ICS 35.240.40
CCS A 11

团　体　标　准

T/BFIA 014—2022

金融技术产品开源项目管理指南

Guidelines for open source project management of financial technology products

2022－08－16 发布　　2022－08－16 实施

北京金融科技产业联盟　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。

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专利的责任。

本文件由北京金融科技产业联盟归口。

本文件起草单位：中国工商银行股份有限公司、北京金融科技产业联盟、深圳前海微众银行股份有限公司、上海浦东发展银行股份有限公司、麒麟软件有限公司。

本文件主要起草人：潘润红、徐翥、吴冕冠、闫冬梅、周文泽、张远征、刘阳、王豪赞、聂丽琴、胡达川、李明艳、李寻、李璐、钟燕清、康悦、张榕秀、杨欣捷、弓豪怡、彭颖、王悦良、郑爽。

引　言

金融信息系统发展过程中，诞生了部分具有先进性的自研技术产品，且应用场景在同业机构间往往高度一致，如果通过依法合规分享开源技术应用经验，共享开源技术研究成果，将会促进金融科技产业降本增效，提升开源技术整体应用水平。目前，业界尚缺乏指导金融机构对自研产品进行开源管理的具体指导方法。

为此，本文件为金融机构在以自身技术发展路线为主导进行技术产品开源工作时，提供一种较为通用的项目式管理方法和操作流程，为金融机构逐步完成从规划准备到最终实施落地给予指导。

金融技术产品开源项目管理指南

1 范围

本文件给出了金融机构将自研技术产品进行对外开源时，在体系建设、流程管理、资源配置、运营等方面的指导。

本文件适用于银行业机构对技术产品实施自主开源，可供保险、证券等其他金融机构参考。

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

开源软件 open source software

一种可以获取源代码的计算机软件，这种软件的著作权持有人通过开源许可证将软件的复制、修改、再发布的权利向公众开放。

3.2

开源许可证 open source license

开源协议

用于规范受著作权保护的软件在规定条款和条件下使用或者分发等行为。

注：一般指具备广泛认可性的、具有法律性质的协议，目的是减少作者及用户针对开源软件权责的法律解释成本，常见开源许可证有GPL、MPL、BSD License等。

3.3

自研技术产品 self-developed technology products

金融机构通过内部研发、联合研发等方式，具有自主知识产权（如软件著作权、专利等）的技术产品。

3.4

项目开源 project open-source

将自研技术产品通过内部评估审批后，将源代码发布到代码托管平台并公开；开展推广运营；进行全行业共享共建的机构行为。

3.5

代码托管平台 code hosting platform

是面向开源软件项目托管平台，是存储、管理、维护源代码，促进项目协同开发的网络平台。

3.6

开源社区 open source community

是项目开发的组织形式之一，是由所有参与开发和改进源代码项目的用户组成的社群，在网站、邮件群组等形式组成的虚拟社区、代码托管平台中进行交流、合作开发及成果分享。

3.7

贡献者 contributor

对项目感兴趣并以某种方式做出贡献的个人或法人，贡献行为包括但不限于问题解答、撰写文档、提交代码、捐款等。

3.8

维护者 maintainer
协作者 collaborator

负有审查和合并来自贡献者的贡献内容的职责，并负责项目运维的人员，拥有对代码审核决策的权限。

4 开源项目体系建设

4.1 战略规划

对于存在开源意向的金融机构，宜将开源工作纳入信息化发展规划，制定合理的对外开源策略、具体实施方案。关注以下机制建设：

a) 建立由信息科技条线第一负责人牵头的顶层决策机制；
b) 设置“开源办公室”管理团队，统一内外部开源工作归口，
c) 建立跨部门协调机制，由战略发展、科技、法务、品牌等部门条线密切配合执行；
d) 建立流畅的开源项目评审机制；
e) 建立激励机制，引导、营造开放创新的内部开源文化与氛围。

4.2 组织架构建设

4.2.1 决策团队

负责决策和发布项目开源工作的管理规程和策略，其主要职责应包含以下内容：

a) 对管理团队制定的开源项目管理的流程及要求进行决策；
b) 组织开源项目的立项评审；
c) 组织开源项目版本发布的评审工作；
d) 建立重大决策及上报机制；
e) 建立开源文化推广、激励机制。

