Q/GUOSEN

国 信 证 券 股 份 有 限 公 司 企 业 标 准

Q/GUOSEN-ENG-TAM 01-2024

国信证券开源软件管理规范

2024-08-16 发布 2024-09-02 实施

国信证券股份有限公司 发布

前　　言

本标准根据《关于规范金融业开源技术应用与发展的意见》《金融业开源软件应用管理指南》《国信证券开源软件管理办法》等相关标准规范文件进行编制。

本标准于 2024 年 8 月初次起草发布，9 月首次实施，在编制过程中得到各位同仁的大力支持，在此表示感谢！由于编制时间紧促，难免有遗漏之处，恳请广大参阅者多提高贵意见，以供参考校正。

本标准由国信证券股份有限公司提出。

本标准起草单位：国信证券股份有限公司。

本标准主要起草人：李明军、邓启翔、陈培新、林芊芊。

本标准于 2024 年 8 月首次发布。

1 范围

本标准规定了公司开源技术应用，防范开源技术风险，建立健全开源技术管理机制，提高开源软件管理的规范化水平。

本标准适用于对信息技术部门的开源软件管理能力进行评价和指导。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和缩略语

本文件没有术语和缩略语。

4 组织架构和职责分工

4.1 设立开源治理工作组负责开源技术应用与管理相关事项。开源治理工作组由开源治理管控团队和开源治理实施团队构成。

4.2 开源治理管控团队（以下简称“管控团队”）是开源治理工作的决策和组织协调主体，由分管信息技术条线的公司级领导任组长，技术管理部负责人、金融科技总部负责人、系统运行总部负责人任副组长，主要职责包括：

1）审定开源治理目标、战略、发展规划和年度计划；

2）审定开源软件管理制度、细则、流程和规范；

3）决策和组织处理开源治理工作的重大事项、风险事项和争议事项；

4）负责组织制定开源治理目标、战略、发展规划和年度计划，并推动落实相关工作；

5）组织制定、维护开源治理工作相关细则、流程和规范，推进开源治理各制度的落地实施；

6）负责推动开源治理工作的跨部门合作与执行；

7）负责开源治理相关环节评审和审批工作；

8）负责统筹对外开源项目评审和运营规划工作；

9）按需就开源治理的各类专题工作进行审议及决策；

10）听取开源治理实施团队对开源治理工作的汇报。

4.3 开源治理实施团队是开源治理工作的执行主体，由技术管理部/软件架构与平台研发组、系统运行总部/基础架构与安全部/信息安全组和系统运行总部/基础架构与安全部/基础架构组相关人员构成，负责日常开源治理工作的具体组织和推进，主要职责包括：

