开源治理良策

作者：OSPO联盟和GGI参与者
版本： v1.2
日期：2025-03-10

Contents

1 概述

本书介绍了在各类组织机构内进行专业的开源治理的方法。阐述了企业如何正确、高效地使用开源软件，以及如何保护企业规避相关的技术、法律和知识产权风险，最大限度地发挥开源的优势。无论您的企业正在面临上述何种挑战，本文档均能为您提供解决思路和办法，助力您的开源工作持续发展直至成功。

1.1 背景

大多数系统集成商和大型行业用户已经在其信息系统、信息产品和技术服务部门中使用开源软件 (FOSS)。开源合规已成为一个备受关注的问题，许多大型企业已经设立了“合规负责人”这个岗位。然而，尽管厘清公司的开源供应链至关重要（这是开源合规的重要体现），用户**必须**回馈开源社区并持续贡献开源整体生态也同样重要。我们看到开源治理涵盖整个生态系统，包括与本地社区互动交流，与开源软件供应商和开源技术专家建立共赢关系等。这都将开源合规提升到一个更高的水平，这就是 *《开源治理良策》* 的意义所在。

开源治理这一概念事实上超出了开源合规的范畴。它是在最终用户（通常是软件开发者）和系统集成商构成的社区中建立共识，在全球开源生态中建立互利共赢的纽带关系。

《开源治理良策》可以帮助各种类型的组织机构（包括各类企业、事业单位、高校和科研机构等）进行人力资源部署、设计流程、协助技术开发和战略制定，最大限度地发挥开源的优势并获得开源带给组织的各种增益。因此，最大限度地发挥开源的优势，尤其是在中国和欧洲，即便没有人知道自己在领域前沿技术中实际上处于什么水平，我们依然可以持续学习，不断创新。

本书旨在帮助各种类型的组织通过以下方式实现上述目标：

- 通过一个结构清晰的**工作步骤**，为开源软件实施专业化的治理设定一个路线图。
- 一套用于定义、监控、汇报和沟通的**过程管理工具**。
- 一条**清晰且有效的路径**，通过低成本、低负担的形式来降低风险、开展培训、优化流程、加强组织内外的沟通。
- 本书及相关**开源许可、开源实践案例、培训**和**生态系统共建**的指导和一系列参考资料，有助于推广开源思想和开源文化，有助于巩固开源知识体系提升个人领导力。

在本书的编著过程中考虑了以下需求：

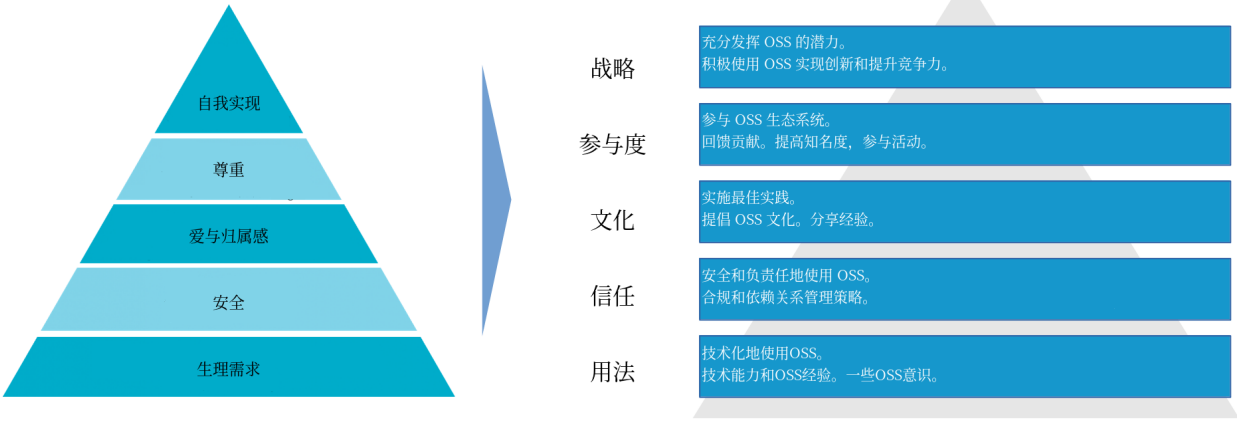
- 涵盖任何类型的组织：从中小型（SMEs）到大型企业和非营利组织，从第三方行业组织到大型科研机构。本书提供了制定开源治理战略的重要组件和战略实践的提示，但企业开源治理的**具体执行**情况完全取决于企业自身的背景条件，以及其直接负责人。同时企业应该积极寻求专业的咨询服务并与业界同行相互交流。
- 不对组织机构内或项目组内的知识水平做出任何假设。例如，一些企业需要建立完整的培训课程，而其他企业可能仅向团队提供部分资料。

当然有些工作内容并不适合所有企业的现状，本文档为大家提供了一个详尽的路线图，并为企业制定不同的开源治理战略做了铺垫。

1.2 GGI（Good Governance Initiative）项目介绍

在 OW2 社区中所有工作都是为了满足市场需求而共同努力。GGI 项目提出了一个在组织机构内部实施开源的专业化治理的方法论。

GGI 项目是基于一个综合模型，该模型受到广泛流行的马斯洛人类需求和动机层次结构的启发，如下图所示。



亚伯拉罕·马斯洛的行为动机层次　　OW2 旨在实现 OSS 的良好治理

通过这些理念、指导方针和活动计划，GGI 项目为负责开源软件专业管理的实体部门（也称为开源管理办公室,OSPO）开展工作提供了建设蓝图。这种方法其实就是一套用于定义优先级、实施监控和共享进程的管理系统。

当企业开始进行开源治理时，我们将帮助其在以下多个维度提高技能，包括：

- **使用**开源: 在企业内部正确地、安全地使用开源软件，以期提升软件的复用性、可维护性和软件开发效率;
- **降低风险**: 降低在与外部技术合作和外部代码集成时可能导致的潜在的法律和技术风险;
- **统一认识**: 整个团队中，从软件开发者到团队负责人乃至管理层都要明确各自所需进行的培训，这有助于大家统一思想，树立一致的发展目标;
- **优先等级**: 确定目标和相关工作的优先级，帮助企业制定高效的开源战略;
- **促进交流**: 充分利用开源战略，促进企业内部以及与产业生态之间的高效交流;
- **能力提升**: 提升企业的竞争力和对顶尖开源人才的吸引力。

1.3 OSPO 联盟介绍

OSPO 联盟由 OW2、Eclipse Foundation、Open Forum Europe 和 Foundation for Public Code 等欧洲知名的开源非营利组织发起的产业联盟，旨在提升欧洲乃至全球对开源的认识、推动企业和事业单位对开源进行结构化和专业化的管理。

虽然 GGI 的重点是制定管理机制，但 OSPO 联盟的目标则更加宽泛，即帮助企业（特别是非科技领域企业）、事业单位和科研机构重视和理解开源，指导他们开展开源治理相关工作并从中受益，并帮助企业的 OSPO 部门发展。

OSPO 联盟已经建立了 **OSPO 联盟**官网https://ospo-alliance.org。OSPO 联盟网站为社区提供了一个安全场所来交流和讨论有关开源管理办公室相关工作的话题，并为企业、事业单位、高校和科研机构提供一套完整的资源库。OSPO 联盟与欧洲和世界各地的 OSPO 以及相关社区组织建立了联系。联盟鼓励大家身先士卒，对开源产业生态持续性贡献。访问OSPO 联盟网站，可快速概览相关的实践案例。

OSPO 联盟网站也是收集社区有关 GGI 项目反馈和建议 (任何信息和活动) 的重要途径。

1.4 翻译译本

GGI 手册最初以英文撰写。感谢社区正在进行的 GGI 手册的翻译工作，目前社区已经提供了法语、德语、葡萄牙语、荷兰语、意大利语、西班牙语和中文版本。GGI 手册中文版译名为《开源治理良策》。由于翻译工作进展迅速，建议您查看官方网站以获取其他可用翻译版本的完整列表。

> 请参阅https://ospoalliance.org/ggi/

GGI 手册的翻译使用了Weblate，其为开源项目提供免费托管服务。我们要向他们以及所有翻译贡献者表示深深的谢意。你们太了不起了。

> 请参阅https://hosted.weblate.org/projects/ospozoneggi/#languages

1.5 以下人员为本文档做出了贡献

贡献者名单:

- Frédéric Aatz（微软法国）
- Boris Baldassari（Castalia Solutions，Eclipse 基金会）
- Philippe Bareille（巴黎市政府）
- Gaël Blondelle（Eclipse 基金会）
- Vicky Brasseur (Wipro)
- Philippe Carré （诺基亚）
- Pierre-Yves Gibello (OW2)
- Michael Jaeger （西门子）
- Sébastien Lejeune (Thales)
- Max Mehl（欧洲自由软件基金会）
- 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 基金会）
- Igor Zubiaurre (Bitergia)

1.6 许可证

2 组织机构

2.1 术语

《开源治理良策》（GGI 手册中文版）由四个核心概念构成：目标设定、常规工作、定制计分卡和持续迭代。

- **目标设定**: 目标是具有相同关注点的一系列工作的集合，通常分为五个目标：使用目标、信任目标、文化目标、参与目标和战略目标。目标可以通过一系列工作独立地、并行地、迭代地完善。
- **常规工作**：围绕一个目标，一项工作可以解决单一问题或发展问题（如管理法律合规性），可以将其视为实现目标的渐进步骤。GGI 定义的一系列工作的集和称为常规工作。
- **定制计分卡 (CAS)**：为了在指定的组织机构中执行 GGI、规范工作必须适应指定机构的具体情况，进而要构建一套定制计分卡。定制计分卡描述了如何在指定机构现状下开展工作以及如何监控进度。
- **持续迭代**：开源治理是一个管理系统，因此需要定期评估、审查和修订。试想一个组织机构中的会计系统，它是一个持续完善的过程，至少要有年度审查，即资产负债表；同样，开源治理的流程至少需要进行年度审查，但根据不同的工作内容，这些审查可以拆分为多个，也可以设置为多次。

2.2 目标设定

GGI 定义的常规工作围绕目标进行组织。每个目标都涉及到流程中的特定维度进展。从使用到战略，目标涵盖了从开发团队到高级管理者的所有人员的相关问题。

- **使用目标**：此目标涵盖使用开源软件的基本步骤。与使用目标相关的工作涵盖了开源计划的第一步，确定如何高效使用开源以及其给组织机构带来的收益。它包括培训和知识管理, 制作一份内部正在使用的现有开源软件清单，并罗列出可以在整个过程中使用的开源技术。
- **信任目标**：此目标是关于如何安全地使用开源。信任目标涉及法律合规性、技术依赖性和漏洞管理, 旨在为组织机构如何使用和管理开源树立自信心。
- **文化目标**：此目标包括旨在帮助团队适应开源、独立参与到协作中、了解和体验开源的实践案例。这一目标有助于提升个人对开源社区的归属感。
- **参与目标**：此目标是关于以企业立场参与开源生态。人力资源和财务预算将用于反哺开源项目。在此，组织机构可以宣称自己是一名有担当的“开源公民”，并对开源产业生态的可持续发展承担应尽义务。
- **战略目标**：此目标是关于让企业最高管理层能够重视开源、拥抱开源。这有助于企业将开源作为数字主权、流程创新等企业战略的核心构成，将开源视为企业美誉度和企业吸引力的重要来源。

2.3 常规工作

常规工作是《开源治理良策》的核心。在早期版本中，本书为每个目标提供了 5 项常规工作。常规工作将使用以下预定义概念进行描述：

- **描述**：所涉及主题的工作以及完成所需步骤的概要。
- **可行性评估**：描述开展此工作的原因和时间。
- **进度评估**：描述如何衡量工作的进度和如何评估工作的成绩。
- **工具**：可以帮助实现此工作的技术或工具列表。
- **建议**：从 GGI 参与者收集的提示和实践案例。
- **资源**：阅读有关此项工作主题的更多链接内容和参考资料。

描述

这部分提供了有关工作的高级描述，和在目标范围内以开源方式确定工作目的的主题摘要。

可行性评估

为了帮助构建迭代方案，每项工作均应设置“可行性评估”环节，并附上一些疑问。可行性评估的重点是开展这项工作的相关原因，以及其解决了哪些问题。可行性评估这一环节有助于确定工作的预期工作内容、所需的资源，有助于预估成本和投资回报率。

进度评估

此步骤的重点是定义关键对象、关键绩效指标（KPI）和提供有关评估工作进度的**可验证点**。建议验证点具备以下两个特征，可以帮助定义开源治理的路线图、相关事务的优先级，以及如何量化这些进度。

工具

这里列出了可以帮助工作交付或监测工作特定步骤的工具。这里的工具既不是强制性的，也不能保证全面，而是根据现有情况给出的一些建议或工具类别。

建议

这部分会定期更新用户的反馈信息以及所有有助于管理此项工作的建议。

资源

此处汇集了更多关于背景研究、参考资料、线下活动或线上内容等相关资源，这将进一步丰富和完善相关的工作。资源并不详尽，它们只是在个体背景下可以开展工作的一个起点或建议而已。

2.4 定制计分卡

定制计分卡 (CAS) 比常规工作稍微细化一些。CAS 涵盖了实施 GGI 开源治理的组织机构的详细信息。本文档 4.3 节有定制计分卡（CAS）的详细介绍。

[kpi]：绩效指标或关键绩效指标是绩效衡量的一种。KPI 评估组织或其参与的特定活动的进展和成功。

3 企业内源

当前，基于各组织机构所属开发团队开源实践的成功，企业内源正在成为企业的一种发展路径，在越来越多的企业中日渐流行。然而，实施企业内源不仅仅是复制和粘贴那些案例。企业内源必须适应公司自身的企业文化和内部组织结构。让我们仔细看看内源到底是什么、不是什么，以及其带来了哪些挑战。

3.1 什么是企业内源？

该术语是由 Tim O Reilly 先生于 2000 年首次提出, 指出企业内源是 **“在公司内部使用开源开发技术”**

据InnerSource Commons相关文章作为参考，企业内源是” 在一个组织机构内部通过使用开源规则和实践来进行软件开发工作”(InnerSource is the “*Use of open source principles and practices for software development within the confines of an organization.*”)

