ICS 35.240
CCS L 70

团 体 标 准

T/CESA 1270.2—2023

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 governance and assessment model

2023-09-28 发布　　2023-09-28 实施

中国电子工业标准化技术协会　发布

目　　次

前　　言 V
引言 VII
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 1
5 企业开源治理评估模型 1
5.1 概述 1
5.2 企业开源治理评估模型 2
6 组织架构 2
6.1 总体要求 2
6.2 开源管理 2
6.3 法务专家 2
6.4 治理专家 3
6.5 安全专家 3
6.6 基础设施支撑 3
6.7 社区运营 3
7 制度政策 3
7.1 开源使用制度 3
7.2 开源贡献制度 3
7.3 风险管理制度 3
7.4 开源培训制度 3
8 开源声明周期管理 3
8.1 开源项目引入 3
8.2 开源项目使用更新 5
8.3 开源项目退出 6
8.4 开源项目使用规则 6
8.5 开源项目贡献 6
8.6 开源项目商业被动引入 7
9 风险管理 8
9.1 安全漏洞风险 8
9.2 许可证合规风险 8
9.3 知识产权风险 9
9.4 出口管制风险 9
10 基础设施 9
参 考 文 献 10

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。

本文件是T/CESA 1270《信息技术 开源治理》的第2部分。T/CESA 1270已经发布了以下部分：

——第 1 部分：总体框架；

——第 2 部分：企业治理评估模型；

——第 3 部分：社区治理框架；

——第 4 部分：项目评估模型；

——第 5 部分：开源贡献者评估模型。

请注意本文件的某些内容可能涉及专利。 本文件的发布机构不承担识别这些专利的责任。

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：中国电子技术标准化研究院、中兴通讯股份有限公司、开放原子开源基金会、浪潮电子信息产业股份有限公司、苏州棱镜七彩信息科技有限公司、浙江九州未来信息科技有限公司、上海计算机软件技术开发中心、蚂蚁集团集团股份有限公司、北京百度网讯科技有限公司、中移（苏州）软件技术有限公司、普元信息技术股份有限公司、北京华胜天成科技股份有限公司、东软集团股份有限公司、浪潮云信息技术股份公司、中移系统集成有限公司、深圳市金蝶天燕云计算股份有限公司。

本文件主要起草人：杨丽蕴、李响、于秀明、李成双、江大勇、庄表伟、张百林、但吉兵、章津楠、沈颖、郭智慧、马红伟、钱岭、孟庆余、梁钢、赵赫、黄先芝、杨佳丽、李智琪、于昕、边思康、王旭、梁大功、杨静、孙福洲、朱其罡、王荷舒、储兰芳、邝敏越、付辉、彭晋、郭皓、王林、黄浩东、王媛媛、魏弋钧、葛建新、徐冠群、田晓利。

引言

为规范开源领域治理活动，提升开源治理能力，系统性地指导开源各组织开展开源治理策略与政策编制，结合开源治理实际情况，制定开源治理标准。T/CESA 1270旨在为开源治理的事项与活动提供依据，拟由5个部分构成。

——第 1 部分：总体框架。目的在于为不同开源参与组织确立完善、规范的开源治理框架和组成要素。

——第 2 部分：企业治理评估模型。目的在于规定企业在自身开源治理过程中具备的方法、流程和能力。

——第 3 部分：社区治理框架。目的在于描述了开源社区治理与运营总体框架的利益相关方、治理原则、框架与组成要素、成熟度模型、成熟度评估和数据评价方法。

——第 4 部分：项目评估模型。目的在于确立了建立开源项目多维度指标模型，系统性评价开源项目发展情况。

——第 5 部分：开源贡献者评估模型。目的在于确立了开源贡献者参与开源技术贡献和治理贡献的评估模型。

信息技术 开源治理 第2部分:企业治理评估模型

1 范围

本文件确立了企业开源治理评估模型，规定了企业在自身开源治理过程中的流程和能力要求。
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