1）负责开源软件引入和使用前的技术选型、社区评估，更新或退出等关键环节的技术评估；

2）开源软件引入或对外开源项目的功能、性能、兼容性、稳定性测试；

3）负责开源软件及组件的安全扫描工作，定期跟踪开源软件安全漏洞风险；

4）负责开源安全风险评估工作；

5）制定安全漏洞风险的修复方案、缓解措施或其他处理措施；

6）协调相关人员开展开源软件安全漏洞风险和合规风险的处置工作，跟进开源安全风险的修复情况；

7）建立和更新项目软件物料清单；

8）负责存量开源软件、组件的识别和盘点，建立开源软件清单和开源软件使用台账并持续维护；

9）负责开源软件库和组件库出库、入库及更新等运维工作；

10）负责开源许可证合规审查工作，定期维护开源许可证清单；

11）负责开源许可证条款解读及使用指导，提供法务支持；

12）负责跟踪和回归开源软件合规风险的治理情况；

13）负责开源管理平台运行维护；

14）负责落实内外源运营规划；

15）负责内外源项目的发布、技术支持和维护工作；

16）结合开源产业相关活动、资源平台进行对外开源项目宣传，并根据项目的运营表现、舆情等信息进行分析、反馈及处置；

17）负责对外开源项目的宣传渠道搭建、商标设计及其他日常运营及推广；

18）配合开源治理管控团队审核对外开源项目的整体投入合理性与充足性；

19）协助开源治理管控团队定期评估对外开源项目价值；

20）配合开源治理管控团队参与开源软件评审工作。

5 选型评估标准

开源软件选型，需从以下六个方面进行综合评估：

1）开源软件：软件的语言、平台以及实现的功能应符合国信证券 IT 规划的技术路线发展要求。

2）开源许可证：应采用商业友好开源许可证的开源软件，若采用不友好的需结合使用场景评估相应法律风险。

3）技术质量：应选择代码整洁，注释完善，并且在引入测评中测试覆盖率高的软件。

4）软件文档：应选择项目文档齐全，社区内的邮件列表的存档比较完善的软件。

5）版本要求：软件版本应选择经过一段稳定运行期检验的正式发布版本，如 release 版，无特殊要求原则上不允许使用非正式版本。

6）安全要求：应选择安全风险少、软件安全治理机制完善、安全风险修复响应快的软件。

6 开源软件生命周期管理

6.1 开源软件的引入

6.1.1 开源软件首次引入

1）不在开源软件可使用基线范围内的开源软件，使用前需由开源软件使用者发起引入申请。

2）开源软件使用者提出开源软件引入申请，由开源治理管控团队组织相关专家对软件来源、软件是否符合国信证券技术路线等进行评审;对开源技术版权、专利、商标、声明等进行事前合规审查，通过审查开源许可证遵从性和兼容性、梳理开源技术间依赖性等，避免法律纠纷。可根据需要引入第三方合规审查服务。

6.1.2 开源软件分类分级

1）根据开源软件的重要性、安全性等分类如下:

1 类:经扫描工具扫描后无漏洞的软件。

2 类:经扫描工具扫描后存在漏洞，属于某个特定领域、适用范围较小，且后续不会扩大适用范围的开源软件。

3 类:经扫描工具扫描后存在漏洞，属于通用领域或适用范围较大的开源软件。

4 类:经扫描工具扫描后存在漏洞，但通过信息安全组安全评估或漏洞处置后，可以进入试用的开源软件。

2）对于 1、2 类开源软件，经软件架构与平台研发组审核后可加入制品库和开源软件白名单。

3）对于 3、4 类开源软件，根据项目组申请，软件架构与平台研发组可将软件加入制品库，并对其进行标记为“试用”。项目组应对开源软件进行 1-3 个月的试用，试用通过后，通知软件架构与平台研发组去掉“试用”标记，进入开源软件白名单。如未通过试用，但确需引入使用的开源软件，项目组应以例外事项，经开源管控组审批通过后正式应用。

4）对于审核不通过的开源软件，由开源软件申请者根据预审意见修订后，重新发起引入评审。

5）对于整体技术体系发生重大改变的开源软件版本，使用者需重新发起引入流程。

6.1.3 开源软件引入测评。

1）开源软件使用者负责核实开源软件的来源。由产品提供商带入的开源软件，需由厂商说明开源软件的来源，并保证开源软件的安全性。如无产品提供商，开源软件介质应由开源使用者从开源软件官网或认证的其他代码托管网站获取，保证其来源安全可溯，无植入后门或木马。

2）开源软件使用者负责搭建开源软件测试环境，从功能、非功能（性能、易用性、安全性等）维度进行全面测试，并记录测试数据、整理测试结果。同时按照附件《开源技术引入评估表》开展技术、安全和合规评估。

3）测评工作完成后，开源软件使用者需编写《开源软件测评报告》，并提交开源治理管控团队评审。评审内容包括测试指标达成情况、测试范围、测试工作执行结果、缺陷解决情况、遗留缺陷等内容。对不合格的报告，开源软件申请者需要重新组织测试。对通过评审的开源软件，由开源治理管控团队给出应用范围和应用建议。

6.1.4 开源软件引入发布

1）开源软件申请者应编制该开源软件使用规范及部署手册，帮助使用及维护人员快速掌握该软件，避免常见错误。

2）开源软件申请者负责将评审通过的开源软件打包，软件包应包括开源软件、源代码、开源软件安装配置参数、安装和使用手册等。

3）在上线投产前，应进行风险评估。由开源软件使用者发起开源软件归档申请，经软件架构与平台研发组评估通过后，将开源软件包提交开源软件资产库。

4）开源软件提交开源软件资产库后，由开源软件申请人通过开源管理平台录入《开源软件应用台账》。

5）完成上述环节后，由软件架构与平台研发组更新《开源软件基线表》。

6.2 开源软件的维护

开源软件引入后，根据不同的类别，由不同团队进行维护。在开源软件引入时，申请者应提出维护团队的建议，由开源治理管控团队审议决策。开源软件投产后由软件架构与平台研发组及开源软件维护者负责运维。

