ICS 35.240.20
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0290—2024

金融业开源软件应用　管理指南

Open source software applications in financial industry—Management guidelines

2024－01－15 发布　　2024－01－15 实施

中国人民银行　　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提出。

本文件由全国金融标准化技术委员会（SAC/TC180）归口。

本文件起草单位：中国人民银行科技司、北京金融科技产业联盟、上海浦东发展银行股份有限公司、中国工商银行股份有限公司、中国农业银行股份有限公司、中国银行股份有限公司、中国建设银行股份有限公司、中国邮政储蓄银行股份有限公司、平安银行股份有限公司、深圳前海微众银行股份有限公司、中国光大银行股份有限公司、北京国家金融标准化研究院有限责任公司、中信百信银行股份有限公司、浙江网商银行股份有限公司、中国银联股份有限公司、网联清算有限公司、华为技术有限公司、腾讯云计算（北京）有限责任公司、阿里云计算有限公司。

本文件主要起草人：李伟、陈立吾、周祥昆、詹志建、刘帅、潘润红、聂丽琴、胡达川、李寻、万化、杨欣捷、弓豪怡、江一鸣、徐翥、孙刚、刘阳、闫晓林、刘建珍、王丽静、黄凯、金磐石、李鑫、胡军锋、张兰英、朱礼华、冯志强、郝巍、杜胜、丛洋、刘玉花、周夕崇、谢彦丽、张晋钰、李佳凝、薄舜添、周欢、辛子英、陆碧波、赵峰、边思康、周继恩、弓祎斌、杨阳、郭林、薛松源、吴涛、白阳、耿航、董宾、陈明、胡伟琪、王晶昱。

引　言

开源软件与传统闭源软件相比，在技术安全与运维等方面存在较多外部影响因素，可能导致安全合规问题。因此金融机构在应用开源软件时，宜对开源软件进行体系化的统一管理，提高应用效率，降低潜在风险。

本文件旨在针对开源软件特性提出对应的全流程管理方法，提升金融机构开源软件管理能力，控制开源软件应用风险。本文件可作为金融机构开源软件应用管理的参考标准，也可作为行业主管部门开展相关工作的参考依据。

金融业开源软件应用　管理指南

1　范围

本文件提供了金融机构在应用开源软件时的全流程管理指南，对开源软件的使用和管理提供了配套组织架构、配套管理规章制度、生命周期流程管理、风险管理、存量管理、工具化管理等方面的指导。

本文件适用于金融机构规范自身对开源软件引入、使用及退出的过程管理以及风险管控。

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。

GB/T 28458—2020　信息安全技术　网络安全漏洞标识与描述规范

GB/T 30276—2020　信息安全技术　网络安全漏洞管理规范

GB/T 30279—2020　信息安全技术　网络安全漏洞分类分级指南

JR/T 0289—2024　金融业开源技术　术语

JR/T 0291—2024　金融业开源软件应用　评估规范

3　术语和定义

JR/T 0289—2024 界定的术语和定义适用于本文件。

4　管理架构

开源软件管理架构如图 1 所示，其中包括配套组织架构、配套管理规章制度、生命周期流程管理、风险管理、存量管理和工具化管理等 6 部分内容，覆盖 2 个制度要素和 3 个技术管理流程，宜配置 1 个管理工具。金融机构可通过对以下 3 个层面的管理效果开展成熟度自评估，不断完善整体技术管理能力。

