OpenChain 规范

版本 2.1

此规范功能上等同于：

- **OpenChain 规范 2.0**
- **ISO/IEC 5230:2020**

OpenChain 2.1 – 开源许可证合规行业标准

了解详情：www.openchainproject.org

目录

简介 iv

1 范围 1

2 术语和定义 1

3 要求 2

3.1 计划基础 2

3.1.1 政策 2

3.1.2 能力 2

3.1.3 认知 3

3.1.4 计划范围 3

3.1.5 许可证义务 3

3.2 定义并支持相关任务 3

3.2.1 联络通道 3

3.2.2 有效的资源支持 4

3.3 开源内容的审核和批准 4

3.3.1 材料清单 4

3.3.2 许可证合规 5

3.4 合规文件的创建和交付 5

3.4.1 合规文件 5

3.5 理解开源社区参与 5

3.5.1 贡献 5

3.6 遵守本规范的要求 6

3.6.1 遵从 6

3.6.2 有效期 6

附录 A （重要） 本规范的翻译 7

附录 B 中英术语对照说明 8

简介

本文为高质量的开源许可证合规计划定义了关键要求。包含开源软件的软件产品会在不同组织间流动，本文旨在为这种流动建立信任。遵从了本规范，就意味着有计划能确保每个软件产品生成必要的合规文件（即法律声明、源码等）。本文的关注点是合规计划“做什么”以及“为什么要做”，而不是“如何做”、“何时做”。因为不同组织有不同的规模、不同的市场，它们需要灵活地选择能匹配自己规模、目标和经营范围的具体政策和流程。例如，OpenChain 遵从计划既可以针对一条产品线，也可以针对整个组织。

本简介为所有潜在读者提供了背景知识。第2 章定义了全文中的关键术语。第3 章 定义了遵从本规范所必须满足的要求。一条要求会包含一份或多份核查材料（即记录），生成这些材料才能满足对应的要求。核查材料不一定要公开，但有些组织可能会选择签订保密协议（NDA）后将其提供给其他方。

本文最早作为公开倡议而撰写，后收到来自两百多位贡献者的反馈。如果想细究本文的历史演变，可以查看本规范的邮件列表及常见问题。

信息技术 — OpenChain 规范

1 范围

本文为高质量的开源许可证合规计划定义了关键要求。包含开源软件的软件产品会在不同组织间流动，本文旨在为这种流动建立信任。

2 术语和定义

本文遵循以下术语定义。

2.1
合规文件
能体现合规计划结果的一系列文件，会伴随软件产品一起交付。

注意：文件可能会包括（但不限于）以下一种或多种：致谢声明、源码、编译和安装脚本、许可证副本、 著作权声明、修改说明、书面要约、开源组件清单和 SPDX 文档。

2.2
已识别许可证
使用适当的方法，识别出构成软件产品的开源组件后，这些组件所遵从的许可证。

2.3
OpenChain 遵从
满足本文所有要求的计划。

2.4
开源
采用开源许可证发布的软件，此类许可证须满足开源促进会（Open Source Initiative）对开源软件的定义（见 opensource.org/osd），或自由软件基金会（Free Software Foundation）对自由软件的定义（见 gnu.org/philosophy/free-sw.html），或其他类似许可证。

2.5
计划
组织内开源许可证合规活动所涉及的政策、流程和人员的集合。

2.6
计划参与者
定义、负责或参与准备所交付软件的任何员工或合作方。

注：在不同组织中，计划参与者可能包括（但不限于）软件开发者、发布工程师、质量工程师、产品营销人员和产品管理人员。

2.7
SPDX
Linux 基金会的 SPDX（Software Package Data Exchange）工作组创建的格式标准，用于交流特定软件包的材料清单，包括相关的许可证和著作权信息（见 spdx.org）。

2.8
交付软件
组织分发给第三方（即其他组织或个人）的软件。

2.9
核查材料
能证明满足特定规范要求的材料。

ISO 和 IEC 在以下网址维护用于标准化的术语数据库：

— ISO 在线浏览平台：位于 https://www.iso.org/obp

— IEC 电子百科：位于 http://www.electropedia.org/

3 要求

3.1 计划基础

3.1.1 政策

必须有一份书面的开源政策来治理交付软件的开源许可证合规。此政策必须在内部进行传达到位。

核查材料：

- 3.1.1.1 一份开源政策文档。
- 3.1.1.2 一份操作文档，能让计划参与者知悉开源政策的存在（如通过培训、内部 wiki 或其他可行的沟通方式）。

理由：

确保有措施来制定、记录开源政策，并让计划参与者知悉其存在。虽然此处没有对政策内容提出要求，但其他章节可能会提出此类要求。

3.1.2 能力

该组织必须

- 识别哪些角色及其职责会影响到计划的作用和有效性；
- 确定计划参与者担任每个角色所必需的能力；
- 根据计划参与者的学历、所受培训和（或）经验来确保他们能胜任；
- 如果可行，采取行动来获得必要的能力；
- 保留适当的文档作为能力的证明。