6.3 开源软件的使用

开源软件资产库是合法获取开源软件的唯一来源。在选择开源软件产品时，应选择白名单中的开源软件。评审不通过的开源软件禁止在国信证券各信息系统使用，确需使用的应以例外事项经项目组所属部门负责人、开源管控组审批通过后方可使用。对于违规使用开源软件造成生产事件或信息安全事件的，按照国信证券相关管理办法处理。

6.3.1 开源软件使用申请

1）开源软件使用前，开源软件使用者应结合应用研发项目做好适用性评估，确保开发人员了解开源软件的关键技术、参数配置等要求，在安全可靠的前提下安装/使用开源软件。

2）开源软件使用者应从开源软件白名单库检索可用开源软件信息。

3）对未列入开源软件白名单库中的开源软件，应按照引入管理的要求完成开源软件准入，方能从开源软件资产库中获取软件包。

4）开源软件使用者根据安装手册安装开源软件，如遇问题可向开源软件管理维护者或软件架构与平台研发组申请技术支持。

6.3.2 开源软件使用审批

1）白名单库中的开源软件，由开源软件使用者完成开源软件应用台账录入后即可使用，如未录入引发后续使用不规范、更新不同步等问题，由使用者负责。

2）如需使用非白名单库中的开源软件，需由开源治理管控团队完成审批通过后，方可使用。如未提出申请，引发后续使用或生产事故等问题，由使用者负责。审批通过后，开源软件使用者应更新开源软件应用台账。

6.3.3 开源软件使用检查

1）软件架构与平台研发组定期对开源软件使用工作进行检查对于使用了非白名单开源软件的系统，通知系统负责人制定整改计划，系统负责人及时反馈整改情况，并更新应用台账。

2）对于违反基线标准且无特殊情况的，由开源软件使用者组织人员进行整改。

3）如遇特殊情况，开源软件使用者应向软件架构与平台研发组提出申请并说明实际情况，经开源治理管控团队评审通过后方可继续使用。

4）软件架构与平台研发组应组织技术专家组对整改完成的系统进行验收审核，验收不通过则开源软件使用者继续进行整改。

6.3.4 开源软件问题管理

开源软件使用过程中遇到的开发、维护相关问题，如不能自行解决，可咨询技术服务商协助解决。问题解决后应将问题解决方法归集至开源知识库管理系统。

6.4 开源软件版本升级

6.4.1 开源软件漏洞修复/版本升级申请

1）开源软件维护者应及时跟踪开源软件的最新动态，包括金融管理部门要求、开源社区的版本升级、性能和安全漏洞等情况，及时向开源软件使用者提出升级建议。

2）开源软件使用者或信息安全管理人员发现开源安全漏洞也可通知开源软件维护者对开源软件资产库中的开源软件进行版本升级并标记。

6.4.2 漏洞修复/版本升级审批

1）对于非技术体系有重大变更的开源软件升级，视为补丁版本，由开源治理管控团队进行版本更新审批。

2）对于开源软件整体技术体系有重大变更的软件升级，需重新启动引入流程。

3）由开源软件使用者配合，开源软件维护者牵头负责制定开源软件升级方案，软件升级申请应包括以下内容:

- 升级的必要性及代码来源。
- 升级的兼容性情况。
- 升级的风险和测试方案。
- 升级影响的应用系统或功能范围评估。
- 升级的项目组织和工作计划。

4）对于存在重大风险或影响范围较大的升级，开源软件使用者应配合开源软件维护者选择典型应用进行升级适应性测试。

5）开源软件维护者负责组织软件升级、改造评审会议，对本地改造需求和升级需求进行评审，并明确影响程度，会议评审结论应提交开源治理管控团队审批。

6）对于审批不通过的申请，由开源软件维护者根据评审意见修订相关方案，并重新提出申请。

6.4.3 漏洞修改

开源软件相关系统负责人应按照《国信证券股份有限公司信息系统安全漏洞管理办法》执行漏洞的修复工作，如不能及时完成处置，需采取妥善的风险缓释措施。

漏洞修复完成后，开源软件使用者应更新开源软件应用台账。

6.5 开源软件的停用

6.5.1 开源软件在使用和维护中若发现已不适合继续使用，须及时停用，防止因开源软件问题引发生产事故或安全风险。开源软件停用过程包括停用申请，停用审批、软件更换等流程。

