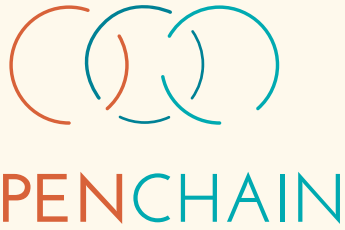


開源軟體授權條款合規的一般公眾指南

目錄

介紹

開源軟體(OSS)已經成為現代軟體開發的基礎。OSS幾乎被應用到所有電子產品中，包括超級電腦、雲端服務、個人電腦、家電產品、汽車、工業設備和物聯網設備。即使在激烈的競爭中，企業也需要開發出高品質、並能更快及時投入市場的產品或服務。企業還必須跟上最新的技術趨勢。OSS在這一激烈角逐中是不可或缺的。

許多OSS是通過來自世界各地不同組織的專業開發者協作開發而成的。OSS通常是各領域高階創新的驅動源。參與開源開發的軟體工程師有機會提高他們的技能，並直接體驗這種創新。

任何遵守相關授權條款條件的人都可以自由地使用、修改和散布OSS。在散布OSS時，散布者被要求在散布時遵守授權條款的條款與條件。在某些案例中，散布者曾因未能履行其法律義務而被起訴並敗訴。因此，為了減少使用OSS所帶來的風險，所有相關人員都必須理解OSS的基本原理。

這本小冊子是由Linux基金會的OpenChain專案所編寫，旨在讓盡可能多的人了解關於OSS的基本原理。

May 2019

學習開源軟體

讓我們學習一下開源軟體(OSS)的基礎知識。

本小冊子解釋以下內容：

1. 什麼是開源軟件？
2. 您需要做什麼來獲得OSS的益處
3. 不能履行OSS職責可能產生的風險

不幸的是，曾發生過這樣的案例：一家公司未能履行其OSS授權條款職責，結果被著作權人起訴。

4. 供應鏈問題
5. 您需要做什麼來確保每個人都能從OSS中受益

第3點和第4點可能是相互關聯的。如果OSS是通過供應鏈獲得的，那麼供應鏈中的所有環結都必須符合授權條款的條件。如果任何一個環結未能滿足授權條款的條件，那麼供應鏈後段的組織將無法彌補這些缺失的條件。獨自作業的受雇者或公司無法履行所有的職責，也無法滿足所有的要求。

當帶有OSS軟體的專案被交付給另一方時，必須提供與OSS相關的所有資訊。以下人員應理解在取得及散布OSS時應遵循的正確程序：

- **開發人員和工程師：** 除了軟體開發人員外，硬體工程師也深入參與為其硬體，開發設備驅動程式軟體、開發板支援套裝軟體(BSP)和軟體開發套件(SDKs)。
- **採購人員：** OSS可能包含在供應鏈的交付物中，例如軟體、硬體模組、SoCs、半導體產品，以及由ODM/OEM製造商設計和開發的產品。
- **銷售人員：** 銷售人員應了解客戶需要OSS相關資訊的原因，包括著作權和授權條款資訊。
- **品質保證人員：** 包含在產品中的OSS可能會影響其品質或引入程式錯誤。品質保證人員需要了解這些問題。
- **法律/智慧財產權人員：** 法律和智慧財產權人員需要了解與OSS授權條款解釋和遵守相關的法律、法律判例和法律補救措施。
- **管理人員和經理：** 管理人員和經理開發策略，圍繞於使用、貢獻和散布開源；構建團隊以促進OSS的使用；監督OSS流程，以及對所需軟體工具進行投資。

* ODM: Original Design Manufacturer（原始設計製造商）
OEM: Original Equipment Manufacturer（原始設備製造商）

OSS的定義

準確地回答“什麼是OSS?”並不容易。不同的人有不同的答案。然而，大多數人會同意以下觀點：

> OSS是提供源碼的軟體。著作權人允許其他人使用、查驗、修改和共享軟體。

OSS的範例

Linux可能是最廣為人知的開源軟體範例。作業系統(OS)是為其他軟體提供平台而設計的軟體。Linux就是這樣一個作業系統。Linux用途廣泛。它幾乎被應用到每個主要的電腦系統中，包括超級電腦、股票交易所伺服器、網路伺服器、使用Android軟體疊層的智慧型手機、家電產品、汽車和工業設備。Linux支持世界上極大比例的核心技術基礎設施。

