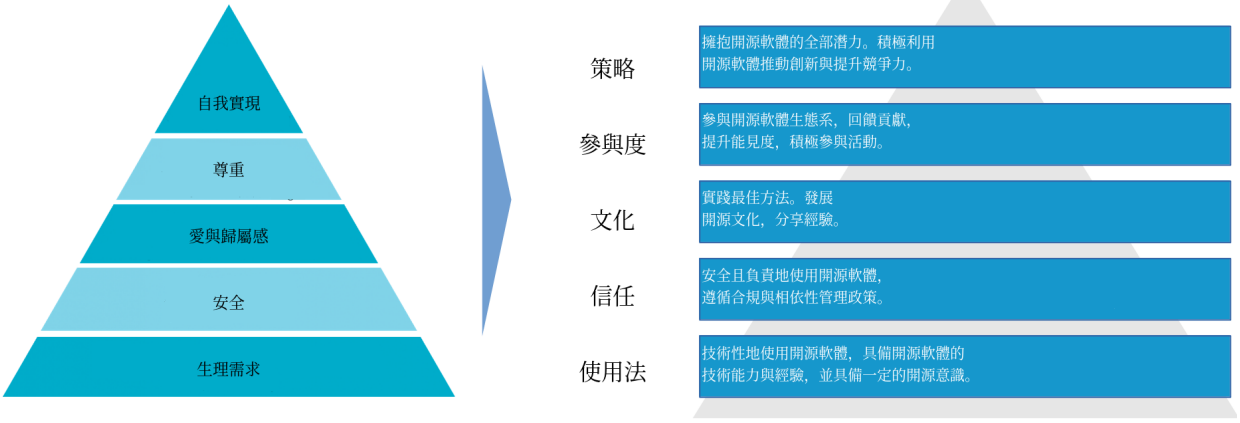
- 任何類型的組織皆涵蓋在內：從中小企業（SMEs）到大型公司及非營利組織，從地方政治單位（例如：鎮民代表會）到大型機構（例如：歐盟或政府機構）。這個框架提供了策略的基礎與策略實現的提示，但**具體如何執行**這些行動，完全取決於計畫的脈絡並由專案經理決定。這對於尋求諮詢服務及與同行同儕交流可能會有所幫助。
- 不對組織內的技術知識水準或其業務領域作任何假設。例如，有些組織可能需要建立完整的培訓課程，而另一些組織則可能僅向團隊提供臨時的學習資料。

某些行動可能並不適用於所有情境，但整個框架仍然提供了一份全方位的路線圖，為量身定作的策略奠定基礎。

## 1.2 關於良善治理倡議

在 OW2 社群中，倡議是一項為應對市場需求的共同合作行動。良善治理倡議提出了一套方法框架，用以在組織內實行開源軟體的專業化管理。

良善治理倡議 (GGI) 是基於一個全面的模型，其靈感來自廣為人知的馬斯洛人類需求層次與動機理論，如下圖所示。




亞伯拉罕·馬斯洛的行為動機層次理論　　OW2 的目標是開源軟體的良善治理

透過理念、指導方針和行動，「良好治理倡議」為專責管理開源軟體的組織實體提供了實施藍圖，這些實體也被稱為 OSPO（開源計畫辦公室，Open Source Program Offices）。該方法論同時是一種管理系統，用於確定優先事項，並監控與共享進度。

在實施開源軟體良好治理方法論的過程中，組織將在多個方向上提升技能，包括：

- **使用開放原始碼軟體**：在企業內部正確且安全地運用開放原始碼軟體，以提升軟體的重用性、可維護性和開發效率;
- **降低風險**：降低外部程式碼及協作相關的法律和技術風險;
- **確認需求**：確認所需的團隊培訓，從開發人員到團隊領導和管理者，確保每個人都擁有一致的願景;
- **優先排序**：確認目標與行動的優先順序，以制定高效的開源策略;
- **有效溝通**：無論是在公司內部還是對外部世界都進行有效溝通，以充分發揮開源策略的效益;
- **提升能力**：提升組織的競爭力及對頂尖開源人才的吸引力。

## 1.3 關於 OSPO 聯盟

**OSPO 聯盟**是由一個歐洲主要的開源非營利組織組成之聯盟所發起，包括 OW2、Eclipse 基金會、OpenForum Europe 和公共程式基金會。其使命是提升歐洲及全球的開源意識，並推動企業與行政機構對開源的結構化與專業化管理。

雖然良善治理倡議專注於發展一套管理的方法論，但 OSPO 聯盟的目標更為廣泛，旨在協助企業（特別是非技術領域的企業）和公務機關認識並了解開源技術，使這些組織開始受益於執行各種相關行動，並發展到能自行設置 OSPO（開源計畫辦公室）。

該聯盟已建立 **OSPO 聯盟**的官方網站，網址為 https://ospo-alliance.org。該網站為社群提供了一個安全的交流平台，用於討論開源計畫辦公室（Open Source Program Offices, OSPO）相關的議題，並為企業、公務機關以及研究學術組織提供一個全面的資源庫。OSPO 聯盟連結歐洲及全球各地的 OSPO 以形成支持性社群組織。該網站也致力於推廣最佳實踐案例，並促進對開源生態系統永續發展的貢獻。請造訪 OSPO 聯盟網站，快速了解 IT 管理最佳實踐的互補框架。

OSPO 聯盟 網站也是我們收集來自社群的回饋意見的地方，這些回饋涉及倡議及其內容（例如：行動、知識體系）等。

## 1.4 翻譯版本

本書最初是用英語撰寫的，並且已經有法語、德語、葡萄牙語、荷蘭語、義大利語和西班牙語版本，這些都得益於社群不斷進行 GGI 手冊翻譯的工作。由於翻譯進展快速，我們建議您查閱我們的官方網站，查看可用翻譯版本的完整清單。

> 詳見 https://ospo-alliance.org/ggi/

GGI 手冊是通過開放原始碼專案與平台Weblate進行翻譯的，該平台提供免費的開源專案托管服務。我們在此想向他們和所有參與翻譯的人員致上深深的謝意。你們實在太棒了。

> 詳見 https://hosted.weblate.org/projects/ospo-zone-ggi/#languages

## 1.5 貢獻者們

以下這些出色的人士為良善治理倡議手冊做出了貢獻：

- Frédéric Aatz（微軟法國）
- Boris Baldassari (Castalia Solutions, Eclipse 基金會)
- Philippe Bareille (巴黎市政府)
- Gaël Blondelle（Eclipse 基金會）
- Vicky Brasseur (Wipro，威普羅公司)
- Philippe Carré（諾基亞）
- Pierre-Yves Gibello (OW2)
- Michael Jaeger（西門子）
- Sébastien Lejeune (Thales，達利斯集團)
- Max Mehl（歐洲自由軟體基金會）
- Catherine Nuel (OW2)
- Hervé Pacault (Orange)
- Stefano Pampaloni (RIOS)
- Christian Paterson (OpenUp)
- Simon Phipps (Meshed Insights)
- Silvério Santos (Orange Business)
- Cédric Thomas (OW2)
- Nicolas Toussaint (Orange Business)
- Florent Zara（Eclipse 基金會）
- Igor Zubiaurre (Bitergia)

## 1.6 授權條款

# 2 手冊組織架構

## 2.1 術語

OSS 良好治理方法論藍圖圍繞四個關鍵概念構建：目標設定、標準行動、定制行動評分卡和迭代。

- **目標設定**：目標是一組與共同關注領域相關的行動，共有五個目標：使用目標、信任目標、文化目標、參與目標和策略目標。這些目標可以獨立實現、並行推進，並透過行動進行迭代改進。
- **標準行動**：在一個目標內，一項行動解決單一關注點或開發主題（例如管理法律合規性），這些行動可以作為實現計畫目標的增量步驟。由 GGI 定義的完整一系列行動稱為標準行動。
- **自訂行動評分卡（CAS）**：為了在特定組織中實施 GGI，標準行動必須根據具體情境進行調整，從而建立一組定制的行動評分卡。定制行動評分卡描述了行動在組織情境中的實施方式及如何監控進展。
- **迭代**：OSS 良好治理方法論是一種管理系統，因此需要定期評估、審查和修訂。可以將其比作組織中的會計系統，這是一個持續的過程，至少每年設置一個檢查點（例如資產負債表）；同樣，OSS 良好治理過程每年至少需要進行一次審查，但根據行動的不同，可以進行部分或更頻繁的審查。

## 2.2 目標設定

GGI 定義的標準行動被組織在各個目標中。每個目標皆針對過程中的特定進展領域。從使用到策略，這些目標涵蓋與所有利害關係人相關的問題，從開發團隊到高階管理主管。

- **使用目標**：此目標涵蓋使用開放原始碼軟體的基本步驟。與使用目標相關的行動涵蓋開放原始碼計劃的初期步驟，包括識別開放原始碼的使用效率及其為組織帶來的價值。這包括培訓與知識管理，製作已在組織內使用的現有開放原始碼的清單，以及介紹可在整個過程中使用的一些開放原始碼概念。
- **信任目標**：此目標關注如何安全地使用開放原始碼。信任目標處理法律合規性、相依性和漏洞管理，並通常旨在建立對組織使用和管理開放原始碼的信心。
- **文化目標**：文化目標包括許多行動，這些行動旨在讓團隊對開放原始碼感到舒適，讓個人參與協作行動，理解並實施開放原始碼的最佳實踐。這一目標促進了個人對開放原始碼社群的歸屬感。
- **參與目標**：此目標旨在從企業層面參與開放原始碼生態系統。企業編列人力和財務資源，以回饋開放原始碼專案。在這個部分，組織表明自己是負責任的開放原始碼公民，並認知到自己有責任確保開放原始碼生態系統的永續性。
- **策略目標**：此目標關注如何讓企業管理的最高階層認識並接受開放原始碼。這涉及了認識到開放原始碼是數位主權、流程創新和一般而言，吸引力與良好聲譽的策略推動者。

## 2.3 標準行動

標準行動處於 GGI 藍圖的核心。在其初期版本中，GGI 方法論為每個目標提供五個標準行動，共計 25 個。標準行動將使用以下預定義部分進行描述：

- **描述**：簡要說明該行動所處理的主題及完成步驟。
- **機會評估**：描述為什麼以及何時需要展開這項行動。
- **進度評估**：描述如何衡量行動的進展並評估其成功與否。
- **工具**：列出有助於實現此行動的技術或工具。
- **建議**：從 GGI 參與者蒐集的提示和最佳實踐。
- **資源**：連結和參考資料，讓您深入了解該行動所涵蓋的主題。

#### 描述

此部分提供關於行動的鳥瞰式描述，彙整並概述該主題，以在目標內的開放原始碼方法的脈絡中，設定行動的目的。

#### 機會評估

為了幫助構建迭代方法，每個行動都有一個「機會評估」的部分，並附帶一個或多個問題。機會評估著重於為什麼需要執行這項行動，這項行動處理了哪些需求。評估機會有助於確定預期的努力、所需的資源，並幫助評估成本與預期的投資回報率（ROI）。

#### 進度評估

這一步驟著重於定義目標、關鍵績效指標（KPI）[^kpi]，並提供有助於評估行動進展的**驗證要點**。這些驗證要點屬於建議性質，能幫助制定良好治理過程的路線圖、確定優先事項以及衡量進展的方式。

#### 工具

以下列出了可以幫助實現該行動或特定步驟的工具。這些工具並非強制推薦，也不保證詳盡無遺，而是根據現有情境提出的建議或分類，供進一步擴展。

#### 建議

此部分會定期更新，提供使用者的回饋以及有助於管理該行動之各種建議。

#### 資源

資源包括背景研究、參考文件、活動或線上內容，旨在豐富和發展與該行動相關的方法。這些資源並非詳盡無遺，而是作為起點或建議，以根據自身情境來擴展行動的意義。

## 2.4 自訂行動計分卡

自訂行動評分卡（CAS）比標準行動稍微更詳細一些。CAS 包含專為實施 GGI 的組織所定的細節。使用 CAS 的方法可以詳見方法論部分。

[^kpi]：績效指標，亦稱關鍵績效指標（KPI），是一種衡量績效的工具，用於評估組織或其參與的特定行動的進展和成效。

# 3 InnerSource

InnerSource 在當今企業中越來越受歡迎，因為它提供了基於開源實踐成功經驗的方法，應用於組織內部的開發團隊。然而，實施 InnerSource 並不僅僅是直接複製這些實踐。它需要根據企業的獨特文化和內部組織進行調整。讓我們一起更深入了解什麼是 InnerSource，什麼不是，以及其相關挑戰。

## 3.1 什麼是 InnerSource？

該術語最早由 Tim O'Reilly 在 2000 年提出，Innersource 所指的是「[...] **在企業內部使用開源開發技術**」

根據 InnerSource Commons ，一份該主題的參考依據，InnerSource 是指「**在組織範圍內，使用開放原始源原則與實踐軟體開發**。」

## 3.2 為什麼需要 InnerSource？

根據 InnerSource Commons 的觀點，「**對於主要開發封閉原始碼軟體的公司，*InnerSource* 是一個極佳的工具，可幫助破除部門隔閡、促進並擴大內部協作、加速新工程師的入職，並發掘將軟體貢獻回開放原始碼世界的機會**。」

有趣的是，InnerSource 的益處不僅能影響公司的工程部門，還能惠及其他部門。因此，一些公司在以下領域發現了具體的優勢：

- 法律職能：透過使用現成的法律框架（如 InnerSource 授權），加速跨部門協作的建立。
- 人力資源：透過核心且經驗豐富的團隊來管理稀缺技能，而該團隊本身是負責整合資源與專業知識。

## 3.3 InnerSource 的爭議

InnerSource 常常被批評者提及的一些普遍迷思圍繞。雖然它並非真正的開放原始碼，但對於在內部採用這種方法的組織來說，卻展現了巨大的潛在效益。以下是一些常見的迷思：

- 「迷思」InnerSource 是以犧牲開放原始碼（主要是對外貢獻的部分）為代價的：
  - 軟體專案保留在公司防火牆內。
  - 對開放原始碼的外部貢獻減少。
- 「迷思」把持開放原始碼的精神，而非真正接近其核心理念。
- 「迷思」從未有 InnerSource 專案成功轉變為開放原始碼專案。
- 「迷思」推行 InnerSource 的動機在於它類似於開放原始碼。但事實上，如果開發者認為其有價值，那麼應始終優先選擇直接對開放原始碼進行貢獻。