核查材料：

- 3.1.2.1 一份记录计划中不同参与者及其对应职责的清单。
- 3.1.2.2 一份明确各角色能力的文档。
- 3.1.2.3 每个计划参与者能力评定的书面证明。

理由：

确保计划参与者具备足够的能力来胜任各自的角色和职责。

3.1.3 认知

该组织必须确保计划参与者了解：

- 开源政策；
- 相关开源目标；
- 他们对计划有效性的作用；及
- 未能遵守计划要求的潜在影响。

核查材料：

- 3.1.3.1 计划参与者认知评定的书面证明——应包括计划目标，个人在计划中所起作用，及未能遵从计划的潜在影响。

理由：

确保计划参与者对他们在计划中的角色和职责有足够的认知。

3.1.4 计划范围

不同的计划治理的范围可能有所不同。例如，一个计划可以治理一条产品线、一整个部门或者整个组织。每个计划需要明确指定其范围。

核查材料：

- 3.1.4.1 一份明确定义计划范围和边界的书面声明。

理由：

能灵活构建最适合组织需求范围的计划。有些组织可以选择为某个特定的产品线实施一个计划，但也有些组织可以用同一个计划治理整个组织的交付软件。

3.1.5 许可证义务

必须有流程来审核已识别的许可证，以确定每个许可证授予的义务、限制和权利。

核查材料：

- 3.1.5.1 一份操作文档，用于审核和记录每个已识别许可证授予的义务、限制和权利。

理由：

确保组织在可能遇到的各种应用场景中，有流程来审核和识别每个已识别许可证带来的义务（见§3.3.2 定义）。

3.2 定义并支持相关任务

3.2.1 联络通道

维护一个能有效回应外部开源咨询的流程。公开指定一种方式让第三方能进行开源合规咨询。

核查材料：

- 3.2.1.1 有公开可见的方式能让任何第三方进行开源许可证合规咨询（例如公开的电子邮件地址，或 Linux 基金会的开源合规名录）。

- 3.2.1.2 一份内部的操作文档，描述如何回应第三方开源许可证合规咨询。

理由：

确保第三方能通过合理的方式联系到组织，进行开源合规方面的咨询，且组织已经准备好有效回应。

3.2.2 有效的资源支持

识别计划任务并给予资源支持：

- 授予责任以确保计划任务的成功执行；
- 计划任务得到足够的资源支持：
  - 已分配执行任务的时间；且
  - 已分配充足的资金。
- 有流程用于审核和更新政策，以及支持任务；
- 需要指导的人可以联系到开源许可证合规方面的法律专家；且
- 有流程用于解决开源许可证合规的问题。

核查材料：

- 3.2.2.1 一份文档，记录了计划已确定角色中的人名、组名、或职能名。
- 3.2.2.2 计划已确定角色的人员都已安排到位，并获得了充足的资金。
- 3.2.2.3 支持解决内外部开源许可证合规问题的法律专家的身份。
- 3.2.2.4 一份操作文档，描述开源合规的内部责任分配。
- 3.2.2.5 一份操作文档，描述如何审核和纠正不合规项。

理由：

确保：1) 计划的职责得到了有效支持和资源投入；2) 定期更新政策和支持性的流程，以适应开源合规最佳实践的变化。

3.3 开源内容的审核和批准

3.3.1 材料清单

必须有流程为交付软件创建和管理材料清单，其内容包括构成该软件的所有开源组件（及其已识别许可证）。

核查材料：

- 3.3.1.1 一份操作文档，用于识别、跟踪、审核、批准和归档构成交付软件的开源组件信息。
- 3.3.1.2 交付软件的开源组件记录，以证明上述操作得到了正确执行。

理由：

确保有流程为交付软件创建和管理开源组件材料清单。清单用于系统性地审核和批准每个组件的许可证条款，以理解它给交付软件的分发带来的义务和限制。

3.3.2 许可证合规

计划必须有能力管理参与者在交付软件中遇到的常见开源许可证使用场景，可能包括以下场景（注意下面列表可能不全，也可能不是每条都适用）：

- 以二进制形式分发；
- 以源码形式分发；
- 和其他开源软件集成在一起，可能触发额外的许可证义务；
- 包含修改过的开源软件；
- 包含许可证跟交付软件中的其他组件不兼容的开源或其他类软件；且/或
- 包含带有署名权要求的开源软件。

核查材料：

- 3.3.2.1 一份操作文档，描述如何处理交付软件中开源组件的常见许可证使用场景。

理由：

确保有一个强有力的计划足以应对组织中常见的开源许可证使用场景。确保有操作程序支持合规活动并被遵守。

3.4 合规文件的创建和交付

3.4.1 合规文件

必须有流程来为交付软件创建一套合规文件。

核查材料：

- 3.4.1.1 一份操作文档，描述按照已识别许可证的要求，随交付软件分发合规文件的流程。
- 3.4.1.2 一份操作文档，描述如何归档交付软件的合规文件——从上次交付起计，归档物应保存合理的时长[1]，或按照已识别许可证的要求保存（以时间较长者为准）。并且有相关记录证明已正确遵守了此操作程序。