3.2 为什么选择企业内源？

根据InnerSource Commons的观点,”* 对于主要构建闭源软件的公司来说，企业内源可以作为一个很棒的工具，有助于打破信息孤岛、鼓励和扩大内部协作、加速新工程师的成长，并找到向开源世界贡献软件的机会。*”

有趣的是，内源的优势不仅可以影响工程师，还可以影响公司内其他部门。因此，一些公司在以下领域发现了企业内源的具体优势:

- 法律部门: 通过使用现成的法律框架 (内源许可证) 来加速内部跨部门协作。
- 人力资源部门: 通过集中专业骨干的且经验丰富的核心团队来管理稀缺技能。

3.3 企业内源的争议

围绕企业内源有许多来自反对者的质疑。尽管不是真正意义上的开源，但它在组织机构内部部署后，为该组织机构带来了巨大的潜在利益。以下是一些质疑的内容：

- 「质疑」内源是以牺牲 (对外部) 开源为代价的:
  - 软件项目处于企业的防火墙之后。
  - 对开源的外部贡献较少。
- 「质疑」绑架开源精神而不是汲取开源精神。
- 「质疑」没有一个内源项目转化为开源项目。
- 「质疑」实施内源的动机是其类似于开源。但实际上，如果开发人员重视其价值，那么更应该做的是直接进行开源贡献。

以下是有关内源实践的事实情况，回击了前面大部分质疑:

- [事实] 内源是一种吸引主要闭源公司融入开源的途径。
- [事实] 由于大部分开源贡献都是由志愿者做出的，我们可以通过列出 “预期收益” 来号召工程师们参与开源。
- [事实] 或许在大多数情况下，公司没有遵循一个有序且可控的开发流程，而本书可以作为一种方法帮助他们管理此类问题。
- [事实] 从封闭许可转换到开放许可仍需要做**大量**工作。
- [事实] 这是一些已经开源的真实的内源项目案例：
  - Twitter（Bootstrap）。
  - Google(Kubernetes)。
  - dotCloud(Docker)。
  - React Native。
- [事实] 开源得益于熟悉开源技能的软件工程师规模的提升，得益于越来越多的软件工程师熟悉开源，而内源正在为此努力。

3.4 谁在做这件事？

许多企业已经开始实施内源项目或建立了内源管理办公室（ISPO），其中一些企业已经持续了很长时间，一些则是新近启动。以下是一份主要聚焦欧洲公司的不完全名单:

- 桑坦德银行 (Banco de Santander) (source)
- 英国广播公司 (BBC) (source)
- 博世 (Bosch) (source)

- 康卡斯特 (Comcast）(source)
- 爱立信 (Ericsson）(source)
- 恩吉 (Engie) (source)
- 国际商业机器 (IBM) (source)
- 梅赛德斯 (Mercedes) (source)
- 微软（Microsoft）(source)
- 耐克 (Nike)(source)
- 诺基亚 (Nokia) (source)
- 法国国家铁路公司 (SNCF) (source 1, source 2)
- 贝宝 (Paypal)(source)
- 飞利浦 (Philips)(source)
- 雷诺 (Renault)(source)
- 思爱普 (SAP) (source)
- 西门子 (Siemens)(source)
- 法国兴业银行 (Société Générale)(source)
- 泰雷兹 (Thales)(source)
- 法国 VP 知名电商 (VeePee)(source)

3.5 内源社区是一个重要参考

内源社区 (InnerSource Commons) 是一个积极活跃的内源从业者社区，该社区遵循开源原则，详情参见内源社区。社区提供了方法论patterns、学习路径 learning path和电子书等许多有用资源来帮助大家快速了解内源。如:

- 《内源入门》作者：Andy Oram。
- 《对内源工作清单的理解》作者：Silona Bonewald。

3.6 内源治理的差异

内源面临着一些特定的开源没有面对过的挑战。大多数组织机构正在通过开发私有软件来解决这些问题:

- 为内源项目定制专有的、公司特定的许可证 (适用于多个法人实体的大型企业)。
- 开源的公有属性使其免受转让定价的挑战。内源的私有属性使得跨国企业面临在不同司法管辖区域运营的公司间利润转移的责任风险。
- 贡献的动机差异巨大:
  - 因为受限于组织机构自身规模，内源的潜在贡献者阵营较小。
  - 展示自身专业技能是做出贡献的动因之一。内源将这种展示限制于组织机构内部。
  - 推动社会进步是做出贡献的另一个动因，这也同样受限于内源。
  - 因此内源的驱动力更需要依赖任务安排和贡献奖励，并付出更大的努力。
  - 由于代码的有限可见性，内源可以更容易的克服如”冒名顶替综合征”类似的完美主义者的恐惧。
- 日渐频繁的劳动力外包，将在多方面影响治理。
- 由于是在内部开发，评估企业内源的充分性将更加容易。
- 可发现性是一个问题。对于企业，域内检索信息的优先级并不高。如 DuckDuckGo、Google 或 Bing 这样的公共搜索引擎表现得更加出色，而内源却无法借助他们的优势。
- 因为其存在于企业内部，内源在出口控制方面有一点微弱的优势。
- 需要对如源代码等知识产权泄漏进行权限管控。

随着越来越多的企业采用其原则、分享其经验，内源仍在持续发展。本文档的后续版本将提供 GGI 相关内源实践案例的精选集。

4 方法论

实施《开源治理良策》终将是一项具有重要意义和深远影响力的工作。它涉及到公司的多个维度，人员、服务和流程，从日常行为到人力资源管理, 从开发人员到高级管理人员。确实不存在实施开源治理良策的” 灵丹妙药”(银弹机制)。不同类型的组织机构、企业文化和现状需要不同的开源治理方案。对于每一个组织机构，都会有不同的限制条件和期望目标，从而导致管理流程选择的路径和方法不尽相同。

考虑到这一点，GGI 提供了一个通用的开源治理工作规划，可以根据组织机构自身领域、文化和要求进行定制。尽管该规划比较全面，但还是应该实事求是按部就班地逐步实施。在特定条件下通过简单选择最适当的目标和工作内容即可启动内源方案。这个思路是通过制定一个路线图初稿，来帮助制定自身的工作方案。

除此之外，我们还强烈建议与如欧洲OSPO 联盟、TODO 社区、OSPO++ 等开源机构建立的关系网中的同事们保持沟通。重要的是能够与实施类似内源方案的同事们交换意见，分享所遇问题和相应的解决方案。

4.1 准备工作

为了对《开源治理良策》树立信心和扩大影响，与组织机构内部各类人员的沟通就非常重要。比较合适的做法是帮他们建立一套现实可行的预期和要求，引起兴趣和获得支持，以便取得良好的开端。在组织机构内部的协作平台上发布定制计分卡是一个不错的主意，此举可以促进他们与其他利益相关者进行沟通。以下是一些提示:

- 确定关键利益相关者，促使其认可一系列主要目标。成功的吸纳他们，并将相关工作列入他们自身的工作计划。
- 获得初步支持，就工作步骤和进度达成一致，并设置定期检查，以向他们通报进展情况。
- 确保他们了解可以实现的收益及其涉及的内容：预期的提升过程应该是明确的，结果应该是清晰可见的。
- 在候选组织机构中进行一个初步的开源现状诊断。输出成果: 一个包含可以实现的目标、组织机构现在的处境以及后续发展方向的文档。

4.2 工作流程

作为当代软件开发者，我们倾向于采用敏捷开发方法，它强调定义少许可控的增量。同时，定期重新评估情况并提供有价值的最小中间成果，这一点非常务实。

还有一点尤为重要，在开源管理办公室的日常工作过程中，随着时间的变化，许多因素都会随之变化，包括组织机构的开源战略及其反响，以及人员的可用性和参与度。定期的重新评估和迭代不仅有助于调节该工作的适应性，还能更好的跟踪当前趋势和机遇，为利益相关者和整个组织机构带来少许增量收益。

理想情况下，该方法可以分以下五个阶段实施：

1. **发现阶段**理解核心概念，掌握方法论，调整预期目标。
2. **定制阶段**根据组织机构的自身情况调整工作描述和可行性评估。
3. **制定优先级阶段**确定目标和关键成果、分项任务和工具，规划时间表并设定里程碑。
4. ** 启动阶段 ** 在 Issue 上，制定计分卡、制定预算、分配任务并做好文档记录。
5. **迭代阶段**定期评估并量化结果，标明问题点，不断进行优化和调整。每季度或每半年进行一次迭代。

为首次迭代作的准备:

- 确定第一组要处理的任务，并根据需求 (与期望状态的差距) 和时间表排出它们的优先级。输出成果: 一份迭代期间内所要处理的任务列表。
- 定义一系列要求和改进领域，与利益相关者和最终用户沟通，并获得他们的认可或承诺。
- 填写计分卡以跟踪进度。计分卡模板可以从 GGI 在线存储库下载。GGI repository。

在每次迭代结束时，进行回顾并为下一次迭代做好准备：

- 交流最新的改进内容。
- 评估目前的状况，如果目标任务已经完成，则相应地完善路线图。
- 检查剩余的痛点或问题点，必要的话，寻求其他参与者的支持或者服务。
- 根据更新后的状态重新排出任务的优先级。
- 定义要执行的新任务子集。

4.3 手动设置：使用定制活动计分卡

定制活动计分卡 (CAS) 是一种描述根据组织机构具体情况定制的规范工作的表单。总而言之，定制活动计分卡 (CAS) 提供了管理开源软件的路线图。

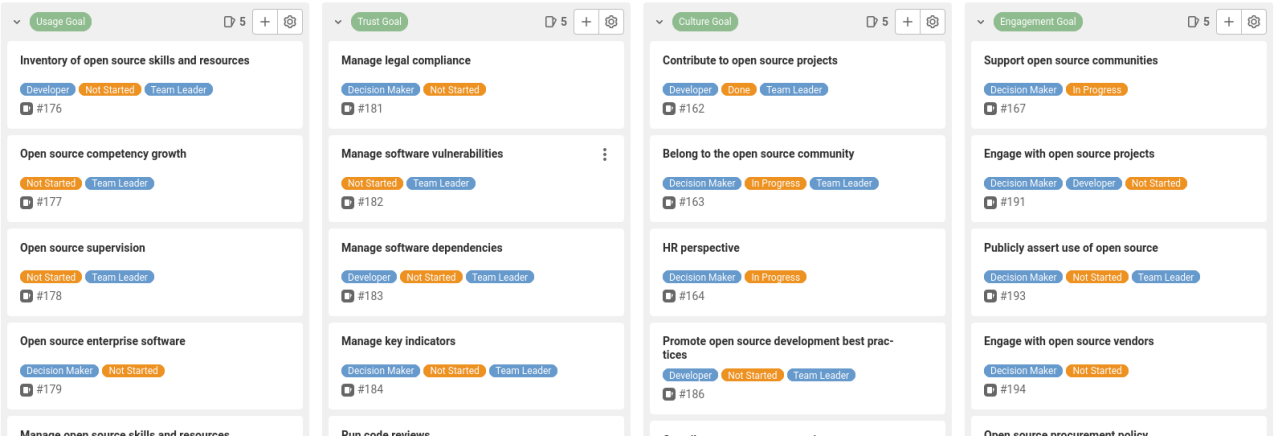
请注意，根据此方法的早期经验，将规范工作适用于一个组织机构的特定的定制计分卡需要一个小时左右的时间。

定制活动计分卡（CAS）包含以下内容:

- **开篇明义**首先，用几分钟时间来了解这个工作的可能涉及的内容及其相关性，以及它如何融入您整体的开源软件管理过程。
- **定制描述**根据组织机构的特定需求和特点，调整工作内容，并界定其范围。确定工作的具体范围，明确你将面对的具体问题。
- **可行性评估**解释开展此工作的相关原因，它满足什么需求。我们的痛点是什么？有哪些发展机遇？从中能得到什么？
- **目标**为此项工作确定几个至关重要的目标。待解决的痛点，发展机遇和愿景。在本轮迭代中要完成的目标。
- **工具**工作中所使用的技术、工具和产品。
- ** 操作说明 ** 说明此项工作进展的途径、方法和策略。
- **关键成果**定义可衡量、可验证的预期结果。选出能够呈现目标进展成果的指标。在此标明 KPI。
- **进度和评分**进度是指工作任务达成的百分比；评分则是个人对工作任务成功度的打分。
- **个人评价**对于每项成果，你可以附上一段简明的说明，并在评分中体现对个人满意度的评估。
- ** 时间线 ** 提供起止日期、阶段性任务、关键步骤和里程碑等信息。
- **工作量**评估所需的时间和来自内部以及第三方的物资。预期的工作量有多大？预计成本有多少？我们需要哪些具体资源？
- ** 责任人 ** 说明哪些人参与其中。分配任务或分配工作的领导权和责任范围。
- **问题**识别关键问题、可预见困难、风险、障碍、不确定性、关注点和关键依赖。
- **现状**在此提供对工作现状的一个综合评估：进展是否顺利？是否延期？等等。
- **总体进度评级**您对工作进展进行的高维度、管理导向的综合性评估。

4.4 自动设置：使用 GGI 部署功能

从本文 1.1 版本开始，GGI 推出My GGI Board，这是一个自动化工具，用于将您自身的 GGI 实例部署成为一个 GitLab 项目。该安装流程仅需不到 10 分钟便能完成配置，拥有详尽的文档资料，并提供了一种简洁可靠的方式实现工作定制，监控它们的执行进度，并及时与利益相关者沟通成果。您可以在GitLab 平台上查看到部署的实时案例，同时，其自动生成的网站也可在GitLab 页面上直接访问。



以下是使用部署功能的标准工作流程：

1. 将 My GGI Board 项目 fork 到您自己的 GitLab 实例或项目空间，并按照项目的 README 中的说明进行设置https://gitlab.ow2.org/ggi/my-ggi-board。这时会进行：