以下是一些關於 InnerSource 實踐的事實，可以破除前述大多數迷思：

- 「事實」InnerSource 是一種方法，旨在引導主要封閉型公司逐步進入開放原始碼的領域。
- 「事實」儘管大多數開放原始碼貢獻是由志願者完成的，但我們可以利用這份「感知利益」清單，向工程師宣傳參與開放原始碼的好處。
- 「事實」在某些（或大多數？）情況下，企業並未遵循有序且受控的開發實踐模式，而這（GGI）可以成為幫助他們管理此問題的一種方式。
- 「事實」將封閉授權轉換為開放授權仍然需要**大量**的工作。
- 「事實」確實存在將 InnerSource 專案轉為開放原始碼的案例：
  - Twitter 釋出的 Bootstrap。
  - Google 釋出的 Kubernetes。
  - dotCloud 釋出的 Docker（過往公司名稱為 Docker Inc.）。
  - React Native。
- 「事實」開放原始碼受益於越來越多的軟體工程師熟悉開放原始碼的實踐，因為 InnerSource 的實踐與其非常相似。

## 3.4 誰在進行這件事？

許多公司已經啟動了 InnerSource 計劃或 ISPO（InnerSource 計畫辦公室），其中一些已經運行了很長時間，其他則是近期才開始。以下是主要聚焦於歐洲公司的非詳盡清單：

- 西班牙桑坦德銀行 (Banco de Santander) (source)
- 英國廣播公司（BBC）(source)
- 博世（Bosch）(source)

- Comcast (source)
- 易力信（Ericsson）(source)
- Engie (source)
- 國際商業機器（IBM）(source)
- 賓士（Mercedes-Benz）(source)
- 微軟（Microsoft）(source)
- NIKE (source)
- 諾基亞（Nokia）(source)
- 法國國鐵（SNCF Connect & Tech）(source 1, source 2)
- PayPal (source)
- 皇家飛利浦（Philips）(source)
- 雷諾（Renault）(source)
- SAP (source)
- 西門子（Siemens）(source)
- 法國興業銀行（Société Générale）(source)
- 達利思（Thales）(source)
- VeePee（法國零售商）(source)

## 3.5 InnerSource Commons ，一個必要的參考文獻

一個活躍且充滿活力的 InnerSource 實踐者社群，依循開放原始碼原則運作，可以在 InnerSource Commons 中找到。他們提供許多實用資源，幫助您快速掌握相關議題，包括 模式、學習路徑 以及簡短的電子書：

- 開始使用 InnerSource 由 Andy Oram 編寫。
- 《理解 InnerSource 的檢查清單》（Understanding the InnerSource Checklist）作者：Silona Bonewald。

## 3.6 InnerSource 治理的差異

InnerSource 帶來了一些在「開放原始碼」中未曾遇到的特定挑戰。然而，大多數創建封閉軟體的組織已經在應對這些挑戰：

- 專為公司設計的 InnerSource 專案專屬授權（適用於擁有多個法律實體的大型公司）。
- 開源的公開性避免了移轉定價（transfer pricing，跨國企業內部交易的價格設定）的挑戰，而 InnerSource 的私密性可能使跨司法管轄區運營的企業面臨利潤轉移的責任。
- 促進貢獻的動機存在很大差異：
  - 由於 InnerSource 侷限於組織內部，其潛在貢獻者的範圍較小。
  - 展現專業技能是促進貢獻的一個驅動因素，但 InnerSource 將這種影響力限制在組織的範圍內。
  - 為改善社會作出貢獻是另一個驅動因素，但在 InnerSource 中這一點受到限制。
  - 因此，在滿足動機需求之餘，將更加仰賴貢獻獎勵和任務指派。
  - 在 InnerSource 中，因為程式碼的可見性有限，處理如冒名頂替症候群等完美主義恐懼更為容易。
- 勞務外包日漸頻繁，這在多方面影響了治理。
- 由於 InnerSource 是在內部開發的，因此評估其對企業的適用性更加容易。
- 可查找性往往會是一個問題。企業對資訊索引的優先程度較低，而公共的搜尋引擎（如 DuckDuckGo、Google 或 Bing）在這方面表現更優，但 InnerSource 無法加以利用。
- InnerSource 因其運行於內部環境，相較之下在出口管控方面具備略優的條件。
- 需要對原始碼的智慧財產權洩漏進行邊界管控。

InnerSource 隨著越來越多公司採用其原則並分享經驗而持續發展。本手冊的未來版本將提供精選清單，列出與 GGI 行動相關的 InnerSource 實踐者。

# 4 方法論

實施開源軟體良善治理方法論最終是一項有深遠影響且具意義的倡議。它涉及多類型的公司人員、服務和流程，從日常實踐到人力資源管理，從開發人員到高階主管。實施開放原始碼良善治理並沒有萬能之策。不同類型的組織、公司文化和情況會需要不同的開源治理方法。每個組織會有不同的約束條件和期望，從而引導出不同的管理方案途徑和方式。

考慮到這一點，良善治理倡議提供了一個通用的行動藍圖，可以根據組織自身的領域、文化和需求進行調整。雖然這個藍圖宣稱具有全面性，但其方法論是可以逐步實施的。可以根據具體情境，挑選最相關的目標和行動來啟動計畫。該藍圖的核心思想是構建一個初步的路線圖，幫助建立組織自身的倡議。

除了這個框架，我們也強烈建議透過已建立的網絡（例如歐洲 OSPO 聯盟 倡議、TODO 工作群組或 OSPO++ 的其他志同道合的倡議）與同行交流。重要的是能夠與執行類似倡議的人交換經驗，分享遇到的問題以及現有的解決方案。

## 4.1 準備工作

考慮到良善治理方法論的雄心和潛在的廣泛影響，與組織內各類人員進行溝通非常重要。適當的做法是給予他們引導，建立初步符合現實的期望和需求，從而有個良好的開端，吸引興趣和支持。一個不錯的方向是將定制行動計分卡發布在組織的協作平台上，以便與利害關係人進行溝通。以下是一些建議：

- 識別關鍵利害關係人，並讓他們達成共識，確定一系列主要目標。讓他們將倡議的成功列為他們自身目標的一部分。
- 獲得初步支持，達成對步驟和進度的共識，並設置定期檢查以通報進度。
- 確保他們理解所能實現的益處及其所涉及的內容：預期的改善成果應該要是明確的，並且能看到結果。
- 在候選組織中進行開放原始碼的初步診斷或現狀評估。結果應為一份文件，描述該計畫將實現的目標、組織目前的狀態及其未來的目標。

## 4.2 工作流程

作為現代軟體開發者，我們偏好敏捷式的方法，這強調先定義小且可控的改變，因為定期重新評估情況並產出具意義的最小階段性成果，是一種良好的實踐方式。

在運作中的 OSPO 計畫脈絡下，這一點尤其重要，因為許多外部因素會隨著時間變化，包括組織的策略和對開放原始碼的應對、員工的可投入程度與參與度。定期的重新評估和迭代，也有助於提升運作中計畫的受接納程度，更好地追蹤當前趨勢與機會，並為利害關係人及整個組織帶來小而遞增的利益。

理想情況下，這套方法論可以分為以下五個階段來實施：

1. **發現階段**：理解關鍵概念，掌握方法論的實施權責，對齊目標期望。
2. **自定導入階段**：根據組織的具體情況調整行動描述和機會評估。
3. **優先排序階段**：確定目標和關鍵成果、任務和工具，設定里程碑並草擬時間表。
4. **啟動階段**：定下計分卡、預算、任務分配，並在問題管理工具上記錄任務。
5. **迭代階段**：評估和評量結果，提出問題、改進並調整。每季度或每學期進行一次迭代。

準備第一輪計畫迭代：

- 確定一組要處理的初步任務，並根據需求（與期望狀態的差距）和時間表進行優先排序。結果應為一份在迭代期間要處理的任務清單。
- 定義一系列需求和改進領域，並將其傳達給利害關係人和終端使用者，獲得他們的認可或承諾。
- 填寫計分卡以追蹤進展。可以從 GGI 儲存庫 下載計分卡範本。

每次迭代結束時，進行回顧並為下一輪迭代做準備：

- 傳達最新的改進成果。
- 評估當前情況，如果目標任務已完成，就根據情況調整路線圖。
- 檢查剩餘的痛點或問題，並在需要時向其他相關人員或服務尋求支持。
- 根據更新的情境重新排出任務的優先順序。
- 定義一組新的子任務來執行。

## 4.3 手動設置：使用自訂行動計分卡

自訂行動計分卡是一份表單，描述根據組織具體情況定制的標準行動。將其匯集起來，一副自訂行動計分卡將提供管理開放原始碼軟體的路線圖。

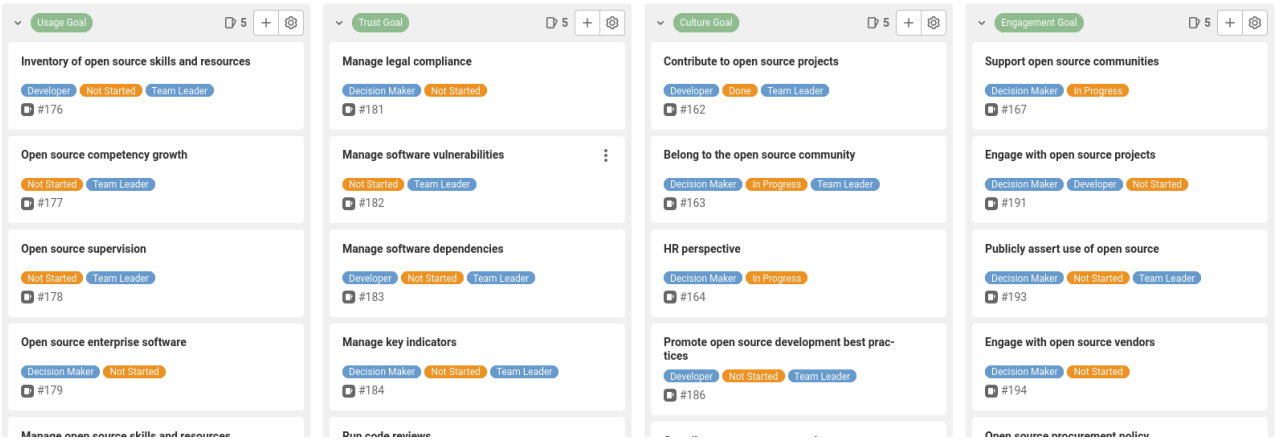
請注意，根據早期的實踐經驗，將標準行動轉換為組織特定的自訂計分卡通常需要長達一小時的時間。

自訂行動計分卡包含以下幾個部分：

- **標題釐清**首先花幾分鐘來了解該行動的內容及其相關性，並思考它如何適應您的整體開放原始碼管理過程。
- **自訂描述**根據組織的具體情況調整行動，界定範圍。定義該行動的範疇以及您將要處理的特定使用案例。
- **機會評估**解釋為什麼需要執行這項行動，它解決了哪些需求。我們的痛點是什麼？有哪些進步的機會？可以獲得什麼成果？
- **目標**為該行動定義幾個關鍵目標。要解決的痛點、進展機會、期望。識別關鍵任務。我們在本次迭代中打算達成的目標。
- **工具**在此行動中使用的技術、工具和產品。
- **操作說明**闡述在此行動中的方針、方法、及進展策略。
- **關鍵成果**定義可衡量、可驗證的預期結果。選擇能夠顯示目標進展的結果，並在此處標明 KPI。
- **進度與計分**進度是以百分比表示的結果完成率；計分是個人成功的評分。
- **個人評估**每個結果可以附上一段簡短的解釋，並解釋反映在計分中您對結果的個人滿意度。
- **時間表**指定開始和結束日期，階段性任務、關鍵步驟和里程碑。
- **工作量**評估所需的時間和物質資源，包括內部資源和第三方資源。預期的努力是什麼？需要多少成本？我們需要哪些資源？
- **負責人**說明誰參與其中。分配任務或行動的領導權和責任。
- **問題**識別關鍵問題、預見的困難、風險、障礙、不確定因素、注意事項和關鍵相依項目。
- **狀態**在此處撰寫對行動進度的綜合評估：順利？延遲？等等。
- **整體進度評比**進行自己概略的、管理導向的行動進展綜合評估。

## 4.4 自動設置：使用 GGI 部署功能

從手冊 1.1 版本開始，GGI 提供了 My GGI Board，這是一個自動化工具，用於將您自己的 GGI 實例部署為 GitLab 專案。安裝過程僅需不到 10 分鐘，並有完整的文件支援，提供了一個簡單可靠的方式來自訂行動，隨著進展追蹤執行進度，並與利害關係人溝通結果。您可以在 倡議的 GitLab 中查看部署的實際範例，並在 GitLab 頁面 上查看自動生成的網站。




以下是使用部署功能的標準工作流程：

1. 將 My GGI Board 專案 Fork 到您自己的 GitLab 實例或專案，並按照專案 README 中的指示進行設置：https://gitlab.ow2.org/ggi/my-ggi-board。此操作將完成以下任務：

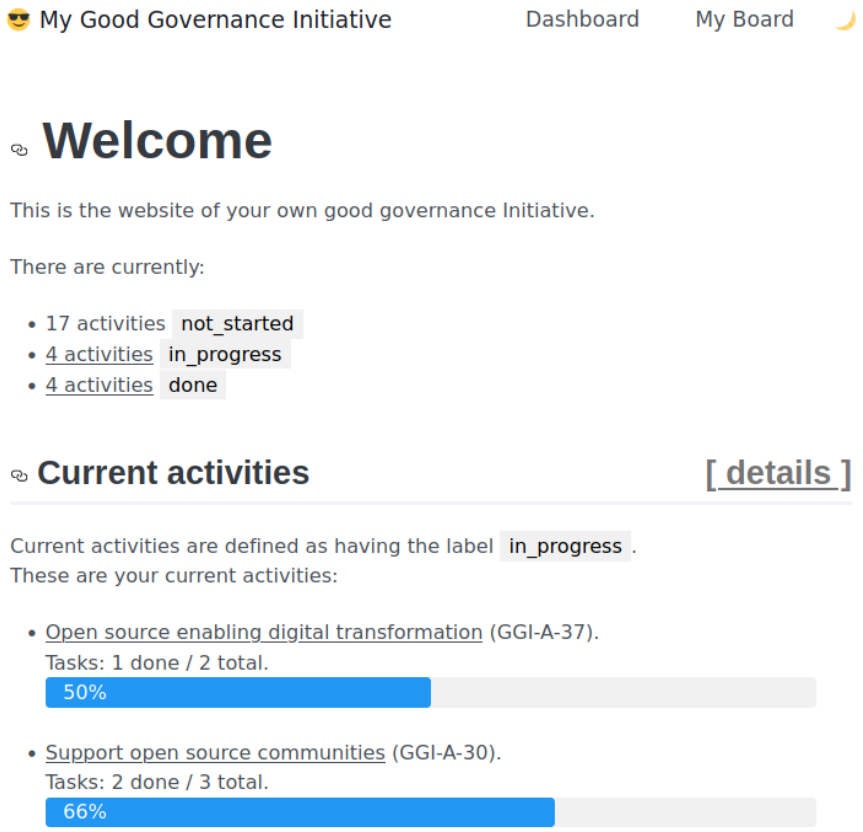
- 在專案中將所有行動建立為 issue。
- 建立一個簡潔的看板，幫助您視覺化和管理這些行動。
- 透過 GitLab 頁面建立一個靜態網站，該網站直接擷取了行動的資訊。
- 更新專案描述，提供通往行動看板和靜態網站的正確連結。