a）制度层面：在配套组织架构和配套管理规章制度上设置针对开源软件应用的管理要求。

b）流程层面：在开源软件从引入到退出的生命周期流程管理、风险管理和存量管理等 3 个方面提出管理要求。

c）工具层面：宜通过构建基础设施支撑开源软件管理，引入或搭建自动化工具提高管理效率。

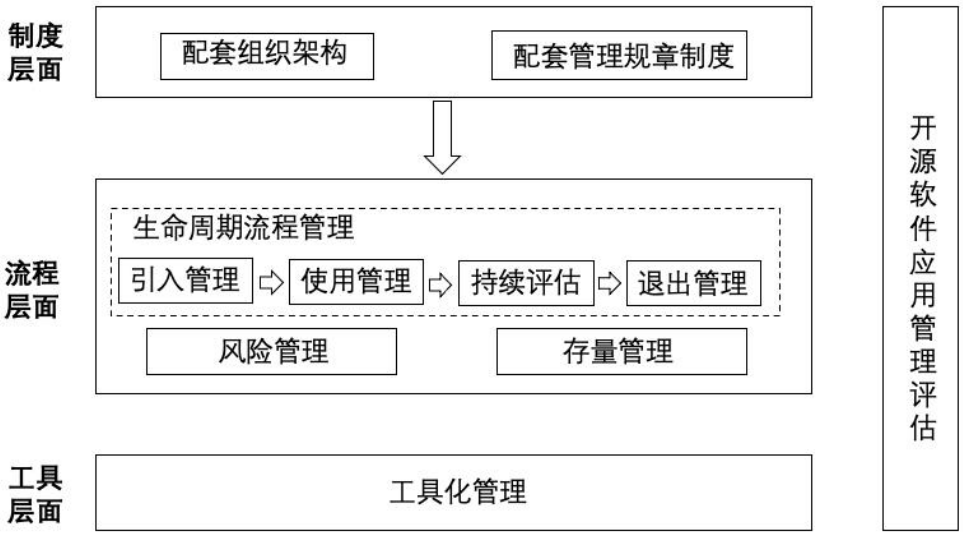

图 1　开源软件管理架构

5　配套组织架构

5.1　总则

金融机构宜健全开源软件应用管理的配套组织架构，明确职责分工。配套组织架构中主要包括决策团队和管理团队。

5.2　决策团队

决策团队第一负责人宜为金融机构技术条线总责任人，负责决策和发布开源软件应用管理规章制度、管理流程和管理策略。

5.3　管理团队

管理团队可为实体组织或虚拟型组织，负责制定和执行开源软件管理规章制度和管理流程，至少包含以下岗位人员及岗位职责。

a）专项人员：负责起草与维护开源软件管理规章制度和管理流程，并负责开源软件全生命周期日常管理的具体工作。

b）技术人员：负责对各类开源软件开展技术评估与运行维护工作。

c）安全人员：负责识别和跟踪开源软件安全漏洞风险和修复情况，实现全程可视、可追溯。

d）法务合规人员：针对开源软件引入和使用过程中所涉及的知识产权等法律问题，负责给出专业的法律建议，提供法务支持。

在管理团队中，除法务合规人员外，其余岗位人员及岗位职责可根据金融机构内部实际资源配置情况，选择职责兼并、一岗多责等形式建立和完善配套组织架构。

6　配套管理规章制度

6.1　生命周期管理

对开源软件在引入、使用及退出的全生命周期提出明确的管理规定，至少覆盖以下方面。

a）引入管理：制定开源软件引入流程规范，确保流程的统一性，明确要求开源软件经评估通过后再正式引入。

b）使用管理：制定内部开源软件使用规范，统一开源软件使用规则。

c）持续评估：针对开源软件应用过程中的风险点进行持续跟踪，规范各环节管理举措，至少包括以下措施。

——版本管理：制定开源软件的版本规范，宜明确更新版本及推荐版本，通过可信下载源获取并在制品仓库中统一管理。

——持续跟踪：明确开源软件全生命周期中应识别和处置的风险点，安排专项人员对其进行登记和追踪，并反馈相关人员进行处置。

d）退出：建立健全开源软件退出规则与操作流程，确保所制定的退出规则不与整体研发和运维基线要求发生冲突。

6.2 应急处置管理

针对开源软件出现重大安全漏洞、停服等突发情况，宜制定特定或整体的开源软件应急处置预案，规范应急处置流程，合理安排预案演练，做到及时有效地实施应急处置工作，降低风险影响。