4.2.2 管理团队

负责根据项目类型与目标，执行开源策略，推动相关成员落实具体任务，其主要职责应包含以下内容：

a) 根据开源项目的战略定位、产品特性、资源投入等因素，评审项目是否适宜开源；
b) 规划项目发展路线、项目运营决策模式；

c) 保证项目在代码安全、功能性能、法规要求等方面达到可以对外开源的条件；
d) 确认开源许可证类型及适用于项目发展的代码托管平台，并负责代码托管平台相关权限管理；
e) 根据项目开源的目标，定期评估项目价值；
f) 建立对外沟通联络机制，方便业内沟通协作；
g) 对决定停止维护的项目，确定移交对象或发布停止维护公告。

4.2.3 执行团队

执行团队至少包含安全组、专业组、法律组共同配合开源工作，可根据项目评审结果设立运营组、财务组提供对应支持。各组主要职责如下。

a) 安全组：
   1) 对静态代码进行安全扫描，包括代码检查、静态结构分析、代码质量度量等静态测试；
   2) 对项目开展代码安全审查，包括项目中引用的其他开源代码；
   3) 对发现的漏洞等安全问题进行处置。
b) 专业组：
   1) 开源项目的技术架构把控，确保开源项目的技术架构水平符合业界主流水平；
   2) 制定项目文档清单，定义和审核开源项目的各类文档，包括项目介绍、安装使用说明、技术白皮书等；
   3) 制定开源代码规范，明确开源代码的代码格式、命名原则、文档注释等规范要求，提高开源代码的易读性，降低维护难度。
c) 法律组：
   1) 为开源项目组提供有效的许可证选型建议，确保声明、许可证中的披露要求、权利义务及免责等条款满足项目开源需求；
   2) 检查开源项目是否遵循并满足项目中引用的其他开源代码的许可证要求；
   3) 检查开源项目是否符合所在国家、地区的法律法规、政策、相关监管要求，如是否涉及商业机密、数据隐私等；
   4) 评估、审查预选的代码托管平台安全性、合规性，避免供应链风险，向管理团队提出建议；
   5) 开展侵权排查、许可证兼容性冲突检查等工作，确保项目的许可证、声明以及分发策略的合法性；
   6) 必要的软件著作权、专利、商标等知识产权保护申请。
d) 运营组：
   1) 根据不同级别的开源项目，规划相应的宣传方案、渠道和实施策略；
   2) 结合开源产业相关活动、资源平台进行外部宣传，并根据项目的运营表现、舆情等信息进行分析、反馈及处置；
   3) 协助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。
e) 财务组：
   1) 审核项目的整体投入合理性与充足性；
   2) 协助定期评估项目价值。