Linux是通過世界各地成千上萬的開發人員的協作開發出來的。Linux開發每天都在積極地進行著。任何人都可以自由使用、修改和散布Linux，只要遵守Linux開發者選擇授權條款的條件。使用Linux的公司理解並遵守Linux的授權條款是非常重要的。

除了Linux之外，還有大量其他的OSS專案。其中包括用於HTTP伺服器的Apache專案、廣泛使用的編譯器GNU Compiler Collection (GCC)和Eclipse整合式開發環境，等等。

OSS和授權條款

OSS的著作權人並沒有放棄程式碼中的著作權，而是基於使用者對軟體授權條款的遵守，授予使用者對軟體的某些權利。在某些情況下，著作權人可能授予使用者專利授權。對於開源軟體的使用者來說，理解他們所使用的每一個OSS的授權條款是至關重要的。

幾乎所有的OSS授權條款都免除OSS開發者的責任。在幾乎所有的情況下，OSS開發者都不承擔使用OSS的責任；而是要求使用者、產品整合商，和供應商自己承擔此一責任。

並非所有軟體都受著作權保護。如果您需要判斷某一特定片段的OSS是否為受著作權保護的素材，您應該向律師或智慧財產權專家諮詢。

透過授權條款(著作權)授予什麼

對於某些OSS授權條款，著作權人授予其他人使用或散布軟體的權利。本授權授予發生在著作權人和使用者之間沒有直接溝通的情形，但只有當使用者遵守著作權人在授權條款中提供的條件時才授予該使用權。當使用者不能遵守這些授權條件時，就會產生嚴重的問題。

透過授權條款(專利)授予什麼

對於某些OSS授權條款，OSS的著作權人授予其他人自由使用其透過軟體實踐並由著作權人擁有的專利的權利。並不是每個OSS授權條款都授予這樣的專利授權。包含此類專利授權的授權條款的範例包括Apache授權條款和GNU通用公眾授權條款(GPL) 第3版。

典型的OSS授權條款

開放源碼促進會(OSI)是一個推廣OSS的組織。它定義了構成OSS的標準，並核可數十個不同的授權條款為有效的OSS授權條款。

https://opensource.org/licenses
https://opensource.org/osd

大多數OSS都是採用OSI核可的授權條款提供授權的。除此之外，一些採非OSI核可授權條款授權的軟體也仍可能被視為開源軟體。此類軟體是否應被視為OSS(或以其他模式看待)，應就軟體供應者和接收者之間的協議來決定。

您需要做什麼來獲得OSS的益處

當您使用OSS時，最重要需要了解的事項是與軟體散布相關的義務。

幾乎所有的OSS授權條款都定義了以下內容：

- OSS開發者對使用該軟體的影響不承擔責任
- 當軟體被個人或法人(散布者)散布時，有些義務必須被履行。

在以下章節中，散布者可以指個人，也可以指公司等法人。

任何遵守本授權條款條件的人都可以自由使用和散布本軟體。

然而，不同的授權條款有不同的條件。有些授權條款只要求在源碼散布中包含授權條款聲明和著作權聲明。其他授權條款要求揭露源碼並提供獲取源碼的書面文件。有些授權條款的條文會影響第一個軟體能與哪些其他OSS結合使用。散布者必須遵守授權條款中定義的所有義務。

有幾種模式視為散布軟體。一種模式是銷售包含OSS軟體的產品。另一種模式是提供一個可以下載軟體的網站。當包含OSS的專案被散布時，散布該專案的實體必須遵守該OSS的授權條款。

OSS散布範例

有幾種不同的模式可以散布OSS。在每種狀況下，散布者都必須遵守OSS授權條款。

1. **散布OSS的一種模式是使用半導體供應商提供的SDK(軟體開發套件)開發產品。**

   如果SDK中包含的OSS在開發過程中被併入到產品中，那麼這意味著半導體供應商通過包含到SDK來散布OSS，而產品開發人員則通過包含到產品來散布OSS。這種情況下，產品供應商有責任遵守授權條款。但它們依賴於半導體供應商。如果半導體供應商沒有提供有關包含到SDK中OSS的適當資訊，則產品供應商無法遵守OSS授權條款。

2. **OSS可以被散布的另一種模式是採用ODM或OEM的委託方式為製造商設計和開發產品。ODM或OEM可能將OSS併入到產品中，這是產品經銷商需要了解的。**

   即使是OEM或ODM製造了該產品，該產品的品牌所有者也會散布併入在該產品中的OSS。品牌所有者必須遵守OSS授權條款。如果ODM或OEM製造商沒有提供有關OSS的適當資訊，則產品的品牌所有者無法遵守OSS授權條款。