6.5.2 开源软件停用申请

1）软件架构与平台研发组定期收集开源软件使用情况信息，对监管部门、审计部门、安全部门提出停用意见的开源软件，对于不适合国信证券技术规范的，有开源社区停止更新的开源软件进行分析。发现开源软件需要停用的情况，应及时推动开源软件使用者及维护者根据相关信息，评估严重程度、影响范围、响应处置时限等，制定解决方案，提交开源治理管控团队审批。

2）需要停用的开源软件，由开源软件维护者向软件架构与平台研发组提起停用申请，说明停用的软件名称、使用范围、停用原因、停用计划和替换方案，替换方案应覆盖所有受停用开源软件影响的系统。

6.5.3 开源软件停用审批

3）软件架构与平台研发组对提出停用的软件进行影响性、风险等综合评估，并征求相关部门意见。

4）开源治理管控团队对开源软件停用申请和停用计划、替换方案等开展评审，根据评审结论予以审批。

5）软件架构与平台研发组更新开源软件状态为“限期替换”。

6.5.4 开源软件白名单更新及开源软件更换

软件架构与平台研发组定期发布开源软件白名单。受影响的系统应当按照替换方案和改造计划，制定系统的替换方案，按计划完成停用开源软件的退出。

更换工作完成后，开源软件使用者需更新开源软件应用台账，软件架构与平台研发组更新开源软件资产库中相应开源软件状态为“停用”。

7 开源软件资产库

开源软件资产采用研发制品库进行统一管理,通过研发制品库存放正式使用的开源软件、源代码及相关技术文档，实现开源软件的版本可控制、可追溯、安全可信的管理目标。开源软件引入申请者应在系统上线前提交开源软件资产的上传申请，经软件架构与平台研发组审核通过后，将开源软件相关资产分类上传到指定位置。资产库中存放程序包、配置文件、测试报告、技术手册等。具体分类目录参考如下(可根据实际情况增补):

1）Dev：用于存放在进行二次开发的开源软件。

2）Test：用于存放测试阶段的开源软件。

3）Release：用于存放正式使用的开源软件，即生产制品库，比如用于系统开发、生产部署的软件。

4）Src：开源软件源代码和相关文档。

8 开源风险管理

8.1 安全风险管理

8.1.1 开源软件安全风险识别

信息安全团队负责对新引入开源软件和存量开源软件进行安全风险识别。通过采用专业的漏洞扫描工具进行安全风险检出，识别开源软件所携带的安全风险信息。

8.1.2 开源软件安全风险评估

1）信息安全团队按照《国信证券股份有限公司信息系统安全漏洞管理办法》对识别出的安全风险进行风险评估，并联合开源软件使用者对漏洞进行分析，确定引入开源软件到系统开发的影响范围，影响范围评估维度包含但不限于：

- 影响软件级别；
- 漏洞危害等级；

- 漏洞利用成熟度；
- 漏洞利用方式。

2）根据安全风险评估结果，开源软件使用者负责制定开源软件引入后的开源软件使用方案，并同时制定引入后切换回原有开源软件方案的回退机制。

3）根据安全风险评估结果，信息安全团队组织开源软件使用者、信息技术各专业团队，按照《国信证券股份有限公司信息技术风险管理办法》《国信证券股份有限公司信息系统安全漏洞管理办法》对识别出的安全风险问题进行漏洞分类分级，制定安全风险修复方案及风险控制措施，由开源软件使用者进行风险处置。

8.1.3 开源软件安全风险处置

1）开源软件使用者根据信息安全团队下发的安全风险修复方案及风险控制措施，对开源软件安全风险进行风险修复及处置，并在规定期限内反馈漏洞处置进展。

2）如果因特殊原因，开源软件使用者无法按时完成漏洞修复，应及时向信息安全团队反馈原因，并申请延期。

3）对开源软件安全风险进行风险修复及处置时，如出现操作后未修复完成或者引发其他安全风险，开源软件使用者应及时将相关情况反馈信息安全团队，由信息安全团队重新发起开源软件安全风险评估，并下发安全风险修复方案及风险控制措施。