7 生命周期流程管理

7.1 总则

金融机构宜建立开源软件流程管理机制，规范开源软件全生命周期中重点环节的管理举措。开源软件生命周期流程管理环节如图2所示。

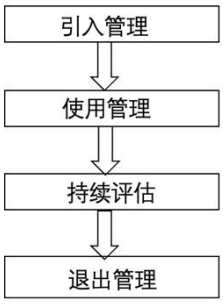

图2 开源软件生命周期流程管理环节

7.2 引入管理

金融机构建立开源软件引入流程时，宜对引入的开源软件进行全面记录；在引入评估时宜充分考虑各类开源软件的差异性。开源软件引入管理流程如图3所示，主要包括以下事项。

a）引入评估：

——对开源软件进行分类分级，例如根据开源软件技术领域、软件语言、软件颗粒度等进行分类分级。

——按照不同的分类分级标准，安排相应专业领域的技术人员对拟选用的开源软件进行评估。

——按照 JR/T 0291—2024 中的引入评估内容对各类开源软件进行综合评估。

b）信息管理：

——对引入的开源软件建立清单，详细记录开源软件版本、开源许可证等信息。

——构建制品仓库，安排专人对开源软件的来源进行统一控制和管理。

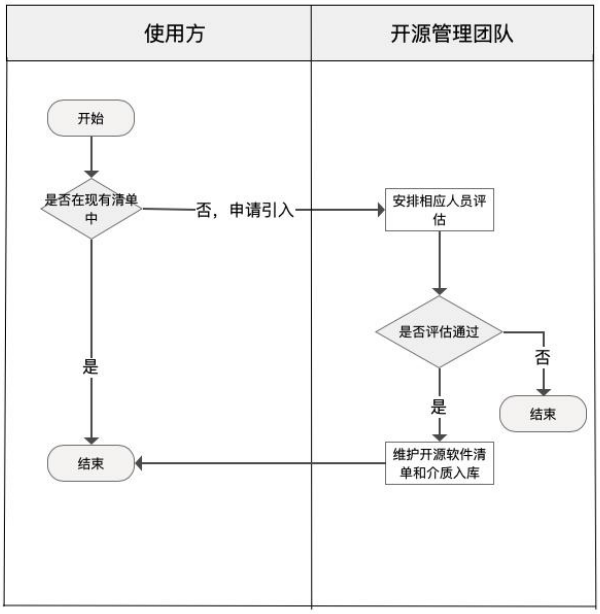

图 3　开源软件引入管理流程图

7.3　使用管理

金融机构宜明确开源软件使用规则，依据开源软件类别进行统一管理，至少建立开源软件应用台账，保证开源软件使用有迹可循。开源软件使用管理流程如图4所示，主要包括以下事项。