3. **散布OSS的其他模式包括販售產品、釋出行動應用軟體，或者為之前販售的設備提供軟體更新。**

   如果OSS被包含在產品、行動應用程式或軟體更新中，這就構成了OSS的散布。販售產品或散布軟體的實體必須遵守OSS授權條款。

4. **網頁中使用的JavaScript構成散布：**

   當網頁被傳輸到使用者的機器上時，可能會發生一種有趣的OSS散布情況。

   當使用者訪問頁面時，被包含到網頁中的JavaScript作為頁面資料的一部分，被從網站伺服器傳輸到使用者機器上的瀏覽器。如果此JavaScript程式是OSS，那麼這就構成了散布，授權條款將會發生效力。

當OSS被散布時需要履行的義務。

當OSS被散布時需要履行的義務因授權條款而不同。在一個被散布的產品或程式中辨識所有的OSS和相關的授權條款是很重要的。

這需要清楚地理解所有必須被滿足的不同授權條款。

寬鬆授權條款

MIT授權條款、BSD授權條款和Apache授權條款要求的義務很少。這些授權條款要求散布軟體的著作權聲明和授權條款文本。聲明應該清楚地顯示在收受OSS的人能夠閱讀的地方。

互惠授權條款

GPL授權條款、LGPL授權條款、AGPL授權條款和Mozilla公眾授權條款要求揭露相關軟體的源碼。(源碼中的授權條款和著作權不得刪除。)如果散布者修改了源碼，那麼所有源碼的修改也必須被揭露。互惠授權條款旨在建立一個環境，在這個環境中，人們可以在軟體的所有使用者和開發者之間共享修改與改進。

除了揭露源碼之外，這些授權條款通常還要求履行其他義務。要在互惠授權條款下散布軟體，您必須理解這些義務。如有需要，您應該諮詢您的法律及智慧財產權工作人員。

您不能授予的專利

在某些情況下，OSS授權條款可能要求散布者為其使用者授予包含在其使用的或添加到OSS軟體中的專利授權。如果您有這樣一個不能授予使用者授權的專　利，您就不能散布包含此種授權條款的OSS。