8.1.4 开源软件安全风险跟踪

1）信息安全团队对安全风险处置完成的开源软件进行备案登记，并定期对开源软件进行安全风险扫描、安全性测试、安全风险监控、紧急风险处置等。

2）安全风险扫描：信息安全团队应通过专业的漏洞扫描工具，定期对开源软件资产库和信息系统进行扫描，及时发现并评估潜在的安全漏洞。

3）安全性测试：信息安全团队定期对使用的开源软件进行安全性测试，通过静态代码分析、漏洞扫描、攻击测试等方式，及时发现潜在的安全隐患。

4）安全风险监控：信息安全团队应对潜在的和未修复的开源技术风险进行监控，关注风险变化情况。

5）紧急风险处置：开源技术发生紧急安全风险时，信息安全团队、开源软件使用者按照《国信证券信息系统应急响应总预案》的相关要求进行紧急响应和处置。

8.2 合规风险管理

8.3 开源合规管理人员应对开源协议进行准确解读，并协同技术人员，根据企业实际情况明确在软件开发过程中可使用的开源协议（许可证白名单）和不应使用的开源协议（许可证黑名单）

8.4 开源软件合规风险识别

1）技术人员负责对新引入开源软件进行合规风险识别，判定新引入开源软件合规风险是否满足《开源软件合规风险策略》。通过采用专业的 SCA 扫描工具或者通过人工识别，对引入的开源软件进行合规风险预检，识别引入开源软件的合规风险信息，包括但不限于许可证名称、许可证类型、版权信息、风险类型等，经开源合规管理人员审核通过后，方可入库。

2）新引入开源软件合规风险未通过开源合规管理人员审核时，由技术人员评估开源软件引入的必要性，反馈原因，确需引入使用时，以例外事项由开源管控组审批。

3）通过专业的 SCA 扫描工具或者人工识别方式定期对存量开源软件进行合规风险识别。

8.5 开源软件合规风险评估

1）开源合规管理人员协同技术人员对于企业使用开源协议的风险进行系统评估，结合使用场景确定引入开源软件到系统的影响范围，影响范围评估维度包含但不限于传染性风险、侵权风险、违反开源许可证、版权瑕疵等。

2）根据合规风险评估结果，开源协议合规管理人员协同技术人员制定开源软件引入后的开源软件使用方案，并同时制定引入后切换回原有开源软件方案的回退机制。

3）根据合规风险评估结果，评估不通过时，由开源合规管理人员说明原因，并告知研发团队及技术人员，技术人员需另行引入可替换开源软件，或者由开源合规管理人员协同技术人员共同制定风险缓解方案或试用措施。

4）根据合规风险评估结果，评估不通过时，对识别出存量的合规风险问题，由开源合规管理人员协同技术人员，共同制定合规风险修复方案及风险控制措施。修复方案及风险措施包括但不限于宽松许可证替代、自研模块替代、代码隔离等，由研发团队进行处置。

8.6 开源软件合规风险处置

1）研发团队根据开源软件合规风险修复方案及风险控制措施进行风险修复及处置，并在规定期限内反馈处置进展。

2）如果因特殊原因，研发团队无法按时完成合规风险修复，应及时向开源协议合规管理人员反馈原因，并申请延期。

8.7 开源软件合规风险监测

1）开源合规管理人员对合规风险处置完成的开源软件进行备案登记，定期监测开源软件合规风险，包括但不限于回归扫描、许可审计、许可变更停更监测等。

2）回归扫描：由开源合规管理人员对开源许可证风险处置后的系统进行开源许可证回归扫描，确认合规风险处置完成。

3）许可审计：由开源合规管理人员对软件许可证进行定期审计，以确保所有的软件和项目均在许可证的规定下运行。

4）许可变更停更监测：开源使用方和运维方负责跟踪开源软件许可证变更事件，及时评估许可证变更后的合规风险和治理措施，并重新评估许可证是否涉及传染性、兼容性和冲突等风险，及时作出应对措施，保障使用的开源许可证合规性。