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

T/CESA 1269-2023 信息技术 开源 术语与综述

3 术语和定义

T/CESA 1269-2023 界定的以及下列术语和定义适用于本文件。

3.1

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]

3.2

制品 artifact

由源代码编译构建生成的二进制文件。

4 缩略语

下列缩略语适用于本文件。

CI/CD：持续集成/持续交付（Continuous Integration/Continuous Delivery）

CLA：贡献者许可协议（Contributor License Agreement）

DCO：开发者原创证书（Developer Certificate of Origin）

OSPO：开源项目办公室（Open Source Program Office）

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 企业开源治理评估模型

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则、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 法务专家

应包含法务专家团队，负责管控企业在使用开源项目时面临的法律风险。包括开源许可证合规风险，知识产权风险，出口管制风险等。

6.4 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。

6.5 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。

6.6 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。

6.7 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 开源生命周期管理

8.1 开源项目引入

8.1.1 开源选型规则

企业应制定开源项目选型规则，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。宜按照但不仅限于下列方面予以衡量：
   1) 功能满足度；
   2) 性能满足度；
   3) 易用性满足度；
   4) 可靠性满足度；
   5) 可维护性满足度；
   6) 可移植性满足度。
b) 项目成熟度。宜按照但不仅限于下列方面予以衡量：
   1) 是否持续的发布了一定数量的稳定版本；
   2) 是否具有比较稳定的核心贡献者团队；
   3) 是否具有比较明确的技术规划；
   4) 是否具有比较明确的版本发布计划；
   5) 是否具有比较完备的文档；
   6) 是否具有比较可靠的故障和漏洞提交和解决机制；
   7) 是否具有自动化构建和测试能力；
   8) 是否具有比较稳定充足的CI/CD环境和相应资源；
   9) 是否具有比较可靠的代码托管机制；
   10) 是否具有多个代码托管地。
c) 开源许可证：
   1) 企业应建立允许引入使用的开源许可证清单或不准许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不准许清单；
   2) 不准许使用许可证不明的开源项目；
   3) 宜尽量使用具有知识产权条款的开源许可证的开源项目；
   4) 当企业的研发项目为对外发布的非开源项目时，应评估引入开源项目的开源许可证传染性，防止出现违反开源许可证要求的合规问题。
d) 项目活跃度。宜按照但不仅限于下列方面予以衡量：
   1) 最后一个版本发布距今的时间；
   2) 开源项目版本发布更新频率；
   3) 软件BUG和安全漏洞的修正周期；
   4) 开源贡献者数量；
   5) 开源贡献来源多样性；
   6) 相关开源社区活动的形式和频率。
e) 行业认可度。宜按照但不仅限于下列方面予以衡量：
   1) 是否有行业主要厂商的支持。
f) 风险评估。宜按照但不仅限于下列方面予以衡量：
   1) 开源项目版本中是否含有安全漏洞风险；
   2) 开源项目版本中是否含有知识产权风险；
   3) 开源项目版本中是否含有出口管制风险。

8.1.2 开源引入规则

企业应制定开源项目的引入流程规则，各研发项目依据此规则将开源项目引入企业内部使用。此引入流程规则一般可包括：

——明确选型需求：包括功能需求，性能需求等；

——开源项目选型：依据开源项目选型规则选择开源项目，输出有优先级的备选清单；

——开源项目选型确认：通过测试验证确定备选清单中的开源项目是否确实满足了选型需求，并最终确定唯一的选型结果；

——开源项目代码/制品入库：将选定的开源项目的代码/制品拉取到企业内部，并入企业开源项目管理库，供后续进行使用和管理。代码/制品需要从官方或者可靠的源下载，避免引入安全隐患；

