ICS 35.100.15
CCS L 79

# 团　体　标　准

T/CESA XXXX—202X

# 信息技术 开源治理 第1部分：总体框架

Information technology—Open source governance—Part 1：Overall framework

征求意见稿

**在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。**

已授权的专利证明材料为专利证书复印件或扉页，已公开但尚未授权的专利申请证明材料为专利公开通知书复印件或扉页，未公开的专利申请的证明材料为专利申请号和申请日期。

202X-XX-XX 发布　　202X-XX-XX 实施

中国电子工业标准化技术协会　发布

# 目　　次

# 前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由华东师范大学提出。

本文件由中国电子技术标准化研究院、中国电子工业标准化技术协会归口。

本文件起草单位：

本文件主要起草人：

# 信息技术 开源治理 第1部分：总体框架

## 1 范围

本文件分别从标准体系、治理原则、治理框架、治理事项、事项规范五个方面给出了开源治理总体框架，为不同开源参与组织提供了完善、规范的开源治理框架和组成要素。

本文件适用于指导不同类型的组织对开源治理规范的编制与使用。

## 2 规范性引用文件

本文件没有规范性引用文件。

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**开源治理 governance of open source**

以开源为对象的治理，专注于开源活动体系及其效能和风险管理的一组治理规则。

注1：规则由治理主客体、组织结构和过程组成，以确保参与开源活动能够支撑组织的目标。

注2：开源项目治理是通过建立开源治理机构，协调内外资源，对开源软件的许可模式和开源的知识产权保护提供法律和法理的保障。开源项目通过制定治理流程和合规规范来保障其健康发展。

注3：开源社区治理是从人文的角度来保障社区的稳定和健康，社区文化、社区的领导力等是维护社区可持续发展的基础。

3.2

**治理要素 governance element**

实施开源治理应关注的关键治理对象或过程。

## 4 治理原则

为了促进组织有效、高效、合理地使用开源技术、贡献开源项目、发起并运营开源社区，宜尽可能在组织的开源战略规划、建设、运营和维护过程中，提出开源技术相关的治理要求，从而实现战略一致、风险可控、运营合规和绩效提升的目标。

组织可按本部分建立开源治理体系，形成文件并实施、持续改进并优化，确保开源技术使用、开源项目贡献和开源社区运营的效能和符合性。组织可以遵循以下治理原则：

a) 开源治理的最高决策者为开源治理最终负责人，决策层为开源治理主体；
b) 建立开源治理机构（如开源项目管理办公室），成员至少包括监督部门、业务部门和技术部门等；
c) 明确风险偏好和风险容忍度，防范因违规造成的重大财务和声誉损失、监管处罚、法律制裁等；
d) 确保利益相关方理解预期收益、支持开源投资，接受可能存在的风险及应对措施；
e) 建立开源治理的战略、制度、文化和创新机制，支撑组织业务模式变革、技术进步和管理提升。

## 5 治理框架

治理框架由治理要素以及要素之间的结构组成。开源治理要素包含治理的利益相关方、治理主体、业务需求、治理策略模型、治理事项、审查策略和资源七大要素，要素之间的结构见图1。

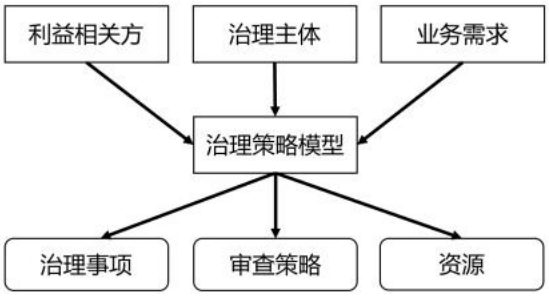


图 1　开源治理框架

开源治理框架能为各类组织机构提供构建开源治理体系的指导，包括企业、政府、基金会、行业协会、高校、科研机构等。该框架为组织提供了一个蓝图，使得治理主体负责对开源治理各个要素进行专业化管理。

### 5.1　治理主体

治理主体应通过开源的战略和方针，指导管理者对开源的治理体系进行完善，并对开源治理相关的方案和规划进行评估与修正、对开源治理绩效和符合性进行监督。组织应结合治理目标和原则，在开源治理实施的过程中，开展自我监督、自我评估和审查工作，并持续改进。