9 内源生态建设

9.1 内部开源工作流程

1）由项目创建方提交拟贡献资源，提交内容应包括资源说明文档或使用指引。

2）由信息安全团队对拟贡献资源的安全性、保密性等进行审核。

3）开源合规管理人员对项目适用的许可证风险进行审核。

4）经技术、安全、合规等相关方审核通过后由项目创建方将拟贡献资源上传至内部资源共享平台。

5）经技术、安全、合规等相关方评审后需停止共享的资源应及时退出平台，并发布停止共享说明。

9.2 内部资源整合与共享

1）通过内部资源共享平台对代码库、技术文档、最佳实践、工具和模板等内部资源进行整合共享。

2）由项目创建方提供相应资源的技术支持。

9.3 内源社区运营

1）应对内源社区访问权限进行控制，确保内部资源和信息的安全性和合规性。

2）定期开展开源知识培训，宣传内部开源工作流程及文化，鼓励员工积极参与知识分享、合作和开放式交流。

3）定期举办内部分享会、沙龙等，宣传内部开源项目的成果及价值，增加员工的参与度和认可度。

4）定期评估内部开源社区的运营效果，包括项目健康度、项目应用情况、社区活跃度等，并根据评估结果进行优化调整。

5）根据社区活跃度、项目应用情况和贡献情况等定期对开源技术贡献突出的团队和个人进行奖励。

10 开源生态建设

10.1 对外开源

10.1.1 为确保选取符合公司战略、社区需求和技术标准的对外开源项目，以解决行业共性问题、推动公司创新、强化社区合作，并提升产品质量和可持续发展，对外开源项目应进行选型评估，评估内容主要包括：

1）业务价值：选择项目时应为非核心业务，且为通用技术，并考虑其与国信证券业务目标和价值观的符合性。

2）技术贡献：评估项目对技术生态系统的贡献情况。

3）社区需求：分析社区对该项目的需求，以及项目在社区和所属领域的稀缺程度。

4）可持续发展：考虑项目的维护和可持续发展可行性。

10.1.2 完成对外开源项目选型后，应在国信证券内部逐步完成对拟开源项目的孵化。

1）初期内部开发：在国信证券内部先行开发和测试的项目，应确保项目质量和功能；如拟开源项目为已开发完成项目，则忽略该步骤。

2）内部社区培养：在内部开源社区培养早期贡献者，积累项目知识和文档。

3）逐步开放：逐步将项目对外开放，吸引更多的贡献者和用户参与。

10.1.3 拟开源项目孵化过程中应依据项目类型选择适合项目需求的开源许可证，确保选择的许可证不存在合规和兼容等风险，并且与法律政策和国信证券的开源策略相符。

10.1.4 拟开源项目孵化过程中应对项目进行全面评估和审查，以确保项目符合预期要求。对外开源项目评估可包括以下方面：

1）安全性：评估项目的安全措施，包括代码漏洞修复、安全审计和身份验证等，以确保项目对潜在威胁有足够的防范措施。

2）合规性：评估项目的开源许可证，确保项目的开源许可证符合国信证券安全标准及法律合规要求。

3）代码质量：评估项目代码的结构、文档、规范性和易读性等方面，以确保代码质量符合公司标准，并有利于项目的可持续发展。

10.1.5 拟开源项目应经过开源治理管控团队和开源治理决策团队审批后方可对外开源。

10.1.6 安排专人或团队负责对已开源项目进行持续运营，保持项目的活跃性和健康性。持续运营内容包括但不限于：

1）问题修复和维护：及时发现问题和修复 bug，确保项目的稳定性。

2）新特性支撑：根据用户需求和项目方向，逐步添加新的功能特性。

10.2 支持加强与科技企业、高等院校、科研院所、中介服务等机构交流合作，基于市场化原则开展开源技术联合研发和运营，加强开源技术人才培养，推进开源技术迭代升级，促进开源技术成果转化：

