OPENCHAIN

OpenChain 规范书

1.1 版

内容

1) 简介 ..... Error! Bookmark not defined.
2) 定义 3
3) 要件 5
G1：了解你的自由开源软体责任 5
G2：分担责任以达到合规 7
G3：审查及核准自由开源软体内容 8
G4：传递自由开源软体内容文件及档案集 9
G5：理解自由开源软体社群参与 10
G6：依循 OpenChain 要件进行认证 11
附录 I：语言翻译 12

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.

本文为 OpenChain 专案的正式翻译。其由原始英文文本翻译而来。当本翻译与英文版本混淆，英文文本应优先。

1) 简介

OpenChain 促进会始于 2013 年，当时一群软体供应键开源执事人员观察到两个新兴型态：1) 于具有成熟开源合规方案组织间重要程序的相似性；以及 2) 仍然有大量的组织采较低度发展的方案来交换软体。后一观察现象导致伴随软体交换的合规稽证在一致性和质量上缺乏信任。因此，在供应键的每一层，下游组织经常重做上游组织已经执行过的合规工作。

一个研究团队被成立来考量是否可以创建一份标准方案规范书，以：i) 促进产业间共享的开源合规资讯有更佳的质量及一致性；和 ii) 降低与开源合规工程重覆施行有关的高交易成本。该研究团队发展为一个工作团队，并于 2016 年 4 月，正式编组为 Linux Foundation 下的协作专案。

OpenChain 促进会的愿景和任务如下：

- **愿景：** 一个传递自由开源软体 (free/open source software, FOSS) 时附随可靠和一致合规资讯的软体供应键。

- **任务：** 为软体供应键参与者制定可达到 FOSS 有效管理的要件，并使来自软体供应键、开源社群，以及学术界的代表们，能开放且协力地发展本要件及相关附属文件。

依据愿景和任务，本规范书定义了一系列的要件，尽管一个满足所有规范书要件的方案并不能保证完整合规；然当要件被满足时，将大为增加开源合规方案达到充足质量、一致性，及完整性等级的可能性。这些要件呈现一个方案被视为遵循 OpenChain 所必须满足的基础等级（最小）要求。相较于「如何」及「何时」的考量，本规范书聚焦于合规方案「什么」及「为什么」的特性。这确保了实际操作的灵活度，使不同的组织能定制他们的政策及程序以适切符合他们的目标。

第二章介绍贯穿本规范书所使用关键用语的定义。第三章介绍规范书要件，每个要件都有一个或多个审核稽证的列表。为了让给定的要件被视为满足，它们代表必须存在的证据。倘若给定方案的所有要件都达到，该方案将根据 OpenChain 规范书 1.1 版被视为遵循 OpenChain。审核稽证并非被指定公开，然得以在保密协议下或应 OpenChain 组织的私下要求来提供以验证一致性。

2) 定义

FOSS（自由开源软体） - 软体程式依据一个或多个授权条款，该条款符合开放源码促进会(OpenSource.org) 发布之开放源码定义(Open Source Definition) 或自由软体基金会发布之自由软体定义(Free Software Definition) 或类似条款。

FOSS 联系人- 被指派接收外部 FOSS 垂询的指定人员。

确认条款 - 依循适当方法而确认的一组 FOSS 授权条款。

遵循 OpenChain - 满足本规范书所有要件的方案

软体工作人员 - 任何对提供软体进行范围界定、贡献，或负责准备的雇员或承包商。依据组织，可能包括（但不限于）软体开发人员，发布工程师，品管工程师，产品行销以及产品管理。

SPDX 或软体套件资料交换 - 由 SPDX 工作团队为给定软体套件创建用以交换授权与著作权资讯的标准格式。有关 SPDX 规范的说明，可见 www.spdx.org。

提供软体 - 组织向第三方交付的软体。

审核稽证 - 为了使给定要件被视为满足，所必须存在的证据。

3) 要件

G1：了解你的自由开源软体责任

1.1 **存在一份成文的 FOSS 政策书，用于管理提供软体散布时的 FOSS 授权合规。**该政策必须于内部传达。

审核稽证：

- 1.1.1A 存在一份被列册的 FOSS 政策书。
- 1.1.2A 存在一份被列册的流程，使得所有的软体工作人员知悉 FOSS 政策书的存在。（例如，透过教育训练，内部共笔，或其他实际可行的传达方式。）