——开源项目引入台账：对于上述选型，确认，入库等流程信息，需要在企业内部予以记录。

8.1.3 开源项目守护

企业应制定开源软件在引入企业内后的守护规则。每个开源软件在被引入企业进行使用后应设置一个守护团队，守护团队的职责包括但不限于：

——应跟踪所守护开源项目的技术动向，识别开源项目的功能增减和性能变化等重要技术特征，为使用此开源项目的企业内研发项目提供使用建议；

——应跟踪所守护开源项目的缺陷，安全漏洞。及时向企业内部使用了此开源项目的研发项目推送升级建议或补丁；

——应跟踪开源项目使用开源许可证的变更情况，及时向企业内部使用了此开源项目的研发项目提供指导意见；

——宜建立面向所守护开源项目的软件构建和测试环境，建立测试验证方案，具备构建和测试验证能力；

——当开源社区不能及时提供缺陷和安全漏洞的解决方案和补丁时，守护团队宜自行制定解决方案并研发补丁；

——对其守护的开源项目宜制定一个可以使用的版本基线，这个基线可以是一个版本集合，要求企业内研发项目使用此开源项目时，只能使用这个集合中的版本。基线版本除开源项目版本的原始内容外，还应包含解决了此版本中缺陷和安全漏洞的补丁；