a）从制品仓库获取相关介质，不宜自行下载。

b）依据开源软件使用情况建立台账，实时记录开源软件的使用版本、使用部门、系统名称、联系人等，保证开源软件的使用情况可追溯，并安排技术人员对开源软件提供运维支持。

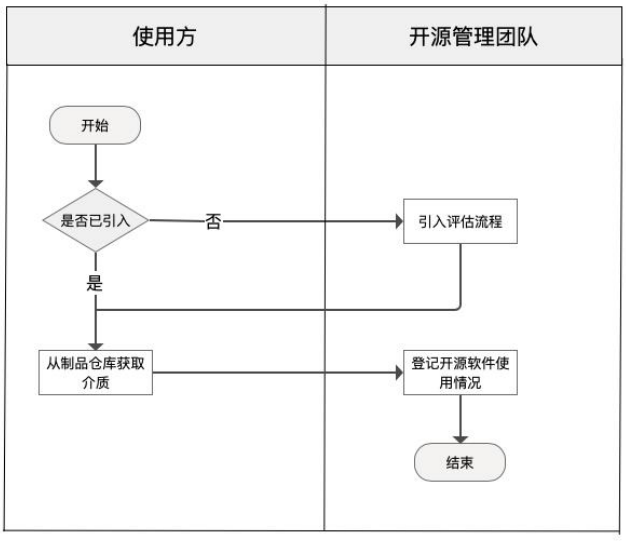

图4　开源软件使用管理流程图

7.4　持续评估

金融机构宜持续关注开源软件使用过程中存在的风险情况，进行监控、登记、反馈，根据风险类型快速采取措施并及时处置，避免造成安全合规等方面问题，开源软件持续评估流程如图5所示。评估内容主要包括以下事项。

a）安全漏洞评估：

——持续评估开源软件安全漏洞信息，评估是否存在公共信息渠道中公开的安全漏洞信息。

——安全人员对安全漏洞进行登记，形成安全漏洞详情文件，包括安全漏洞详情、受影响的软件及其版本，并将安全漏洞信息及时反馈给相关使用部门和技术人员，可结合 GB/T 30276—2020、GB/T 30279—2020 相关要求进行处置。

b）版本评估：以开源基础软件为主，定期评估是否存在版本过低、更新频次过低等问题，对于需要废除的软件版本或软件，通知相关人员进行版本升级或软件更换。

c）开源许可证评估：以开源基础软件为主，定期跟踪开源许可证情况，出现开源许可证变更时，更新软件清单并重新评估开源许可证是否为著佐权许可证、是否存在开源许可证兼容性问题等风险。

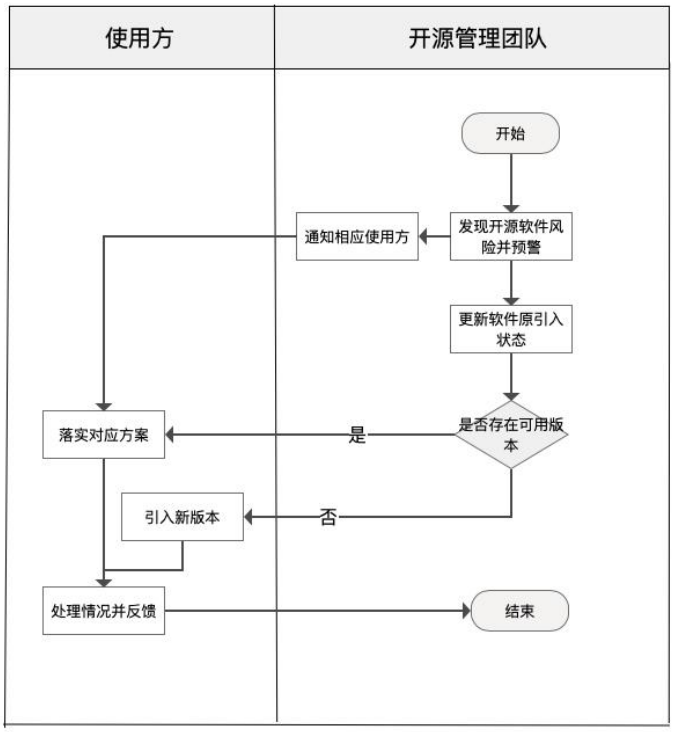

图 5　开源软件持续评估流程图

7.5　退出管理

当金融机构所应用的开源软件已无法满足功能需求和性能需求、发现当前版本存在重大风险隐患或该开源软件已停止更新等情况时，宜进行退出评估。可按照 JR/T 0291—2024 中的有关要求，对于评估后需退出的开源软件，制定退出计划，进行统一记录和管理，建立对应的流程化管理机制，开源软件退出管理流程如图 6 所示。开源软件的退出可通过开源软件版本升级或开源软件更换来实现，主要包括以下事项。

