ICS 35.240.40
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0291—2024

金融业开源软件应用　评估规范

Open source software applications in financial industry—Specification for evaluation

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/TC 180）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、网联清算有限公司、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、上海浦东发展银行股份有限公司、平安银行股份有限公司、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、深圳前海微众银行股份有限公司、浙江网商银行股份有限公司、中国平安保险（集团）股份有限公司、华为技术有限公司、腾讯云计算（北京）有限责任公司、浪潮集团有限公司、北京百度网讯科技有限公司、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、强群力、郑仕辉、刘超千、张群、郭林、张文凌、赵彤、薛松源、吴涛、包仕翔、孙刚、罗致力、刘阳、蔡仕志、闫晓林、刘建珍、王丽静、黄凯、金磐石、李鑫、杨欣捷、弓豪怡、杜胜、贾凯、刘玉花、周夕崇、谢彦丽、张晋钰、李佳凝、薄舜添、周欢、辛子英、钟燕清、丛洋、陆碧波、谭翔、赵峰、龙凯、苏威硕、白阳、邱成锋、胡正策、耿航、董宾、姜江、陈明、杜守志、刘牧、黄云、胡伟琪、王晶昱。

引　言

在金融业信息系统建设过程中，开源软件得到了广泛应用，在促进金融机构科技创新和数字化转型等方面发挥了积极作用，但也带来安全、合规等方面的风险与挑战。因此，有必要对开源软件的引入、维护、退出阶段进行规范，提出相应的评估指标。

本文件旨在针对开源软件使用过程中的风险与难点，提出一套完整的开源软件生命周期管理各阶段评估项与评估方法，降低金融机构开源软件评估过程的复杂度和时间成本，提升金融机构开源治理能力。

金融业开源软件应用　评估规范

1　范围

本文件规定了金融机构在应用开源软件时的评估要求，对开源软件的引入、维护和退出提出了实现要求、评估方法和判定准则。

本文件适用于金融机构对应用的开源软件进行评估。

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。

JR/T 0289—2024　金融业开源技术　术语

3　术语和定义

JR/T 0289—2024界定的以及下列术语和定义适用于本文件。

信息系统　information system

由计算机系统、网络系统软件硬件及其相关设备、设施、应用软件等构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

[来源：JR/T 0140—2017，3.2]

4　缩略语

下列缩略语适用于本文件。

CPU：中央处理单元（Central Processing Unit）

CVE：公共漏洞与曝光（Common Vulnerabilities and Exposures）

HTTP：超文本传输协议（Hypertext Transfer Protocol）

I/O：输入/输出（Input/Output）

QPS：每秒请求查询次数（Query Per Second）

TCP：传输控制协议（Transmission Control Protocol）

TPS：每秒事务处理次数（Transaction Per Second）

5　总体要求

在金融业信息系统的建设过程中，引入的开源软件按照实际应用情况，可分为开源基础软件、开源组件和开源工具3类，各阶段应用评估要求主要包括以下内容。

a）引入时，不同开源软件的功能特性、性能效率存在差异，且可靠性、安全性、兼容性、可扩展性等方面也应全面考察，因此开源软件引入评估应包含引入流程和较为全面的引入指标。
b）维护时，规范阐述如何确保开源软件运行过程的自主可控，对简单使用类、深度使用类与定制开发类的开源软件分别提出不同的维护要求。
c）退出时，应根据业务需求或软件迭代进展，有序完成版本更新或软件更换。

6 开源软件引入评估

6.1 开源软件引入流程

开源软件引入流程共分为3个阶段，如下图所示。

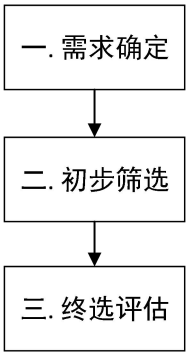

图 开源软件引入流程图

开源软件的引入流程具体内容如下。
a）需求确定阶段应明确软件功能需求与非功能需求。
b）初步筛选阶段应根据需求展开调研，依照初选评估要求（见6.2），对开源软件进行评估，建立若干可进入终选评估的开源软件名单。
c）终选评估阶段应根据初选阶段建立的开源软件名单，依照终选评估要求（见6.3）进行评估，并确定最终引入的开源软件。
对于开源组件类,若对应的应用程序通过了各项测试,可认为该程序中所有组件均满足了相关要求。
对于开源工具类，可在引入、维护、退出阶段适配对应指标。