1. 從這裡可以開始檢視不同的行動，並填寫計分卡部分。

- 計分卡部分是上述 ODT 格式計分卡的電子版（也是簡化版），用於調整行動以符合您的情境，包括列出當地資源、風險和機會，並定義完成行動所需的定制目標。
- 如果某些行動不適用於您的情境，就將其標記為「未選擇（Not Selected）」或直接關閉。
- 這是一個耗時的過程，但非常必要，因為它會一步步幫助您定義自己的路線圖和計畫。

1. 當行動被定義後，便可開始實施您的 OSPO（開源計畫辦公室）。選擇一些您認為需要由此開始的行動，將其進度標籤從「未開始（Not Started）」更改為「進行中（In Progress）」。您可以使用 GitLab 的功能（例如評論、指派對象等）或其他工具來協助組織工作。這些工具能很輕易地連結到行動，還有許多優秀的整合方式可供使用。
2. 定期（每週、每月，視時間表而定）評估和審查當前行動。當行動完成時，將其標籤從「進行中（In Progress）」更改為「完成（Done）」。選擇其他行動並從第 3 步開始重複，直到所有行動完成。

這個網站提供當前和過去行動的快速概覽，並提取議題中的計分卡部分以僅顯示本地相關的資訊。當 issue（行動）有所改動時，網站會自動更新。請注意，CI pipelines 將於每晚自動執行網站生成，但您也可以輕易地在 GitLab 專案的 CI/CD 部分手動啟動。下圖展示了自動生成的網站介面。




您可以在我們的 GitLab 主頁對部署功能提出疑問或獲取技術支援。我們也非常歡迎您的回饋。

GGI 部署首頁：https://gitlab.ow2.org/ggi/my-ggi-board

## 4.5 暢享成果與歷程

與他人分享您的成功，並享受開放原始碼策略帶來的安心感！

開源軟體良善治理（OSS Good Governance）是一種部署持續改進計畫的方法，正因如此，它永無止境。然而，強調中間步驟並欣賞其所帶來的變化非常重要，這可以讓進展可見並分享成果。

- 與利害關係人和終端使用者溝通，讓他們了解這項倡議所帶來的優勢和好處。
- 促進計畫的永續性。確保從計畫中學到的最佳實踐和經驗教訓始終得以應用和更新。
- 與同行分享您的經驗：向 GGI 工作小組與您所在的 OSPO 採用社群提供回饋，並分享您的方法。

# 5 使用目標行動清單

## 5.1 開源技能和資源清單

行動編號：GGI-A-17。

### 描述

在任何階段，從管理的觀點來看，應以清單方式整理開放原始碼資源、資產、使用情況及其狀態，並逐條彙整對應的潛在需求與解決方案。同時評估填補這些差距所需的努力與技能。

這項行動旨在針對開放原始碼解決方法進行一次快照式的盤點工作，以評估組織內部與市場間的對接情形。

- 軟體開發供應鏈中開放原始碼使用，以及在生產現場中使用的軟體產品和組件的清單。
- 識別符合需求並能改善流程的開放原始碼技術（解決方案、框架、創新功能）。

但，不包含

- 識別並評估相關的開放原始碼生態系統與社群。（文化目標）
- 識別對開放原始碼庫和組件的相依性。（信任目標）
- 識別所需的技術技能（例如程式語言、框架）及軟實力（例如協作、溝通）。（屬於下一行動：開放原始碼能力增長與開放原始碼軟體開發技能）

### 機會評估

一份可用的開放原始碼資源清單，有助於最佳化投資並優先發展技能。

此行動為提高開發生產力創造條件，特別是在現代應用程式與基礎設施的開發中，考量開放原始碼組件、開發原則與工具的效率與普及性。

- 這可能需要簡化開放原始碼資源的組合。
- 這可能需要對人員進行再培訓。
- 此行動有助於識別需求，並為 IT 路線圖提供支援。

### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- ☐ 完成了一份清楚的開放原始碼資源清單，包括「我們使用的」、「我們整合的」、「我們產出的」、「我們託管的」，以及相關技能
- ☐ 已發現並識別出先前未列入考量的開放原始碼資源（可能已逐步滲入），並著手制定相關政策。
- ☐ 已發現並識別出此前都未列入考量的開放原始碼資源（可能已逐步滲入，而針對這些是否著手制定相關政策了？）
- ☐ 請求新專案支持或重用現有的開放原始碼資源。
- ☐ 我們對組織內開放原始碼使用範疇有合理且安全的理解與掌握。

### 工具

建立此類清單的方法有許多種，其中一種方式是將開放原始碼資源分類為以下四類：

- 我們使用的開放原始碼軟體：指在生產或開發過程中使用的軟體
- 我們整合的開放原始碼軟體：例如，整合到定製應用程式中的開放原始碼庫
- 我們產出的開放原始碼軟體：例如，我們在 GitHub 上發布的程式庫，或我們開發或定期貢獻的開放原始碼專案.
- 我們託管的開放原始碼軟體：指我們運行來提供內部服務的開放原始碼軟體，例如 CRM、GitLab、Nexus 等。範例表格參考如下：

| 我們使用了 | 我們整合了 | 我們產生了 | 我們託管了 | 相關技能 |
|---|---|---|---|---|
| Firefox、OpenOffice、Postgresql | Library slf4j | Library YY on GH | GitLab, Nexus | Java, Python |

相同過程也應用於技能的識別

- 現有團隊具備的技能與經驗

- 可透過內部發展或培訓獲得的技能與經驗（包括訓練、請教練、實驗等形式）
- 需要從市場上尋求或透過合作夥伴 / 外包獲得的技能與經驗

#### 建議

- 保持簡單。
- 這是一項相對高層次的練習，並非為會計部門準備的詳細清單。
- 雖然此行動是很好的起點，但不需要完全完成 100% 的清單才能啟動其他行動。
- 與**軟體開發**相關的問題、資源和技能，請詳見行動 #42。
- 清單應涵蓋所有 IT 類別：作業系統、中介軟體、資料庫管理系統（DBMS）、系統管理、開發與測試工具等。
- 開始識別相關社群：當專案社群已經認識你時，獲得支持和回饋會更加容易。

#### 資源

- 由 Dirk Riehle 教授開設的自由（自由軟體）與開放原始碼軟體課程 (FOSS)，是一門極具價值的課程。

#### 建議的下一步行動

- GGI-A-18 - 開放原始碼能力增長 識別開放原始碼的技能與資源，有助於組織開始鞏固並加強其意識與能力。
- GGI-A-19 - 開放原始碼監管 當開放原始碼軟體與技能清單完成後，便可以開始在組織內進行開放原始碼的使用監控與管理。
- GGI-A-28 - 人力資源觀點 人力資源部門可以基於此行動產生的清單，制定適當且相稱的發展計劃、合約和流程。
- GGI-A-33 - 與開源供應商合作 在與供應商建立外部關係之前，需充分了解自身的開放原始碼軟體與技能。
- GGI-A-42 - 管理開放原始碼技能與資源 當開放原始碼資產與技能的清單完成後，可以開始正確地管理這些資源，並利用現有的內部資源進一步發展。

## 5.2 開源能力增長

行動編號：GGI-A-18。

#### 描述

此行動旨在規劃並啟動與開放原始碼相關的技術能力與初步經驗，條件是完成了相關清單 (#17)。同時這也是建立基礎且簡易技能發展路線圖的良好契機。

- 識別所需要的技能與培訓。
- 啟動試驗專案，以展開此方法、透過實踐學習並建立首個成就里程碑。
- 善用所學經驗並構建一套知識體系。
- 開始識別並記錄後續步驟，以推動更廣泛的採用.
- 擬定未來幾個月或一年內的策略，爭取管理層與財務支持。

行動範疇：

- Linux、Apache、Debian、系統管理技能。
- 開源資料庫 MariaDB、MySQL、PostgreSQL 等。
- 開源虛擬化與雲端技術。
- LAMP 技術隊也及其替代方案。

#### 機會評估

如同其他 IT 技術，甚至尤有過之，開放原始碼帶來了創新。開放原始碼增長迅速且變化快速，這需要組織保持最新的技術動態。

此行動有助於識別培訓需求，以提高人員使用開放原始碼的效率和信心，並幫助組織進行員工發展決策。播種基礎的開放原始碼技能能提供以下機會評估：

- 利用由生態系統開發的現有市場技術擴展 IT 解決方案。
- 開發組織內部及外部的新協作方式。

- 獲得新穎且創新的技術能力。

#### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- ☐ 建立技能矩陣。
- ☐ 主動定義使用的開放原始碼技術範圍，避免不受控的技術使用。
- ☐ 針對這些技術獲得令人滿意的專業水準。
- ☐ 團隊們已經接受了「開放原始碼基礎」訓練，準備好上線活用。

#### 工具

此處的核心工具是稱為「行動矩陣」或「技能矩陣」的工具。

如何進行此行動：

- 使用線上教學（網上有許多免費資源），
- 參與開發者研討會活動，
- 接受供應商培訓等。

#### 建議

- 以安全且高效的方式使用和開發開放原始碼元件，需要開放且協作的思維，而這種思維需要自上而下（管理層）以及自下而上（開發者）共同認可並推廣。
- 確保該方法得到管理層的積極支持與推動。如果沒有高層的承諾，任何事情都無法推進。
- 讓人們（開發者、利害關係人）參與此過程：舉辦圓桌會議並傾聽他們的想法。
- 為人們提供時間與資源去探索、嘗試並玩轉這些新概念。如有可能，讓這個過程變得有趣——遊戲化和獎勵是很好的激勵措施。

一個依循下述步驟的試驗專案，可具有拋磚引玉的作用：

- 找出要使用的技術或框架。
- 尋找線上培訓、教學及範例程式碼以供實驗。
- 建立最終解決方案的原型。
- 聘請一些專家對實施進行挑戰與輔導。

#### 資源

- 什麼是技能矩陣 (What is a Competency Matrix): 一篇簡短的介紹文章。
- 如何爲您的團隊打造技能矩陣 (How to Make a Skills Matrix for your Team)：一份帶有評論的技能矩陣範本。
- 關於自由文化的 MOOC (僅有法語)：這是六系列的課程，包括著作財產權、智慧財產與開放原始碼授權的介紹

#### 建議的下一步行動

- GGI-A-28 - 人力資源觀點 審慎規劃內部技能組合與能力增長，是人力資源視角的重要部分。

### 5.3 開放原始碼監管

行動編號：GGI-A-19。

#### 描述

此行動旨在管控開放原始碼的使用，並確保開放原始碼軟體能被主動管理。這涉及多個層面，無論是使用開放原始碼工具與商業解決方案，還是將開放原始碼作為自身開發的元件，或者修改軟體版本以適應自身需求等。此外，也包括識別那些開放原始碼已成為實際標準（有時是隱性標準）的領域，並評估其適用性。

可能必要的澄清事項：

- 所需的功能是否已被滿足？
- 是否有額外的功能不需要但增加了「構建」與「運行」階段的複雜性？
- 授權要求是什麼？有哪些法律限制？

- 此決策是否使組織免於對供應商的依賴？
- 是否有滿足業務需求的支持選項？成本如何？
- 總擁有成本 (TCO, Total Cost of Ownership) 是多少。
- 管理層是否瞭解開放原始碼的優勢，例如超越「節省授權費用」的價值？熟悉開放原始碼有助於從專案社群與供應商的合作中獲取最大效益。
- 評估是否應透過向社群分享自身的開發成果來分攤開發成本，以及相關的授權合規性影響。
- 檢查社群支持或專業支持的可用性。

#### 機會評估

定義針對開放原始碼的決策流程，以最大化其效益。

- 避免開放原始碼技術的不受控滲透與隱性成本。
- 促成知情且對開放原始碼有認知的策略與組織決策。

成本：此行動可能重新評估並質疑非最佳化的開放原始碼使用，認為其效率低下或風險較高等。

#### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- ☐ 開放原始碼已成為選擇新軟體時的可以放心的選項。
- ☐ 開放原始碼不再被視為例外或危險的選擇。
- ☐ 開放原始碼已成為選擇新軟體時的主流選項。
- ☐ 主要參與者充分相信，開放原始碼解決方案具有值得投資的策略優勢。
- ☐ 能證明基於開放原始碼的解決方案總擁有成本 (TCO) 高於替代方案的價值。
- ☐ 有評估表示，供應商獨立性如何節省成本或在未來潛在地節省成本。
- ☐ 有評估表明，解決方案的獨立性可降低更換解決方案成本過高的風險（避免使用封閉的數據格式）。

#### 工具

在此階段，我們尚未能想到與此行動相關或受其影響的工具。

#### 建議

- 主動管理開放原始碼的使用需要具備基本的意識與基礎知識，因為在任何開放原始碼的決策中，這些基礎觀念都應納入考量。
- 比較所需功能，而非僅尋找已知封閉原始碼解決方案的替代品。
- 確保有支持與進一步開發的能力。
- 考量該解決方案的授權條款對組織的影響。
- 說服關鍵利益相關者，讓他們認識到開放原始碼的優勢，而不僅是「節省授權成本」。
- 保持誠實，不要誇大開放原始碼解決方案的效果。
- 在決策過程中，評估不同的開放原始碼解決方案同樣重要，以避免因錯誤的期望而失望，並明確組織需要履行的責任以及這些開放解決方案所帶來的所有優勢。

#### 資源

- 開放原始碼的五大好處（Top 5 Benefits of Open Source）：有資金支持業配文，但仍值得快速閱讀的有趣文章。
- 衡量開源的隱性成本（Weighing The Hidden Costs Of Open Source）：IBM 贊助的業配文章，討論開放原始碼支持成本的角度。

### 5.4 開源企業軟體

行動編號：GGI-A-20。

#### 描述

此行動旨在主動選擇由供應商或社群支持的開放原始碼解決方案，應用於商業導向的領域。同時也涵蓋了為選擇開放原始碼商業應用軟體制定偏好政策。

雖然開放原始碼軟體多數由 IT 專業人員使用，例如作業系統、中介軟體、資料庫管理系統（DBMS）、系統管理與開發工具，但在以商業專業人員為主要使用者的領域中，其重要性尚未被廣泛認可。