### 5.2　治理策略模型

治理策略模型是不同组织根据其情况（利益相关方、治理主体、业务需求等），制定对应的开源策略与目标，见图2。


图 2　开源治理策略模型

a)　技术采用：建立使用开源技术的初步意识，知道如何高效地使用开源创造价值，建立起使用开源的各项技能与经验积累；
b)　安全可信：安全可靠地使用开源技术，符合法律规范，能够胜任对合规、依赖、漏洞等管理职责，组织建立起使用与管理开源的信心；
c)　社区参与：加入开源社区，符合法规与社区行为准则，建立并享受开源协作的模式，个体开始形成对开源社区的归属感；
d)　社区参与：成为开源社区的一份子，符合法规与社区行为准则，建立并享受开源协作的模式，个体开始形成对开源社区的归属感；
e)　生态共建：开源作为组织愿景的核心要素，通过主动回馈开源社区，成为开源生态建设与可持续发展的重要成员，包括技术生态、用户生态、开发者生态等；
f)　战略创新：通过开放式创新与开放组织，将开源作为数字化转型与数字主权的基石。

### 5.3　治理事项

治理事项是在某个具体的开源治理参与策略指导下，解决某一具体的治理问题或主题的行动事项。不同的开源策略与目标，对应着不同的治理事项。

### 5.4 审查策略

审查策略是实施执行开源治理的重要方法与工具，是根据治理组织的特点和需求，围绕如何实现高质量开源治理而进行系统设计的策略，组织根据自身需要选择合适的审查策略模型进行实施。

### 5.5 资源

开源治理的支撑资源能够有效覆盖组织开展治理工作过程中所用到的工具与资源，包括人员、软件工具、基础设施、咨询、培训、文档等方面。

## 6 基本事项

基本事项对应开源治理框架中的治理策略模型，共五层，每层包含五个基本事项。不同的组织机构，根据不同的目标需求和开源参与程度，可进行有效的选取与组合使用，基本事项说明见表1。

**表 1 基本事项说明**

| 策略与目标 | 事项 | 说明 |
| --- | --- | --- |
| 技术采用 | 开源技能与技术使用的基础信息 | 对组织内使用、贡献、创建的开源组件基础信息进行整理 |
| | 开源能力增长路线图 | 建立基本的开源技术发展路线图 |
| | 开源技术采用的管理 | 了解开源技术的使用现状，并主动管理开源技术 |
| | 开源技术解决方案供应管理 | 在组织的业务领域中，主动选择开源技术供应商或开源社区提供的开源解决方案 |
| | 管理开源技术开发技能与资源 | 管理开发人员的开源技能、整体开发流程、方法和工具 |
| 安全可信 | 开源合规性管理 | 实施合法合规流程，确保使用和参与开源项目的合规 |
| | 软件漏洞管理 | 管理已知漏洞并防止来自软件依赖项的威胁 |
| | 软件依赖项管理 | 识别与管理代码库中使用的软件依赖项 |
| | 度量与指标管理 | 收集和监控关键治理事项的指标，为开源相关的日常管理决策和事务提供信息 |
| | 实施代码审查工作 | 在团队层面开展协作开发的代码审查工作 |
| 社区参与 | 积极推广开源最佳实践 | 在开发团队中定义、推广和实施开源最佳实践 |
| | 积极为开源项目和社区做贡献 | 鼓励为使用到的开源项目做贡献，避免成为简单的被动消费者 |
| | 建立成员对开源社区的归属感 | 培养开发人员对开源社区的归属感，为开源社区进行可持续性贡献 |
| | 促进人力资源部门对开源贡献的认可 | 使人力资源部门认识到开源贡献为组织带来的好处，并调整人力资源政策 |
| | 制定开源上游优先策略 | 提高组织人员对回馈和执行上游优先策略好处的认识 |
| 生态共建 | 制定组织层面参与开源项目与社区的策略 | 在组织层面推动开源贡献，使所有组织成员看见开源贡献的价值 |
| | 积极参与开源生态的持续建设 | 与开源生态中的各种组织机构进行互动融合 |