因未能遵守而引起的風險

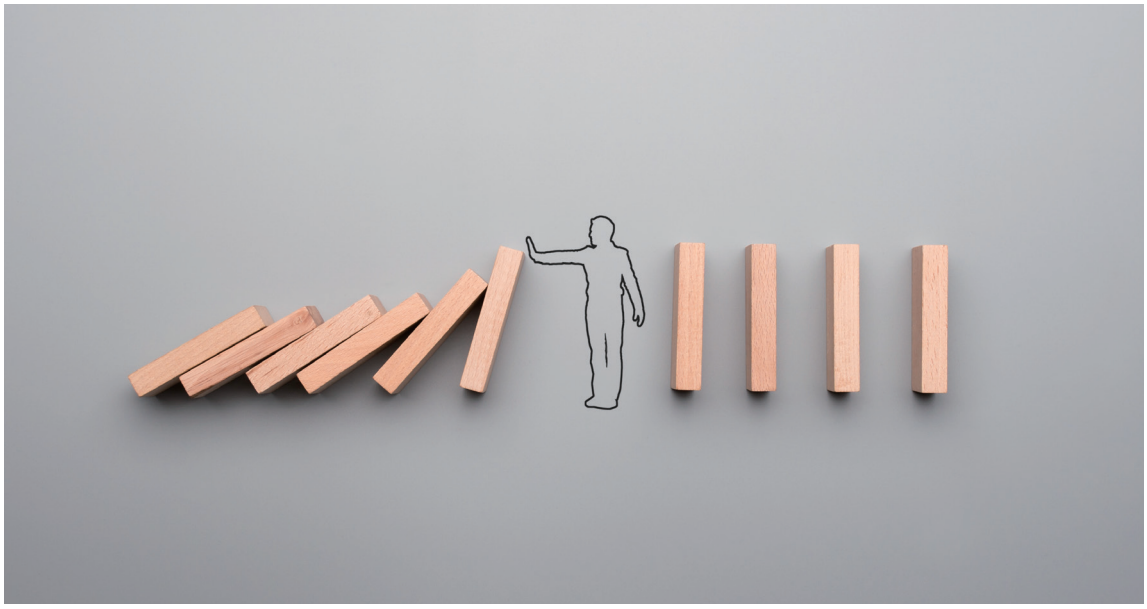
OSS著作權人對未能遵守授權條款的公司提起訴訟。

不幸的是，由於未能遵守OSS授權條款，導致OSS著作權人對使用者(和散布者)提起訴訟是曾經發生的。在至少一宗案件裡，曾有判決要求被告暫停販售包含有OSS的產品。

2009年12月，發生了一起名為“Busybox”的開源軟體有關的訴訟。Busybox程式被廣泛地併入到嵌入式系統中，並根據GPL第2版授權條款進行授權。在這起案件裡，有14家公司成為訴訟對象，其中包括一些消費電子業的公司。這宗案件值得注意之處在於，公司因ODM製造商生產的產品而被起訴。

在每宗案例中，都是因散布者未能遵守OSS授權條款而導致訴訟。為避免訴訟，工作上使用OSS的實體應：

- 辨識要散布的軟體中的每一個OSS
- 理解OSS授權條款定義的義務，並遵守這些義務。



訴訟中失去了什麼

當公司被起訴時，對公司最大的損害之一就是其名譽(名譽風險)。未能遵守軟體授權條款的壞名譽可能會導致公司失去其他公司的信任。一個公司越了解其信任關係的重要性，並努力在整個行業建立信任，就越會認真地去避免名譽風險。

回應訴訟需要大量的勞力和費用。在沒有訴訟的情況下，涉及法律、採購、工程和合規的人力資源可以用於更具建設性的任務。這意味著，一家公司花費時間回應訴訟，可能會錯失那些人力資源有可能從事的其他商業機會。特別是，聘請一個勝任的律師進行OSS訴訟是非常昂貴的。

和解或法律判決可能需要支付金錢或罰款。在極端情況下，判決可能導致產品的暫停販售，這有可能造成相當大的損失和昂貴的代價。

與OSS社群建立良好的關係

為了減少訴訟風險，理解OSS原則並遵守OSS授權條款的義務是至關重要的。此外，鄭重地建議您為OSS社群做貢獻，並與您所使用的OSS開發者建立良好的關係。

如果您理解為什麼作者為他們的軟體選擇了特定的開源授權條款，以及支持OSS專案的OSS社群的意志，它將幫助您更進一步，而非僅僅履行OSS授權條款的字面意思。理解開發者的意志是與OSS社群保持良好關係的最重要的益處之一。

與OSS社群保持良好關係可能使公司能夠將自己的新創意納入OSS中。OSS社群可能會根據您的創意和需求來改進軟體。此外，您公司的工程師可能有機會與高技術的OSS開發者合作，這將造就您的工程師更加稱職與更佳技術。

隨著系統軟體在規模和功能上的增加，它變得越來越複雜。編寫出沒有程序錯誤的軟體越來越難。然而，如果一家公司與OSS開發者具有良好的關係，社群可能會幫助您的工程師在開發軟體時發現並解決程序錯誤。

為OSS社群做貢獻

為OSS社群做貢獻的方法有各式各樣：提出程序錯誤修正方案和新功能、翻譯文件、提供社群成員可以交流的場所和論壇、贊助和參與支持OSS的專案和商貿協會（例如Linux基金會）。

供應鏈問題

OSS合規不能由一個人單獨完成。

隨著軟體變得越來越大、越來越複雜，軟體供應鏈也變得越來越大、越來越複雜。現代軟體供應鏈可能包括一個OSS社群、一個軟體供應商、一個提供SDK的半導體供應商和一個終端產品供應商。如果大型、複雜的軟體供應鏈中任何成員不能遵守授權義務或不能提供適當的授權資訊，則將對有義務遵守授權條款的供應商造成重大影響(圖1)。違規可能導致產品被暫停販售。如果供應商在販售前不知道違規，則可能會收到著作權人或第三方提出的關於違規的詢問，而供應商無法對此作出回應。

然而，如果在上游供應鏈中適當地管理軟體合規，這些問題則是可以避免的。為了促進OSS授權條款的遵從，供應鏈中的所有參與者都必須履行自己的職責，在整個供應鏈中建立信任，並就被包含的軟體進行適當的資訊交流。