此行動適用於以下範疇：辦公套件、協作環境、用戶管理、工作流程管理、客戶關係管理（CRM）、電子郵件與電子商務等。

#### 機會評估

隨著開放原始碼逐漸成為主流，其應用已遠超作業系統與開發工具，逐步滲透到資訊系統的高層結構，甚至進入商業應用領域。因此，識別哪些開放原始碼應用成功滿足了組織需求，以及如何將其轉化為組織節省成本的首選，是極具相關性的。

此行動可能涉及一定的再培訓與遷移成本。

#### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- ☐ 已建立一份推薦的開放原始碼解決方案清單，以解決商業應用中的未決需求。
- ☐ 已草擬一份選擇開放原始碼商業應用軟體的偏好政策。
- ☐ 正在將現有的專有商業應用與開放原始碼等效方案進行評估。
- ☐ 採購流程和提案邀請已明確規定開放原始碼的優先考量（若法律允許）。

#### 工具

此階段尚未想到推薦與此行動相關的工具。

#### 建議

- 與同事交流，學習其他類似公司的實踐經驗。
- 參加當地產業活動，瞭解開放原始碼解決方案與專業支持。
- 優先嘗試社群版與社群支持，再決定是否採用付費支持計畫。

#### 資源

- 什麼是企業級開放原始碼？(What is enterprise open source?)：一篇關於企業級開放原始碼的簡短介紹。
- 101 個幫助您的企業發展的開源應用程式 (101 Open Source Apps to Help your Business Thrive)：一份幫助企業蓬勃發展的開放原始碼應用指導性清單。

#### 建議的下一步行動

- GGI-A-33 - 與開源供應商合作 透過與開放原始碼專業人士的合作提升對資產的信心。
- GGI-A-43 - 開放原始碼採購政策 透過瞭解現有資產並制定清晰的採購政策，最佳化於企業使用開放原始碼。

### 5.5 管理開源技能和資源

行動編號：GGI-A-42。

#### 描述

本行動專注於**軟體開發**的技能與資源。它包含開發者所需的技術及特定開發技能，以及整體的開發流程、方法與工具。

開放原始碼技術擁有龐大的生態系統所提供的文件、論壇及公開資源。為了充分受益於開放原始碼方法，必須建立目前資產與目標的路線圖，為團隊建立一致性的開發技能、方法與工具計畫。

#### 應用領域

需要確定此計畫所適用的領域，以及如何提升程式碼及實務的品質與效率。例如，如果只有一位開發人員使用開放原始碼元件，效果將與整個開發生命週期經優化並採用開放原始碼最佳實務有所不同。

必須定義開放原始碼開發所涵蓋的範圍：技術元件、應用程式，或是現代化或新開發的流程。能夠從開放原始碼中受益的開發實務範例如下：

- 雲端管理。
- 雲端原生應用程式，如何透過這些技術創新。
- DevOps，持續整合 / 持續交付（CI/CD）。

**分類**

- 開發開放原始碼軟體所需的技能與資源：智慧財產權（IP）、授權、實務。
- 使用開放原始碼元件、語言及技術所需的技能與資源。
- 採用開放原始碼方法與流程所需的技能與資源。

**機會評估**

開放原始碼工具在開發人員間越來越受到歡迎。本活動的目的是避免開發團隊內部出現過多異質工具。它有助於制定相關政策，優化訓練與經驗累積，並透過技能盤點來輔助招聘、培訓及關鍵人員離職後的接替規劃。

我們需要一套方法來呈現開放原始碼軟體開發技能的對應全貌。

**進度評估**

以下**檢驗要點**顯示了此行動的進度：

☐ 描述開放原始碼的生產鏈（即「軟體供應鏈」），
☐ 擁有一個發展資源優化的計畫（或需求清單），
☐ 建立一份技能盤點，彙整目前開發人員的技能、學歷與經驗，
☐ 擁有一份技能差距訓練需求清單與培訓計畫，
☐ 制定開放原始碼開發最佳實務的缺失清單與落實計畫。

**建議**

- 從簡單開始，穩步擴展分析及路線圖。
- 在招募時，應強調應徵者的開放原始碼技能與經驗。如果人員本身已具備開放原始碼「DNA」，通常會比培訓與指導來得容易。
- 檢視來自軟體供應商及開放原始碼學校的培訓課程。

**資源**

進一步資訊：

- 什麼是技能盤點？ —— Robert Tanner 提供的介紹。
- 關於開放原始碼技能的文章：5 個開放原始碼技能讓你升級履歷

此行動可以涵蓋以下技術資源與技能：

- **常見語言**（如 Java、PHP、Perl、Python）。
- **開放原始碼框架**（Spring、AngularJS、Symfony）及測試工具。
- 敏捷、DevOps 和開放原始碼的**開發方法與最佳實踐**。

**建議的下一步行動**

- GGI-A-28 - 人力資源觀點 一旦內部已識別出開放原始碼資源，應讓人力資源部門對現有與未來員工的這些技能加以重視，以提升開放原始碼意識。

# 6 信任目標行動清單

## 6.1 管理法律合規

行動編號：GGI-A-21。

### 描述

組織需要實施法律合規流程，以確保其在開放原始碼專案中的使用與參與符合法律要求。

在組織內部及整個供應鏈中，成熟且專業的法律合規管理涉及以下方面：

- 進行徹底的智慧財產分析，包括授權識別和相容性檢查。
- 確保組織能夠安全地使用、整合、修改和再分發開放原始碼組件，作為其產品或服務的一部分。
- 為員工和承包商提供一個透明的流程，說明如何創建和貢獻開放原始碼軟體。

**軟體組成分析**（*SCA*）：許多法律和智慧財產問題源於使用的元件所釋出的授權，這些授權之間可能不兼容，或與組織希望使用和再分發這些元件的方式不兼容。SCA 是解決這些問題的第一步，因為「了解問題是解決問題的前提」。這個過程是透過在材料清單文件中識別專案中涉及的所有元件，包括構建和測試相依關係。

**授權檢查**：授權檢查過程使用工具自動分析程式碼庫，並識別其中的授權和著作權。如果定期執行並理想地整合到持續構建和集成流程中，這可以及早發現智慧財產問題。

### 機會評估

隨著開放原始碼軟體在組織資訊系統中使用的不斷增加，評估和管理潛在的法律風險變得至關重要。

然而，檢查授權和著作權可能是棘手且昂貴的。開發人員需要能夠迅速檢查智慧財產權和法律問題。擁有一個專門處理智慧財產和法律問題的團隊及企業負責人，能夠確保積極且一致的法律問題管理，幫助確保開放原始碼元件的使用與貢獻，並提供清晰的策略視野。

### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- ☐ 有一個簡單易用的授權檢查流程可供專案使用。
- ☐ 專案可使用簡單易用的授權檢查流程。
- ☐ 組織內有專責人員或團隊負責法律合規事宜。
- ☐ 定期進行稽核以評估法律合規性。

其他設立驗證要點的方式：

- ☐ 有一個簡單易用的授權檢查流程。
- ☐ 有一個簡單易用的法律/智慧財產權（IP）團隊。
- ☐ 所有專案提供必要的資訊，供人員使用及貢獻於專案。
- ☐ 團隊內有專責聯絡人處理與智慧財產權及授權相關的問題。
- ☐ 企業指定一名負責人專責智慧財產權及授權事宜。
- ☐ 有一個專門處理智慧財產權（IP）和授權相關問題的團隊。

### 工具

- ScanCode
- Fossology
- SW360
- Fossa
- OSS 審查工具包

### 建議

- 向相關人員說明使用與業務目標相衝突的授權可能帶來的風險。
- 為專案提供簡單的解決方案，以便在其程式碼庫上設置授權檢查。
- 傳達授權檢查的重要性，並協助專案將其整合到 CI（持續整合）系統中。
- 提供專案結構的範本或官方指南，幫助統一規範。

- 配置自動化檢查，以確保所有專案符合指引。
- 考慮進行內部稽核，以識別公司基礎設施中使用的授權類型。
- 考慮進行內部稽核，以識別公司基礎設施中使用的授權類型。
- 為負責人提供完整的智慧財產權與授權培訓。
- 設立流程，將智慧財產權與授權問題升級至負責人處理。

請記住，合規性不僅涉及法律，還包括智慧財產權（IP）。以下是一些問題，幫助您了解法律合規性的後果：

- 如果我發佈開放原始碼元件而未遵守授權條件，將構成違反授權（法律影響）。
- 如果在希望分發/發佈的專案中使用開放原始碼組件，該授權可能要求公開某些程式碼元素，這可能影響公司機密性和戰略優勢（法律與機密性影響）。
- 是否為希望發佈的專案使用開放原始碼授權會影響相關的智慧財產權（IP 影響）。
- 如果我在任何專利程序**之前**將一個專案開源，這**可能**排除針對該專案創建專利的可能性 --> 智慧財產影響。
- 如果我在任何專利程序**之後**將一個專案開源，這**可能**允許針對該專案創建（防禦性）專利 --> 智慧財產的潛力。
- 在包含許多元件和多種相依性的複雜專案中，開放原始碼授權條款的多樣性可能導致授權之間的不相容性 --> 法律影響（詳見行動 GGI-A-23 - 管理軟體相依性）。

#### 資源

- 現有 OSS 合規小組頁面上有一個涵蓋範圍廣泛的工具清單。
- 企業開放原始碼合規實踐推薦 由 Linux 基金會的 Ibrahim Haddad 撰寫的一本書，探討企業開放原始碼合規實踐。OpenChain Project

#### 建議的下一步行動

- GGI-A-24 - 管理關鍵績效指標 使法律合規的關注點、流程和結果可視化且可衡量。這將幫助人們在流程早期意識到其重要性。

### 6.2 管理軟體漏洞

行動編號：GGI-A-22。

#### 描述

一段程式碼的安全性取決於其最不安全的部分。近期的案例（例如 heartbleed[^heartbleed]、equifax[^equifax]）已證明檢查並發現非本組織直接開發部分程式碼中的漏洞至關重要。漏洞暴露的後果可能包括數據洩露（對聲譽造成巨大影響）、勒索軟體攻擊以及威脅業務的服務不可用性。

開放原始碼軟體在漏洞管理方面通常比專有軟體更為優秀，主要原因是：

- 更多的人會檢視開放的程式碼和流程以發現並修復問題。
- 開放原始碼專案修復漏洞並釋出修補程式和新版本的速度要快得多。

例如，WhiteSource 的一項研究顯示，在其分析的專有軟體中，95% 的開放原始碼元件中的漏洞在分析時已釋出了修復程式。因此，問題在於無論是閉源還是開源軟體，都需**更好地管理程式碼基礎和其相依性中的漏洞**。

為了減輕這些風險，需要建立一個軟體資產的評估計畫以及定期執行的漏洞檢查流程。部署工具來提醒受影響的團隊，管理已知漏洞並防範來自軟體相依性的威脅。

#### 機會評估

任何使用軟體的公司都需要注意以下方面的漏洞：

- 其基礎設施（例如雲端基礎設施、網路基礎設施、數據儲存設施），
- 其業務應用程式（人力資源、客戶關係管理工具、內部和客戶相關的資料管理），
- 其內部程式碼（例如公司的網站、內部開發專案等），
- 以及所有直接和間接的軟體及服務相依性。

漏洞的投資回報率（ROI）在發生不良事件之前通常很難被了解。需要考量重大數據洩露或服務不可用性帶來的後果，從而估算漏洞的真正成本。

同樣地，應避免公司內部對安全相關問題的隱瞞和保密文化。相反，應共享並討論漏洞狀態的信息，以便從開發者到高層主管找到最佳解決方案。

透過謹慎管理軟體漏洞來預防網路攻擊有以下多重益處：

- 避免聲譽風險，
- 避免因漏洞利用而導致的損失（如分散式阻斷服務攻擊、勒索軟體攻擊、重建替代 IT 系統所需的時間），
- 遵守資料保護相關法規。

管理開放原始碼軟體的漏洞只是更廣泛的網路安全過程的一部分，該過程全面處理組織內系統和服務的安全性。

#### 進度評估

應設有專人或專屬團隊負責監控漏洞，以及提供開發者可以依賴的簡便流程。漏洞評估是持續整合過程的一個標準部分，人們可以在專用的儀表板中監控當前的風險狀態。

以下**檢驗要點**顯示了此行動的進度：

- ☐ 當所有內部軟體和服務都被評估並監控已知漏洞時，此行動即被視為完成。
- ☐ 當在軟體生產鏈中實施專用工具和流程，以防止日常開發例程中引入問題時，此行動即被視為完成。
- ☐ 指定人員或團隊負責評估 CVE/漏洞風險與暴露情況。
- ☐ 指定人員或團隊負責將 CVE/漏洞分派給相關人員（如系統運維、DevOps、開發者等）。

#### 工具

- GitHub 工具
  - GitHub 提供了用於保護託管在該平台上的程式碼的指南和工具。更多資訊請參閱 GitHub docs。
  - GitHub 提供 Dependabot，自動識別相依性中的漏洞。
- Eclipse Steady 是一款免費的開放原始碼工具，可分析 Java 和 Python 專案中的漏洞並協助開發者減輕其影響。
- OWASP dependency-check：一個開放原始碼漏洞掃描器。
- OSS Review Toolkit：一個開放原始碼編排工具，能從配置的漏洞數據服務中收集使用的相依性安全諮詢。

#### 資源

- MITRE 的漏洞數據庫 包括 CVE 資料。另請參閱 NIST 的安全數據庫 和其他相關資源，例如 CVE Details。
- 同樣請檢視 Google 的新倡議：開放原始碼漏洞。
- OWASP 工作組在其 網站 上公佈了漏洞掃描工具的列表，包括來自商業和開放原始碼領域的工具。
- J. Williams 和 A. Dabirsiaghi. 《不安全庫的遺憾現實》(The unfortunate reality of insecure libraries)，2012 年。
- 開放原始碼相依性中的漏洞檢測、評估和緩解 (Detection, assessment and mitigation of vulnerabilities in open source dependencies)，作者 Serena Elisa Ponta、Henrik Plate 和 Antonino Sabetta，《經驗軟體工程》期刊第 25 卷，第 3175-3215 頁 (2020)。
- 開放原始碼軟體漏洞修復的人工編輯資料集 (A Manually-Curated Dataset of Fixes to Vulnerabilities of open source Software)，作者 Serena E. Ponta、Henrik Plate、Antonino Sabetta、Michele Bezzi 和 Cédric Dangremont。此外，還有一個正在開發的工具包，用於實現上述資料集。

#### 建議的下一步行動

- GGI-A-24 – 管理關鍵指標 使已識別的漏洞可見。這將幫助人們意識到其軟體的安全性或潛在風險，並凸顯選擇適當相依性的必要性。

[^heartbleed]：https://www.wikipedia.org/wiki/Heartbleed [^equifax]：https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/