| 策略与目标 | 事项 | 说明 |
| --- | --- | --- |
| | 制定与开源技术供应商的高效合作策略 | 鼓励与重要的开源技术供应商签订商业合同，以为组织提供持续的维护，同时支持开源生态的持续发展 |
| | 公开声明组织使用到的开源项目情况，做到信息透明 | 公开声明在组织信息系统、应用程序或新产品研发中使用到的开源技术 |
| | 制定有利于开源生态发展的开源采购策略 | 建立高效的选择、获取、购买开源技术和服务的流程 |
| 战略创新 | 制定组织层面的开源战略，获取开源生态中的有利位置 | 为组织内部的开源治理设立明确的开源战略，确保内部使用和外部参与贡献方法的一致性和可见性 |
| | 开源基因工程与开源文化建立 | 将开源融入到整个组织战略和内部工作中，自上而下的推动开源战略 |
| | 建立基于开源的数字主权 | 通过开源战略解除供应商的锁定，实现数字主权的自由 |
| | 建立开源赋能创新的体系 | 通过开源带来的多样性、协作性和开放性等，是开源成为提升创新能力的关键因素 |
| | 开源驱动的数字化转型策略 | 让开源成为数字化转型的核心推动要素 |

## 7 事项规范

治理事项是开源治理具体操作执行的核心，其事项规范包含以下六项：

——事项描述：治理事项涉及的主题和摘要，对完成该治理事项的关键点和流程进行了说明；

——目标管理：对开源治理的特定目标进行管理，详细说明为什么开展该项治理工作、何时开展、以及需要解决的问题是什么。将有助于确定组织的预期工作量和所需资源、评估所需成本和预期价值；

——过程评估：对具体的治理事项进行进度监控与效果评估，包括定性与定量的方法。通过定义目标驱动的指标体系，明确评估治理事项所需的验证点，进而支持治理路线图、优先事项、以及绩效评价等工作；

——评价方法：提供实现和完成治理事项的评估手段、技术、数据或工具列表，进而高效的交付治理成果，支撑治理主体科学有效的开展工作；

——建议指导：从开源治理各方参与者中广泛收集最佳实践，定期更新用户的反馈意见，以及有助于各个事项管理的建议与指导；

——基础设施：提供能支撑开源治理工作有效开展的建设性基础性资源，包括软件工具、数据、咨询、培训、文档等各方面。

# 附 录 A
（资料性）
## 开源治理框架在企业开源治理中的应用

在企业治理方面，从开源治理的通用框架导出企业开源治理框架，以及企业开源基本事项检查清单，见图A.1。

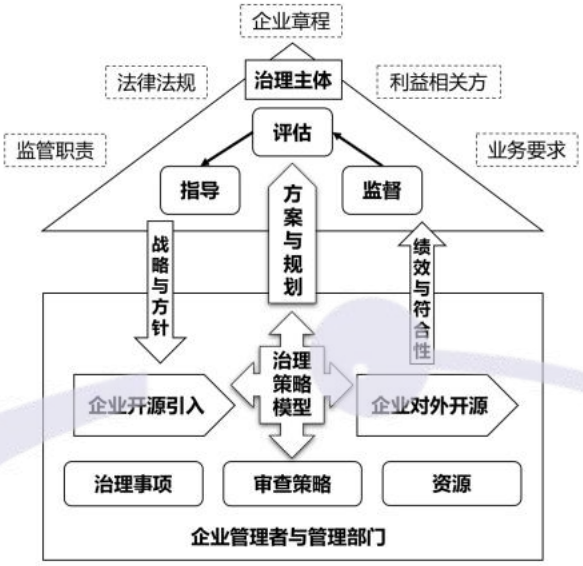


图 A.1 企业开源治理框架

企业作为开源治理主体，根据法律法规、企业章程、监管职责、利益相关方期望、以及业务要求等因素，制定企业开源战略与方针，并选择与之匹配的治理策略模型，进而开展开源引入、对外开源等活动，同时，通过监督、评估、指导的闭环形成不断迭代与优化的治理过程。

# 参 考 文 献

[1] GB/T 34960.1—2017 信息技术服务 治理 第1部分：通用要求
[2] ISO 37000:2021 Governance of organizations – Guidance
[3] The OW2 Open Source Good Governance Handbook, 2021.