4.3 规范开源流程

4.3.1 规划阶段

规划阶段工作由项目发起方牵头，管理团队和执行团队各组共同参与，具体流程包含：

a) 明确项目开源的目标及意义，识别内外部可能参与或者受益的群体、自身须投入的资源，为项

目设立可持续发展的路线；

b) 针对项目开源涉及的法律合规、市场调研、运营宣传等工作与相关支持部门、小组提前沟通，进行可行性分析验证后，进入项目开源的立项评审流程。

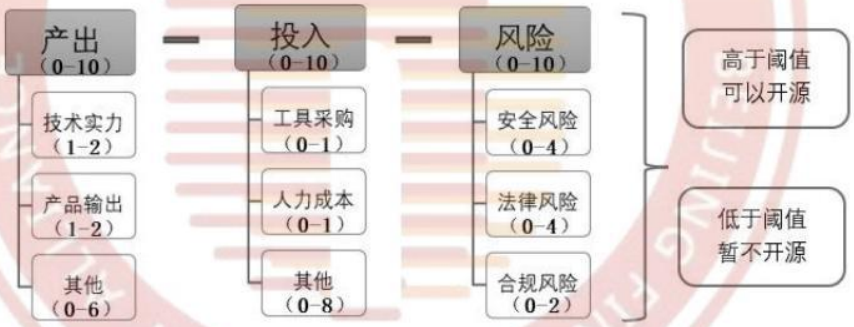
4.3.2 评审阶段

评审阶段由决策团队负责牵头，管理团队和执行团队相关工作组共同参与，流程及评估内容如下。

a) 评估投入及产出、安全及法律风险等因素：
   1) 产出项通常包含品牌、商誉、技术实力、产品输出、人才培养、社会责任；
   2) 投入项通常包含人力成本、资金占用成本、咨询费、平台建设与工具采购等费用；
   3) 安全及法律合规风险通常包含商业秘密泄露、许可证冲突、供应链投毒、漏洞攻击、知识产权侵权等。

b) 评估项目的等级分类，可参考以下形式分级：
   1) 战略级项目：评估认为产出巨大的机构级战略项目，宜由信息科技条线第一负责人、CTO决策。
   2) 成熟性项目：评估认为产出较高、目标清晰且可落地的项目。
   3) 孵化性项目：评估认为可落地实践，在某产出项上能够明显得到提高的项目。
   4) 不成熟项目：目标不清晰、投出产出不明确、安全及法律风险未排除的项目。

c) 参考上述评估因素，机构宜设置打分项、评分模型，给出具备开源条件的阈值，开源项目决策示例可参考图1。



注：各项具体分值由机构自行订立。

图1 开源项目决策示例

4.3.3 准备阶段

准备阶段工作由管理团队负责牵头，执行团队的各组共同参与，流程包含：

a) 按照内部开发过程管理规范、软件测试管理办法等相关要求，完成开发、测试、项目检测等工作；

b) 制定开源项目名称，根据项目初步分类，评估是否设计徽标、宣传标语等开源项目标识；

c) 完善相关文档，宜包含说明文档（readme）、代码规范、项目规划、功能说明、应用案例、贡献者指南、开源许可证等，便于项目开源后的推广应用；

d) 完善基础信息，如涉及商标、软件著作权等自主知识产权，宜先完成申请、备案等工作；

e) 选择许可证及代码托管平台，结合自身需求综合评估进行选择，所选的代码托管平台宜以易于开发者参与项目作为重要考量因素，如预期的生态伙伴、贡献者多数以中文为母语，宜优先考虑国内代码托管平台；

f) 如项目存在共建方，宜与共建方提前规划各阶段工作分工；

g) 规划建立开源社区，增强项目运营基础；
h) 制定项目开源后的社区规章制度、运营方式、贡献机制；
i) 由决策团队牵头建立检查清单，如功能性审查表、安全性审查表、法律合规审查表、代码来源记录表等，并对上述工作进行发布前审查，审查结果提交决策团队上级负责人批准后，正式对外开源。

4.3.4 实施及运营阶段

实施及运营阶段由管理团队牵头推动，执行团队各组负责对应工作，流程包含：
a) 项目审批通过后，将代码、文档等上传至代码托管平台，并正式对外开源；
b) 当项目存在重大版本更新或进行重要分支归并时，应在机构内部对项目的代码、文档等内容重新进行审查和审批；
c) 管理团队需定期根据项目开源检查清单进行重检，并同步检查结果；
d) 通过积极建设项目的社区，扩大项目影响力，定期实施渗透性测试，实现项目持续优化。

4.4 建立激励措施

4.4.1 制定企业级开源文化推广方案

企业级开源文化推广方案由运营组牵头，其他各组共同参与，具体内容包含：
a) 制定阶段性开源文化推广方案，内容可涵盖：开源理念传播、知识产权保护、开源商业模式解读、开源软件治理及社区运营知识等；
b) 围绕项目开源目标，制定以机构为责任主体的运营体系及流程，促进形成机构内部及外部广泛应用的活跃生态，制定项目的版本迭代计划、营销渠道等推广方案。

4.4.2 制定团队激励政策

管理团队定期评选出在推动开源项目功能迭代、品牌影响等方面表现突出的项目团队，主要评判标准可参考以下方面：
a) 项目取得阶段性成果或重大突破，如发布新版本；
b) 社区表现活跃，如沟通反馈频率高。