——可参与所守护开源项目的外部社区开源贡献活动，将企业自行研发的功能和补丁贡献到开源社区。

8.2 开源项目使用更新

企业应制定开源项目使用更新规则，列出研发项目应更新其所使用的开源项目的情况，更新包括升级版本和自行打补丁。这些情况可包括：

——功能/性能需求：研发项目发现在用的开源项目版本不能满足功能或性能需求，需要通过升级来满足需求；

——现使用版本存在重大安全漏洞：企业应根据业界通用的漏洞库的漏洞等级确定哪些级别的漏洞应通过更新来解决；

——现使用版本过于老旧：企业应规定开源项目版本老旧的标准，应选用开源项目最新的几个版本，和/或当前开源项目版本最旧发布时间；

——现使用的开源项目许可证发生了变更，变更为企业不能接受的开源许可证，企业应对此开源项目进行重新选型，使用同等功能的其他开源项目替换。

注：如企业对一个开源项目已经通过其守护团队建立了可以使用的版本基线，则研发项目在对这个开源项目进行更新时就必须选用基线范围内的版本。

8.3 开源项目退出

开源项目版本在企业内已经没有研发项目使用时，则应将其从企业开源管理库中清理退出。

企业也可根据开源项目更新规则在满足更新条件时，强制将需更新的开源项目版本从企业开源管理库中清理退出，并通知仍在使用的项目立即更新。

8.4 开源项目使用规则

8.4.1 开源项目使用方法

企业在使用开源项目时遵守以下使用规则：

——应通过开源项目引入规则引入开源项目来使用，不准许自行随意使用开源项目；

——应从企业内的开源项目管理库获取开源项目的代码和制品，不准许自行从企业外部拉取代码和制品；

——应严格遵守开源项目所用开源许可证的要求；

——宜整体使用开源项目的版本，不宜仅使用开源项目的代码片段。

8.4.2 研发项目开源软件清单

企业研发项目应明确本项目使用了哪些开源项目，维护一个所用开源项目列表，并确保其正确性。

8.4.3 研发项目发布要求

企业研发项目在对外作为产品发布时应明确其使用开源项目的情况并满足开源许可证的要求，应提供：

——产品所包含的 SBOM；

——产品所包含的开源项目的开源许可证；

——产品所包含的开源项目的版权声明；

——如产品所包含的开源项目的开源许可证有要求，需要提供所使用的开源项目代码以及衍生物代码。

8.4.4 研发项目应急响应

企业研发项目应建立面向开源项目的应急响应机制，明确当开源项目出现严重的故障和安全漏洞后应该采取的措施，以及响应时间要求。

8.5 开源项目贡献

8.5.1 开源贡献战略

企业宜根据自身产品和技术发展战略等原因，制定开源贡献策略，指引企业各产品和研发项目对外开源贡献工作。

8.5.2 自发开源项目贡献

企业根据开源贡献战略将企业私有研发项目对外开源，即自发开源项目。

a) 企业宜制定自发开源开源的贡献规则，其内容包括：

1) 制定开源贡献合规规则，指导员工在开源贡献时遵循开源许可证等合规要求；

2) 制定开源贡献审批流程，以规范员工对外开源贡献的内容范围，防止商业泄密；
3) 制定自发开源项目选择开源许可证的原则，帮助研发部门在试图对外开源私有项目时确定所使用的开源许可证；
4) 对自发开源项目，企业制定 CLA 或 DCO 供贡献者签署；
5) 制定自发开源项目代码的编程规则，并由参与贡献的员工带头遵守。

b) 企业应提供充分的人力和物力资源保证自发开源项目的研发运转和社区运营；
c) 企业宜制定开源贡献奖励机制，以鼓励员工参与自发开源项目的贡献。

8.5.3 既有开源项目贡献

企业宜根据开源贡献战略参与企业外部既有的开源项目，对外实现开源贡献。

a) 企业宜制定对既有开源项目的贡献规则，其内容包括：
1) 宜制定开源贡献合规规则，指导员工在开源贡献时遵循开源许可证等合规要求；
2) 宜制定开源贡献审批流程，以规范员工对外开源贡献的内容范围，防止商业泄密；
3) 宜制定规则要求员工遵守开源项目代码编程规则。

b) 企业宜提供充分的人力和物力资源保证对既有开源项目贡献的顺利实施；
c) 企业宜制定开源贡献奖励机制，以鼓励员工对既有开源项目进行开源贡献。

8.6 开源项目商业被动引入

8.6.1 概述

企业的研发项目中可能包含有外购的商业部件，这些商业部件中可能包含开源项目，从而造成企业被动引入开源项目。

8.6.2 商业部件引入

企业应对被动引入开源项目的情况、存在的风险以及商业部件供应商应该承担的责任予以明确。

a) 企业应要求供应商提供与商业部件中包含的开源项目相关的交付物：
1) 供应商应提供商业部件中包含的 SBOM；
2) 供应商应提供商业部件中包含的开源项目的许可证合规材料，包括许可证文本，源代码包/源代码获取方法说明等；
3) 供应商应提供开源项目合规承诺书，明确声明已经满足开源项目合规要求，承担违规责任；
4) 供应商应提供商业部件中包含的开源项目的开源传染性情况说明，防止导致企业在使用商业部件时出现开源传染性风险。

b) 企业宜将商业部件中包含的开源项目纳入本企业开源生命周期管理中进行统一管理。
c) 对于商业部件中包含的开源项目的安全漏洞：
1) 供应商应保证在交付商业部件时已经解决了所有对产品安全有影响的安全漏洞；
2) 供应商应对于商业部件中包含开源项目的新增安全漏洞承诺提供临时处理方案和最终解决方案，如提供补丁、开源项目替换等。

8.6.3 外包研发引入

企业的研发项目中可能包含有外包研发的部件，这些外包部件中可能包含开源项目，从而造成企业被动引入开源项目。

企业应对这些被动引入开源项目的情况、存在的风险以及外包商应该承担的责任予以明确。

a) 发包企业要求外包商提供与外包部件中包含的开源项目相关的交付物：
   1) 外包商应提供外包部件中包含的 SBOM；
   2) 外包商应提供外包部件中包含的开源项目的许可证合规材料，包括许可证文本，源代码包/源代码获取方法说明等；
   3) 外包商应提供开源项目合规承诺书，明确声明已经满足开源项目合规要求，承担违规责任；
   4) 外包商应提供外包部件中包含的开源项目的开源传染性情况说明，防止导致发包企业在使用外包部件时出现开源传染性风险。
b) 发包企业宜将外包部件中包含的开源项目纳入本企业开源生命周期管理中进行统一管理；
c) 发包企业宜要求外包商遵循发包企业自身的开源软件选型和使用规则；
d) 对于外包部件中包含的开源项目的安全漏洞：
   1) 外包商应保证在交付外包部件时已经解决了所有对产品安全有影响的安全漏洞；
   2) 外包商应对于外包部件中包含开源项目的新增安全漏洞承诺提供临时处理方案和最终解决方案，如提供软件补丁、用其他开源项目替换等；
   3) 发包企业宜要求外包商将其对安全漏洞的解决方案，如软件补丁等，贡献到相应的开源社区；
   4) 发包企业宜要求外包商将外包商自己发现的新安全漏洞遵照国家关于漏洞管理的相关规范，如《网络产品安全漏洞管理规定》，将安全漏洞上报到规范中规定的相关单位以及相应开源社区。