理由说明：

确保 FOSS 政策书被创建、纪录，并使软体工作人员知悉其存在的步骤被执行。虽然什么应该要被包括到政策书里在此并未被提出，然其他章节可能会施加要求。

1.2 存在对所有软体工作人员必须性的 FOSS 教育训练，使得：

- **该教育训练，至少包括以下主题：**
  - **FOSS 政策书及至何处取得副本；**
  - **涉及 FOSS 及 FOSS 授权条款的智慧财产法律基础知识；**
  - **FOSS 授权概念（包括宽松式及 copyleft 授权的概念）；**
  - **FOSS 专案授权模式；**
  - **软体工作人员的角色及其与具体 FOSS 合规及一般 FOSS 政策相关的责任；及**
  - **于提供软体里确认，纪录和／或追踪 FOSS 元件的程序。**
- **软体工作人员必须在过去 24 个月内完成 FOSS 教育训练（方被视为当期）。得使用测验方式许可软体工作人员满足此一教育训练的要求。**

审核稽证：

- 1.2.1 存在涵盖上述各主题的 FOSS 教育训练素材（例如，投影片、线上课程，或其他教育训练素材）。
- 1.2.2 追踪所有软体工作人员完成教育训练的方法。
- 1.2.3 根据上述定义，至少 85% 的软体工作人员是当期的。

理由说明：

确保软体工作人员参与了近期的 FOSS 教育训练，且一组核心的 FOSS 相关主题被包含其内。此目的是为了确保核心基础层面的主题得到涵盖，然典型的教育训练方案可能比此处的要求更为全面。

1.3 存在审查确认条款的程序，以确定每个授权条款授与的权利，其义务性要求及限制。

审核稽证：

- 1.3.1 存在一份被列册的流程，使每个管理提供软体之确认条款，其授与的权利，义务性要求及限制得被审查与纪录。

理由说明：

确保在各种使用案例里，用于审查及确认每一个确认条款授权义务性要求的程序存在。

G2：分担责任以达到合规

2.1 确认 FOSS 联系人的职责

- **指派人员负责接收外部的 FOSS 垂询；**
- **FOSS 联系人必须尽其商业上合理的努力以合宜地回应 FOSS 合规垂询；及**
- **公开地确认一个他人能够连络到 FOSS 联系人的途径。**

审核稽证：

- ☐ 2.1.1 FOSS 联系人的职责是公开地确认（例如，透过一个已公布的连络电邮地址，或透过 Linux Foundation 的开源合规联系目录）。
- ☐ 2.1.2 存在一份被内部列册的流程，以分配接收 FOSS 合规垂询的责任。

理由说明：

确定第三方就 FOSS 合规垂询有合理的管道能连络组织，并且此责任已被有效率地分派。

2.2 确认内部 FOSS 合规内部的角色分配

- **指派人员负责管理内部的 FOSS 合规。此一 FOSS 合规角色与 FOSS 联系人可能为同一人员。**
- **FOSS 合规管理活动得到充份资源：**
  - **履行该角色的时间已被分配；及**
  - **商业上合理的预算已被分配。**
- **分派开发及维护 FOSS 合规政策与程序的责任；**
- **与 FOSS 合规有关的法律专家可为 FOSS 合规角色接触咨询（例如，可为内部或外部专家）；及**
- **存在一套解决 FOSS 合规争议的程序。**

审核稽证：

- ☐ 2.2.1 FOSS 合规角色分配的人员姓名，团体或职责在内部被确认。
- ☐ 2.2.2 确认内部或外部法律专家的源头资讯能被 FOSS 合规角色获得。
- ☐ 2.2.3 存在一份被列册的流程，以分派 FOSS 合规的内部责任。
- ☐ 2.2.4 存在一份被列册的流程，以处理不合规案例的审查与补正。

理由说明：

确定相当程度 FOSS 责任分担已被有效率的分派。

G3：审查及核准自由开源软体内容

3.1 存在一个程序用于建立与管理 FOSS 元件素材清单，该清单包含所发布提供软体里每一个元件及其确认条款。

审核稽证：

- 3.1.1 存在一份被列册的流程，以确认，追踪，及将构成所发布提供软体的 FOSS 元件集合资讯建档保存。
- 3.1.2 每个发布的提供软体皆存在 FOSS 元件的纪录，以证明该列册流程被合宜的遵循。

理由说明：

为确定建立与管理 FOSS 元件素材清单，以构成提供软体的程序存在。一份支持系统性审查每一个元件授权条款的素材清单是必要的，以理解当它适用于提供软体的散布时，义务性要求及限制为何。