a）升级机制：

——制定开源软件版本更新方案，存在软件版本收敛需求时，宜明确推荐的版本。

——定期升级为推荐版本。

——升级版本时，按照 7.2 履行对应的评估工作。

b）更换机制：

——制定开源软件更换方案。

——按照 7.2 履行对应的评估工作。

c）退出机制：

——定期评估之后，有规划地对开源软件进行退出操作。

——进行退出操作后，及时通知相应人员更新相关信息。

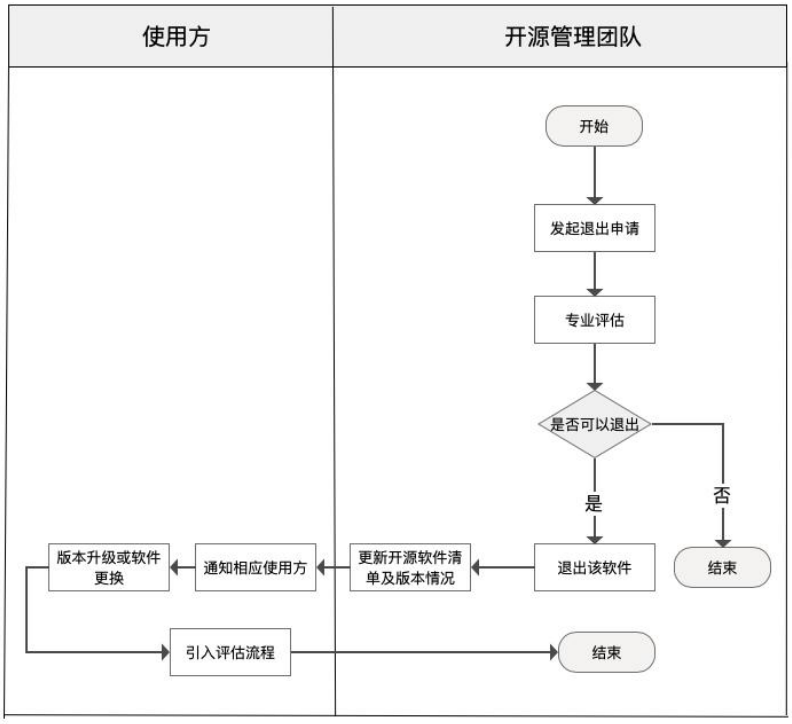

图 6　开源软件退出管理流程图

8　风险管理

8.1　总则

金融机构宜建立开源软件风险管理机制，对开源软件全生命周期中存在的风险点作出识别、记录，进行动态管控与及时处置。

8.2　风险识别

为提高开源软件风险防范意识，金融机构可通过以下风险点进行识别。

a）法律风险：

——根据潜在的定制开发需求、所应用的业务系统重要等级等因素，评估开源许可证在发生变更、出现兼容性问题、未履行开源许可证要求时，可能出现侵害知识产权的风险。

——对于不存在专利许可条款说明的开源许可证，可通过专业的法务合规人员进行评估。

b）安全漏洞风险：在引入开源软件前进行漏洞扫描，排查是否存在安全漏洞，以及评估安全漏洞的等级。

c）供应链风险：在开源软件使用过程中，注意上游社区资源发生转移、源码或文档中承载政治主张、恶意代码注入等风险。对于第三方服务商提供的开源软件或开源代码，宜要求第三方服务商在可交付成果中提供开源软件或开源代码的相关信息。