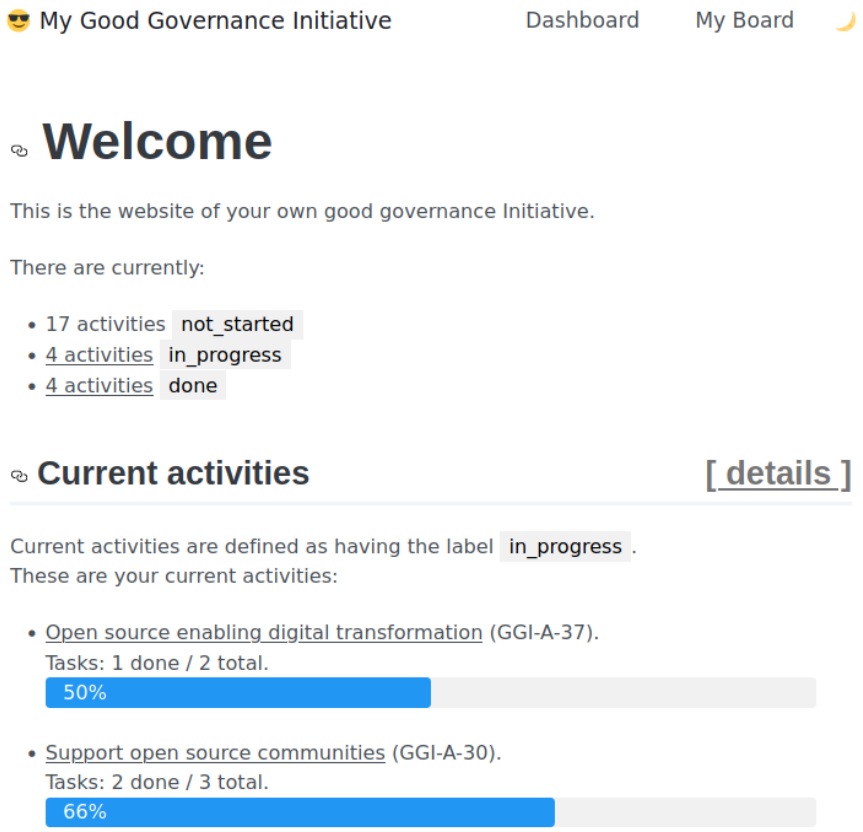
- 将所有工作创建为项目中的 issue。
- 创建一个漂亮的看板来帮助您可视化的管理工作。
- 在您的 GitLab 实例页面上创建一个静态网站，网站信息是从工作中提取出来的。
- 更新项目描述，将链接正确地指向工作看板和静态网站页面。

1. 在此，您可以开始查看不同的工作并填写计分卡部分。

- 计分卡部分相当于前述 ODT 计分卡的电子版和简化版。它们通过列出当地的资源、风险和机遇，并设定为完成工作所需的定制目标等方法，被用来调整工作以适应到您的具体情况。
- 如果某些工作与具体情况不匹配，则只需简单将其标记为“未选择”或者关闭即可。
- 这是一个相当耗时的过程，但却非常必要，因为它将帮助您一步一步地定义您自己的路线图和计划。

1. 定义工作后，您可以开始建立您自己的开源管理办公室了。选择一些您认为与启动相关的工作，并将其进度标签从“未启动”更改为“进行中”。您可以使用 GitLab 功能或任何其他工具来帮助您组织这些工作（如评论、责任人等）。链接到工作很容易，并且还有很多优秀集成可以调用。
2. 定期评估和审查（每周或每月，取决于您的时间表）当前的工作，并在完成后将标签从“进行中”更改为“已完成”。选择其他几个并重新执行步骤 3，直到全部完成。

网站提供了对当前和过往工作的快速概览，并从 Issue 中提取计分卡部分，只展示与本地相关的信息。当 Issue（或工作）发生变更时，这些变更会自动反映在网站上。请注意，网站的自动生成是通过 CI（持续集成）流水线实现的，这些流水线每晚都会自动运行，但您也能通过 GitLab 项目的 CI/CD（持续集成/持续部署）部分轻松启动它们。以下图片展示了由系统自动生成的网站界面。



您可以在我们的 GitLab 主页提问或获取有关部署的技术支持，欢迎提出宝贵建议。

GGI 的部署主页:https://gitlab.ow2.org/ggi/my-ggi-board

4.5 享受过程

分享您的成功，并享受先进开源策略带来的安心与宁静！

开源治理良策是一种推动持续改进的方法，因此它是一个永无止境的过程。正因如此，重要的是要明确展示每个阶段性成果，并欣然接受它所带来的改变，这样做可以让进步变得显而易见，并能够与他人分享这些成果。

- 与利益相关者和最终用户多沟通，让他们了解此项工作所带来的优势和机遇。
- 促进此项工作的可持续性。确保项目中形成的实践案例和汲取的经验教训始终得到实施和及时更新。
- 与同行分享您的经验：向 GGI 工作组和您的 OSPO 社区提供反馈，并分享您的方法。

5 使用目标

5.1 开源技能和资源清单

活动编号：GGI-A-17。

描述

在任何阶段，从管理者的角度来看，都应该有一个清晰的开源资源清单，包括开源的资源和资产的使用情况和状态，以及潜在需求和可行的解决方案。此外，还需要评估实现这些解决方案所需的工作量和技能。

此项工作旨在对组织机构内部及市场上的开源状况进行一次快照式的盘点，并评估两者的资源对接情况。

- 盘点在软件研发过程中以及软件供应链中所使用的软件产品和组件中，开源软件的使用情况。
- 识别可以满足您的需求并帮助改进软件研发流程的开源技术（解决方案、系统框架和创新功能）。

但不包含，

- 识别并评估相关开源软件生态系统和社区。（文化目标）
- 识别相关开源软件库和组件的依赖关系。（信任目标）
- 识别实现开源项目所需的技术技能（如编程语言、框架等）和非技术技能（如协作、沟通等）。（这属于下一阶段工作：开源软件能力增长和开源软件开发技能）

可行性评估

编制一份开源资源清单，以帮助优化资源投入和优先技能的培养。

此项工作为提高生产力创造了有利条件，特别是在现代应用系统和基础设施开发中，开源组件、开发理念和工具的高效性和普适性尤为突出。

- 这可能需要对开源软件资源的组合进行简化。
- 这可能需要对人员进行二次培训。
- 这有助于明确需求，也有助于补充完善 IT 发展路线图。

进度评估

以下**验证点**将呈现此项工作的进展：

- □ 生成一个可行的开源软件资源列表，如” 我们使用了什么”, ” 我们集成了什么”, ” 我们研发了什么”, ” 我们托管了什么”, 以及相关技能
- □ 我们是否正在通过使用最先进的方法和工具来提高效率。
- □ 我们是否发现了之前未被记录过的开源软件资源（这些资源可能一直在悄然增加，而我们是否有方法来定义与此相关政策）
- □ 我们要求新项目认可或复用现有的开源软件资源。
- □ 我们对组织机构内部开源软件的使用范围是否有了相对安全的认识和理解。

工具

有许多不同的方法来建立此类清单。其中一种方法是将开源资源分为四类：

- 我们使用的开源软件：我们在研发和生产过程中使用的软件
- 我们集成的开源软件: 例如, 我们集成到定制应用程序中的开源软件库
- 我们研发的开源软件: 例如, 我们在 GitHub 发布的, 或者是由我们研发或定期参与贡献的开源软件库。
- 我们托管的开源软件: 我们为了对内提供服务而运行的开源软件, 例如 CRM, GitLab, nexus 等。示例图表如下所示:

我们使用了	我们集成了	我们研发了	我们托管了	相关技能
Firefox, OpenOffice, Postgresql	Library slf4j	Library YY on GH	GitLab, Nexus	Java, Python

以同样的方法识别相关的技能

- 现有团队所具备的技能和经验
- 可以通过内部培训, 指导和历练获得的技能和经验
- 可以通过合作伙伴外包或在市场上找到的技能和经验

建议

- 行事保持简单。
- 这是一项相对高阶的实践工作，而不是会计部门的详细清单。
- 尽管此项工作是一个很好的起点，但您不需要 100% 完成之后再开展其他工作。
- 在 #42 工作中处理与**软件开发**相关的问题、资源和技能。
- 清单应涵盖所有 IT 类别：操作系统、中间件、数据库、系统管理、研发和测试工具等。
- 开始识别相关的社区：在这些社区了解你后，你会更容易获得他们的反馈和支持。

资源

- 这里有一个由 Dirk Riehle 教授开设的关于自由/开源软件的优秀的课程。

下一步工作建议

- GGI-A-18 - 开源能力增长 识别开源技能和资源有助于组织机构开始巩固和提升其意识和能力。
- GGI-A-19 - 开源监管 一旦这份开源软件和技能的清单完成，人们就可以对组织机构内部的开源软件使用进行管控。
- GGI-A-28 - 人力资源视角 人力资源部门可以根据此工作清单制定适当的人力资源培养和发展计划、员工或外包合同以及与开源相关的人力资源管理流程。
- GGI-A-33 - 与开源供应商合作 人们需要先了解他们的开源软件和技能情况，然后再与外部供应商建立关系。
- GGI-A-42 - 管理开源技能和资源在完成开源资产和技能清单后，就可以对其进行管理，并在现有内部资源的基础上来构建程序。

5.2 开源能力提升

活动编号：GGI-A-18。

描述

此项工作是关于在清单编制之后，如何规划和启动与开源软件相关技术能力和早期经验 (#17)。这也是开始建立一个基础的、轻量级技能发展路线图的机会。

- 确定所需的技能和培训。
- 建立一个试点项目来启动该方法，通过实践来学习，建立第一个里程碑成果。
- 利用学到的经验教训，建立知识体系。
- 确认并记录后续步骤，以实现大范围的应用。
- 为接下来的几个月或一年制定战略，以争取到管理层支持和资金支持。

活动范围：

- Linux、Apache、Debian 等系统管理技能。
- 开源数据库 MariaDB、MySQL、PostgreSQL 等。
- 开源虚拟化和开源云计算技术。
- LAMP 开源技术栈及其平替技术方案。

可行性评估

和其他 IT 技术相比，开源带来了更多创新。开源发展迅速，日新月异。它要求组织机构拥有持续更新的能力。

此项工作有助于通过培训提高人员工作效率，更加安全的使用开源技术。同时此举将帮助他们做出研发决策。培养基本的开源技能有助于把握以下机遇：

- 利用市场上现有技术生态来扩展我们的 IT 解决方案。
- 探索组织机构内部和外部之间新的协作模式。
- 掌握新兴技术和创新技术的能力。

进度评估

以下**验证点**将呈现此项工作的进展：

- □ 制定一个技能矩阵。

- ☐ 主动定义开源技术的使用范围，即避免开源技术的不受控使用。
- ☐ 这些技术已达到令人满意的专家级水准。
- ☐ 团队已经完成了”开源基础知识”培训，为工作起步做好了准备。

工具

这里有一个关键工具称为“活动矩阵”（或能力映射）。

此项工作这可以通过以下方式进行：

- 使用在线教程（互联网上有许多免费资源），
- 参加开发者技术峰会，
- 接受供应商培训等。

建议

- 安全、高效地使用和研发开源组件需要一种开放、协作的心态，而这需要同时得到组织机构内从高层（管理者）和底层（开发者）的认可和推广。
- 确保管理层支持并积极推动。如果没有管理层的坚定承诺，就难以取得进展。
- 邀请相关人员（开发者、利益相关者）参与其中：组织圆桌会议，倾听他们的想法。
- 为人们提供时间和资源来探索、尝试和运用这些新概念。如果可行的话，让这个过程变得有趣些——通过游戏化和奖励机制来激发兴趣。

一个包含以下步骤的试点项目，可以起到促进作用：

- 确定最初的技术或框架。
- 找到在线培训、教程和代码样例进行实验。
- 构建最终解决方案的原型。
- 找一些专家来找出问题和指导实施过程。

资源

- 能力矩阵是什么：这是简介。
- 如何为您的团队制作技能矩阵：这里是带注释的模板。
- 关于自由文化的 MOOC(仅限法语): 这是关于自由文化的六部分课程, 版权介绍, 知识产权, 开源许可等

下一步工作建议

- [GGI-A-28 - 人力资源视角](https://ospo-alliance.org/ggi/activities/ human_resources_perspective) 精心规划内部技能和潜在能力的提升是人力资源工作的重要部分。

5.3 开源监督

活动编号：GGI-A-19。

描述

此项工作旨在控制开源软件的使用，并确保开源软件得到主动的管理。这涉及多个维度，无论是使用开源软件工具或商业解决方案，还是将开源以组件的形式体现在自己的研发中，亦或是修订一个软件版本以适应自己的需求等。它还涉及识别开源已经形成的事实解决方案（有时是隐蔽的）的领域，并评估其适用性。

可能有必要澄清以下几点：

- 是否提供了所需的功能？
- 是否提供了不必要的，却会增加构建和运行阶段复杂性的附加功能？
- 许可证有何要求，有哪些法律约束？
- 该决策使您的组织机构在多大程度上不受供应商限制？
- 是否存在符合您业务需求的支持选项，它的成本是多少？
- 总体拥有成本是多少。
- 管理层是否了解开源的优势，例如，不仅仅是“节省许可成本”？熟悉和拥抱开源有助于在与开源项目社区和开源供应商的合作中获得最大利益。
- 考虑将自己的研发成果贡献给社区来分摊研发成本以及所有相关影响（如许可证合规等）是否有意义。
- 检查社区支持或专业支持的可用性。

可行性评估

定义针对开源的决策流程是一种收益最大化的方法。

- 它避免了开源技术不受控制的悄然使用和隐性成本。
- 它促进了基于充分信息且对开源软件有深刻理解的战略性和组织性决策。

成本：此项工作可能会对开源软件事实上的使用条件提出挑战并重新考虑，因为涉及效率和风险等问题。

进度评估

以下**验证点**将呈现此项工作的进展：

- ☐ 开源软件已成为选择新软件时的一个重要选项。
- ☐ 开源软件不再被视为额外的或危险的选项。
- ☐ 开源软件已成为“主流”选项。
- ☐ 核心参与者充分相信开源解决方案具有值得投资的战略优势。
- ☐ 可以证明，基于开源解决方案的总体拥有成本可以给您的组织机构提供一个比替代方案更高的价值。
- ☐ 有评估表明，供应商独立性可以节省资金或在未来可能节省资金。
- ☐ 有评估认为，解决方案的独立性可以降低（因非开放的数据格式导致的）迁移成本过高而无法更换解决方案的风险。