理由：

确保尽商业上合理的努力，来准备已识别许可证要求的合规文件，随交付软件一起提供。

3.5 理解开源社区参与

3.5.1 贡献

如果组织考虑为开源项目做贡献，那么

- 必须有书面的政策来治理对开源项目的贡献；
- 此政策必须在内部传达到位；且
- 必须有流程来实施此政策。

[1] 取决于领域、司法辖区和/或客户合同

核查材料：

如果组织允许为开源项目做贡献，那么必须有以下文件：

- 3.5.1.1 一份开源贡献政策文档；
- 3.5.1.2 一份治理开源贡献的操作文档；和
- 3.5.1.3 一份操作文档，能让计划参与者知悉开源贡献政策的存在（如通过培训、内部 wiki 或其他可行的沟通方式）。

理由：

确保当一个组织允许对开源项目做贡献时，它已经合理考虑过建立和实施开源贡献政策。此政策可以是整体开源政策的一部分，也可以是一个独立的政策。

3.6 遵守本规范的要求

3.6.1 遵从

如果一个计划被视作遵从了 OpenChain，那么组织必须确认此计划满足了本文档提出的要求。

核查材料：

- 3.6.1.1 一份文档，能确认§3.1.4 中详细定义的计划满足了本文档的所有要求。

理由：

确保如果有组织宣布一个计划遵从了 OpenChain，那么此计划已经满足本文档的所有要求。仅满足部分要求不视作遵从。

3.6.2 有效期

宣布遵从此版本 OpenChain 规范的计划，从遵从生效日起必须维持至少 18 个月。在 OpenChain 的项目网站上可以找到遵从生效的登记步骤。

核查材料：

- 3.6.2.1 一份文档，能确认计划在遵从生效起 18 个月内，都满足本文档的所有要求。

理由：

如果组织想长期保持遵从状态，让合规计划和最新的规范同步是很重要的。如果组织想长期保持遵从状态，此要求确保了支持合规计划的流程和管控措施不会逐渐失效。

附录 A
（重要）

本规范的翻译

为便于本规范在全球落地，欢迎不同语种的翻译。因为 OpenChain 以开源项目的方式运作，所以译文都来自于那些愿意贡献自己时间和专业知识的人。译文以 CC-BY-4.0 许可证授权，并和项目的翻译政策保持一致。政策的细节和已有的译文可参见 OpenChain 项目的 wiki。

附录 B

中英术语对照说明

本附录由译者编写。对于标准文档的翻译，术语很重要，但术语无论如何选择，可能都无法让所有读者满意。对于原文中的一些重要术语，译者在本附录中补充说明其在翻译上的考虑，以期能帮助读者更好地理解本规范。欢迎指正。

industry

译为“行业”。industry 既有“工业”，也有“行业”的意思，但中文的“工业”并没有“行业”的意思。虽然读者译文看得多了，也能明白在不少语境中，“工业”实际上是指“行业”，但本文还是选用更符合中文习惯的说法。

program

译为“计划”。这个词是指为达成一个特定的长期目标而设立一系列措施和活动，在中文中并没有完全对应的词汇，但类似的语境中，多数翻译成“计划”，如“开发者计划”、“火星登陆计划”等。注意和 plan 的区别。

process 和 procedure

process 译为“流程”。它是指把输入转化为输出所需要经历的活动，强调做什么。

procedure 译为“操作”。是指实施具体活动的方法，强调如何去做。这个词的翻译要看具体的语境，本文多处出现 documented procedure 这个短语，均译为“操作文档”。

compliant 和 conformant

compliant（或其名词形式）译为“合规”，这个词多用于法律领域，隐含了“因外部要求不得不做”的意思。

conformant（或其名词形式）译为“遵从”，这个词适用范围更广，并且含有“主动去做”的意思。

在本文原文中，compliant 用于开源许可证，conformant 用于 OpenChain 规范。

reasonable commercial efforts

译为“商业上合理的努力”。这是一个法律术语，本身在英语中的意义边界也不是特别明确，通常会跟“best efforts”做对比，它的努力程度不如“best efforts”。大致意思表示为了某个目标，要努力投入资源，但投入应该在商业逻辑可接受范围内，如果仅仅为了达到一个不算很重要的目标而投入重大的资源，这就不是“商业上合理的努力”。

artifact

简单译为“文件”。这个词原意指非天然的、人工制成的物件，在不同的语境中有很多怪异的译法，本文没有采用。在本文中，就是指证明合规的交付物，可能会包含代码、文档等形式。