8.3 风险记录

专项人员对开源软件风险点进行记录与及时反馈，主要包括以下事项。

a）持续评估：对开源软件的安全漏洞、版本、开源许可证等信息进行全面、统一记录。

b）建立内部沟通机制：安排技术人员、安全人员及法务合规人员对风险进行管控，遇到问题宜及时通过内部沟通渠道反馈给相关人员。

8.4 风险处置

金融机构对识别发现的开源软件风险问题进行分析，并制定处置方案，根据风险类别主要分为安全漏洞风险、法律风险和供应链风险，具体处置方式如下。

a）若存在安全漏洞风险，宜从以下方式中选择：

——安装开源社区、开源软件厂商发布的升级补丁以修复安全漏洞。

——及时更新至安全漏洞修复版本。

——修复安全漏洞并提交社区合并。

b）若存在法律风险，例如出现开源许可证兼容性问题，若难以采取其他可替代软件、隔离等有效风险应对措施进行规避，则进行退出操作。

c）若存在供应链风险，则对开源软件进行升级操作或退出操作。其中，对于第三方引入风险，由第三方供应商进行处置，同时宜加强对软件供应商在开源软件风险方面的约束，可通过开源软件成分分析、获取开源软件物料清单、要求提供安全合规评测结果、制定约束性条款等方式避免风险损失。

8.5 风险评价

开源软件管理部门宜定期通过以下3个方面进行风险评价。

a）开源软件使用情况。

b）开源社区支持情况。

c）开源软件供应商服务品质。

9 存量管理

金融机构宜针对开源软件的存量情况进行梳理、记录与分析，管理措施至少包含以下内容。

a）制定和更新存量开源软件的管理策略与计划。

b）识别、记录开源软件，对开源软件的版本号、开源许可证、官方网站地址或可信下载源、制品仓库地址等进行记录并持续更新，形成开源软件清单。

c）对使用开源软件的系统名、联系人、使用部门等进行记录，形成开源软件应用台账。

d）监控和全面排查存在风险的存量开源软件，参考GB/T 28458—2020记录安全漏洞情况，与责任人建立沟通。

10 工具化管理

金融机构在进行内部软件资产盘点时，如评估认为自身引入的开源软件类型丰富、数量较多，可通过构建工具的方式对开源软件进行高效管理。工具类型主要包括以下2种。

a）构建金融机构内部管理平台，通过开源软件的线上流程化管理，实现以下需求：

——组织架构：通过平台内置金融机构内部相关人员职责分工，线上处理有关工作及向相关人员反馈问题。

——流程管理：通过平台实现开源软件全流程线上化、自动化管理。

——开源软件信息展示：将开源软件引入记录、评估结果、推荐版本、基础信息、应用台账等信息集合到平台上，便于对开源软件进行可视化展示及统一管理。

——社区信息展示：获取代码托管平台上的开源软件在社区内的相关数据，并在平台上进行展示，帮助金融机构进行开源软件评估选型。

——制品仓库：统一管理开源软件制品仓库。

b）第三方开源软件自动化扫描工具能够帮助金融机构更快速、准确地跟踪和记录开源软件相关信息，实现以下需求：

——开源软件台账：实现定期扫描开源软件使用情况，自动记录更新使用开源软件的系统、联系人等，形成开源软件台账。

——安全漏洞跟踪：通过定期扫描开源软件代码，查看是否存在中高危安全漏洞。

——开源许可证跟踪：定期扫描开源许可证，查看和提醒是否存在变更或存在兼容性问题等风险。

11　开源软件应用管理评估方法

11.1　评估层级

金融机构可通过将开源软件应用管理程度划分等级、明确管理项目的方式，对开源软件的管理效果开展成熟度自评估，提升开源软件治理能力。管理成熟度从低到高分别为如下层级。

a）探索级：执行了开源软件应用管理的部分工作，尚未形成规范性流程和制度。

b）提升级：形成明确的架构分工和完善的管理流程制度，对开源软件进行流程化管理。

c）成熟级：通过利用开源软件管理工具等对开源软件进行专业化和自动化管理。

11.2　评估模式

表 1 可作为评估开源软件管理效果的依据，通过对照开源软件在管理维度、层级、具体管控项达成情况，提升相应的开源软件应用管理能力。

表 1　开源软件应用管理成熟度表

维度	管理程度	管理子项	达成情况
配套组织架构	探索级	职责分工	对开源软件进行分散管理，尚未建立明确的职责划分。
	提升级	职责分工	a）有相应人员负责开源软件管理工作，有较为清晰的职责分工。 b）外部法务人员兼任开源法务咨询工作。