工具

目前，我们无法推荐任何与此项工作相关或涉及的工具。

建议

- 主动管理开源软件的使用需要对开源基础知识有一定的认识和理解，因为在任何开源软件相关的决策中都应该考虑它们。
- 比较所需的功能，而不是寻找已知闭源解决方案的替代品。
- 确保有技术支持和后续发展。
- 考虑解决方案的许可证对您的组织机构的影响。
- 让所有核心参与者了解开源优势的价值，而不仅仅是“节省许可费用”。
- 要诚实地、不要夸大开源解决方案的效果。
- 在决策过程中，同等重要的是评估不同的开源解决方案，以避免因错误的期望而感到失望，明确组织机构需要采取的行动以及解决方案的开放性所能带来的全部优势。这些问题必须逐个确认，以便组织机构能够根据自身的具体情况进行评估。

资源

- 开源的 5 大好处：赞助博客，但仍然很有趣，快速阅读。
- 衡量开源的隐性成本：IBM 赞助的开源软件支持成本概览。

5.4 开源企业软件

活动编号：GGI-A-20。

描述

此项工作是关于面向业务方向主动选择要由供应商或社区提供支持的开源解决方案。它还可能包括了关于如何选择开源商业应用软件的偏好策略。

尽管如操作系统、中间件、数据库、系统管理和开发工具等开源软件被 IT 专业人员普遍使用，但其在业务人员为主要用户的领域还未得到广泛认可。

此项工作涉及以下领域：办公套件、协作环境、用户管理、工作流程管理、客户关系管理、电子邮件、电子商务等。

可行性评估

随着开源成为主流，它的范围远远超出了操作系统和开发工具，它越来越多地进入上层信息系统，甚至进入了业务应用系统。识别哪些开源软件应用程序能够有效满足组织机构需求，并使其成为组织机构节约成本的首选方案，这一点至关重要。

然而，此项工作可能会增加一些二次培训和迁移的成本。

进度评估

以下**验证点**将呈现此项工作的进展：

- ☐ 制作开源解决方案的推荐列表，用于解决业务应用程序中的待解决问题。
- ☐ 制定开源商业应用软件选择偏好政策。
- ☐ 对在用的专有商业软件的开源软件平替品进行评估。
- ☐ 采购流程和招标要求明确指出对开源的偏好（如果法律上可行）。

工具

目前，我们无法推荐任何与此项工作相关或涉及的工具。

建议

- 与同事交流，向其他与您公司有类似经验的公司学习。
- 参与当地的行业活动，寻找开源解决方案和专业支持。
- 在确定购买付费支持方案前，先尝试一下社区版本和社区支持。

资源

- 什么是企业开源？：快速了解企业级开源。
- 101 个开源应用助力您的业务发展：面向业务的开源解决方案的指示性列表。

下一步工作建议

- GGI-A-33 - 与开源供应商合作 通过与开源专业人士合作，提升对开源资产的信心。
- GGI-A-43 - 开源采购政策 通过了解现有资产并制定明确的采购政策，可以优化企业对开源软件的使用。

5.5 管理开源技能和资源

活动编号：GGI-A-42。

描述

此项工作的重点是**软件开发**的技能和资源。它包括开发人员的技术和特定的开发技能，以及整体研发流程、方法和工具。

从开源生态和公共资源可以获得大量的开源技术相关的文档、论坛和讨论等内容。为了充分从开源中受益，必须建立当前资产和期望目标的路线图，以便为团队的开发技能、方法和工具建立一个连贯的计划。

应用领域

需要确定程序的应用领域，以及其如何提高代码和实际应用的质量和效率。例如，只有一个开发人员运维开源组件的情况和优化整个开源实践的全部开发生命周期的情况，此项工作的收益将会有所不同。

需要定义开源开发的范围：技术组件、应用程序、先进性或创造性新开发模式。以下是可以从开源中受益的开发实践包括：

- 云管理。
- 云原生应用程序，如何利用这些技术进行创新。
- DevOps、持续集成/持续交付。

类别

- 研发开源软件所需的技能和资源：知识产权、许可证、实践方法。

- 使用的开源组件、开发语言和相关技术进行软件研发所需的技能和资源。
- 使用开源的方法和流程所需的技能和资源。

可行性评估

开源工具在开发者群体中日趋流行。此工作避免了开发团队内部的异构工具激增。这有助于在该领域中定义使用策略。同时还有助于优化培训和积累经验。技能清单将用于招聘、培训和继任计划，以防关键员工离开公司。

我们需要一种方法来映射开源软件的开发技能。

进度评估

以下**验证点**将呈现此项工作的进展：

☐ 制作一份关于有开源开发流程（软件供应链）的描述
☐ 制作一份合理的研发资源的投入方案（或预期清单），
☐ 制作一个关于当前开发者的技能、教育程度和工作经验的技能概要清单，
☐ 制作一个针对技能缺陷的培训预期清单和方案，
☐ 制作一份关于开源开发实践的欠缺清单以及采用它们的方案。

建议

- 从简单开始，按照路线图逐步分析稳步推进。
- 招聘时，重点关注开源技能和经验。当人们已经拥有开源 DNA 后，总会比培训和指导他们更容易。
- 检查软件供应商和开源学校的培训计划。

资源

更多信息：

- Robert Tanner 对什么是技能清单？ 的介绍。
- 关于开源技能的文章：提升您水平和简历的五项开源技能

此项工作包含的技术资源和技能，如：

- **流行的开发语言**（例如 Java、PHP、Perl、Python）。
- **开源框架**（Spring、AngularJS、Symfony）和测试工具。
- 敏捷开发、DevOps 和开源的**开发方法和最佳实践**。

下一步工作建议

- GGI-A-28 - 人力资源视角 一旦组织机构内部认识到开源意识有助于获取开源资源，就应该让人力资源部门也认识到其价值对现有的和未来的员工的重要性。

6 信任目标

6.1 管理法律合规性

活动编号：GGI-A-21。

描述

组织机构需要实施法律合规流程，以确保其使用和参与开源项目的安全性。

在组织机构内部和整个供应链中，成熟且专业的法律合规管理意味着：

- 对知识产权进行彻底分析，包括许可证的识别和兼容性检查。
- 确保组织机构可以安全地使用、集成、修改和重新分发开源组件作为其产品或服务的一部分。
- 为员工和承包商提供一个关于如何创建和贡献开源软件的透明流程。

软件成分分析 *(SCA)*：法律和知识产权问题的很大一部分是来自于使用了互不兼容的许可证或与组织机构希望使用和重新分发的要求不兼容的组件。软件成分分析 (SCA) 是解决这些问题的第一步，因为“你需要先知道要解决的问题”。这个过程包括在物料清单（Bill of Material, BOM）文件中识别项目涉及的所有组件，包括构建和测试依赖项。

许可证检查：许可证检查的过程是使用自动化工具分析代码库并识别其中的许可证和版权。如果定期执行并在理想情况下集成到持续构建和集成链中，就可以尽早发现知识产权问题。

可行性评估

随着组织机构中对开源软件使用的日益普及，评估和管理潜在的法律风险至关重要。

然而，检查许可证和版权可能很棘手且成本高昂。开发者需要能够快速检查知识产权和法律问题。建立一个专门负责知识产权和法律问题的团队和合规专职人员，可以确保对法律问题进行积极和一致性的管理，有助于确保开源组件的使用和贡献，并提供清晰的战略愿景。

进度评估

以下**验证点**将呈现此项工作的进展：

- ☐ 为项目制作一个易用的项目许可证检查流程。
- ☐ 为项目制作一个易用的项目知识产权检查流程。
- ☐ 在组织机构内设置负责法律合规工作的团队或人员。
- ☐ 为组织评估法律合规性设定定期议程。

设置验证点的其他方法：

- ☐ 有一个易用的许可证检查流程。
- ☐ 有一个易用的法律/知识产权团队。
- ☐ 所有项目都要为使用和贡献项目的人提供所需的信息。
- ☐ 在团队中指定一位联系人负责解答与知识产权和许可证相关的问题。
- ☐ 指定一位合规专职人员负责知识产权和许可证事宜。
- ☐ 设置一个专业团队负责解答与知识产权和许可证相关的问题。

工具

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

建议

- 让人们了解与业务目标相冲突的许可证相关风险。
- 为项目制定一个简单的解决方案，以便在其代码库上设置许可证检查。
- 传达其重要性并帮助项目将其添加到其持续集成研发流程中。
- 提供项目结构的模板或官方指南。

- 设置自动检查以确保所有项目都符合指南要求。
- 考虑进行内部审计，以识别公司基础设施的许可证。
- 为每个团队至少一名人员提供基础的知识产权和许可证培训。
- 为管理者提供全面的知识产权和许可证培训。
- 建立一个流程，将知识产权和许可证问题上报给管理者。

请记住，合规并不仅仅是法律，它还涉及到知识产权。因此，这里有几个问题有助于了解法律合规的重要性：

- 如果我没有遵守许可证条件发布了开源组件，那么我就侵犯了许可证。（法律后果）。
- 如果我在一个希望发布或发行的项目中使用了开源组件，那么该许可证可能会要求我公开我不希望开源的代码元素--> 对我公司战略优势和第三方的保密性造成影响（法律后果）。
- 这是个公开讨论的话题，关于我想使用开源许可证发布的项目是否可以授予相关知识产权（知识产权后果）。
- 如果我在任何专利程序**之前**将项目开源，则**可能**无效了与该项目相关的专利申请（知识产权后果）。
- 如果我在任何专利申请程序**之后**将项目开源，则**可能**认可了与该项目相关的（防御性）的专利申请（知识产权后果）。
- 在引入具有复杂依赖性的多组件的复杂项目中，大量开源许可证的共存可能会导致许可证之间的不兼容性（法律后果）（参见活动 GGI-A-23-管理软件的依赖性）。

资源

- 现有开源软件合规性群组页面 上有详细的工具列表。
- 针对企业开源合规实践的建议。Linux 基金会的 Ibrahim Haddad 撰写的一本关于企业开源合规实践的书。OpenChain 项目

下一步工作建议

- GGI-A-24 - 管理关键指标 关注法律合规问题及其流程和结果的可见性和可度量性。这有助于人们在此过程的尽早理解其重要性。

6.2 管理软件漏洞

活动编号：GGI-A-22。

描述

一段代码的安全性取决于其最不安全的那部分。最近的案例（如 heartbleed2、equifax3 等）已经证明了检查组织机构非直接开发的那部分代码的漏洞的重要性。其暴露的后果包括数据泄露（会带来巨大的声誉受损的负面影响）、勒索软件攻击和业务停服威胁。

众所周知，开源软件比专有软件具有更好的漏洞管理，主要是因为：

- 更多双眼睛时刻盯着发现并解决开放代码及其流程中的问题。
- 开源项目可以更快地修复漏洞并发布补丁和新版本。

例如，一份来自白宫的关于专有软件研究报告指出，在开源组件中发现的 95% 的漏洞在其进行分析的同时就已经发布了修复程序。因此，真正的问题是要如何 ** 更好地从代码库和依赖性上管理漏洞 **，而不是讨论它们是开源的还是闭源的。

为了降低这些风险，必须制定一个软件资产评估计划并定期执行漏洞检查流程。实施工具应向受影响的团队发出警报、管理已知漏洞并防止来自相关依赖软件的威胁。

可行性评估

任何使用软件的公司都必须重视以下方面的漏洞：

- 基础设施类（例如云基础设施、网络基础设施、数据存储等），
- 业务应用类（HR、CRM 工具、组织机构内部与客户相关的数据管理）、
- 内部代码类：如公司网站、内部开发项目等、
- 以及所有直接和间接的软件和服务依赖的组件。

在问题出现之前，漏洞管理的投资回报率（ROI）鲜为人知。人们必须考虑到重大数据泄露或服务停摆的后果，并以此来预估漏洞管理的真实成本。

同样，必须不惜一切代价避免公司内部出现隐瞒安全相关问题和保密的文化。相反，有关漏洞状态的信息必须被共享和讨论，直到从开发人员到高级管理者中找到最合适的人并得到最佳应对方案。

通过谨慎管理软件漏洞来预防网络攻击的好处是多方面的：

- 避免声誉受损风险；
- 避免漏洞攻击带来损失（DDoS 公司、勒索软件、被攻击后重建信息系统所需的时间）；
- 遵守数据保护法规。

开源软件的漏洞管理只是广义网络安全流程中的一部分，该流程旨在解决组织机构内部的系统和服务的安全问题。

进度评估

应该有专职人员或专职团队来进行漏洞监测和开发人员可依赖的易用流程。漏洞评估是持续集成开发过程的标准环节，人们可以在专用面板中监测当前的风险状态。

以下**验证点**将呈现此项工作的进展：

- ☐ 此项工作应覆盖所有内部软件和服务的已知漏洞都被评估和监控。
- ☐ 此项工作应覆盖软件开发流程中的专用工具使用和专业流程的实施，以防止在日常开发过程中的引入问题。
- ☐ 由专人或团队负责评估 CVE 漏洞的爆发风险。
- ☐ 由专人或团队负责将 CVE 漏洞信息发送给相关人员（系统运营、开发运营、开发人员等）。

工具

- GitHub 工具
  - GitHub 提供了指南和工具来保护平台上托管的代码。有关更多信息，请参阅 GitHub 文档。
  - GitHub 提供了 Dependabot 来自动识别依赖项中的漏洞。
- Eclipse Steady 是一款免费的开源工具，它能够分析 Java 和 Python 项目中的漏洞并帮助开发人员降低漏洞风险。
- OWASP dependency-check：是一款开源的漏洞扫描工具。
- OSS Review Toolkit：是一款开源编排器，能够从配置好的漏洞数据服务中收集所使用的依赖组件的安全建议。