4.4.3 制定个人激励政策

管理团队定期评选在开源方面做出突出贡献的员工，主要包括两种类型：
a) 对推动项目社区发展、扩大影响力等起到重要作用；
b) 在项目的建设与推广过程中表现积极。

4.4.4 开源贡献积分制

团队或个人对项目开源或推广开源文化的贡献程度，管理团队可根据其具体行为采用积分制策略，便于量化统计与实施奖励。主要评判参考如下：
a) 举办或参与项目推广活动的次数；
b) 缺陷修复的次数；
c) 代码贡献量；
d) 问题反馈量。

5 规划阶段要求

5.1 明确工作目标

开源决策团队在项目开源之前宜明确如下事项。

a) 明确开源目的：
   1) 通过开源模式惠及其他行业，承担社会责任；
   2) 希望利用外部资源来进一步构建和完善自身产品；
   3) 探索发展商业模式。
b) 选择适宜开源的自研技术产品：
   1) 产品宜已具有一定的应用成果，宜解决金融机构在同质场景下的共性需求；
   2) 如果市场上已经有类似的开源软件，则更适合加入到已有的开源社区中去，避免浪费自身资源；
   3) 与管理团队沟通，提出对应的评估、审查要求。

5.2 规划项目决策机制

为推动项目成长，宜建立高效、中立的决策机制，决策团队宜采用平衡项目控制结构与贡献者积极性的决策方法，达到以下效果：

a) 确保各项决策符合项目的根本利益，不被其他特定的个人或组织所垄断；
b) 根据项目的发展、参与者的贡献情况，应允许逐步让渡部分或全部决策权及管理权给外部贡献者。

5.3 评估项目价值

根据项目开源目的、分级，管理团队及财务组宜从以下几类可量化指标对项目价值进行预测及持续性评估：

a) 经济效益评估：对于具备商业价值的开源项目，宜从项目的收益额、经济寿命周期、维护成本、市场竞争状况等方面进行评估；
b) 软件效能评估：对规划开源的软件其功能完善程度、资源利用率、代码复杂度、运维复杂度等内容进行评估；
c) 市场影响力评估：可从预期宣传渠道及频率、受众群体规模、已知及潜在参与机构数量等方面进行评估。

5.4 基本资源配置

管理团队为项目提供必要的资源投入，包括以下内容：

a) 项目开源之后须为感兴趣的开发者提供技术咨询与解答，吸引开发者快速参与到项目的贡献中；
b) 为项目的启动和维护提供所需的托管环境、构建环境、测试环境等基础设施资源的支持；
c) 创建项目统一交流访问所需的沟通发布平台，如项目官方网站、社区论坛、邮件列表、微信交流群等；
d) 如选择境外代码托管平台，或同步在境外代码托管平台进行镜像开源，提供项目全面信息的外语专业翻译。

5.5 其他配套支持

为促进项目开源之后的社区活跃度与行业反响，运营组可进一步提供提升项目影响力所需的运营、推广类资源，主要涉及以下内容：

a) 为开展技术培训提供讲师、专家等人力资源；
b) 建立和注册项目品牌商标；
c) 建立项目宣传网站并注册相应的域名，为用户提供更全面详细的项目介绍、管理组织、应用范围、相关标准、活动信息、代码托管平台链接等核心信息；
d) 为项目注册社交媒体统一账号。

6 准备阶段要求

6.1 技术及安全审查

技术及安全审查由安全组和专业组牵头，其他各组共同参与，具体内容包括：

a) 功能性审查：确保自研技术产品能够切实满足某一具体需求或解决问题；宜通过传统的市场分析、参与开源会议等手段，了解其他机构及开发者的需求，并尝试验证产品是否可以解决相应问题；
b) 安全性审查：确保开源的代码中不存在已知重大漏洞、不包含带有自身商业机密的代码注释或私有接口以及不适宜公开的其他内容。