表1　开源软件应用管理成熟度表（续）

维度	管理程度	管理子项	达成情况
配套组织架构	成熟级	职责分工	a）具备清晰具体的管理角色与分工，有相应的专项、安全及法务团队。 b）实现线上处理相关工作，及时向相关人员反馈，责任到人。
配套管理规章制度	探索级	制度规范	形成配套管理规章制度，但尚未规范全生命周期中各环节管理举措。
	提升级	制度规范	形成完善的管理规章制度，对开源软件的全生命周期管理提出明确规定，明确全生命周期中的风险点。
	成熟级	制度规范	根据内部实际情况持续更新优化开源软件管理规章制度内容。
流程管理	探索级	使用管理	制定重大系统使用的开源软件管理规章制度，可对其进行全流程管理和安全漏洞持续跟踪。
	提升级	引入管理	a）从多个维度对开源软件进行评估。 b）形成开源软件清单，对拟引入的开源软件进行统一的记录和管理。
		使用管理	a）制定开源软件使用规范，记录开源软件使用情况。 b）构建制品仓库，对开源软件的来源进行控制和管理。
		持续评估	a）对开源软件的版本、开源许可证和安全漏洞进行定期的跟踪。 b）对安全漏洞信息进行监控、记录，形成安全漏洞详情。
		退出管理	a）制定开源软件退出机制，明确开源软件退出或废除操作流程。 b）退出后有具体后续操作要求。
	成熟级	引入管理	通过工具或平台，安排不同领域的技术人员对开源软件进行评估，实现开源软件线上管理。
		使用管理	a）可利用工具实现自动记录开源软件的使用情况，形成开源软件使用台账。 b）通过平台，对开源软件进行分类分级管理。 c）对制品仓库进行管控，定期进行统计和更新。 d）定期组织开源软件的技术交流和培训。
		持续评估	a）通过工具定期自动化扫描开源软件漏洞、开源许可证、版本等信息。 b）自动通过开源社区、代码托管平台等渠道获取相关信息进行评估。

表1　开源软件应用管理成熟度表（续）

维度	管理程度	管理子项	达成情况
流程管理	成熟级	退出管理	通过平台对开源软件进行快速退出操作。
风险管理	探索级	记录与处置	出现安全漏洞时通过人工方式排查，并进行记录和处置。
	提升级	记录与处置	a）建立开源软件风险管理机制，实现对各类风险点进行记录和风险管控。 b）建立流程化风险控制机制，可进行全面的风险识别，规范风险记录和处置措施。
	成熟级	记录与处置	a）通过平台，对开源软件风险进行实时监测、信息记录和线上管理，实现快速反应、处置和登记结果。 b）建立敏捷沟通途径，发现风险时做到及时和相关人员进行沟通反馈。 c）针对开源许可证等相关风险，通过系统提示，快速采取处置措施。
存量管理	探索级	梳理盘点	人工记录分析主要应用的存量开源软件相关信息。
	提升级	梳理盘点	通过清单及台账对存量开源软件进行全面排查。
	成熟级	梳理盘点	通过自动化工具对存量开源软件信息进行详尽记录，并将变更情况做实时更新记录。
工具化管理	探索级	高效管理	分散记录开源软件相关信息，尚未实现全流程线上化管理。
	提升级	高效管理	构建金融机构内部管理平台，实现开源软件全流程线上化管理。
	成熟级	高效管理	引入自动化扫描工具与内部管理平台对接，更快速、准确地跟踪和记录开源软件相关信息。

参 考 文 献

[1] GB/T 42927—2023 金融行业开源软件测评规范

[2]《中国人民银行办公厅 中央网络安全和信息化委员会办公室秘书局 工业和信息化部办公厅 中国银行保险监督管理委员会办公厅 中国证券监督管理委员会办公厅关于规范金融业开源技术应用与发展的意见》（银办发〔2021〕146号）.2021-9-28