ICS 35.240
CCS L 70

团　体　标　准

T/CESA XXXX—202X

信息技术 开源治理 第2部分：企业治理评估模型

Information technology—Open source governance—Part 2：enterprise open source governance and evaluation model

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。

本文件由中国电子技术标准院研究院提出。

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2部分:
企业治理评估模型

1 范围

本文件规定了企业在自身开源治理过程中应该具备的方法、流程和能力。
本文件适用于所有使用和贡献开源项目的企业单位。

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

开源项目 Open Source Project

以开源协作模式运作的项目。

3.2

开源社区 Open Source Community

开源组织的一种，是具有共同目标、愿景、与价值观的共同体，又称开源共同体。

3.3

源代码 Source Code

以适宜于汇编器、编译器或其他翻译器作为输入的形式所表达的代码。

[来源：GB/T 5271.7-2008 07.04.38]

3.4

制品 Artifact

由源代码编译构建生成的二进制文件。

4 缩略语

以下缩略语适用于本文本。

OSPO：开源项目办公室（Open Source Program Office）
CI/CD：持续集成/持续交付（Continuous Integration/Continuous Delivery）
SBOM：软件物料清单（Software Bill of Material）

5 企业开源治理评估模型

5.1 概述

企业使用开源的过程中主要面对的风险包括：许可证合规风险，安全漏洞风险，知识产权风险，出口管制风险等，规避和消除上述诸类风险是企业开源治理的主要目标。

5.2 企业开源治理评估模型

企业开源治理评估模型见图1。本模型包含企业开源治理工作中的人员、制度和资源三个方面。其中人员部分描述了开源治理团队的组织架构以及包含的各种成员角色;制度部分描述了企业规范开源治理工作的相关制度政策；资源部分描述了企业完成开源治理工作的相关基础设施。

图 1　企业开源治理评价模型

6　组织架构

6.1　总体要求

企业针对于开源治理应建立明确的组织架构，配置相应的专职或兼职人员。应设置OSPO或承担相同职能的部门，作为统领企业整个开源治理工作的领导部门。

OSPO负责制定开源合规规范、开源治理流程和协调资源，统筹规划和推动企业开源治理工作。OSPO包含若干角色、工作团队，负责相应职责的工作。

6.2　开源管理

应设置开源管理职责角色，负责制定企业开源治理政策、治理制度和治理流程，并能够基于此推动企业完成相应的开源治理工作，同时通过确定治理目标和考核奖惩制度确保开源治理的效果。

6.3　治理专家

应设置治理专家团队，开源治理专家根据企业的开源治理制度和流程，具体的指导某一个研发项目的开源治理工作。包括制定具体的治理计划、划分具体的治理任务、监督治理进展、核查治理效果和确保研发项目完成企业总体的开源治理要求。

6.4　安全专家

应设置安全专家团队，负责通过各种渠道和手段，从企业外部获取开源软件漏洞的情况，确定开源安全漏洞治理方案，及时通知各研发项目消除安全风险。同时需遵循国家关于漏洞管理的相关规范，代表本企业将安全漏洞及时上报。

除开源安全漏洞以外，安全专家还应负责与开源相关的数据安全，个人信息安全等其他安全事项。

6.5　基础设施支撑

宜设置基础设施支撑团队，负责开源治理基础设施的建设和维护，保障企业开源治理工作的顺利进行。

6.6　社区运营

宜设置社区运营团队，负责与外部开源社区的交流和运营工作。包括推动企业牵头、赞助和参与开源社区的各种活动以及大型会议，推广企业自发开源项目，以及相关商业宣传等。

7 制度政策

7.1 开源使用制度

企业应制定引入开源项目到企业内部使用的管理制度。包括开源项目的引入、开源项目的更新以及开源项目的退出。

对于产品中有包含外购商业部件和外包研发部件的企业，还应制定因使用商业部件和外包研发而被动引入开源项目的管理制度。

7.2 开源贡献制度

企业应制定开源贡献制度。包括对外部现有开源项目的贡献，以及企业将私有项目主动对外开源。

7.3 风险管理制度

企业应制定针对于各类风险的预防和消除制度，以及风险应急预案。需应对的风险包括安全漏洞风险、许可证合规风险、知识产权风险和出口管制风险等。

7.4 开源培训制度

企业应制定面向企业内的开源培训制度，使得员工了解企业关于开源的各项制度和规程，确保各项规避风险的制度能被贯彻落实。

8 开源声明周期管理

8.1 开源项目引入

8.1.1 开源选型规范

企业应制定开源项目选型规范，指导企业研发项目在需要引入开源项目时对其进行评价对比，以判断是否使用。开源选型应综合考虑开源项目的各方面情况进行判断，宜采用以下几个维度作为评判因素，企业可以根据研发项目的需要和特点来从其中进行选择和设置权重。

a) 需求满足度。宜参照但不仅限于以下方面予以衡量：
   - 功能满足度，
   - 性能满足度，
   - 易用性满足度，
   - 可靠性满足度，
   - 可维护性满足度，
   - 可移植性满足度。

b) 项目成熟度。宜参照但不仅限于以下方面予以衡量：
   - 是否持续的发布了一定数量的稳定版本。
   - 是否具有比较稳定的核心贡献者团队，
   - 是否具有比较明确的技术规划，
   - 是否具有比较明确的版本发布计划，
   - 是否具有比较完备的文档，
   - 是否具有比较可靠的故障和漏洞提交和解决机制，
   - 是否具有自动化构建和测试能力，
   - 是否具有比较稳定充足的CI/CD环境和相应资源，
   - 是否具有比较可靠的代码托管机制，
   - 是否具有多个代码托管地。

c) 开源许可证。
   - 企业应建立允许引入使用的开源许可证清单或禁止引入使用的开源许可证清单。可根据不同的业务场景制定不同的允许清单或禁止清单。
   - 应禁止使用许可证不明的开源项目。
   - 宜尽量使用具有知识产权条款的开源许可证的开源项目。