建議供應鏈中的每個公司都建立一個團隊，以確保供應鏈中的OSS遵從性。Linux基金會的OpenChain專案提供了一個自我認證程序，公司可以使用它來實現此一目的。該自我認證程序將幫助公司檢查其合規的流程。認證測試有多種語言版本可供選擇，任何人都可以自由使用。

https://certification.openchainproject.org/

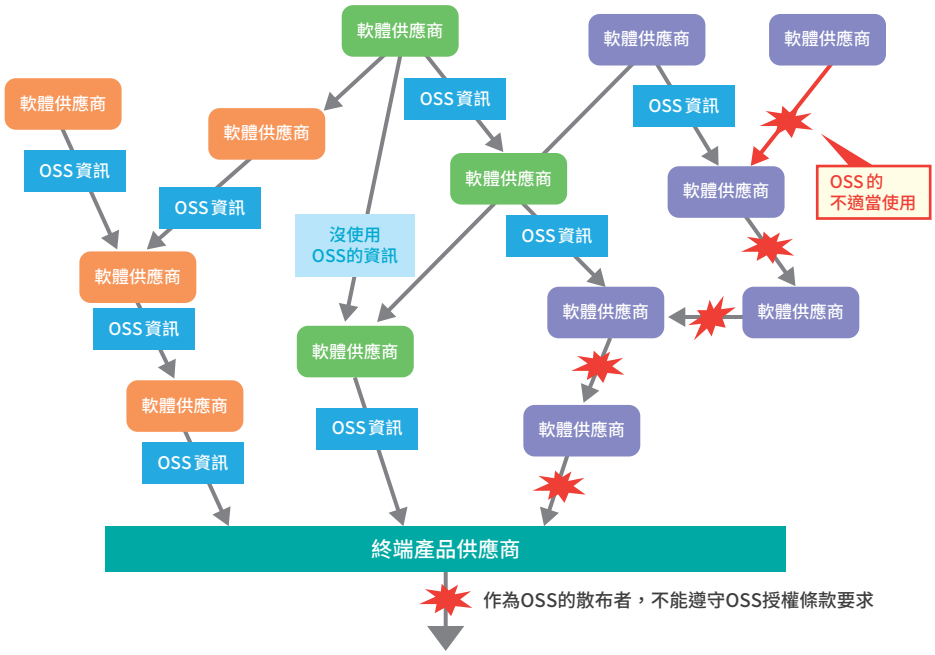


圖1 軟體供應鏈問題

對供應鏈參與者的要求

當供應商散布軟體時，供應商被要求應向每個收受者提供遵守OSS授權條款所需的資訊。收受者應仔細審閱資料和文件，並驗證其準確性。

對於單個產品，軟體散布者可能將多個供應商的軟體包含其中。這種情況下，散布者被要求接收關於其接收到的軟體的每個OSS元件的資訊。

如果沒有收到OSS元件相關的資訊，則不應將此類OSS併入到產品中。

公司中不同的角色對OSS合規承擔不同的責任

軟體開發人員

軟體開發人員應該管理、記錄和儲存軟體的組態。這包括以下內容：

- OSS及其授權條款
- 鏈結(如軟體使用的函式庫、動態或靜態鏈結等等)
- 修改。也就是說，對軟體所做的任何修改的技術細節。

必須標識並列出這些專案。每當軟體的組態發生變動時，都應該更新列表。對於特定的專案，授權條款可能從一個軟體版本到下一個版本時發生變動。建議創建和管理列表，以便每個OSS專案可被輕鬆地索引和審閱。有些授權條款(例如，GPL授權條款)要求散布者揭露源碼。鄭重的建議使用源碼控制管理軟體來追蹤原始源碼和對源碼的任何更改。

軟體採購人員

軟體採購人員必須取得來自外部軟體的任何有關OSS的資訊，以便軟體工程師進行記錄。OSS可能被包含在軟體中，如半導體供應商提供的SDK。

採購人員需要注意公司收受到所有不同類型的交付物中的軟體。

銷售人員

銷售人員需要與客戶就OSS進行溝通。客戶可能有與OSS使用相關的特殊要求。例如，公司可能制定了一個OSS政策來禁止使用帶有特定授權條款的OSS。

對於銷售人員來說，了解客戶對OSS的要求，並將這些資訊傳達給內部軟體開發人員是非常重要的。

法律/智慧財產權人員

與法律和智慧財產權人員的合作對於理解OSS授權條款是不可缺少的。法律和智慧財產權人員應該審閱管理公司使用的OSS之授權條款，並就其使用向開發人員提供建議：

- 使用OSS需要哪些核可？ (一般來說，OSS授權條款免除軟體開發者的責任。)
- 散布OSS需要什麼？
- 當軟體被下游收受者使用時，包含到OSS會不會產生問題？