1）由开源治理管控团队和开源治理决策团队负责与科技企业、高等院校、科研院所、中介服务等机构的日常联络和协调工作。

2）在联合研发和运营过程中，应遵循市场化原则，确保各方利益的平衡和合理回报。

3）积极推广开源技术成果，可通过展览展示、技术交流会等活动，提高开源技术的知名度和影响力。

10.3 支持加入合法合规的开源社区、开源基金会等开源社会组织，参与开源技术规划设计、研发决策、社区运营等活动。

10.3.1 拟加入开源社会组织前，应该做如下的审核与评估：

4）资质审核：在加入开源社会组织前，应确保其具备合法合规的运营资质，避免涉及非法活动。

5）风险评估：对目标开源社会组织进行风险评估，包括其声誉、历史活动、成员构成等，以确保加入后的合作环境健康稳定。

6）合规性审查：审查开源社会组织的章程、协议等文件，确保其符合相关法律法规及监管要求。

10.3.2 加入开源社会组织应经过开源治理管控团队和开源治理决策团队审批方可加入。

10.3.3 参与开源社会组织应该遵循：

1）遵守章程：应严格遵守开源社会组织的章程、协议等规定，尊重组织的决策程序和规则。

2）透明沟通：在开源技术规划设计、研发决策等过程中，保持与开源社会组织的透明沟通，确保信息的准确性和及时性。

3）尊重知识产权：在参与开源项目时，尊重他人的知识产权，避免侵犯他人的合法权益。

4）积极贡献：积极参与开源社区的讨论、代码编写、测试等活动，为开源项目的发展做出贡献。

11 附件

表 1 开源技术引入评估表

评估类别	评估维度	评估方法

技术评估	行业认可度	考察开源软件使用情况，要求至少有 1 家相关领域公司使用
	产品活力	评估开源软件产品活跃度、社区活跃度、代码生命周期等情况，包括： 1）评估开源软件最近 3 个版本的发布间隔情况，周期越短则优先考虑； 2）评估开源软件最近一年中每季度的代码贡献量情况，贡献量越多则优先考虑； 3）评估开源项目支持度、项目关注数、项目复刻数、提问回复情况，数量越多则优先考虑。
	服务支持	评估开源软件文档质量、运维服务等支撑情况，包括： 1）优先考虑提供协助运维或托管运维方面支持的服务商； 2）评估开源软件文档支持情况。文档的数量宜多不宜少；软件源码、官网中的说明文档、帮助文档文字规模宜多不宜少；文档覆盖范围越全则优先考虑。
	兼容性	考察开源软件对不同硬件的兼容性、对不同操作系统的兼容性，是否能满足使用需求
	可维护性	评估开源软件模块化程度及代码规范性，包括： 1）查看千行代码的注释量不低于 5%； 2）应使用模块化设计； 3）紧密耦合组件宜少不宜多。 4）支持一般故障支持自动化处理（无需人工介入）； 5）开源软件的配置宜简单。
	可扩展性	评估开源软件对资源扩展及架构扩展的支持程度、二次开发的难易程度，包括： 1）支持大集群规模，水平扩展； 2）支持动态扩容和缩容； 3）优先选择定制开发改动量小，代码扩展性好的开源软件。
	功能性	评估开源软件功能是否完备，能否满足预期功能需求
	可靠性	评估开源软件容错性、易恢复性等，包括： 1）具备自动故障切换能力； 2）评估开源软件出现故障后是否可以快速恢复开源软件的功能，故障恢复时间宜低不宜高； 3）具备数据恢复能力，开源软件在故障下应保证数据一致性和防止数据丢失。

	易用性	评估开源软件对用户的使用、配置等的友好程度，包括： 1）有充分的应用案例，重要场景包含完整的示例代码； 2）评估安装和部署简易程度，如支持图形化安装部署、一键脚本安装部署等方式。
	性能效率	评估开源软件处理效率、容量、资源占用等，包括： 1）开源软件的 TPS 满足预估需求； 2）开源软件的 QPS 满足预估需求； 3）开源软件的平均响应时间满足预估需求； 4）开源软件的最大并发数满足预估需求； 5）服务调用成功率满足预估需求； 6）响应时间标准差满足预估需求； 7）主机 CPU 使用率满足预估需求； 8）内存占用率满足预估需求。
安全评估	安全性	评估开源软件漏洞情况，包括： 1）已暴露的漏洞宜少不宜多； 2）评估已暴露的安全漏洞是否已修复，或核查是否采取安全措施保证重大安全漏洞不会触发； 3）代码静态扫描结果无严重或高危漏洞。
合规评估	开源许可证	查看开源软件许可证信息，确保： 1）开源许可证信息明确； 2）自身无兼容性风险； 3）开源许可证信息不在公司开源许可证黑名单中。