9 风险管理

9.1 安全漏洞风险

企业应建立开源项目安全漏洞分析和跟踪机制，应对安全漏洞风险：

——制定产品发布安全红线，不准许产品携带已知的较高等级的安全漏洞对外发布；

——通过扫描工具、外部漏洞库跟踪等方式持续收集安全漏洞信息，提醒研发项目及时治理安全漏洞；

——对安全漏洞提供统一且有效的治理方案供企业内所有研发项目使用；

——建立研发项目对安全漏洞的治理跟踪机制。研发项目应明确已发布到企业外的哪些产品中包含了哪些在发布时尚未发现的安全漏洞，并联合开源项目的守护团队，提供解决方案和时间承诺；

——建立漏洞的上报机制和对外反馈机制，将企业内部新发现的漏洞遵照国家关于漏洞管理的相关规范，如《网络产品安全漏洞管理规定》，将安全漏洞上报到规范中规定的相关单位以及相应开源社区。

9.2 许可证合规风险

企业建立开源许可证合规规则，应对许可证合规风险：

——应建立允许引入使用的开源许可证清单或不准许引入使用的开源许可证清单；

——对常见和重要的开源许可证，企业应制定相应的许可证分析和使用指引，指导研发项目合规的应用使用了此许可证的开源项目；

——宜制定自发开源项目选择开源许可证的原则，帮助研发部门在试图对外开源私有项目时确定所使用的开源许可证。

9.3 知识产权风险

企业应建立开源项目知识产权规则，应对此类风险：

a) 对计划引入的开源项目进行知识产权审查，尽力确保其中不会埋藏专利等知识产权风险；
b) 建立对外开源知识产权审查制度，防止对外开源贡献造成商业秘密泄露，专利权益损失，防止贡献的项目代码和制品中含有隐私数据及其他风险信息；
c) 建立开源项目软件著作权相关规则，规避开源项目软件著作权风险。包括但不限于：
   1) 应不准许消除和篡改代码中的版权信息；
   2) 应不准许使用开源项目的部分代码片段。
d) 企业应在引入时明确开源项目中是否存在注册商标，明确正确使用注册商标的方法，防止出现商标侵权。

9.4 出口管制风险

企业应建立开源项目与出口管制相关的规则，使得企业满足各国出口管制规范制度。

10 基础设施

企业建立并维护开源治理相关的基础设施，以支撑开源治理工作的顺利进行。

——应建立企业研发项目对开源项目使用情况的数据库，存储各研发项目使用了哪些开源项目，这些开源项目存在哪些安全漏洞，这些安全漏洞的填补情况，已发布到企业外部版本的安全漏洞填补情况等重要数据；

——宜建立企业引入使用的开源项目管理数据库，用于存储开源项目元数据等重要信息；

——宜建立企业内部的开源项目仓库，存储从外部拉取的开源项目代码、制品、数据等；

——宜引入开源软件扫描工具，帮助研发项目发现使用了哪些开源项目版本；

——宜建立对开源项目进行构建和测试验证的环境，用于开源项目版本构建，版本测试，故障和漏洞修复验证等工作。

参 考 文 献

[1] GB/T 5271.7-2008 信息技术 词汇 第7部分：计算机编程