管理人員和經理人

要有效率且恰當地使用OSS，需要公司內部不同人員的協作。

管理人員和經理人或需要促進內部組織之間的協調，及決定建立一個專職團隊來管理OSS相關的問題。這包括對人力資源、培訓和發展環境的投資。

需要與軟體一起提供的OSS資訊

為了確保每個人都能從OSS中受益，人們需要了解關於OSS的哪些資訊必須與軟體交付物一起提供。

本小冊子解釋了維護OSS列表和遵守OSS授權條款的重要性。

軟體交付物應該提供哪些關於OSS的資訊呢？本節解釋必須與OSS一起散布的特定資訊。由於所需的資訊因業務和公司策略的不同而有所差異，請與每個收受公司進行細節溝通。

當軟體交付物中沒有包含OSS時，您應該清楚地向收受者傳達“交付物沒有包含任何OSS”。然後收受者將可以採取相應作為。

當OSS被包含在軟體交付物中時，您必須清楚地標識出這樣的軟體及其授權條款。例如，授權條款可能在不同版本的OSS之間產生改變。每個OSS元件的名稱和版本是不可或缺的資訊。對於每個元件，提供軟體的下載位置或主要專案來源站或網站是有幫助的。這讓收受者得以驗證有關軟體、其版本和授權條款的資訊。

當OSS授權條款要求散布者揭露源碼時，請提供源碼。具體被要求的源碼取決於OSS授權條款。例如，GPL/LGPL授權條款的第3版要求，除了軟體的源碼之外，您還必須提供基於該源碼修改之二進制碼重新安裝所需的資訊。

必須與OSS一起散布的資訊

以下資訊必須與包含OSS的交付物一起散布。

- OSS元件列表

對於每個OSS元件：

- 辨識軟體的資訊(版本號、源碼來源(例如，網站URL)以及如何獲取軟體)
- 可適用的授權條款列表、以及(如果多於一個)哪一個您的公司正用來散布這個OSS
- 您對軟體所做的任何修改

關於授權條款中要求散布者提供授權條款和著作權聲明的OSS：

- 實際的授權條款文本和著作權聲明

關於授權條款中要求揭露源碼的OSS：

- 所需的源碼(對於GPL，除了源碼外，還必須提供腳本以用於從源碼創建生成可執行程式)

某些情況下，當一個OSS元件本身包含一個次級的OSS元件時，還必須為次級的OSS元件提供資訊。

大致如上述資訊。一個客戶可能需要某些資訊，而另一個客戶則可能需要其他資訊。與客戶就他們需要的資訊及其格式進行溝通是非常重要的。

SPDX專案

託管於Linux基金會的SPDX®(軟體套件資料交換®)專案，具有用於交換授權條款資訊的標準格式。

任何人皆可以使用這種格式，強烈建議在整個供應鏈中使用。有關此格式的資料，請瀏覽：

https://spdx.org/

源碼掃描工具

有掃描工具可以檢測軟體套件裡的OSS並自動產出一些資訊。例如，託管於Linux基金會的 FOSSology專案開發了這樣一個掃描工具。FOSSology工具採OSS授權條款提供，且可被任何人自由使用。也有其他商業授權的掃描工具存在。建議在開發期間和販售之前使用這些工具來驗證軟體套件中的OSS授權條款。

有些掃描工具能夠依據SPDX規範產出報表。這些掃描工具對於產出資訊非常有用，資訊可以直接包含在交付給客戶的交付物中。

關於OpenChain專案

OpenChain專案透過使開源授權條款合規更簡單、更一致，從而建立對開源的信任。OpenChain規範定義了每個優良品質的合規程序都必須滿足的一組核心要件。OpenChain一致性允許組織展示它們對這些要件的依從性。OpenChain課程透過為有效的開源培訓和管理提供廣泛的參考資料，來支持此一流程。其成果是，對於軟體供應鏈的所有參與者來說，開源許可證合規變得更加可預測、可理解和高效率。

https://www.openchainproject.org/

關於Linux基金會

Linux基金會致力於圍繞開源專案建構可永續的生態系統，以加速技術開發和企業應用。

Linux基金會成立於2000年，透過資金和知識資源、基礎設施、服務、活動和培訓，為開源社群提供了無與倫比的支援。透過共同努力，Linux基金會及其專案在創建共享技術方面形成了最具雄心和最成功的投資。

https://www.linuxfoundation.org/