资源

- CVE 的 MITRE 漏洞数据库。另请参阅 NVD 的 NIST 安全数据库 以及 CVE 详细信息 等卫星资源。
- 另请检查 Google 的这项新举措：开源漏洞。
- OWASP 工作组在其网站上发布了来自商业和开源领域的漏洞扫描程序列表。
- J. Williams and A. Dabirsiaghi. 《不安全图书馆的不幸现实》，2012 年。
- 检测、评估和缓解开源依赖项中的漏洞，Serena Elisa Ponta、Henrik Plate 和 Antonino Sabetta，经验主义的软件工程第 25 卷，第 3175–3215 页（2020 年）。
- 一个手搓的开源软件漏洞修复数据集，Serena E. Ponta、Henrik Plate、Antonino Sabetta、Michele Bezzi、Cédric Dangremont。还有一个实现上述数据集的正在开发的工具包。

下一步工作建议

- GGI-A-24 - 管理关键指标 让已发现的漏洞可见。这将有助于人们清楚他们的软件有多么安全或多不安全，并证实选择适当依赖组件的重要性。

[^heartbleed]：https://www.wikipedia.org/wiki/Heartbleed

6.3 管理软件的依赖性

活动编号：GGI-A-23。

描述

依赖项识别程序用于查找代码库中实际使用的依赖组件。因此，组织机构必须建立并维护其代码库的已知依赖组件列表，并关注已认定供应商的后续更新。

建立和维护已知依赖组件列表是下列工作的核心推动因素和先决条件：

- 知识产权和许可证检查：某些许可证不能混合使用，即使作为依赖组件也是如此。人们必须了解其依赖关系才能评估相关的法律风险。
- 漏洞管理：最脆弱的那部分软件决定了整个软件的脆弱程度（可参考Heartbleed 缺陷案例）。人们必须了解其依赖关系才能评估其相关的安全风险。
- 软件的生命周期和可持续性：依赖组件社区的活跃程度对于 bug 修复、优化和新功能开发是一个的积极特征。
- 根据“成熟度”标准审慎地选择所使用的依赖组件：其目标是使用安全的，拥有健全的运维良好的开源组件库，其社区具备健康、活跃、反应迅速，以及愿意接受外部贡献的特点。

可行性评估

识别和跟踪依赖组件是降低与所有代码复用相关风险的必要步骤。此外，实施工具和流程来管理软件依赖关系是妥善管理产品质量、合规性和安全性的先决条件。

要考虑以下问题：

- 如果软件被破坏、攻击或被起诉，公司的风险是什么（成本、声誉等）？
- 代码库对于人员、该组织机构或业务是否至关重要？
- 如果应用程序所依赖的组件改变了，其代码仓库会发生什么？

最基本的首要步骤是进行一次软件成分分析（SCA）。为了展开全面的 SCA 分析或依赖关系映射，可能需要业内专业的咨询公司支持。

进度评估

以下**验证点**将呈现此项工作的进展：

- ☐ 对所有公司内部开发的代码中识别依赖组件。
- ☐ 对所有公司内部执行的外部代码识别依赖组件。
- ☐ 将一个容易配置的软件组成分析工具（SCA）或依赖组件识别程序添加到项目的持续集成研发流程中。
- ☐ 使用依赖组件的分析工具。

工具

- OWASP 依赖项检查：dependency-Check 是一种软件成分分析 (SCA) 工具，尝试检测项目依赖项中包含的公开披露的漏洞。
- OSS Review Toolkit：一套帮助审查开源软件依赖项的工具。
- Fossa：快速、便携、可靠的依赖性分析。支持许可证和漏洞扫描。语言无关；与 20 多种构建系统集成。
- Software 360。
- Eclipse Dash 许可证工具：获取依赖项列表并请求 ClearlyDefined 检查其许可证。
- FOSSology 项目：FOSSology 是一个开源项目，其使命是促进开源许可证的合规性。

建议

- 定期对依赖组件和知识产权进行审核，以降低法律风险。
- 理想情况下，将依赖组件管理集成到持续集成研发流程中，以便尽快识别并修复问题（新的组件依赖关系、许可证不兼容等）。
- 持续跟踪与依赖组件相关的漏洞信息，及时让用户和开发人员了解这些情况。
- 通报与错误许可证相关的风险。
- 为项目制定一个简单的解决方案，以便在其代码库上设置许可证检查。
- 传达其重要性并帮助项目将其添加到其持续集成研发流程中。
- 针对依赖组件的相关风险设置明确的关键绩效指标（KPI）。

资源

- 现有的OSS 许可的 OSS 许可证合规性工具页面。
- 自由开源软件许可证合规性：软件成分分析工具，作者：Philippe Ombredanne, nexB Inc.
- 软件可持续性成熟度模型。
- CHAOS：开源社区健康度分析开源软件。

下一步工作建议

- GGI-A-21 - 管理法律合规性 在能够跟踪知识产权和许可证不兼容之前，需要识别其开源软件中的所有依赖组件。
- GGI-A-22 - 管理软件漏洞 在能够跟踪其代码资产中的漏洞之前，需要识别其开源软件中的所有依赖组件。

6.4 管理关键指标

活动编号：GGI-A-24。

描述

此项工作收集并监控的一系列指标，为日常的管理决策和专业管理开源软件的战略提供了支撑。

开源软件的关键指标构成了治理计划有效实施的背景。此项工作包括选择了一些面向团队和管理层发布的指标，并定期通过新闻简报和公司新闻等途径来发送更新内容。

此项工作需要：

- 与利益相关方讨论并确定计划的目标
- 实施与基础设施开发相连接的测量工具和数据采集工具
- 为利益相关方和所有参与人员发布至少一个面板。

指标必须为从相关来源采集的数据。所幸的是，我们有大量开源软件工程的资源。示例资源的来源包括：

- 开发环境、CI/CD 开发流程、
- 人力资源部门，
- 测试工具和 SCA 软件成分分析工具，
- 代码仓库。

指标示例包括：

- 按照许可证类型显示，已解决的依赖项数量。
- 过期的或存在安全漏洞的依赖项的数量。
- 检测到的许可证和知识产权问题的数量。
- 对外部开源项目的贡献次数。
- 缺陷修复的时间。
- 单个开源组件的贡献者数量，有效提交次数等。

此项工作旨在定义这些要求和度量标准，并制作一个显示面板，以简单高效方式来显示该工作的主要指标。

可行性评估

关键指标有助于理解和更好地管理已经投入到开源软件的资源，有助于评估结果，以便高效沟通并充分获得投资收益。通过广泛沟通，越来越多的人会跟进这项工作，并将置身其中，最终使其成为整个组织机构的重点工作和发展目标。

虽然每项工作都有评估标准来回答过程中所触及问题，但我们仍需要用数字和量化指标来进行监测。

无论是小型初创企业还是大型跨国公司，关键指标都有助于团队集中精力和监控绩效。衡量标准至关重要，因为它们是对决策的重要支撑条件，是监督已做出决策的基础工具。

通过简单实用的数字和图形，组织机构全体成员将能够跟踪和同步相关的开源工作，使其成为共同关注点和协同行动。这也有利于让不同参与者更容易地参与进来为项目做贡献，并获得收益。

进度评估

以下**验证点**将呈现此项工作的进展：

- ☐ 制定评估标准列表和数据采集方法。
- ☐ 使用工具进行数据采集、存储、处理和指标显示。
- ☐ 所有参与者都可以通过一个通用显示面板来查看该工作取得的进展。

工具

- 来自 Bitergia 的 GrimoireLab。
- 当根据确定目标设置了适当的连接器时，如 elasticsearch、grafana、R/Python 可视化等通用 BI 工具也是个不错的选择。

建议

- 制定明确的开源治理的目标和路线图。
- 在组织机构内部就具体行动和进展状态保持沟通。
- 邀请大家参与到 KPI 的制定过程，以确保
  - KPI 得到大家完全理解，
  - 确保 KPI 能够全面反映需求
  - 确保 KPI 被大家重视和遵循。
- 构建至少一个可以被每个人查阅的显示面板（例如在房内的公共屏幕上），展示关键指标以显示进展和整体情况。

资源

- CHAOSS 社区 有许多与开源指标相关的优秀参考资料和资源。
- 从 OW2 市场就绪程度方法中查看项目属性的指标。
- Liz Laffan 的衡量开放性的新方法：开放治理指数 是一本关于开源项目开放性的有趣读物。
- 治理指标：用户指南 是联合国关于治理指标的指南。虽然它适用于国家的民主、腐败和透明度，同时也适用于治理的衡量和指标的基础知识非常值得一读。

下一步工作建议

- GGI-A-37 - 开源助力数字化转型 开源助力数字化转型可以使用生成的指标作为通用开源策略的一部分。

6.5 进行代码审查

活动编号：GGI-A-44。

描述

代码审查是一项常规任务，涉及到在向客户发布产品或交付项目之前对应用程序源代码进行的手动/自动审查。对于开源软件而言，代码审查不仅仅是为了及时发现错误，更是一种在团队层面进行协作开发的综合方法。

代码审查应适用于内部开发的代码以及从外部资源获取的复用代码，因为它提高了对代码的总体信心并加强了所有权属性。这也是提升团队内成员的全球化技能和知识，促进团队协作的绝佳方式。

可行性评估

当组织机构开发软件或复用外部软件片段时，代码审查非常重要。尽管代码审查是软件工程流程中的一个标准步骤，但在开源背景下，代码审查会带来一些特定的好处，例如：

- 在发布内部源代码时，确保遵守适当的质量准则。
- 在为现有开源项目做贡献时，确保遵守目标项目的指南。
- 公开的文档也会相应地更新。

这也是推行和强化公司法律合规政策规则的绝佳机会，例如：

- 不得删除复用的开源代码中的现有许可证头文件或版权声明。
- 未经法律团队事先许可，请勿从 Stack Overflow 复制和粘贴源代码。
- 在需要时，请包含正确的版权声明。

代码审查将为代码带来信任和信心。如果人们担心软件产品的质量或潜在风险，他们应该进行同行评审和代码评审。

进度评估

以下**验证点**将呈现此项工作的进展：

- ☐ 开源代码审查被认定为必要步骤。
- ☐ 开源代码审查已被列入工作计划（定期或在关键节点进行）。
- ☐ 进行开源代码审查的流程已得到团队整体的参与和认可。
- ☐ 开源代码审查成为开发流程的标准组成部分。

建议

- 代码审查是一项集体任务，在良好的协作环境中效果更好。
- 勇敢地使用开源世界的现有工具和模式，代码审查几十年来一直都按其标准操作。

资源

- 什么是代码审查？：Red Hat 的开放实践库中关于代码审查的指南读物。
- 代码审查的最佳实践：从另一个有趣的角度阐述代码审查的意义。

下一步工作建议

- GGI-A-26 - 贡献开源项目 代码审查是开源项目的常见做法，因为它能提升代码质量和促进知识共享。参与代码审查的贡献者们通常更乐于接受外部贡献和合作。

7 文化目标

7.1 推广开源开发的实践

活动编号：GGI-A-25。

描述

此项工作的目的是在开发团队中定义、积极推动和进行开源实践。

作为起点，可以考虑关注以下内容：

- 用户和开发者文档。
- 在公开可访问的代码仓库中妥善组织项目。
- 推动并执行可控的代码复用。
- 提供完整的最新产品文档。
- 配置管理：Git 工作流程、协作模式。
- 发布管理：尽早且频繁地发布稳定版本和开发版本。

开源软件项目有一种独特的集市模式运作方式。为了促进这种协作和思维方式，推荐采取以下方法实践，以便于第三方开发者可以进行协作和分布式开发以及参与贡献...

社区文档 确保公司内的所有项目都能提供以下文档：

- README —— 项目的简介、如何进行互动以及相关的资源链接。
- 贡献——为愿意参与贡献的人提供的介绍。
- 行为准则 —— 在社区内可接受或不可接受的行为准则。
- LICENSE—— 本代码仓库的默认许可证。

代码复用 代码复用是欧洲自由软件基金会提出的一项倡议，旨在提高软件的复用率，简化开源软件和许可证合规性。

可行性评估

尽管这在很大程度上取决于团队对开源软件基本常识的认知，但进行人员培训并创建规范的流程总是有益的。当出现以下情况时这一点尤其重要：

- 潜在的用户和贡献者不详、
- 开发人员不习惯开源开发方式。

进度评估

以下**验证点**将呈现此项工作的进展：

- ☐ 该项目制定了一份开源实践清单，以供参考。
- ☐ 监控项目以保持其与实践一致。
- ☐ 开发团队已经建立了遵守开源实践的意识。
- ☐ 定期评估新的开源实践，并努力地执行下去。

工具

- 软件复用辅助工具 可帮助版本库符合REUSE 实践。它可被纳入许多开发流程，以确认当前状态。
- ScanCode能够列出存储库中的所有社区和法律文档：参见 功能描述。
- GitHub 有一个很好的功能来检查丢失的社区文档。可以在存储库页面 >“洞察”>“社区” 中找到。

建议

- 开源实践的列表应根据项目的背景和领域来确定，并且应该以持续改进的方式定期重新评估。应监控和定期评估这些实践，以跟踪进展情况。
- 对人员进行有关复用开源（作为消费者）和反哺开源（作为贡献者）的培训。
- 鼓励如 #14 那样实施软件的复用。
- 建立流程来管理与软件复用和软件贡献相关的法律风险。
- 明确鼓励人员为外部项目做出贡献。

- 提供项目结构的模板或官方指南。
- 设置自动检查以确保所有项目都符合指南要求。

资源

- OW2 的开源实践案例清单 来自市场成熟度评估方法。
- 软件复用官方网站 包含规范、教程和常见问题解答。
- GitHub 社区指南。
- 使用 GitHub 配置管理的实践案例。

下一步工作建议

- GGI-A-42 - 管理开源技能和资源 您可以将确定的开源开发实践列表添加到一般培训资料中。
- GGI-A-44 - 进行代码审查 代码审查是开源开发实践的基本要素。

7.2 贡献开源项目

活动编号：GGI-A-26。

描述

为开源项目做出贡献是开源治理良策的基本原则之一。关键点是避免成为一个简单被动的消费者，而是要回馈项目。当人们出于自己的目的添加功能或修复错误时，他们应该使其具有足够的通用性，并以此为项目做出贡献。必须给予开发人员时间来做出贡献。