### 6.3 管理軟體相依性

行動編號：GGI-A-23。

### 描述

**軟體相依性的識別**程式會尋找程式碼庫中實際使用的軟體相依性。因此，組織必須建立並維護已知軟體相依性的清單，並監控所識別供應商的變動。

建立和維護已知軟體相依性清單是以下工作的前提條件：

- 智慧財產 (IP) 和授權檢查：某些授權條款無法混用，即使是軟體相依性也不行。了解自己的軟體相依性，才能評估相關的法律風險。
- 漏洞管理：整個軟體的安全性取決於最弱的一環。例如 Heartbleed 漏洞。了解軟體相依性才能評估相關的安全風險。
- 生命周期和可持續性：軟體相依性專案中活躍的社群是錯誤修復、優化和新功能的良好指標。
- 根據「成熟度」標準精心選擇使用的軟體相依性，目標是使用安全且有良好維護的程式碼庫，並擁有活躍且積極回應的社群，這樣的社群會接受外部貢獻等。

### 機會評估

識別和追蹤軟體相依性是減輕任何程式碼重用風險的必要步驟。此外，實施工具和流程以管理軟體相依性是妥善管理品質、合規性和安全性的前提條件。

請考慮以下問題：

- 如果軟體被破壞、攻擊或遭到起訴，公司面臨的風險（成本、聲譽等）是什麼？
- 程式碼庫是否對人員、組織或業務具有關鍵性？
- 如果應用程式所相依的元件更改其儲存庫會怎樣？

最基本且首要的步驟是實施一個軟體組成分析 (SCA) 工具。對於全面的 SCA 或軟體相依性映射，可能需要專業諮詢公司提供支援。

### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- ☐ 所有內部開發的程式碼中都已識別出軟體相依性。
- ☐ 公司內執行的所有外部程式碼中都已識別出軟體相依性。
- ☐ 專案可在其持續整合 (CI) 流程中加入易於設置的軟體組成分析或軟體相依性識別程序。
- ☐ 使用軟體相依性分析工具。

### 工具

- OWASP Dependency check：Dependency-Check 是一個軟體組成分析 (SCA) 工具，旨在檢測專案軟體相依性中的已公開漏洞。
- OSS Review Toolkit：一套工具，協助審查開放原始碼軟體的相依性。
- Fossa：快速、便攜且可靠的軟體相依性分析工具。支援授權與漏洞掃描，語言無關，並與 20 多種建置系統整合。
- Software 360。
- Eclipse Dash license tool：接收軟體相依性清單並請求 ClearlyDefined 檢查其授權。
- The FOSSology Project：FOSSology 是一個開放原始碼專案，致力於推進開放原始碼授權合規性。

### 建議

- 定期對軟體相依性和知識產權要求進行審核，以減輕法律風險。
- 理想情況下，應將軟體相依性管理整合到持續整合 (CI) 流程中，以便盡早識別並修復問題（新增軟體相依性、授權不兼容等）。
- 持續追蹤與軟體相依性相關的漏洞，並通知使用者和開發者。
- 向相關人員說明錯誤授權所帶來的風險。
- 為專案提供簡單的解決方案，以便在其程式碼庫上設置授權檢查。
- 傳達授權檢查的重要性，並協助專案將其整合到 CI（持續整合）系統中。
- 針對軟體相依性風險設立可見的 KPI。

### 資源

- 現有的開放原始碼授權合規工具群組頁面。

- Free and Open Source Software licence Compliance: Tools for Software Composition Analysis，作者 Philippe Ombredanne，nexB Inc.
- Software Sustainability Maturity Model。
- CHAOS：社群健康分析開放原始碼軟體。

#### 建議的下一步行動

- GGI-A-21 - 管理法律合規：在能夠追蹤知識產權和授權不兼容性之前，必須先識別開放原始碼軟體中的所有軟體相依性。
- GGI-A-22 - 管理軟體漏洞：在能夠追蹤程式碼資產中的漏洞之前，必須先識別開放原始碼軟體中的所有軟體相依性。

## 6.4 管理關鍵指標

行動編號：GGI-A-24。

#### 描述

此行動收集並監管一系列指標，為專業管理的開放原始碼軟體提供日常管理決策與策略選項的依據。

與開放原始碼軟體相關的關鍵指標，是評估治理計畫推動成效的背景依據。此行動包含選定若干指標、向團隊與管理層公布這些指標，並透過新聞通訊或公司內部新聞定期更新此倡議的進展。

此行動要求：

- 利害關係人參與討論並定義該計畫的目標，
- 實施與開發基礎設施相連的測量與資料收集工具，
- 為利害關係人及所有參與此倡議的人員，至少提供一個儀表板。

指標需根據從相關來源收集的數據來建立。幸運的是，開放原始碼軟體工程有許多可供參考的來源。範例包括：

- 開發環境、CI/CD 生產鏈，
- 人力資源部門，
- 測試與軟體組成分析工具，
- 程式碼儲存庫。

指標範例包括：

- 根據授權類型顯示已解決的軟體相依性數量。
- 過時/存在漏洞的軟體相依性數量。
- 偵測到的授權/知識產權問題數量。
- 對外部專案所做的貢獻。
- 錯誤 (Bug) 開啟時間。
- 元件的貢獻者數量、提交次數等。

此行動的重點是定義這些需求與測量要求，並實施一個儀表板，以簡單有效的方式顯示計畫的主要指標。

#### 機會評估

關鍵指標有助於理解與更好地管理投入到開放原始碼軟體的資源，並透過有效的溝通衡量結果，獲取投資的全部效益。透過廣泛傳播，能讓更多人關注此倡議，並產生參與感，最終將其轉化為組織層級的目標與關切事項。

雖然每個行動都有評估標準，可回答有關進展的問題，但仍需透過數字與量化指標進行監控。

無論是小型新創公司還是大型跨國企業，關鍵指標都有助於團隊專注目標並監控績效。度量指標至關重要，因為它們支援決策並為已做出的決策提供監督依據。

透過簡單實用的數字與圖表，整個組織的成員將能同步關注開放原始碼相關的努力，讓其成為一個共享的目標與行動。這也能讓各方更好地參與其中，為專案做出貢獻，並獲得整體效益。

#### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- □ 已建立指標清單及其收集方式。
- □ 已使用工具來收集、儲存、處理並顯示指標。
- □ 已提供可供所有參與者使用的整合儀表板，顯示倡議的進展情況。

#### 工具

- GrimoireLab，由 Bitergia 提供。
- 通用商業智慧工具（如 Elasticsearch、Grafana、R/Python 視覺化工具等）也非常適用，只需根據定義的目標設置適當的連接器。

#### 建議

- 撰寫開放原始碼治理的目標與路線圖。
- 在公司內部溝通此倡議的行動與進展狀態。
- 讓人們參與 KPI 的定義，以確保
  - 他們充分理解指標，
  - 指標提供了全面的需求視角，
  - 指標受到重視並被持續追蹤。
- 至少建立一個儀表板，讓所有人都能看到（例如，在會議室螢幕上顯示），以顯示關鍵指標來展示進展與整體狀況。

#### 資源

- CHAOSS 社群 提供許多有關開放原始碼指標的參考資料與資源。
- 查看 OW2 市場成熟度等級 方法論 中 專案屬性指標 的指標。
- 《衡量開放性的新方法：開放治理指數》(A New Way of Measuring Openness: The Open Governance Index)，作者 Liz Laffan，探討了開放原始碼專案中的開放性度量。
- 《治理指標：使用者指南》(Governance Indicators: A Users' Guide) ，由聯合國出版，雖然主要應用於民主、貪腐和國家透明度，但治理中測量與指標的基礎知識值得一讀。

#### 建議的下一步行動

- GGI-A-37 - 開放原始碼促進數位轉型：將產生的度量指標作為整體開放原始碼策略的一部分。

### 6.5 執行程式碼審查

行動編號：GGI-A-44。

#### 描述

程式碼審查，是一項日常任務，涉及在發佈產品或交付專案給客戶之前，對應用程式的原始碼進行手動和/或自動檢查。在開放原始碼軟體的情境中，程式碼審查不僅僅是機會性地捕捉錯誤，而是一種在團隊層面執行的協作開發整合方法。

程式碼審查應適用於內部開發的程式碼以及從外部來源重複使用的程式碼，因為這能提升對程式碼的整體信心並強化所有權。此外，這也是一個絕佳的機會來提升團隊的整體技能與知識，並促進團隊協作。

#### 機會評估

程式碼審查在組織開發軟體或重複使用外部軟體元件時都非常有價值。在開放原始碼的背景下，程式碼審查雖然是軟體工程流程中的標準步驟，但它也帶來特定的優勢，例如：

- 發佈內部原始碼時，確認遵守適當的品質指引。
- 貢獻至現有的開放原始碼專案時，確認符合目標專案的指引。
- 公開的相關文件已適時更新。

這也是分享並強化公司法律合規政策規則的絕佳機會，例如：

- 絕不可移除重複使用的開放原始碼中的現有授權標頭或著作權聲明。

- 未經法律團隊事先許可，不可從 Stack Overflow 複製與貼上原始碼。
- 在需要時正確地引用註明著作權條款。

程式碼審查將為程式碼帶來信任與信心。如果人們不確定使用軟體產品的品質或潛在風險，他們應進行同行審查與程式碼審查。

### 進度評估

以下**檢驗要點**顯示了此行動的進度：

☐ 開放原始碼程式碼審查被視為必要步驟。
☐ 開放原始碼程式碼審查已被計畫安排（定期或在關鍵時刻進行）。
☐ 已集體定義並接受執行開放原始碼程式碼審查的流程。
☐ 開放原始碼程式碼審查已成為開發流程的標準部分。

### 建議

- 程式碼審查是一項團隊合作的任務，在良好的協作環境下運作效果更佳。
- 請善加利用開放原始碼領域中現有的工具和模式，因為程式碼審查在該領域已是多年的標準做法。

### 資源

- 什麼是程式碼審查？(What is Code Review?)：Red Hat 的 Open Practice Library 提供的程式碼審查教學讀物。
- 程式碼審查的最佳實踐 (Best Practices for Code Reviews)：另一種對程式碼審查的有趣觀點。

### 建議的下一步行動

- GGI-A-26 - 貢獻至開放原始碼專案：程式碼審查是開放原始碼專案的常見做法，這有助於提升程式碼品質並促進知識共享。進行程式碼審查的貢獻者通常對外部貢獻與協作更感到自信。

# 7 文化目標行動清單

## 7.1 推廣開放原始碼開發最佳實踐

行動編號：GGI-A-25。

### 描述

此行動旨在於開發團隊內部定義、積極推廣並落實開放原始碼最佳實踐。

作為起點，可以考慮以下幾個重點主題：

- 使用者與開發者文件。
- 將專案妥善組織於公開可訪問的儲存庫中。
- 推廣並落實受控重複使用。
- 提供完整且最新的產品文件。
- 配置管理：Git 工作流程、協作模式。
- 發布管理：頻繁發布及早交付，穩定版與開發版之間的管理等。

開放原始碼專案具有特殊的類市集型運作模式。為了促進此合作模式及思維，建議採用一些實務，以支持協作式及分散式開發，並促進來自第三方開發者的貢獻……

**社群文件** 確保公司內所有專案均提供以下文件：

- README —— 專案的簡要說明、如何參與、資源連結。
- Contributing —— 為願意貢獻的人提供的指南。
- Code Of Conduct —— 社群內可接受或不可接受的行為準則。
- LICENSE —— 儲存庫的預設授權條款。

**REUSE 最佳實踐** REUSE 是歐洲自由軟體基金會提出的倡議，旨在改善軟體重複使用並簡化開放原始碼及授權合規流程。

### 機會評估

儘管這在很大程度上取決於團隊的開放原始碼共識知識，但對人員進行培訓及建立落實這些實務的流程仍然大有裨益。這在以下情況下更為重要：

- 潛在的使用者與貢獻者尚未確定，
- 開發者尚未習慣於開放原始碼開發。

### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- ☐ 專案制定了一套符合的開放原始碼最佳實踐清單。
- ☐ 專案監控其與最佳實踐的一致性。
- ☐ 開發團隊已建立對遵循開放原始碼最佳實踐的認識。
- ☐ 新的最佳實踐會定期評估，並努力加以落實。

### 工具

- REUSE 輔助工具 協助讓儲存庫符合 REUSE 最佳實務。該工具可以整合至多數開發流程中，以確認當前狀態。
- ScanCode 能夠列出儲存庫內的所有社群與法律文件：請參閱功能描述。
- GitHub 提供一項功能，可檢查遺漏的社群文件。可以在儲存庫頁面 >「Insights」>「Community」中找到此功能。

### 建議

- 最佳實務清單依專案的背景及領域而有所不同，應定期重新評估，以持續改善方式進行監控與追蹤進度。
- 培訓人員關於開放原始碼的重複使用（作為使用者）及生態系統（作為貢獻者）。
- 落實 REUSE.software（詳見行動 #14）。

- 建立流程以管理與重複使用及貢獻相關的法律風險。
- 明確鼓勵人員貢獻於外部專案。
- 提供專案結構的範本或官方指南，幫助統一規範。
- 配置自動化檢查，以確保所有專案符合指引。

#### 資源

- OW2 開放原始碼最佳實務清單 來自市場成熟度等級評估方法論。
- REUSE 官方網站 提供規範、教程及常見問題解答。
- GitHub 社群指南。
- 使用 GitHub 實現配置管理最佳實務範例。

#### 建議的下一步行動

- GGI-A-42 - 管理開放原始碼技能與資源 你可以將已識別的開放原始碼開發最佳實務納入一般培訓材料中。
- GGI-A-44 - 執行程式碼審查 程式碼審查是開發最佳實務的重要元素。

### 7.2 貢獻至開放原始碼專案

行動編號：GGI-A-25。

#### 描述

向開放原始碼專案貢獻是良善治理的關鍵原則之一。目的是避免成為單純的被動消費者，而是對專案進行回饋。當人們為自己的需求新增功能或修復漏洞時，應將其設計得足夠通用，以便貢獻至專案。開發者必須獲得時間來進行貢獻。

此行動涵蓋以下範疇：

- 與上游開放原始碼專案合作。
- 報告漏洞和功能需求。
- 貢獻程式碼與漏洞（bug）修復。
- 參與社群郵件群組。
- 分享經驗。

#### 機會評估

此行動的主要益處包括：

- 它增加了公司內部對開放原始碼的知識與承諾，因為員工開始進行貢獻並參與開放原始碼專案。他們感受到社會價值並提升了個人聲譽。
- 公司透過貢獻提升了可見度與聲譽。隨著貢獻融入專案，展示了公司實際參與開放原始碼的行動，回饋專案並推廣公平與透明的文化。

#### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- □ 明確且正式的官方貢獻路徑，讓願意參與貢獻的員工有清晰的指引。
- □ 鼓勵開發者回饋他們使用的開放原始碼專案，支持專案的進一步發展。
- □ 建立一套流程，確保開發者的貢獻符合法律合規性與安全要求。
- □ 績效指標（KPI）：外部貢獻的數量（如代碼、郵件列表、議題等），可按個人、團隊或實體進行統計。

#### 工具

追蹤貢獻可能是有幫助的，不僅可以記錄貢獻的內容，還可以有效傳達公司在這方面的投入。可以使用儀表板和活動追蹤軟體來達成此目的。請參閱：

- Bitergia 的GrimoireLab
- ScanCode

#### 建議

鼓勵組織內部人員貢獻於外部專案，方法包括：

- 允許他們編寫通用、經過良好測試的漏洞修復和功能，並將其回饋給社群。
- 培訓如何回饋開放原始碼社群，內容包括技術技能（提升團隊知識）和社群參與（融入開源社群、遵守行為準則等）。
- 提供法律、知識產權（IP）和技術問題的培訓，並在公司內設置聯絡窗口，便於員工在有疑問時獲得幫助。
- 對於公開發表的工作成果提供獎勵。
- 公司或實體的貢獻會反映其程式碼品質和參與度，因此確保開發團隊提交足夠優秀的程式碼。

#### 資源

- Linux 基金會的 CHAOSS 倡議 提供工具和指導，幫助追蹤開發中的貢獻。

#### 建議的下一步行動

- GGI-A-31 - 公開宣告使用開放原始碼 現在組織的貢獻和承諾已具公眾可見性，開始對外宣傳這些成就！
- GGI-A-24 - 管理關鍵指標 將對開源專案的貢獻轉化為可見且可衡量的成果，這有助於倡議的推廣並提升員工士氣。
- GGI-A-27 - 隸屬於開源社群 對開源社群的貢獻是成為其一員的第一步。一旦開始貢獻，人們會更深入參與專案的健康與治理，甚至成為維護者，確保專案的永續發展和健康的路線圖。
- GGI-A-29 - 與開放原始碼專案合作 開源專案重視實力為本（Meritocracy）。當您展示了對程式碼與流程的良好理解後，可以更正式地參與專案，提升貢獻的影響力。
- GGI-A-36 - 開放原始碼促進創新 對開源專案的貢獻及與外部貢獻者的互動，能促進創新。
- GGI-A-39 - 回流優先 對開源專案的貢獻只有在定期且制度化地回流至專案中時，才真正具意義。

### 7.3 隸屬於開源社群

行動編號：GGI-A-27。

#### 描述

此行動旨在讓開發人員培養對更大開放原始碼社群的歸屬感。如同任何社群一樣，個人和組織都必須參與並回饋整體。這不僅強化了實務者之間的聯繫，還為生態系統帶來持續性與活躍性。在技術層面上，這有助於選擇專案的優先順序和路線圖，並提升整體的知識水準與技術意識。

此行動涵蓋以下範疇：

- **識別值得參加的活動**。連結人脈、學習新技術以及建立網絡，是充分發揮開放原始碼效益的關鍵因素。
- 考慮**加入基金會會員**。開放原始碼基金會和組織是開源生態系統的重要組成部分。它們為專案提供技術和組織資源，並作為中立的平台，讓贊助者討論共同問題與解決方案，或制定標準。
- 關注**工作小組**。工作小組是中立的協作工作空間，專家在特定領域（如物聯網、建模或科學）中互動。這是一種非常高效且具成本效益的機制，可共同解決領域特有的共通問題。
- **預算參與**。最終，金錢是推動力。規劃所需的費用，允許人員有薪參與這些活動，預先安排未來的行動，確保計畫不會因短缺資金而在數月後停止。

#### 機會評估

與更廣泛的開放原始碼社群合作時，開放原始碼運作得最好。這促進了錯誤修復、解決方案共享等。

這也是公司展示其對開放原始碼價值支持的一個好方式。宣傳公司參與開放原始碼的行動，對公司聲譽及開放原始碼生態系統都很重要。

#### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- ☐ 草擬出人們可參加的活動清單。
- ☐ 追蹤團隊成員進行的公開演講。
- ☐ 人員可以提交參與活動的請求。

□ 人員可以提交專案以申請贊助。

**建議**

- 透過調查了解哪些活動對人員最感興趣，或對他們的工作最有幫助。
- 建立內部溝通機制（如電子報、資源中心、邀請函等），讓人們了解這些倡議並能參與其中。
- 確保這些倡議能惠及各類人員（開發者、系統管理員、支援人員等），而不僅限於高階主管。

**資源**

- 什麼促使開發者貢獻開放原始碼軟體？(What motivates a developer to contribute to open source software?) 由 Michael Sweeney 在 clearcode.cc 發表的文章。
- 公司為何貢獻開放原始碼 (Why companies contribute to open source) 由 VMware 的 Velichka Atanasova 發表的文章。
- 為什麼員工應該貢獻開放原始碼 (Why your employees should be contributing to open source) 由 CloudBees 的 Robert Kowalski 提供的精彩閱讀內容。
- 公司支持開放原始碼的 7 種方式 (7 ways your company can support open source) Simon Phipps 在 InfoWorld 發表的文章。
- 活動：開放原始碼的生命力 (Events: the life force of open source) 由 RedHat 的 Donna Benjamin 發表的文章。

**建議的下一步行動**

- GGI-A-28 - 人力資源觀點 如果組織屬於開放原始碼社群，將更容易吸引具備技能的人才，這也取決於組織所參與的社群。
- GGI-A-31 - 公開宣示使用開放原始碼 現在您已成為開放原始碼社群的一部分，讓大家知道！這對您的聲譽有益，對專案的健康發展及傳播也有幫助。

## 7.4 人力資源觀點

行動編號：GGI-A-28。

**描述**

切換到開放原始碼文化對人力資源的深遠影響：

- **新流程與合約**：合約需要進行調整，以允許並促進外部貢獻。這包括處理公司內完成工作的 IP 和授權問題，同時也要考慮員工或承包商是否能擁有自己的專案。
- **不同類型的人才**：參與開放原始碼工作的人的激勵和心態，通常與傳統專有軟體的企業員工有所不同。流程與心態需要適應這種以社群聲譽為導向的模式，以吸引並留住新型態的人才。
- **職涯發展**：需要提供一條職涯路徑，培養並重視員工的技術與軟實力，以及組織期望的能力（例如：協作以推動社群工作、擔任公司代言人的溝通能力等）。人力資源部門在將開放原始碼作為文化目標方面，扮演著關鍵角色。

**勞動力**對於長期從事專有（軟體）解決方案的開發者來說，切換到開放原始碼可能是很大的轉變，並需要一定的適應時間。但對大多數開發者而言，開放原始碼帶來的是純粹的好處。

如今，剛從學校或大學畢業的開發者幾乎全都曾接觸開放原始碼。在公司內部，大多數開發者每天都在使用開放原始碼語言，或匯入開放原始碼庫與程式碼片段。相較於觸發內部採購流程（需經過多層管理驗證），直接粘貼幾行開放原始碼代碼進程式顯然更簡便。

開放原始碼讓開發者的工作更具吸引力透過開放原始碼，開發者能持續關注公司外的同行在發明什麼，從而保持在最頂尖的技術。

對於組織來說，需要制定一項人力資源策略：一、對現有員工進行技能提升或再培訓；二、在招聘新人才時，反思並確認公司的定位，以及其在開放原始碼領域的吸引力。

> 關於招聘的見解招募具備良好開放原始碼思維、理解代碼並懂得如何與他人合作的員工，是一個極具價值的選擇。相較於進行傳道、培訓或實習計劃，雖然這些選項同樣值得，但它們往往更昂貴且耗時。
>
> —開放原始碼軟體供應商 CEO

這表明，招聘具備「開放原始碼 DNA」的人才是人力資源策略中值得考慮的一條加速途徑。

### 流程

- 建立或重新檢視職位描述（技術技能、軟實力、能力與經驗）
- 培訓計劃：自我訓練、正式培訓、管理指導、同儕配對、社群活動
- 建立或重新檢視職涯規劃：包含能力、關鍵成果/影響以及職涯階段

### 機會評估

1. 制定開發實踐框架：問題不在於激勵開發者更多使用開放原始碼，而在於確保安全使用、遵守授權條款，且不放棄傳統安全檢查（開放原始碼程式碼可能含有惡意代碼），
2. 重新檢視協作實踐：透過開發實踐，將敏捷性與協作擴展至組織內其他業務領域。內源模式常用於促進這些行為，但可能只是邁向開放原始碼文化的一半路程，
3. 組織文化：最終，這一切都關乎組織文化——開放原始碼可以成為開放性、協作、倫理與永續性的核心價值旗幟。

### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- ☐ 提供培訓以介紹開放原始碼的優勢及其限制（如智慧財產權授權條款的遵從合規性）。
- ☐ 確保每位開發者、架構師及專案負責人（或產品負責人/業務負責人）了解開放原始碼的優勢及其限制（如知識產權授權條款的遵從性）。
- ☐ 鼓勵開發者參與開放原始碼社群並承擔責任，並可獲得相應的培訓支援。
- ☐ 技能與能力應體現在組織的職位描述與職涯發展中。
- ☐ 開發者在開放原始碼中的經驗（如對開放原始碼社群的貢獻、參與內部合規流程、作為公司外部發言人等）應納入人力資源評估過程。

### 工具

- 技能矩陣。
- 公共培訓計劃（如：開放原始碼學校）。
- 來源：GitHub、GitLab、LinkedIn、Meetups、Epitech、Epita...
- 合約範本（忠誠條款）。
- 職位描述（範本）與職涯進階（範本）。

### 建議

如今，大多數開發者已經瞭解一些開放原始碼的原則，並且願意使用及參與開發開放原始碼軟體。然而，管理層仍需採取一些行動：

- 在招募時偏好具備開放原始碼經驗者，即使該職位只涉及專有技術相關的開發者。隨着日益數位轉型，每個開發者未來都有機會參與開源相關工作。
- 開放原始碼培訓計畫：每位開發者、架構師、專案負責人（或產品負責人/業務負責人）都應能夠獲得培訓資源（例如影片或面對面的培訓），這些資源將說明開放原始碼的優勢，以及在知識產權和授權合規方面的限制條件。
- 為希望參與開放原始碼社群及其治理機構的開發者提供培訓（如 Linux 認證）。
- 在人力資源的個人評估流程中，應認可員工（無論是開發者還是架構師）在開放原始碼相關主題上的貢獻，例如對開放原始碼社群的貢獻，以及遵守知識產權授權條款的行為。大多數主題是共享的，並適合納入技術職涯規劃，但某些主題可能或應該是專門設計的。
- 最佳保密策略與公司姿態：需要解決溝通層面的問題（例如這在組織中有多核心，是否應在年度報告中反映出來），以及它如何影響公司的溝通姿態（開放原始碼的貢獻者可能成為公司代言人，包括與媒體的聯繫）。

### 資源

- 關於人員在活動中代表公司對外發言的能力，請參考行動 31：「（參與目標）公開宣示使用開放原始碼」。

## 7.5 回流優先

行動編號：GGI-A-29.

### 描述

此行動關注在提升對回饋貢獻及推行「回流優先」（Upstream First）原則的認識。

在「回流優先」的方法中，對開放原始碼專案的所有開發工作，都必須達到提交給專案核心開發人員並由其發布所需的開放性與品質水平。

### 機會評估

秉持「回流優先」理念編寫程式碼，將帶來以下成果：

- 更高品質的程式碼，
- 可提交給上游專案的程式碼，
- 被合併至核心軟體的程式碼，
- 與未來版本相容的程式碼，
- 獲得專案社群的認可，並促進更良好且更有價值的合作。

  「回流優先」不只是「友善的表現」。這代表你在專案中擁有話語權，這代表可預測性，這代表你能掌控局勢，這代表你是主動而非被動，這代表你真正理解開放原始碼。（Maximilian Michels）

### 進度評估

以下**驗證要點**顯示此行動的進展：是否實施了「回流優先」？

- ☐ 提交至第三方專案的 pull/merge 請求數量顯著增加。
- ☐ 已草擬需套用「回流優先」原則的第三方專案清單。

### 建議

- 識別出與上游開發者互動經驗最豐富的開發者。
- 促進開發者與核心開發者之間的互動（活動、黑客松等）

### 資源

- 對「回流優先」原則的清晰解釋，及其如何契合「文化目標」：https://maximilianmichels.com/2021/upstream-first/。

  「回流優先」意指當你在上游程式碼的副本中解決一個問題，且其他人也可能受益時，應將這些更改回饋給上游，也就是說，提交補丁或開啟 pull request 至上游程式碼庫。
- 什麼是軟體開發中的上游與下游？ 清晰易懂的解釋。
- 摘錄自 Chromium OS 設計文件的解釋：回流優先。
- Red Hat 關於上游及「回流優先」優勢的說明：回流優先。

### 建議的下一步行動

- GGI-A-25 - 推廣開放原始碼開發最佳實踐 回饋上游是開放原始碼的主要最佳實踐之一。將其納入組織的最佳實踐，這將有助於外部貢獻、內部整體品質及知識共享。

# 8 參與目標行動清單

## 8.1 參與開源專案

行動編號：GGI-A-36。

### 描述

此行動旨在對一些對您組織重要的開放原始碼軟體（OSS）專案做出重大貢獻。貢獻會在組織層級進行擴展和承諾（與行動 #26 中的個人層級不同）。貢獻可以採取多種形式，包括直接資助或資源分配（例如人員、伺服器、基礎設施、溝通等），只要它們能以可持續且有效的方式惠及專案或生態系統即可。

此行動是行動 #26 的延續，將開放原始碼專案的貢獻提升到組織層級，使其更具可見性、影響力和效益。在此行動中，貢獻應為 OSS 專案帶來實質性、長期的改進。例如，指派一名開發人員或團隊來開發備受期待的新功能、提供基礎設施資產、為新服務提供伺服器，或接手維護廣泛使用的分支。

這主要概念是設定一定比例的資源，以支持開放原始碼開發者們去撰寫及維護我們所使用的資源庫或專案。

此行動需要對組織所使用的開源軟體進行映射，並評估其重要性，以決定需要支持的專案。

### 機會評估

> 如果每家公司使用開源軟體時至少做出一點貢獻，我們將擁有一個健康的生態系統。https://news.ycombinator.com/item?id=25432248