6.2 合规法律审核

由法律组牵头，其他组共同参与，确保项目代码中涉及的各类许可证、授权或声明信息完备，如含有其他外部开源代码的，整体产品不与其涉及的开源许可证、授权或声明等法律约束存在冲突，并且不涉及侵犯其他机构或个人的知识产权。合规法律审核包括以下内容。

a) 确保开源项目发布的代码均具有明确的许可证和出处，审查验证本机构是否有权发布所有代码、对涉及的商标开展资产权利调查等。
b) 查看项目源代码中其他来源的开源代码对应的许可证要求。如发现许可证之间存在冲突或未遵守协议要求的，则反馈管理团队进行处置。可采用专业的扫描工具对项目源代码进行扫描，确保项目中对其他来源开源代码做出明确引用声明，并包含其对应的开源许可证、版权声明等内容。
c) 结合项目开源的目标与发展规划，评估选择适宜的开源许可证，确保项目所选许可证类型满足以上合规、法律审核要求与机构实际需求。由于开源许可证种类繁多，在选用开源软件时，至少评估如下因素：
   1) 修改源代码后是否需对修改部分进行开源；
   2) 是否允许用于商业用途、允许专利授权；
   3) 该软件的开发者是否免于责任承担；
   4) 开源软件和依赖软件之间许可证兼容性。
d) 为确保贡献者明确贡献内容知识产权归属、遵守开源许可证要求、避免知识产权纠纷，宜制定适宜的贡献者协议。

6.3 项目治理

在项目正式开源之前，各团队为项目治理制定必要的技术需求与决策角色：

a) 开源决策团队负责对管理团队制定的项目发展策略，包括项目技术路线、发布与更新频率、开发优先级等相关内容进行决策，确保所有参与者均能够了解项目变化的原因及发展方向；
b) 管理团队和专业组宜在项目早期建立项目贡献指南，包括特性和缺陷的跟踪方式、代码提交方式、发布流程的管理方式等；

c) 可通过设立项目管理委员会、技术管理委员会，结合规划的开源决策模式，制定项目管理规章制度，明确团队组成、角色职责、选拔投票规则、贡献者晋升路径等；
d) 建立开放友好的贡献机制，通过贡献者协议来明确贡献者行为准则、权利义务、适用范围。

6.4 项目里程碑

管理团队可结合开源项目的类型、业务规划、应用范围及功能迭代等预期，提前规划版本更新的发布频率，提供清晰的项目发展方向，利于吸引更多开发者参与项目开源运营。同时，决策团队宜对管理团队发布的版本进行审核。可参考以下分类：

a) 重点项目，如功能丰富、涉及业务影响较大的项目，可考虑按年为单位作为发布周期；
b) 普通项目，如功能单一、涉及业务影响较小的项目，迭代频繁，可考虑按照月、季度为单位作为发布周期。

6.5 完善配套设施

除了将项目托管第三方代码托管平台上，部分机构托管在自行搭建的仓库中。如选择自建代码托管平台，注意构建以下配套设施：

a) 具备自动化管理流程。通过在平台上集成管理工具等方式，保证项目在整个代码开发、提交、测试、发布过程中衔接平滑；
b) 具备便捷的沟通互动渠道。可将沟通工具集成到开发流程中，确保有较好的沟通方式可以对开源项目的需求、缺陷、问题、特性等提交、反馈和跟踪。当项目有新的代码提交请求、评论反馈、自动化构建或测试失败等任务时能够对项目开发者与社区成员进行实时通知。