此项工作包括以下内容：

- 与上游开源项目合作。
- 提交错误报告和功能请求。
- 贡献代码和修复错误。
- 参与加入社区邮件列表。
- 分享经验。

可行性评估

此项工作的主要收益包括：

- 随着人们开始贡献并参与到开源项目中，它增加了公司内部对开源的整体认知和对开源承诺。他们将感受到公益事业的魅力，同时还提高了个人声誉。
- 随着公司通过对项目的贡献逐步增加，公司的知名度和声誉也将不断提升。这表明公司实际上已经融入开源，回馈了社区，并促进了公平和透明。

进度评估

以下**验证点**将呈现此项工作的进展：

- ☐ 为愿意做出贡献的人来，提供一条清晰且正式的途径。
- ☐ 鼓励开发人员为其使用的开源项目回馈贡献。
- ☐ 制定流程来确保开发人员贡献的法律合规性和安全性。
- ☐ KPI（关键绩效指标）：个人开发者、团队或其他实体的外部贡献量（如，代码、邮件列表、Issue 等）。

工具

持续跟进贡献可能很有用，既可以持续跟进贡献的具体内容，还可以就公司的发展方向进行沟通。显示面板和活动跟踪软件（Tracking Software）均可用于此目的。查看：

- Bitergia 的 GrimoireLab
- ScanCode

建议

过以下方式鼓励组织机构内部人员为外部项目做出贡献：

- 让开发者有时间编写通用的、经过充分测试的错误修复性代码和功能性代码，并将其反馈贡献给社区。
- 为开发者提供有关回馈贡献开源社区的培训。培训既要涉及技术能力（提高团队知识水平），又要涉及社区常识（开源社区的文化、行为准则等）。
- 提供有关法律、知识产权和技术问题的培训，在公司内设立专属联络人，帮助员工回复这些领域的疑问。
- 为已发布的作品提供激励。
- 注意，来源于公司或相关组织机构的贡献将反映他们的代码质量和参与贡献度，因此请确保你们开发团队提供的代码足够优秀。

资源

- Linux 基金会的 CHAOSS 提供了一些关于如何在开发过程中跟踪贡献的工具和指南。

下一步工作建议

- GGI-A-31 - 公开主张使用开源 既然该组织做出了一些公开可见的贡献和承诺，就开始沟通吧！
- GGI-A-24 - 管理关键指标 使对开源软件项目的贡献可见且可衡量。这有利于项目的推广，提升参与人员的士气。
- GGI-A-27 - 融入开源社区为开源软件社区做出贡献是融入社区的第一步。人员一旦开始贡献，他们就会更多地参与项目的健康发展和治理，并最终成为维护者，以确保项目按照可持续的健康的路线图发展。
- GGI-A-29 - 参与开源项目 开源项目重视精英管理。现在你已经对代码和流程有了很好的理解，可以参与该项目并使你的贡献更加规范。
- GGI-A-36 - 开源促进创新 为开源软件项目做出贡献并与外部贡献者互动有利于促进创新。
- GGI-A-39 - 上游优先 如果开源项目的更新能够定期且系统化地集成到上游项目中，那么对这些项目的贡献就非常有意义。

7.3 融入开源社区

活动编号：GGI-A-27。

描述

此项工作旨在培养开发人员对优秀开源社区的归属感。任何社区都一样，个人和组织机构必须参与并为整个社区回馈贡献。这强化了参与者之间的关系，并为整个开源生态带来可持续性的发展能力和活力。从技术的角度上看，它允许选择项目的优先级和路线图，有助于提升社区常识和技术意识。

此项工作包括以下内容：

- **确定**值得参加的活动。人际交往、学习新技术和建立关系网是充分发挥开源优势的关键因素。
- 获得**基金会会员身份**。开源基金会和行业组织是开源生态的重要组成部分。它们为项目提供技术和产业资源，是多方讨论常见问题和解决方案，以及制定标准的中立场所。
- 关注**工作小组**。工作小组是中立协作的工作场所，在此技术专家们可以就如物联网、建模或科学等特定技术话题进行交流互动。这是一种既经济又高效的工作机制，可以共同解决常见的或特定领域的问题。
- **参与制定预算**。最后要说的是，资金是推动力。规划好所需的费用，为参与人员留出带薪工作时间，预期好后续工作，避免几个月后项目因资金短缺而被迫中止。

可行性评估

当与开源社区广泛合作时，开源的效果最好。这有助于错误修复、解决方案共享等。

这也是企业表达认可开源价值的有效途径。就企业参与社区的情况展开沟通，对企业的声誉和开源生态都很重要。

进度评估

以下**验证点**将呈现此项工作的进展：

- □ 起草一份人员可以参加的开源活动清单。

- ☐ 团队成员的公开演讲要有监控机制。
- ☐ 人员可以提交参与活动的请求。
- ☐ 人员可以提交项目以申请赞助。

建议

- 以调研方式了解大家喜欢哪些开源活动，以及哪些活动对他们的工作最有帮助。
- 建立内部沟通机制（新闻通讯、资源中心、邀请函等等），让大家了解这些沟通方式并参与其中。
- 确保这些沟通方式能够惠及各类人员（开发人员、管理人员、支持人员.....），而不仅仅是高级管理者。

资源

- 是什么激励开发人员为开源软件做出贡献？ Michael Sweeney 在 clearcode.cc 上发表的文章。
- 为什么公司要为开源做出贡献VMWare 的 Velichka Atanasova 撰写的文章。
- 为什么你的员工应该为开源做出贡献 来自 CloudBees 的 Robert Kowalski 的精彩文章。
- 公司支持开源的七种方法 Simon Phipps 为 InfoWorld 撰写的文章。
- 开源活动：开源的生命力 RedHat 的 Donna Benjamin 撰写的文章。

下一步工作建议

- [GGI-A-28 - 人力资源视角](https://ospo-alliance.org/ggi/activities/human_resources_perspective) 如果组织机构属于某个开源软件社区，那么以你所参与的社区名义，更容易吸引技术人员。。
- GGI-A-31 - 公开主张使用开源 现在你正式支持一些开源软件社区，请让大家知道！这对你的声誉有好处，对项目的健康发展和传播也有好处。

7.4 人力资源视角

活动编号：GGI-A-28。

描述

转向开源文化会对人力资源工作产生深远的影响：

- **新流程和新合同**：新合同需要适应并促进外部贡献。这包括公司内已完成工作的知识产权和许可证问题，也包括员工或合同工掌控其自身项目的能力。
- **人才不拘一格**：与纯粹的私有企业人员相比，从事开源工作的人员通常会有不同的动机和心态。工作流程和思维方式需要适应这种以社区声誉为导向的范式，才能吸引新型人才并留住他们。
- **职业发展规划**：需要提供一个职业发展规划，培养和重视员工的技术能力和其他软性技能，以及企业所期望的能力（推动社区工作的协作能力、作为公司发言人的沟通能力等）。无论如何，人力资源将会在开源作为文化目标方面发挥关键作用。

劳动力对于长期致力于同一专有解决方案的开发人员来说，转向开源看起来是个很大的改变，并且需要适应。但对于大多数开发者来说，开源软件带来的只是好处。

如今，从中小学或大学毕业的开发人员都一直在使用开源。公司内绝大多数开发人员每天都在使用开源语言，导入开源库或代码片段。在程序中粘贴几行开源代码，确实比启动内部采购流程要容易得多，后者需要通过管理层链条上的多次审批。

开源使开发人员的工作变得更加有趣，因为通过开源，开发人员总是在寻找公司外部的同行的创新发明，因此可以始终处于技术的最前沿。

对于一个组织机构来说，需要制定一个人力资源战略：1、对现有员工提供进行技能培训或二次技能培训。2、反映并定位公司在招聘新人才方面的情况，当涉及到开源时，公司的吸引力是什么。

> “直接招募到具备开源精神的，熟悉代码且具备团队协作能力的人才是非常棒的。通过布道、培训和实习也是值得做的替代方案，但成本更高且耗时更长”。
>
> — 某开源软件供应商首席执行官

这说明直接雇用具有开源基因的人才是人力资源战略中值得关注一条快车道。

流程

- 建立或重新审视岗位描述（技术技能、软性技能、能力和经验）
- 培训计划：自我培训、正式培训、管理辅导、同行对标、社区文化
- 建立或重新审视职业规划：能力、关键成果/影响和职业发展步骤

可行性评估

1. 规范开发行为：问题可能不在于鼓励开发人员使用更多的开源，而是要确保他们安全地使用，遵守每种开源技术的许可证条款，并且不放弃传统的安全检查（开源代码行可能包含恶意代码），
2. 复审协作行为：与开源开发实践中，机遇在于将敏捷性和协作性扩展到组织机构中的其他业务线。企业内源通常促进了这些行为，但企业内源可能仅能实现了一半的开源文化
3. 企业文化：归根结底，这些与企业文化息息相关：开源可以成为开放、协作、伦理和可持续发展等价值观的旗帜。

进度评估

以下**验证点**将呈现此项工作的进展：

- □ 可通过培训介绍与开源有关的收益和限制（知识产权许可证条款合规性）。
- □ 每个开发人员、每个架构师、每个项目负责人（或产品负责人/业务负责人）都要了解与开源相关的收益和限制（知识产权许可条款合规性）。
- □ 鼓励开发人员为开源社区做出贡献，并对其负责，他们可以为此接受适当的培训。
- □ 技能和能力要体现在组织机构的岗位描述和职业发展路径中。
- □ 在人力资源评估过程中，要考虑到开发人员在开源领域获得的经验（对开源社区的贡献、参与内部合规流程、公司外部发言人等）。

工具

- 技能矩阵。
- 公共培训计划（如开源学校）。
- 来源：GitHub、GitLab、LinkedIn、Meetups、Epitech、Epita...
- 合同模板（忠诚条款）。
- 岗位描述（模板）和职业发展规划（模板）。

建议

现在大多数时候，开发人员已经了解到这些开源原则，并且愿意使用和参与开源软件的工作。然而，管理层仍应采取一些行动：

- 在招聘时优先考虑开源软件相关经验，即使开发人员所从事的工作仅与专有技术相关。随着数字化转型的推进，开发人员有朝一日一定会从事开源相关工作。
- 开源软件培训计划：每个开发人员、每个架构师、每个项目负责人（或产品负责人/业务负责人）都应该能够获得培训资源（视频或面对面培训），这些资源介绍了开源的收益以及在知识产权和许可证合规方面的限制。
- 应该为想要为开源社区做出贡献的、和想要参与社区治理的开发人员提供培训（如 Linux 认证）。
- 在人力资源对个人评估流程中认可员工（开发人员或架构师）对相关开源项目的贡献，例如对开源社区的贡献工作以及对知识产权许可证的合规工作。大多数项目都是共享的且与技术职业发展路径相匹配，即使有些情况可能比较特殊。
- 保密和公司立场：这需要解决沟通方面的问题（这对您的组织机构来说非常重要，可能会在您的年报中呈现）以及您沟通时的立场（开源贡献者可以成为您公司的发言人，包括媒体联系人）。

资源

- 关于人们在活动期间在公司外部发言的能力，请参阅活动 #31：“公开主张使用开源”。

7.5 上游优先

活动编号：GGI-A-39。

描述

此项工作旨在提高人们对回馈的益处的认识，并执行上游优先原则。

采用上游优先方法，开源项目的所有开发工作在质量和开放性方面，都应达到提交给项目核心开发人员并由他们发布所需的水平。

可行性评估

在编写代码时首先考虑上游社区，其结果是：

- 更高质量的代码，
- 已经准备好向上游提交的代码；
- 已经合并到核心软件中的代码；
- 已经与未来版本兼容的代码；
- 被项目社区和更多优秀商业公司的认可。

  上游优先比“向善”意义更大。这意味着你在该项目中拥有发言权，这意味着可预测性，这意味着你参与到掌控之中，这意味着你要主动采取行动而不是被动做出反应，这意味着你了解开源。马克西米利安米歇尔斯

进度评估

以下**验证点**显示了该活动的进展情况：上游先行是否已实施？

- ☐ 提交给第三方项目的拉取/合并请求数量显着增加。
- ☐ 已经起草了必须申请上游优先的第三方项目列表。

建议

- 找到在与上游开发人员交流互动最有经验的开发人员。
- 促进开发者和核心开发人员之间的交流互动（社区活动、黑客马拉松等）

资源

- 明确解释”上游优先”原则及其与文化目标相契合的原因：https://maximilianmichels.com/2021/upstream-first/。

  上游优先意味着每当解决上游代码副本中的问题（其他人可以从中受益）时，您都可以将这些更改贡献回上游，即向上游存储库发送补丁或发起拉取请求。

- 什么是软件开发的上游和下游？ 一个清晰的解释。
- 来自 Chromium OS 设计文档的解释：上游优先。
- 红帽关于上游和上游优先的优势。

下一步工作建议

- GGI-A-25 - 推广开源开发的实践 向上游回馈是一项重要的开源实践。将其作为企业开源实践的一部分，将有助于获得外部贡献、有助于内部整体质量提升和知识共享。

8 参与目标

8.1 参与开源项目

活动编号：GGI-A-29。

描述

此项工作旨在为那些对你很重要的开源软件项目做出重大贡献。这些贡献是在组织层面进行扩展和承诺的（而不是如活动 #26 贡献开源项目中所述的个人层面）。有多种形式，从直接资助到资源分配（例如人员、服务器、基础设施、沟通等），只要它们能够可持续和高效地惠及项目或生态系统。

此项工作是活动 #26 贡献开源项目的后续工作，将开源项目的贡献提升到组织层面，使它们更加可见、强大且有益。在此项工作中，贡献应该为开源软件项目带来实质性的、长期的改进：例如，开发人员或团队开发了急需的新功能、基础设施资产、提供新服务的服务器、接管广泛使用的开源项目分支的维护工作。

这个想法是预留一定比例的资源来资助那些编写和维护我们使用的软件仓库或项目的开源开发者。

此项工作意味着要对所使用的开源软件进行摸底，并评估其关键性，以决定支持哪个软件。

可行性评估

> 如果每家使用开源的公司至少做一点贡献，我们就会有一个健康的生态系统。https://news.ycombinator.com/item?id=25432248