支持專案有助於確保其可持續性，並提供訪問資訊的途徑，甚至可能幫助影響和優先處理某些開發（儘管這不應該是支持專案的主要原因）。

潛在益處：確保漏洞報告得到優先處理，並將開發成果整合到穩定版本中；可能的成本：投入專案所需的時間，以及資金上的承諾。

### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- ☐ 識別受益專案。
- ☐ 決定支持的方式，例如直接的財務捐款或程式碼貢獻。
- ☐ 指派任務負責人。
- ☐ 少量的貢獻已發生。
- ☐ 貢獻的成果已經被評估。

驗證點參考了 OpenChain self certification 的問卷：

- ☐ 我們有代表組織貢獻開放原始碼專案的內部政策。
- ☐ 我們有一套流程文件來治理開放原始碼的貢獻。
- ☐ 我們有一套流程文件來所有的軟體員工們意識到開放原始碼的貢獻政策。

### 工具

一些組織提供了支持開放原始碼專案的機制（如果目標專案在他們的資助範圍內，這可能是一個方便的選擇）。

- Open Collective。
- 軟體自由保護協會（Software Freedom Conservancy）.
- Tidelift。

### 建議

- 專注於對組織至關重要的專案：這些是您最希望透過貢獻來支持的專案。
- 以社群專案為目標。
- 此行動需要對目標專案具備基本的熟悉程度。

#### 資源

- 如何支持開放原始碼專案：一篇簡短的文章，提供支持開放原始碼專案的資助建議。
- Sustain OSS：一個專注於支持開放原始碼的對話平台

#### 建議的下一步行動

- GGI-A-26 - 貢獻於開放原始碼專案 參與開放原始碼倡議最自然的方式是直接向專案做出貢獻。作為回報，您將獲得對貢獻的寶貴回饋意見。
- GGI-A-30 - 支持開放原始碼社群 有許多方式可以支持對您的組織至關重要的開放原始碼倡議。參與社群是一種很好的方式來發現並促進這些倡議的發展。

### 8.2 支持開源社群

行動編號：GGI-A-30。

#### 描述

此行動旨在與開放原始碼世界的機構代表建立聯繫。

透過以下方式達成：

- 加入開放原始碼基金會（包括會費成本）。
- 支持並倡導基金會的活動。

此行動需要為開發與 IT 團隊分配時間與預算，以參與開放原始碼社群。

#### 機會評估

開放原始碼社群站在開放原始碼生態系統演進的前線。參與開放原始碼社群有多項優勢：

- 它有助於保持資訊更新與掌握最新趨勢，
- 它提升組織的形象，
- 會員資格附帶多項好處，
- 它為開放原始碼 IT 團隊提供額外的結構與動力。

成本包括：

- 會員費用，
- 分配人員時間與旅費預算，參加社群活動，
- 監控智慧財產權（IP）相關承諾。

#### 進度評估

以下**檢驗要點**顯示了此行動的進度：

☐ 該組織是某個開放原始碼基金會的正式會員。
☐ 該組織參與該基金會的治理。
☐ 該組織開發的軟體已提交或已納入基金會的程式碼基礎。
☐ 會員資格在該組織與社群的網站上均有公開承認。
☐ 已進行會員資格的成本/效益評估。
☐ 已指派社群聯絡窗口。

#### 建議

- 加入與您組織規模與資源相符的社群，也就是能夠聽到您聲音並讓您成為受認可貢獻者的社群。

#### 資源

- 參考 Linux 基金會提供的這個實用頁面，了解加入開放原始碼社群的理由與方法。

**建議的下一步行動**

- GGI-A-31 - 公開宣告使用開放原始碼 既然您已正式支持某些開放原始碼社群，就將這些事實公開！這對您的聲譽有好處，也有助於項目的健康發展與推廣。

## 8.3 公開聲明使用開放原始碼

行動編號：GGI-A-31。

**描述**

此行動旨在承認在資訊系統、應用程式及新產品中使用開放原始碼軟體（OSS）。

- 提供成功案例。
- 在活動中進行展示。
- 資助參與活動。

**機會評估**

目前普遍接受大多數資訊系統皆運行於開放原始碼軟體之上，且新應用程式在很大程度上是透過重複使用開放原始碼軟體所建立。

此行動的主要好處在於為開放原始碼軟體與專有軟體之間創造公平的競爭環境，確保開放原始碼軟體受到同等的重視，並與專有軟體一樣以專業的方式進行管理。

另一個附帶好處是大幅提升開放原始碼軟體生態系的形象，而由於開放原始碼使用者被視為「創新者」，也有助於提升組織的吸引力。

**進度評估**

以下**檢驗要點**顯示了此行動的進度：

- ☐ 商業開放原始碼供應商被授權將該組織的名稱作為客戶參考資料。
- ☐ 貢獻者被允許這樣做，並以組織名義表達意見。
- ☐ 在 IT 部門的年度報告中公開提及使用開放原始碼軟體。
- ☐ 組織對於在媒體（例如採訪、開放原始碼及產業活動等）中說明其使用開放原始碼軟體不存在任何障礙。

**建議**

- 此行動的目標並非讓該組織成為開放原始碼運動的倡導者，而是確保公眾認可其使用開放原始碼軟體時不會遇到任何障礙。

**資源**

- 參考範例 CERN 公開宣告其使用 OpenStack

## 8.4 與開源供應商合作

行動編號：GGI-A-33。

**描述**

與提供您關鍵軟體的開放原始碼供應商簽訂合約。生產開放原始碼軟體的公司與團體需要持續發展，以提供維護與新功能的開發。專案需要他們的專業知識，使用者社群則依賴他們持續營運與貢獻。

與開放原始碼供應商的合作形式包括：

- 訂閱支援計畫。
- 委託在地服務公司。
- 贊助開發。
- 支付商業授權費用。

此行動意味著將開放原始碼專案視為具完整功能、值得付費的產品，與任何專有產品類似，但通常成本遠低於專有產品。

#### 機會評估

此行動的目標是確保組織所使用的開放原始碼軟體擁有專業支援。此舉具有多項好處：

- 透過及時的錯誤修復，確保服務的持續性。
- 透過最佳化安裝，提升服務效能。
- 釐清所使用軟體的法律/商業狀態。
- 獲得早期資訊。
- 預算穩定可預測。

當然，成本主要是所選擇的支援計畫費用。另一項成本可能是從大規模外包轉向與專業中小企業（SMEs）的精細合約合作。

#### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- ☐ 組織內使用的開放原始碼軟體獲得商業支援。
- ☐ 部分開放原始碼專案已簽訂支援計畫。
- ☐ 開放原始碼支援計畫的費用已成為 IT 預算中的合理項目。

#### 建議

- 在可能情況下，尋找當地的專業中小企業（SMEs）。
- 需注意大型系統整合商轉售第三方專業知識（例如轉售由專業開放原始碼 SMEs 實際提供的支援計畫）。

#### 資源

以下連結說明了開放原始碼軟體的商業現實：

- 快速了解商業開放原始碼。

### 8.5 開源採購政策

行動編號：GGI-A-43。

#### 描述

此行動旨在實施一套流程，以選擇、採購和購買開放原始碼軟體及服務。同時，也需考量開放原始碼軟體的實際成本並進行預算規劃。開放原始碼軟體乍看之下「免費」，但其實仍存在內外部成本，例如整合、訓練、維護與支援等。

此政策要求在評估總體擁有成本與品質的最佳組合時，對開放原始碼與專有解決方案進行對等考量。因此，IT 採購部門應積極且公平地考慮開放原始碼選項，同時確保在採購決策中，專有解決方案也被平等對待。

當專有解決方案與開放原始碼解決方案在總成本上沒有顯著差異時，可以明確表示對開放原始碼的偏好，因其具備內在的靈活性。

採購部門必須了解，提供開放原始碼支援的公司通常缺乏參與採購競標的商業資源，並相應調整其開放原始碼採購政策與流程。

#### 機會評估

設定特定開放原始碼採購政策的理由包括：

- 商業開放原始碼軟體與服務的供應不斷成長，無法被忽視，這需要實施專門的採購政策與流程。
- 企業資訊系統中，具有競爭力的商業開放原始碼解決方案供應量日益增加。
- 即使採用免費的開放原始碼組件並將其整合至應用中，仍須提供內部或外部資源來維護該原始碼。
- 總體擁有成本（TCO）通常（雖非絕對）對自由及開放原始碼軟體（FOSS）來說較低：購買/升級時無需支付授權費用、服務供應商具有開放市場選擇、可自行部分或完全提供解決方案。

### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- ☐ 新的徵求提案（RFP）中，主動要求開放原始碼的提交。
- ☐ 採購部門具備評估開放原始碼與專有解決方案的方式。
- ☐ 已實施並記錄簡化的開放原始碼軟體及服務採購流程。
- ☐ 已定義並記錄一套跨部門專業支援的核准流程。

### 建議

- 「在建立流程時，務必充分運用 IT、DevOps、資安、風險管理和採購團隊的專業知識。」（摘錄自 5 Open Source Procurement Best Practices）。
- 競爭法可能要求不得特別提及「開放原始碼」。
- 先選擇技術，再進行 RFP，以客製化和支援服務為主。

### 資源

- 開放原始碼軟體採購的決策因素：這份由英國 OSS-watch 提供的文件雖然不新，但仍是值得閱讀的優秀資源。可參考投影片。
- 5 Open Source Procurement Best Practices：這是一篇關於開放原始碼採購的最新文章，提供實用建議。

### 建議的下一步行動

- GGI-A-33 - 與開放原始碼供應商合作：制定採購政策有助於識別需關注的開放原始碼供應商與社群，並與其建立合作關係。

# 9 策略目標行動清單

## 9.1 建立企業開源治理策略

行動編號：GGI-A-16。

### 描述

在公司內部定義開放原始碼治理的高階策略，能確保內部使用與外部貢獻及參與的作法具一致性與可見性。這能提供清晰且具體的願景與領導力，使公司的溝通更加有效。

轉向開放原始碼帶來許多好處，同時也伴隨著責任與公司文化的轉變。這可能會影響商業模式，並改變組織展現價值與提供服務的方式，以及其對客戶與競爭者的定位。

本行動包括以下任務：

- 設立開放原始碼負責人，並獲得（高層）管理階層的贊助與支持。
- 制定並發布清晰的開放原始碼路線圖，明確列出目標與預期效益。
- 確保所有高階管理層知悉並依循該策略行事。
- 在公司內部推廣開放原始碼：鼓勵人們使用，培養內部相關知識及倡議。
- 在公司外部推廣開放原始碼：透過官方聲明、溝通及參與公開的開源活動。

明確定義、發布並執行一致的策略，有助於獲得公司內部所有人的認同，並促進各團隊推動後續的倡議。

### 機會評估

如果出現以下情況，現在是推動此行動的好時機：

- 管理層缺乏協調的努力，開放原始碼仍被視為臨時性的解決方案。
- 公司內部已有零星的開放原始碼倡議，但未能影響高階管理層。
- 開放原始碼倡議已啟動一段時間，但面臨諸多障礙，且尚未達到預期成效。

### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- □ 公司有明確的開放原始碼治理章程。該章程應包含：
  - 要達成什麼目標、
  - 對象是誰、
  - 策略負責人的權限範圍及限制。
- □ 開放原始碼路線圖已在公司內部廣泛公開並獲得認可。

### 建議

- 建立一組人員及流程來定義並監控公司內的開放原始碼治理。確保高層管理階層對開放原始碼倡議有明確的承諾。
- 在公司內部溝通開放原始碼策略，使其成為一個重要議題，並成為真正的企業承諾。
- 確保從開發團隊到管理層與基礎設施人員，每個人都充分理解路線圖與策略。
- 溝通進展情況，讓人們了解組織在承諾方面所處的狀態，並發布定期更新與相關指標。

### 資源

- 開放治理的清單與參考資料。
- Cédric Thomas（OW2 執行長）於 2020 年 1 月 28 日在巴黎 Orange Labs 舉辦的研討會：《開放原始碼作為數位主權的關鍵議題》（僅提供法文）。
- Linux 基金會所提供的一系列企業開放原始碼管理指南。
- LF Energy 組織發布的開放原始碼策略文件範例

### 建議的下一步行動

- GGI-A-35 - 開放原始碼與數位主權 制定適當的企業開放原始碼治理策略，有助於改善數位主權。現在是根據組織的背景來定義這些策略的最佳時機。
- GGI-A-34 - 高層管理意識 要成功推動企業的開放原始碼策略，必須獲得高層管理階層的參與與支持。教育並吸引他們投入，是實現此目標的重要下一步。

## 9.2 高階主管層級意識

行動編號：GGI-A-34。

### 描述

組織的開放原始碼倡議先從最高層級推行，將開源的核心 DNA 融入公司策略與內部運作時，才能真正發揮其策略性效益。若高層管理者未參與其中，則無法實現各種承諾事項。培訓與開放原始碼的思維模式也必須擴展到那些負責制定政策、決策和整體策略的人，無論是在公司內部還是外部。

此承諾確保實際改進、思維轉變和新倡議能獲得來自高層的一致、友善且可持續的支持，進而促使員工更加積極參與。這同時塑造了外部人士對組織的看法，為組織帶來聲譽與生態系統的相關利益。這也是在中長期內鞏固倡議及其效益的一種方式。

### 機會評估

此行動在以下情境下尤為重要：

- 當組織已設定與開放原始碼管理相關的全球目標，但在實現方面遇到困難。如果缺乏高階管理層的充分了解和明確承諾，該倡議幾乎不可能取得任何成效。
- 當倡議已經啟動並取得進展，但高階管理層未能適當跟進。

開放原始碼的使用應有一貫且周全的策略，而非臨時應對，因為它可能帶來團隊範圍內的影響及文化上的變革。

### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- ☐ 有授權的治理辦公室/專員，負責制定統一的跨部門的開放原始碼策略，並確保其範疇明確。
- ☐ 管理階層對開放原始碼策略有明確且具有約束力的承諾。
- ☐ 管理階層在倡議中保持透明溝通。
- ☐ 管理階層願意參與討論開放原始碼軟體，可以就其承諾進行徵詢與質疑。
- ☐ 為倡議提供適當的預算與資金。

### 建議

與此項行動相關的具體操作案例包含：

- 對高階主管進行開放原始碼培訓，消除其對開源的迷思。
- 獲取高層對開放原始碼使用與策略的明確實質支持。
- 在內部溝通中明確提及並支持開放原始碼計畫。
- 在與公中溝通中明確提及並支持開放原始碼計畫。