7 实施及运营阶段

7.1 发布实施

初始项目完成准备阶段工作及内部审核后，管理团队将源代码、许可证等信息上传托管平台或仓库即完成了正式开源，项目即刻进入运营维护阶段。在项目发布之前，注意如下事项：

a) 确保项目基础设施都是可运行的、安全的、可扩展的；
b) 确保开发者可以加入和查阅项目主页；
c) 源代码及文档信息完备。

7.2 项目运营

各团队宜通过以下方式维护开源项目，促进项目健康、健全发展，实现开源目标。

a) 规范代码审核流程：
   1) 在代码提交方面，金融机构内部和外部贡献者在提交项目代码时，须确保所提代码的功能完整性，并修改相关的功能说明文档与相关非功能说明文档；
   2) 在代码审核方面，维护者宜定期开展代码安全和合规评估与审查，在对代码进行审核时，同时进行新增代码的安全性与合规性审核，确保新增代码不会对项目整体安全合规造成影响；
   3) 在版本发布与分支归并方面，当项目存在重大版本更新或进行重要分支归并时，须在机构内部对项目的代码、文档等内容重新进行审查和审批。
b) 提升项目影响力：
   1) 新项目在发布前期可通过联系种子用户、项目共建方、生态伙伴和所在领域技术栈相关媒体合作，建立初始社区；

2) 根据项目目标与规划，开展必要的营销推广工作；
3) 通过设置社区布道师、任命社区经理、举办交流会及团建等活动，持续组织开发者参与互动，共建社区并保持项目活跃度；
4) 通过参与内外部技术交流、修复缺陷、分享项目建设经验等方式提高项目代码价值。

c) 提升开发者的生产力和效率：
1) 在文化方面，引入开源领域专家不断参与社区活动，充分宣传开源理念，打造开源开放氛围；
2) 在流程方面，建立便于开发者快速实现代码贡献的技术管理策略；
3) 在制度方面，建立导师制度，让经验丰富的资深开源开发者为其他开发者提供指导。

d) 完善应急响应机制措施：
1) 执行团队内各组根据自身职责要求，对项目进行紧急复核，并重新给出评估报告；
2) 管理团队根据执行团队提交的各类评估报告，结合突发情况，制定应急措施，并提交决策团队审议；
3) 决策团队对管理团队提交的针对紧急情况的应急措施进行讨论决策。

e) 维护开源项目：
1）包含项目发展过程中的版本发布、项目文档完善、社区问题解决和需求评估等全流程工作；
2）在组织管理和项目迭代方面，总结项目发展过程中的经验教训，规划项目走向。

8 关闭项目

当开源项目对于金融机构来说不再具有运营维护的价值或意义，或遇上游开源组件供应中断且无可替代方案，宜将项目关闭或将项目移交给其他组织或个人，管理团队可参照以下情况进行评估，经决策团队确认后由执行团队操作处理。

a) 遇使用的上游开源组件供应中断时，宜优先寻求可替代方案，否则需执行项目关闭流程：
1) 确认上游开源组件供应中断原因及对本项目影响程度；
2) 如上游开源组件因侵犯第三方知识产权等法律因素导致其项目被迫关闭，立即停止本项目使用该上游开源组件，并寻找或自研替代该上游开源组件，同时发布公告停止涉及侵权版本下载和使用；
3) 如上游开源组件因自身运营原因关闭，可视该组件重要程度，选择自行独立维护、寻求其他可用开源项目替换或自研替换；
4) 如上游开源组件因技术原因主动衰退或关闭，当该组件为本项目非核心组件时，可寻求其他可用开源项目替换或自研替换该组件；当该组件为本项目核心组件时，本项目需再次进行技术评审，确认当前技术路线是否为主流技术发展路线，是否存在重大缺陷或瓶颈等问题，进而确定本项目是否仍然存在运营维护价值和意义。

b) 因项目不再具有运营维护价值和意义时，可通过移交项目给其他组织或个人，使项目继续得到维护和发展：
1) 在交接项目时进行必要的代码与文档更新；
2) 项目的移交宜通过实际的移交程序来完成，将主要项目和相关资源移交给新的维护者来完成；
3) 如项目建立在自建代码托管平台，需将项目迁移到其他代码托管平台，以使社区成员可继续访问和参与项目贡献，而不必被迫退出项目。

c) 如不能成功移交，则彻底关闭项目：
1) 评估用户量及产品替换难易度等因素，提前发布关闭公告，说明原组织不再继续维护项目，

预留合理时间后正式关闭；

2) 回收被关闭项目的基础设施并发布停止维护公告；

3) 对代码进行归档，如为自建代码托管平台项目，可将最终代码归档至第三方代码托管平台。

d) 移交或彻底关闭的执行决策，在内部审批流程获批后执行。