支持项目有助于提升其可持续性，有助于其获取信息，甚至有助于其影响力和开发优先级（尽管这不应该是支持项目的主要原因）。

此项工作的潜在收益：确保错误报告具有高优先级，确保将开发会集成到稳定版本中。此项工作相关成本为：参与项目的时间、现金的投入。

进度评估

以下**验证点**将呈现此项工作的进展：

- ☐ 确认受益的开源项目。
- ☐ 决定支持方式，例如直接资金捐助还是代码贡献。
- ☐ 指定任务负责人。
- ☐ 已经做出了一些贡献。
- ☐ 贡献的结果已经被评估。

验证点参考了 OpenChain 自我认证 问卷：

- ☐ 我们制定了代表组织机构为开源项目做出贡献的相关政策。
- ☐ 我们有一套流程文件来管理开源贡献。
- ☐ 我们有一套流程文件帮助所有软件员工了解开源贡献的政策。

工具

一些组织机构提供了资助开源项目的机制（如果您的目标项目在其中，会很有帮助）。

- Open Collective。
- 软件自由保护协会。
- Tidelift。

建议

- 对组织机构来讲专注于项目非常重要：这些是你最希望通过你的贡献来帮助的项目。
- 聚焦社区项目。
- 此项工作要求对目标项目有最基础的了解。

资源

- 现在如何支持开源项目：一个简短的页面，其中包含有关资助开源项目的想法。
- 可持续的开源软件：有关可持续开源的对话空间

下一步工作建议

- GGI-A-26 - 贡献开源项目 参与开源计划的最自然方式是直接为项目做出贡献。作为回报，您将收到该贡献相关的宝贵反馈。
- GGI-A-30 - 支持开源社区 有多种方法可以支持对你的组织机构至关重要的开源社区。参与社区是发现和培养社区的好方法。

8.2 支持开源社区

活动编号：GGI-A-30。

描述

此项工作旨在与开源世界的相关参与组织机构展开互动。

需要通过以下方式实现：

- 加入相关的开源软件基金会（包括支付会员费用）。
- 支持并推广基金会相关活动。

此项工作包括为开发团队和 IT 团队分配一些时间和预算，支持他们参与开源社区。

可行性评估

开源社区处于开源生态发展的前沿。参与开源社区有以下几个好处：

- 它有助于了解最新信息并保持更新，
- 它提升了组织机构的形象，
- 会员资格带来的益处，
- 它为开源 IT 团队提供了额外的结构和动力。

成本包括：

- 会员费，
- 分配给参加社区活动的人员时间成本和差旅预算，
- 监督和遵守知识产权相关规范。

进度评估

以下**验证点**将呈现此项工作的进展：

- ☐ 组织机构成为开源基金会的正式成员。
- ☐ 组织机构参与到开源治理工作中。
- ☐ 组织机构开发的软件已提交到或已添加到基金会的代码库中。
- ☐ 会员资格在组织机构自身网站和社区（基金会）网站上得到双向承认。
- ☐ 对会员资格进行了成本/收益评估。
- ☐ 已指定与社区的固定联络渠道。

建议

- 加入一个与你的规模和资源相匹配的社区，即一个能听到你的声音的，且能将你视为贡献者的社区。

资源

- 查看 Linux 基金会的这个有用页面，了解加入开源社区的原因和方式。

下一步工作建议

- GGI-A-31 - 公开主张使用开源 现在你正式支持的一些开源软件社区，请让大家知道！这对你的声誉有好处，对项目的健康发展和传播也有好处。

8.3 公开主张使用开源

活动编号：GGI-A-31。

描述

此项工作旨在确认开源软件在信息系统、应用程序和新产品中的使用。

- 提供成功案例。
- 在开源活动上公开展示。
- 资助人员参与开源活动。

可行性评估

现在普遍认为，大多数信息系统都是在开源软件的基础上运行的，而新的应用软件大多是通过复用开源软件来实现的。

此项工作的主要好处是为开源软件和专有软件之间创建一个公平的竞争环境，以确保开源软件得到与专有软件同等的重视和专业的管理。

这样做的另一个好处是，它极大有助于提高开源软件生态的知名度，而且由于开源软件用户被认定为”创新者”，这也增强了组织机构自身的吸引力。

进度评估

以下**验证点**将呈现此项工作的进展：

- ☐ 被授权使用组织机构名称的商业开源供应商可以作为参考客户。
- ☐ 允许贡献者以组织机构的名义开展工作并发表他们的意见。
- ☐ IT 部门年报中公开提及开源软件的使用。
- ☐ 组织机构在媒体上（采访、开源行业活动等）解释其使用开源软件没有任何障碍。

建议

- 此项工作目的不是让该组织机构成为开源软件的激进团体，而是确保其公开承认使用开源软件没有障碍。

资源

- 欧洲核子研究中心公开宣称使用 OpenStack 的实例

8.4 与开源供应商合作

活动编号：GGI-A-33。

描述

此项工作目标是与为您提供重要软件的开源软件供应商签订安全合同。生产开源软件的公司和单位需要具备可以提供新功能的开发和维护的能力。需要他们拥有项目相关的专业知识，而且用户社区依赖于他们持续的贡献和商业反哺。

与开源供应商合作有多种形式：

- 订阅支持服务方案。
- 与当地服务公司签约。
- 资助开发。
- 支付商业许可费用。

此项工作意味着将开源项目视为值得付费的功能完整的产品，就像任何专有产品一样，而且通常成本低得多。

可行性评估

此项工作旨在确保组织机构中使用的开源软件得到专业支持。它有多个好处：

- 通过及时修复错误实现不间断服务。
- 通过优化安装实现服务提升。
- 澄清所使用软件的法律和商业授权情况。
- 及时获取信息。

- 稳定的成本预算。

成本显然是所选支持服务方案的费用。另一个成本可能是从外包给大型系统集成商转向与专业的中小企业供应商签订的精细合同。

进度评估

以下**验证点**将呈现此项工作的进展：

- ☐ 组织机构使用的开源得到商业支持服务作为后盾。
- ☐ 已为一些开源项目的签订了支持服务协议。
- ☐ 开源支持服务方案的成本是 IT 预算中的一个合理条目。

建议

- 尽可能寻找当地专业的中小型企业供应商。
- 警惕大型系统集成商转包给第三方专业供应商（转包给实际提供支持服务的专业的开源中小型企业供应商）。

资源

几个说明开源软件商业实现的链接：

- 快速了解商业开源。

8.5 开源采购政策

活动编号：GGI-A-43。

描述

此项工作是关于一个实施选择、获取、购买开源软件和服务的过程。它还涉及到开源软件及其配置的实际成本。开源软件乍一看可能是“免费”的，但它并非没有如集成、培训、维护和支持等内部成本和外部成本。

此政策要求在评估性价比时，要对比着考虑开源和专有解决方案，作为总体拥有成本和质量的最佳组合。因此，IT 采购部门应积极、公平地考虑开源选项，同时确保在采购决策中平等考虑专有解决方案。

当专有解决方案和开源解决方案之间没有显著的总体成本差异时，可以根据开源选项的内在灵活性明确表明开源偏好。

采购部门必须了解，为开源软件提供支持的公司通常缺乏参与采购竞争的商业资源，因此必须相应调整开源采购政策和流程。

可行性评估

建立专门的开源采购政策有以下几个原因：

- 商业开源软件和服务的供应正在增长且不容忽视，需要实施专门的采购政策和流程。
- 为企业信息系统提供的极具竞争力的商业开源业务解决方案越来越多。
- 在采用免费的开源软件组件并将其集成到应用程序之后，仍然需要获得内部或外部资源来维护这些源码。
- 开源软件解决方案的总拥有成本 (TCO) 一般情况下更低一些：在购买/升级软件时无需支付软件许可费、对服务提供商开放的市场、还可以自己完成部分或全部的解决方案。

进度评估

以下**验证点**将呈现此项工作的进展：

- ☐ 在新的提案征集中，主动要求提交开源方案。
- ☐ 采购部门有办法对开源解决方案与专有解决方案进行评估。
- ☐ 简化实施和记录开源软件和服务的采购流程。
- ☐ 已定义并记录了跨部门专业知识的审批流程。

建议

- “在创建流程时，一定要利用 IT、DevOps、网络安全、风险管理和采购团队的专业知识”。(摘自5 个开源采购最佳实践）。
- 竞争法案可能要求不要特别提及” 开源”。
- 首先确定所需的特定技术或产品，然后通过征求建议书（RFP）流程来寻找能够提供该技术定制化和支持服务的供应商。

资源

- 开源软件采购的决策因素：这不是一篇新文章，但仍然是英国开源软件观察（OSS-watch）同事撰写的一篇好文章。查看幻灯片。
- 5 个开源采购最佳实践：最近一篇关于开源采购的文章，提供了一些有用的提示。

下一步工作建议

- GGI-A-33 - 与开源供应商合作 定义采购政策可帮助你确定需要关注和参与的开源软件提供商和社区。

9 战略目标

9.1 制定企业开源治理战略

活动编号：GGI-A-16。

描述

在公司内部定义开源治理的高层战略可确保内部使用开源以及外部贡献开源和参与开源方法的一致性和可见性。它通过提供清晰且既定的愿景和领导力，使公司的沟通更加有效。

转向开源不仅带来了许多好处，还给公司带来了一些企业责任和企业文化上的改变。它可以影响商业模式，影响企业展示其价值和产品服务的方式，影响其在面对客户和竞争对手的立场。

此项工作包括以下任务：

- 设立一名开源事务官，并得到公司高管层面的资助和支持。
- 制定并发布清晰的开源路线图，明确目标和预期效益。
- 确保所有高管人员都了解它，并遵守相关规定。
- 在公司内部推广开源软件：鼓励大家使用开源，提升积极性和认知水平。
- 在公司外部推广开源软件：通过官方声明和沟通，并公开参与相关开源活动。

定义、发布和执行一个清晰的、一致的开源治理战略，有助于获得公司内所有人员的认同，为团队后续工作铺路。

可行性评估

以下是开展此工作的契机：

- 管理层没有做出协调努力，开源仍被视为一种临时解决方案。
- 虽然公司内已经有了一些开源行动，但尚未得到高管层的关注。
- 开源活动刚刚启动，面临重重阻力，尚未达到预期效果。

进度评估

以下**验证点**将呈现此项工作的进展：

- □ 公司有明确的开源治理章程。章程应包含：
  - 要实现什么目标，
  - 我们为谁而做，
  - 在此战略下能做什么，不能做什么。
- □ 开源路线图被全公司认可并广泛使用。

建议

- 设立一个团队负责在公司内定义和监控开源治理的流程。确保高级管理者对开源工作做出明确承诺。
- 在组织机构内部宣传开源战略，使其成为重点关注和真正的企业承诺。
- 确保从开发团队、管理层到基础架构团队都能充分理解开源战略和路线图。
- 随时通报进展情况，让大家了解组织机构在履行承诺方面的进展。定期公布最新情况和指标。

资源

- 开放式治理清单和参考资料。
- [开源作为数字主权问题，作者：OW2 首席执行官 Cédric Thomas，巴黎 Orange Labs 研讨会，2020 年 1 月 28 日](https://www.ow2.org/download/OSS_Governance/Level_5/2001-OSSetSouveraineteNumérique -RC3 .pdf)（仅有法语）。
- Linux 基金会提供的一系列管理企业内部开源的指南。
- [LF Energy 小组的开源战略文件的一个很好的例子](https://www.lfenergy.org/wp-content/uploads/sites/67/2019/07/Open-Source-Strategy-V1.0 .pdf)

下一步工作建议

- 详见本书 9.3 节GGI-A-35 - 开源和数字主权 企业开源治理的正确策略应该改善开源和数字主权。现在是在组织背景下定义这些的好时机。
- 详见本书 9.2 节GGI-A-34 -企业高级管理者的意识 需要企业高级管理者参与才能正确实施开源公司战略。教育他们并让他们参与是在这里取得成功的良好下一步。

9.2 企业高级管理者的意识

活动编号：GGI-A-34。

描述

只有通过将开源 DNA 融入到公司的战略和实际工作中，从最高层开始执行，公司的开源计划才能产生战略效益。如果管理层和高级管理者自己不参与其中，这种承诺就不可能实现。培训和开源思想还必须扩展到公司内外有关政策制定、决策制定和战略执行的全部人员。

这种承诺确保了实际改进、思维方式的转变和新举措能够得到来自领导层的一致的、友好的和可持续的支持，从而吸引员工更积极的参与。它塑造了外部参与者如何看待这个组织机构，会带来声誉和生态系统上的收益。这也是确保启动开源计划和中长期效益的方法。

可行性评估

此项工作在以下情况下至关重要：

- 组织机构已经制定了与开源管理相关的全球化目标，但却难以实现。如果没有高级管理者的充分理解和明确承诺，此活动不可能取得任何成果。
- 开源工作已经启动并正在取得进展，但高级管理者并没有及时跟进。

鉴于开源可以带来的对团队边界和文化的变革，我们希望除了临时使用开源之外的任何事情都需要一致且深思熟虑的方法，这一点显而易见。

进度评估

以下**验证点**将呈现此项工作的进展：

- ☐ 设立授权的开源治理办公室/开源治理官，有权在公司范围内制定统一的开源战略，并确保愿景明确。
- ☐ 管理层对开源软件战略有明确的、具有约束力的承诺。
- ☐ 管理层对其对开源工作的承诺进行透明的沟通。
- ☐ 管理层愿意讨论开源软件。可以就此征求不同意见或被质疑。
- ☐ 开源工作需要有适当的预算和资金。

建议

与此项工作相关的操作示例包括：

- 对核心高级管理者进行培训，揭开开源软件的神秘面纱。
- 明确且实际地支持开源软件的使用和策略。
- 在内部沟通中明确提及并支持开源软件计划。
- 在公共传播中明确提及并支持开源软件计划。