3.2 FOSS 管理方案必须能够处理软体工作人员提供软体时，一般会碰到的使用案例，可能包括下列使用案例（注意本列表并未详尽，亦可能不适用于所有的使用案例）：

- **以二进位执行档形式散布；**
- **以源码形式散布；**
- **与其他 FOSS 整合而可能触发 copyleft 义务性要求；**
- **内含修改过的 FOSS；**
- **内含 FOSS 或其他软体，是采与提供软体里其他互动元件不相容的授权条款；及／或**
- **内含 FOSS 带有姓名标示的要求。**

审核稽证：

- 3.2.1 为发布提供软体里的 FOSS 元件，一套能处理一般 FOSS 授权使用案例的流程已被实施。

理由说明：

确定该方案能充份坚实地处理组织常见的 FOSS 授权使用案例。存在一个支持这个活动的流程，且该流程被遵循。

G4：传递自由开源软体内容文件及档案集

4.1 **为每个提供软体准备一组代表其 FOSS 管理方案产出的档案集。此被指称的档案集可能包括（但不限于）以下一个或多个：源码，姓名标示声明，著作权声明，授权条款副本，修改注记，提供源码的书面文件 (written offers)，SPDX 文件及其他。**

审核稽证：

- 4.1.1 存在一份被列册的流程，以确定合规档案集有依确认条款的要求，而与提供软体发布时一同被准备及散布。

- 4.1.2 提供软体发布时的合规档案集副本被建档保存并可轻易取回，且此保存档规划至少在提供软体提供期间，或是依照确认条款的要求期间会存在（以较长者为准）。

理由说明：

确定合规档案集的完整集合，有依管理提供软体之确认条款的要求，并与提供软体及其他报告，被作为 FOSS 审查程序的一部份。

G5：理解自由开源软体社群参与

5.1 存在一份成文的政策书，以管理组织对 FOSS 专案的贡献。该政策必须于内部传达。

审核稽证：

- 5.1.1 存在一份被列册的 FOSS 贡献政策书；
- 5.1.2 存在一份被列册的流程，使得所有的软体工作人员知悉 FOSS 贡献政策书的存在。（例如，透过教育训练，内部共笔，或其他实际可行的传达方式。）

理由说明：

确定一个组织对发展政策以公开贡献 FOSS 已作了合理的考量。此 FOSS 贡献政策可作为组织整体 FOSS 政策的一部份，或作为其独立政策。当贡献完全不被允许的情况下，一个明确表达此立场的政策也应该存在。

5.2 若组织允许贡献 FOSS 专案，则实施 5.1 节描述的 FOSS 贡献政策书之程序必须存在。

审核稽证：

- 5.2.1 倘若 FOSS 贡献政策书允许贡献，存在一份被列册的流程以管理 FOSS 贡献。

理由说明：

确定对组织如何公开贡献 FOSS 有列册的程序。若是贡献完全不被允许，该政策书仍可存在。在这种状况下，没有流程存在是可理解的，且虽然如此本要件仍可被视为达到。

G6：依循 OpenChain 要件进行认证

6.1 为了使组织获得 OpenChain 认证，该组织必须证实其 FOSS 管理方案达到 OpenChain 规范书 1.1 版描述的标准。

审核稽证：

- 6.1.1 该组织证实其 FOSS 管理方案存在，且达到本 OpenChain 规范书 1.1 版的所有要件。

理由说明：

要确定一个组织是否如其宣称拥有方案是遵循 OpenChain 的，该方案要达到本规范书的所有要件。仅是达到这些要件的一小部份，该方案将不会被认为足以保证得到 OpenChain 认证。

6.2 从一致性完成认证日开始，对此版本规范书的一致性状态将会维持 18 个月。一致性认证的要件能在 OpenChain 专案网站上找到。

审核稽证：

- 6.2.1 组织证实其 FOSS 管理方案存在，达到本 OpenChain 规范书 1.1 版的所有要件，且在过去 18 个月内完成一致性认证。

理由说明：

若一个组织想长时间宣称方案具一致性，那与当期规范书保持一致是很重要的。如果他们想要持续宣称与此规范书具一致性的话，此一要件得确定方案的支持程序及控制不会逐步丧失。

附录 I：语言翻译

为了便利全球采用，我们欢迎将本规范书翻译成多种语言的努力。由于 OpenChain 采开源专案方式运作，翻译亦由那些愿意贡献他们时间与专业的人士推动，依照 CC 姓名标示 4.0 授权与本专案的翻译政策来进行。本政策的细节及现有翻译能在 OpenChain 专案规范书网页上找到。