開放原始碼是一種**策略驅動器**，能夠融入**企業文化**。這意味著什麼？

- 開放原始碼可以作為打破供應商壟斷並降低軟體採購成本的機制。
  - 開放原始碼是否應該由**軟體資產管理者**或**採購部門**來負責？
- 開放原始碼授權條款賦予了開放原始碼帶來效益的自由，但同時也附帶**義務**。如果未妥善履行，這些義務可能會給組織帶來法律、商業以及形象方面的風險。
  - 授權條款是否會讓本應保密的資源變得透明？
  - 這是否會影響我組織的專利組合？
  - 應如何對專案團隊進行相關培訓並提供支持？
- 回饋外部開放原始碼專案是開放原始碼最大的價值所在。
  - 我的公司應如何鼓勵（並追蹤）這一過程？
  - 開發者應如何使用 GitHub、GitLab、Slack、Discord、Telegram 或其他開放原始碼專案常用的工具？
  - 開放原始碼是否會影響公司的 HR 政策？
- 當然，開放原始碼不僅僅是回饋，那我的自有開放原始碼專案該如何處理？
  - 我是否準備好進行**開放式**創新？
  - 我的專案將如何管理**外部的**貢獻？
  - 我是否應該投入精力為某個專案培育一個社群？
  - 我應如何領導這個社群，社群成員應該扮演什麼角色？
  - 我是否準備好將路線圖的決策權交給社群？

- 開放原始碼是否可以成為減少公司團隊間孤島現象的有價值工具？
- 我是否需要處理開放原始碼在公司不同實體間的轉移？

**建議的下一步行動**

- GGI-A-31 - 公開聲明使用開放原始碼 高層主管是組織的突出代表，讓他們參與並傳遞組織對開放原始碼的參與與承諾。

## 9.3 開源與數位主權

行動編號：GGI-A-35。

**描述**

數位主權可定義為

> 「個人與機構在數位世界中獨立、刻意且安全地執行其角色的能力與機會。」— 德國公共 IT 能力中心

為了妥善開展業務，任何組織都必須依賴其他合作夥伴、服務、產品與工具。檢視這些相依關係與限制，有助於組織評估並控制其對外部因素的依賴，從而提升自主性與韌性。

舉例來說，供應商綁定是造成依賴的重要因素，這可能妨礙組織的運作流程及附加價值，因此應該避免。開放原始碼是擺脫此綁定的一種方法。開放原始碼在數位主權中扮演著重要角色，提供更大的解決方案選擇、供應商及整合商的彈性，並加強對 IT 路線圖的控制。

需要注意的是，數位主權並非信任問題：我們當然需要信任合作夥伴與供應商，但當這種關係建立在雙方自願與相互認可的基礎上，而非強制契約與限制時，關係會更加穩固。

提升數位主權的優勢包括：

- 提高組織在不受限制下作出自主選擇的能力。
- 提升組織面對外部行為者與因素的韌性。
- 在與合作夥伴與服務供應商談判時，改善議價地位。

**機會評估**

- 離開某個解決方案有多困難或昂貴？
- 解決方案供應商是否可能強加不受歡迎的服務條件（例如，變更授權、更新合約）？
- 解決方案供應商是否可能因我們別無選擇而單方面提高價格？

**進度評估**

以下**檢驗要點**顯示了此行動的進度：

☐ 已評估組織的供應商及合作夥伴的關鍵相依性。
☐ 針對這些識別出的相依性制定備援計畫。
☐ 在評估新解決方案時，列出數位主權的要求。

**建議**

- 識別來自服務供應商與第三方實體的關鍵相依風險。
- 維護開放原始碼替代關鍵服務的清單。
- 在選擇新工具與服務時，增加數位主權的需求作為考量因素。

**資源**

- A Primer on Digital Sovereignty & Open Source: part I 以及 A Primer on Digital Sovereignty & Open Source: part II，來自 Open-Sourcerers 網站。
- 一篇發表於 superuser.openstack.org 的精彩文章，開放原始碼在數位主權中的角色。以下為文章中的一段摘錄：

> 數位主權是 21 世紀的重要議題，尤其是在歐洲。開放原始碼在實現數位主權方面具有重大作用，不僅讓每個人都能取得必要的技術，也透過治理透明度與互通性，確保這些解決方案的成功。

- 歐盟對數位主權的觀點，來自 Open Source Observatory (OSOR)：開放原始碼、數位主權與互通性：《柏林宣言》(Open Source, digital sovereignty and interoperability: The Berlin Declaration)。
- UNICEF 對 數位主權的開放原始碼立場。

## 9.4 開源促進創新

行動編號：GGI-A-36。

### 描述

> 「創新是將想法付諸實踐，進而引入新產品或服務，或改進產品或服務提供方式的過程。」
>
> — Schumpeter, Joseph A.

開源透過多樣性、協作及順暢的想法交流，能成為創新的關鍵因素。來自不同背景和領域的人可能帶來多元的觀點，並為已知問題提供嶄新、改進，甚至顛覆性的解決方案。透過傾聽不同的意見，並積極推動專案與議題的開放式協作，可以有效促進創新。

同樣地，參與開放標準的制定與應用，是推動良好實務與改進公司日常工作的有效方式。這也讓企業能引導並影響創新朝其需求的方向發展，同時提升全球能見度與聲譽。

透過創新，開源不僅能轉型公司銷售的產品或服務，還能創建或調整整個公司所期待蓬勃發展的生態系統。

例如，透過將 Android 以開源形式釋出，Google 邀請了數十萬家公司基於此開源技術構建自己的服務。Google 也因此創造了一個所有參與者都能受益的完整生態系統。當然，只有少數公司擁有足夠的實力，能憑自身決策打造生態系統，但也有許多公司透過結盟，共同創建此類生態系統的例子。

### 機會評估

評估公司與競爭對手、合作夥伴及客戶之間的位置非常重要，因為若客戶、合作夥伴及競爭者使用的標準與技術脫勾過遠，往往會帶來風險。創新顯然意味著與眾不同，但這種差異不宜過於廣泛；否則，公司將無法受益於生態系統中其他公司帶來的軟體開發成果，以及生態系統提供的商業動能。

### 進度評估

以下**檢驗要點**顯示了此行動的進度：

- ☐ 已經識別出對業務產生影響的技術及開發這些技術的開源社群。
- ☐ 已經持續追蹤這些開源社群的進展與發佈內容——甚至在正式公開之前，我已了解他們的策略。
- ☐ 組織的員工是這些開源社群（或其中一些）的成員，透過貢獻程式碼和參與社群治理機構，影響其路線圖和技術選擇。

### 建議

在所有營運業務所需的技術中，您應該識別出：

- 與競爭對手可能相同的技術，
- 應該專屬於您公司的技術。

開源在過去十年中一直是創新推動的核心力量，許多日常強大的工具皆源自於開源（例如 Docker、Kubernetes、Apache 大數據計畫或 Linux）。不需要對所有技術都了如指掌，但應該對前沿技術有足夠的了解，從而識別出有趣的新趨勢。

允許並鼓勵人們提交創新想法，並推動這些想法向前發展。如果可能，投入資源支持這些計劃並促使其成長。依靠人們的熱情與意志，來創造並培育新興的想法與趨勢。

**資源**

- 4 項歸功於開源的創新。
- 開放原始碼的創新, 來自 Dirk Riehle 教授。
- 開源技術，促進創新。
- 開源創新能在企業中奏效嗎？。
- 歐洲：開源軟體策略。
- 2020-2023 年開源軟體策略。

## 9.5 開源促進數位轉型

行動編號：GGI-A-37。

**描述**

> 「數位轉型是指採用數位技術來改變服務或業務，透過用數位化流程取代非數位或手動流程，或以新型數位技術取代舊有數位技術。」（維基百科）

當先行數位轉型的組織透過業務、IT 和財務共同推動改革之時，他們會重新考量以下三大切點：

- 商業模型 (Business model)：價值鏈與生態系統、即服務化（As a Service）、軟體即服務（SaaS）。
- 財務模型 (Finance)**：營運支出與資本支出（Opex/Capex）、人力資源、外包資源。
- 資訊技術 (IT)：創新、舊系統/資產現代化。

開放原始碼是數位轉型的核心，涵蓋以下三個層面：

- 技術 (Technologies)：開放原始碼、敏捷實踐、產品管理。
- 人員 (People)：協作、開放式溝通、開發與決策週期。
- 業務模型 (Business models)：試用與購買（Try & Buy）、開放創新。

在競爭力方面，最顯而易見的流程大概是那些直接影響客戶體驗的流程。我們必須承認，無論是大型企業還是新創公司，透過提供全然前所未有的客戶體驗，已大幅改變了客戶的期望。

客戶體驗以及公司內的所有其他流程都完全依賴於資訊技術（IT）。每家公司都必須轉型其 IT 系統，這正是數位轉型的核心所在。尚未完成數位轉型的公司，現在必須儘快實現，否則面臨被市場淘汰的風險。數位轉型已成為企業生存的必要條件。

數位轉型的預期效益包含：

- 簡化與自動化核心流程，並實現即時處理。
- 利用人工智慧與大數據帶來的機會。
- 利用人工智慧與大數據帶來的益處。

**機會評估**

數位轉型可透過下述方式管理：

- IT 的各階段分工 (Segments of the IT)：生產研發 IT、業務支持 IT（如 CRM、帳單、採購）、支援 IT（如人力資源、財務、會計）、大數據分析。
- 支持性技術或流程 IT 類型 (Type of technology or process supporting the IT)：基礎架構（雲端）、人工智慧、流程管理（自製或購買、DevSecOps、SaaS）。

將開放原始碼引入 IT 的特定領域或技術，表明您希望親自參與該領域或技術，因為您已評估該 IT 領域或技術對公司競爭力的重要性。不僅要與競爭對手相比，還應與其他行業及關鍵參與者在客戶體驗和市場解決方案方面進行比較，評估公司所在的定位是至關重要的。

**進度評估**

□ 第一層級：情境評估 (Level 1: Situation assessment)

我已經識別出：

- 已識別對企業競爭力至關重要的 IT 工作階段，並且
- 確定需要用於開發這些分段應用的開放原始碼技術。因此我決定：
- 那些開發階段是我需要管理的內部開發團隊的專案，並且

- 那些開放原始碼技術，我需要內部的團隊專家。

□ 第二層級：參與 (Level 2: Engagement)

針對公司內使用的部分選定開放原始碼技術，多位開發者已接受培訓，並獲得開放原始碼社群的認可，成為有價值的貢獻者。在部分選定的領域，基於開放原始碼技術的專案已經啟動。

□ 第三層級：普及化 (Level 3: Generalisation)

在所有專案的初期階段，系統性地調查開放原始碼替代方案。爲了方便專案團隊研究這些替代方案，IT 部門設有專屬預算及核心架構師團隊，專門協助各專案進行相關研究。

**關鍵績效指標 (KPIs)**：

- KPI 1. 調查開放原始碼替代方案的比率：（已調查專案數量 / 專案總數）。
- KPI 2. 選擇開放原始碼替代方案的比率：（選擇專案數量 / 專案總數）。

**建議**

數位轉型不僅是一個口號，更是一種思維模式，需要從組織的高層進行根本性變革。管理層應推動倡議與新想法、管理風險，並可能更新現有程序以適應新概念。

熱情是成功的重要因素之一。該領域的主要參與者之一種方法是建立開放的創意空間，讓人們可以提交並自由探索他們關於數位轉型的想法。管理層應鼓勵這類行爲發生。

**資源**

- Eclipse 基金會：歐洲數位轉型與全球開放原始碼合作白皮書 (Eclipse Foundation: Enabling Digital Transformation in Europe Through Global Open Source Collaboration)。
- 歐洲：開源軟體策略。
- 2020-2023 年開源軟體策略。

# 10 結論

正如我們之前所說，開放原始碼的良善治理不是一個終點；它是一段旅程。我們需要關心我們的公共資產，關心那些讓它繁榮的社群和生態系統，因為我們自己的共同成功，進而也是個人的成功，取決於此。

**我們**，作為軟體開發者和開放原始碼愛好者，致力於不斷改進良善治理倡議手冊，並推動其宣傳與擴展。我們深信，組織、個人和社群需要攜手合作，共同建設一個更好、更大的共享資源，讓所有人都能受益。

**您**，歡迎加入 OSPO 聯盟，貢獻我們的工作，傳播這個理念，並成為您自己生態系統中更好開放原始碼意識和治理的推廣大使。外面有大量的資源可供使用，從部落格文章和研究論文到會議和線上培訓課程。我們也在 我們的網站 提供了一些有用的資料，並且我們樂於盡力提供幫助。

**讓我們一起定義並建設良善治理倡議的未來！**

## 10.1 聯絡我們

與 OSPO 聯盟聯繫的首選方式是發送訊息到我們的公共郵件列表，網址為 https://accounts.eclipse.org/mailing-list/ospo.zone。您也可以參加我們通常的開放原始碼活動、加入我們的每月 OSPO OnRamp 網路研討會，或與任何成員聯繫——他們會親切地將您引導至合適的人員。

## 10.2 附錄：自訂行動計分卡範本

最新版本的自訂行動計分卡範本可在 OW2 的 良善治理倡議 GitLab 的 `resources` 區域找到。

| **目標/行動** 文化 1 | **推廣開放原始碼開發最佳實踐案例** | **最後更新** 2025-03-08 |
|---|---|---|

**自訂描述** *必須完成範圍*

簡要核心描述...

- 簡要重點...
-

**機會評估** *為什麼這行動有相關*

- 關鍵痛點...
- 關鍵進展機會...

**目標** *我們在此階段目標達成的成果*

- 目標 1...
- 目標 2...

**工具** *技術， 行動中使用的工具和產品*

- 資源...

**操作備註** *途徑，行動進展的方法*

- 開始於...
-

| **關鍵成果** *我們將如何衡量此階段的成功指標* | **進度** | **分數** | **個人評估** |
|---|---|---|---|
| 1. 關鍵成果 1（至少需有一項關鍵成果） | **xx%** | **.9** | 個人評論 |
| 2. 關鍵成果 2 | **xx%** | **.5** | 個人評論 |
| 3. 關鍵成果 3 | **xx%** | **.5** | 個人評論 |
| 4. 關鍵成果 4（至少需有四項關鍵成果） | **xx%** | **.0** | 個人評論 |
| | | **.475** | |

**時間表** *開始-結束日期、里程碑*

- 日期標示於此

**努力** *時間與材料預算*

- *未來三個月的時間分配*
- *預算補助*

**指派人員** *誰參與? 誰負責領導?*

- XX 準備內部簡報

**問題** *困難、不確定性、阻礙、需注意的重點、相依關係*

- 關注 1...
- 關注 2...

**狀態** *行動進行為何*

對行動狀況的個人評論

| **整體進展評估** | **XX%** |
|---|---|

**備註**

| **來自 GitLab 活動論壇的洞察** |
|---|
| https://gitlab.ow2.org/ggi/ggi/-/blob/main/handbook/content/52_activity_44.md<br>Copy/paste here the content of the Activity description from https://gitlab.ow2.org/ggi/ggi/<br>This will serve as a reference to help develop the Customized Activity Scorecard |