“开源是践行**企业文化**的**战略推动者**。”这句话是什么意思？

- 开源可以作为一种机制来打破供应商垄断地位，并降低软件采购成本。
  - 开源应该由**软件资产管理者**或**采购部门**来管理么？
- 开源许可证既确立了开源软件的自由使用权利，也带来了相应的**义务**。如果这些义务没有相应履行，可能会给组织机构带来法律、商业和形象上的风险。
  - 许可证的条款是否会暴露了本应保密的资源？
  - 是否会对我们组织机构申请的专利组合产生影响？
  - 项目团队如何得到与此相关的培训和支持？
- 回馈外部开源项目是开源最大的价值所在。
  - 公司应该如何鼓励和跟进这一点？
  - 开发人员应该如何使用 GitHub、GitLab、Slack、Discord、Telegram 或其他开源项目常用的工具？

  - 开源是否影响了公司的人力资源政策？
- 当然，这并不全是为了回馈，那我自己的开源项目呢？
  - 我是否准备好进行**开放式**创新？
  - 我的项目将如何管理**提交上来**的贡献？
  - 我是否应该为某个项目建设社区？
  - 我应该如何领导社区，社区其他成员应该扮演什么角色？
  - 我是否准备好将发展路线图的决策权转让给社区？
  - 开源能否成为减少公司团队间孤岛化的有效工具？
  - 我是否需要从一个公司到另一个公司进行开源转移？

下一步工作建议

- 详见本书 8.3 节GGI-A-31 - 公开主张使用开源高级管理者是组织机构的杰出代表，让他们就组织机构参与开源进行交流。

9.3 开源和数字主权

活动编号：GGI-A-35。

描述

数字主权可以定义为

> “个人和组织机构在数字世界中独立地、有意识地和安全地履行其职责的能力和机会。” —— 德国公共 IT 能力中心

为了正常开展业务，任何组织机构都必须依赖其他的合作伙伴、服务、产品和工具。审查这些依赖关系的链路和制约因素，可以使组织机构评估和控制对外部因素的依赖，从而提高其自主性和应变能力。

举例来说，供应商锁定是一个很强的依赖性因素，可能会妨碍组织机构的流程和增值，因此应该避免这种情况。开源是摆脱这种锁定的途径之一。开源在数字主权方面扮演着重要角色，它允许在解决方案、供应商和集成商之间可以更广泛选择，并对 IT 技术路线图进行更有效的管控。

应该指出的是，数字主权并不是一个信任问题：我们显然需要信任我们的合作伙伴和提供商，但如果这种关系是建立在双方意愿和相互认可的基础上，而不是建立在强制合同和施压的基础上，那么这种关系就会变得更好。

以下是提升数字主权的一些优势：

- 提高组织机构不受约束地条件下做出自主选择的能力。
- 提高组织机构对外部参与者和外部因素的应变能力。
- 在与合作伙伴和服务提供商打交道时提升谈判地位。

可行性评估

- 当前解决方案的迁移难度和迁移成本是多少？
- 解决方案提供商是否会因为我们别无选择而单方面提高价格？
- 解决方案提供商是否会在强加不想要的条件（例如许可证变更、合同更新）？

进度评估

以下**验证点**将呈现此项工作的进展：

- ☐ 对组织机构现有供应商和合作伙伴评估对其是否重度依赖。
- ☐ 对存在的这些依赖关系要有后备方案。
- ☐ 在研究新解决方案时，明确要求数字主权。

建议

- 识别来自服务提供商和第三方的重度依赖风险。
- 维护与关键服务相关的开源替代产品列表。
- 在选择使用新工具和新服务时增加一项要求，明确要求数字主权。

资源

- 数字主权与开源入门：第一部分 和数字主权与开源入门：第二部分，来自 Open-Sourcerers 网站。
- superuser.openstack.org 上有一篇关于开源在数字主权中的作用的精彩文章。下面是一小段摘录：

  > 数字主权是 21 世纪的一个关键问题，对欧洲来说尤其如此。开源在实现数字主权方面可以发挥重要作用，不仅可以让每个人都能获得必要的技术，还可以提供这些解决方案取得成功所需的管理透明度和互操作性。

- 欧盟对数字主权的看法，《开源、数字主权和互操作性：柏林宣言》。
- 联合国儿童基金会关于“数字主权开源”的立场。

9.4 开源促进创新

活动编号：GGI-A-36。

描述

> “创新是将想法付诸于实践，从而推出新的产品或服务，或改进所提供的产品或服务的过程。”
>
> — Schumpeter, Joseph A.

通过多样性、协作性和频繁的思想碰撞，开源可以成为创新的关键因素。来自不同领域不同背景的人会有不同的视角，并对已知问题提供崭新的、改进的甚至颠覆性的答案。人们可以通过倾听不同的观点并积极推动项目和话题的开放协作来实现创新。

同样，参与开放标准的制定和实施也能极大地促进优秀想法和实践的形成，从而改善公司的日常工作。此外，它还能让企业根据自身所需来推动和影响创新，并提高其全球知名度和声誉。

通过创新，开源不仅可以改进公司销售的商品或服务，还可以建立建全公司所希望的活跃的生态系统。

例如，通过开源的安卓系统，谷歌正在邀请成千上万家公司基于安卓系统构建他们自身的服务。因此，谷歌正在创建一个完整的生态系统，所有参与者都会从中受益。当然，只有很少有公司有足够的实力自行决定创建他们自己的生态系统。但有很多由企业联盟创建生态系统的例子。

可行性评估

评估贵公司与竞争对手、合作伙伴和客户相比所处的地位非常重要，因为如果公司与其客户、合作伙伴和竞争对手所使用的标准和技术偏离度较大，通常会带来风险。创新显然意味着与众不同，但与众不同的范围不应过大；否则，贵公司将无法从生态系统中其他公司开发的软件中受益，也无法从生态系统提供的商业机遇中受益。

进度评估

以下**验证点**将呈现此项工作的进展：

- ☐ 已经确定了对业务有影响的技术和开发这些技术的开源社区。
- ☐ 持续关注这些开源社区的技术进展和发布信息——甚至在公开发布之前我就知道他们的策略。
- ☐ 部分组织机构员工加入到这些开源社区，并通过提交代码贡献和参与社区治理等行为来影响他们的发展路线图和技术选型。

建议

在企业运营所需的所有技术中，您应该确认：

- 是否与竞争对手的技术相同，
- 是否为贵公司特定的技术。

持续关注新兴技术的最新动态。开源在过去十年中持续推动创新，许多强大的日常工具都来自开源技术（如 Docker、Kubernetes、Apache 大数据项目，以及 Linux）。不需要对所有事情都了如指掌，但应该尽可能了解前沿技术发展态势，以便找到有趣的新趋势。

允许并鼓励人们提出创新思想并向前推进。如果可能的话，为这些创新活动投入资源并助力发展壮大。依靠人们的热情和创新主动性，培育新兴的想法和趋势。

资源

- 归功于开源的 4 项创新。
- 开源的创新，来自 Dirk Riehle 教授。
- 开源技术，赋能创新。
- [开源创新可以在企业中发挥作用吗？](https://www.third Fivetwo.com/blog/can-open-source-innovation-work-in-the-enterprise)。
- 欧洲：开源软件战略。
- 欧洲：2020-2023 年开源软件战略。

9.5 开源助力数字化转型

活动编号：GGI-A-37。

描述

> “数字化转型是采用数字技术来转变服务或业务的过程，通过用数字化流程取代非数字化或手动流程，或用更新的数字技术取代较旧的数字技术。”（维基百科）

当数字化转型中最先进的组织机构通过业务部门、IT 部门和财务部门共同推动转型以推行数字化时，他们会重新考虑：

- 商业模式：具有生态系统的价值链、如 X 即服务、SaaS 模式。
- 财务：运营支出/资本支出、人员和外包成本。
- IT：创新、IT 的资产重组和技术升级改造。

开源是数字化转型的核心：

- 开源技术、敏捷开发、产品管理。
- 人员：协作、开放式沟通、开发和决策周期。
- 商业模式：先试后买和开放式创新。

就竞争力而言，最引人注目的可能是直接影响客户体验的流程。我们必须认识到，无论是大型企业还是初创公司，通过提供前所未有的客户体验，会极大地改变客户的期望。

客户体验和公司内的所有其他流程完全依赖于 IT 技术。每个公司都必须对其 IT 技术进行升级转型，这就是数字化转型的意义所在。尚未这样做的公司现在必须尽快实现数字化转型，否则就有被市场淘汰的风险。数字化转型是生存下去的条件。由于风险如此之高，公司不能完全将数字化转型交给供应商。每个公司都必须掌控其 IT 系统，这就意味着每个公司都必须掌握开源软件，因为没有开源软件就没有 IT 系统。

数字化转型的预期收益包括：

- 简洁的自动化实时相应的核心流程。
- 紧跟竞争态势变化的快速反应能力。
- 充分利用人工智能和大数据技术。

可行性评估

数字化转型可以通过以下方式进行管理：

- IT 相关部门：生产相关、业务支持相关（如 CRM 系统、计费系统、采购系统等）、支撑部门相关（如人力资源管理系统、财务系统、会计系统等）、大数据等。
- 支持 IT 的技术或流程的类型：基础设施（如云计算）、人工智能、流程（自制或外购、DevSecOps、SaaS）。

在特定 IT 细分市场或技术中引入开源表明你希望掌握该细分市场或技术，因为你评估认为该特定 IT 细分市场或技术对于公司的竞争力非至关重要。更重要的是，不仅要评估你的公司与竞争对手的相对地位，还要与其他行业以及主要参与者在客户体验和市场解决方案方面的地位进行比较。

进度评估

□ 第一级：现况评估

我已确定：

- 对我公司竞争力至关重要的信息技术领域

- 在这些领域开发应用程序所需的开源技术。因此我决定：
- 我要管理哪些内部的开发项目
- 我需要储备哪些开源专业知识。

□ 第二级：参与

在公司内部使用的某些选定的开源技术中，已有多名开发人员经过培训，最终被开源社区视为有价值的贡献者。而在某些选定的领域中，已经启动了基于开源的项目。

□ 第三级：常态化

所有项目在初始阶段都会系统地研究开源替代方案。为了便于项目团队研究这些开源替代方案，IT 部门应设立一个由架构师构成的核心团队和独立的预算，致力于为项目提供帮助。

关键绩效指标：

- KPI 1. 调研开源替代方案的比率：（项目数量/项目总数）。
- KPI 2. 选择开源替代方案的比率：（项目数量/项目总数）。

建议

除了标题之外，数字化转型是一种涉及一些根本性变革的思维方式，这种变革理念也应该（甚至主要）来自组织机构的高级管理层。管理层应积极推动新想法和风险管控，并尽可能更新现有流程以使其适应新理念。

热情是成功的重要因素。该领域核心参与者的手段之一是建立一个开放空间来收集新想法，人们在此可以提交并自由地研究关于数字化转型的想法。管理层应鼓励此类行为。

资源

- Eclipse 基金会：通过全球开源协作实现欧洲数字化转型。
- 欧洲：开源软件战略。
- 欧洲：2020-2023 年开源软件战略。

10 结论

正如前文所述，开源治理良策并不是一个终点，而是一个过程。我们需要关注这些公共资产，关注那些快速发展的社区和生态系统，因为它们将决定我们整体和个体的成功与否。

我们作为软件从业者和开源爱好者，致力于持续提升《开源治理良策》及其传播范围和影响力。我们坚信组织机构、个人和社区需要携手合作，共同构建一个庞大和卓越的共同体，让所有人都能受益。

邀请您加入 OSPO 联盟，为我们的工作做出贡献，传播信息，并在开源生态中成为一名开源大使，传递更好的开源意识和治理方法。这里有广泛的资源可用，从博客文章和研究报告，再到会议和在线培训课程。我们还在我们的网站 上提供了一系列有价值的材料，我们很乐意尽我们所能提供帮助。

让我们共同定义和建设《开源治理良策》的未来！

10.1 联系我们

与 OSPO 联盟联系的首选方式是，在我们的公共邮件列表 https://accounts.eclipse.org/mailing-list/ospo.zone 发布消息。您还可以在常规的开源活动中与我们讨论，参加我们每月的 OSPO OnRamp 网络研讨会，或与任何成员取得联系——他们会友好地为您对接到合适的人。中文版本翻译团队联系方式宋可为【skw@choss.cn□□□□□□】杨振涛【邮箱和微信二维码】，中文版翻译周期较短，不足之处还望大家及时反馈建议，十分感谢。

10.2 附录：自定义活动记分卡模板

自定义活动记分卡模板的最新版本可在 OW2 的 Good Governance Initiative GitLab 的 资源部分获得。

目标/活动 文化 1	**推广开源开发最佳实践**	**最后更新** 2025-03-08

自定义描述 *必做事项范围*

简要描述...

- 简要重点...
-

可行性评估 *该活动为什么相关*

- 关键痛点...
- 关键进展机会...

目标 *我们在本次迭代中的目标是实现什么*

- 目标 1...
- 目标 2...

工具 *技术, 活动中使用的工具和产品*

- 资源...

操作说明 *途径，获得活动进展的方法*

- 开始于...
-

关键结果 *我们将如何衡量本次迭代的成功*	**进度**	**分数**	**个人评估**
1. 关键结果 1（至少一个关键结果）	**xx%**	**.9**	个人评论
2. 关键结果 2	**xx%**	**.5**	个人评论
3. 关键结果 3	**xx%**	**.5**	个人评论
4. 关键结果 4（最多四个关键结果）	**xx%**	**.0**	个人评论
		.475	

时间表 *起止日期、里程碑*

- 此处注明日期

努力 *时间和材料预算*

- *未来三个月的时间分配*
- *预算津贴*

指派人员 *谁参与？谁领导？*

- XX 准备内部演示

问题 *困难、不确定性、障碍、关注点、依赖性*

- 关注 1...
- 关注 2...

状态 *活动进展如何*

对活动健康状况的个人评论

总体进度评级	**XX%**

说明

来自 GitLab 活动论坛的洞见
https://gitlab.ow2.org/ggi/ggi/-/blob/main/handbook/content/52_activity_44.md Copy/paste here the content of the Activity description from https://gitlab.ow2.org/ggi/ggi/ This will serve as a reference to help develop the Customized Activity Scorecard