6.2 初选评估要求

6.2.1 开源许可证

金融机构在选用开源软件时，应遵守该开源许可证对使用、修改等行为的规定，开源许可证评估内容见表1。

表1 开源许可证评估内容表

序号	评估项	评估方法	示例	适用对象
1	使用者在修改源码后宜允许对修改部分进行闭源。	查看文档。	核查开源许可证文档，对于修改后的代码无开源要求。	开源基础软件、开源组件。

表 1　开源许可证评估内容表（续）

序号	评估项	评估方法	示例	适用对象
2	宜对变更进行声明。	查看文档。	核查开源许可证文档，条款要求开源软件发生变更时需向用户进行声明。	开源基础软件、开源组件。
3	宜选择宽松型或弱著佐权开源许可证。	查看文档。	核查开源许可证文档，有对应免责条款，无特定IP段限制、无特定设备限制、无企业资本限制、无工作模式限制等限制性条款。	开源基础软件、开源组件。
4	应评估开源许可证兼容性。	查看文档。	a）若开源软件中存在多个开源许可证，确保多个开源许可证之间不存在冲突。 b）比对开源软件和依赖软件之间许可证兼容性，确保开源许可证之间不存在冲突。	开源基础软件、开源组件。
注：1.对于独立于开源许可证的专利授权场景，在引入阶段着重评估此专利授权条款。 2.本文件中的查看文档指查阅代码托管平台记录、设计文档、开发文档、源码、管理文档、漏洞平台、审计报告、自查报告、社区公示信息等相关材料。				

6.2.2　产品认可度

产品认可度反映了开源软件在行业生产实践中的应用情况，产品认可度评估内容见表2。

表2　产品认可度评估内容表

序号	评估项	评估方法	示例	适用对象
1	应评估使用者数量与行业分布。	查看文档。	开源软件在多个行业中广泛使用或在同行业中至少1家机构已使用。	开源基础软件、开源组件。

6.2.3　产品活跃度

产品活跃度反映了开源软件的可持续性和可进化能力，主要从开源软件的版本发布情况、开源社区情况、软件关注情况等方面进行评估。产品活跃度评估内容见表3。

表3　产品活跃度评估内容表

序号	评估项	评估方法	示例	适用对象
1	应评估开源软件的版本发布周期，周期间隔越短则优先考虑，例如最后一次更新时间在3个月内。	查看文档。	核查开源软件最近3个版本的发布间隔，间隔不超过3个月。	开源基础软件、开源组件。
2	应评估参与者的代码贡献量。	查看文档。	核查最近1年中每季度的代码贡献量情况，该数值越高表示社区越活跃，更可能获得长期支持，并优先考虑。	开源基础软件、开源组件。

表 3　产品活跃度评估内容表（续）

序号	评估项	评估方法	示例	适用对象
3	应评估开源社区活跃度。	查看文档。	核查项目支持度、项目关注数、项目复刻数、提问回复情况，社区活跃度高则优先考虑。	开源基础软件、开源组件。
4	应评估项目代码提交情况。	查看文档。	核查开源软件的提交总次数、项目代码合并请求次数，提交次数越多表示开发者活跃程度越高。	开源基础软件、开源组件。
5	应评估贡献者数量。	查看文档。	核查开源软件近3年每季度贡献者数量变化情况，贡献者数量呈上升趋势则优先考虑。	开源基础软件、开源组件。
6	应评估前 10 位贡献者所属组织。	查看文档。	核查前10位贡献者来源是否集中于某1个公司，贡献者来源多则优先考虑。	开源基础软件、开源组件。
7	应评估前 3 位贡献者代码量占比。	查看文档。	核查并统计前3位贡献者的代码量占据前10名总量的比例，比例小则优先考虑。	开源基础软件、开源组件。
8	应评估前 10 位贡献者国别差异。	查看文档。	核查并统计前10位贡献者的国别集中度，国别差异大则优先考虑。	开源基础软件、开源组件。

6.2.4　行业支持情况

行业支持情况反映开源软件在业界提供专业化服务的情况，行业支持情况评估内容见表4。

表4　行业支持情况评估内容表

序号	评估项	评估方法	示例	适用对象
1	应评估商业支持情况。	查看文档。	a）核查服务商提供协助运维或托管运维等方面的支持情况，商业支持种类越多则优先考虑。 b）服务提供商数量越多则优先考虑。	开源基础软件、开源组件。
2	应评估组织、机构对开源软件的贡献情况。	查看文档。	除了个人代码贡献者，以组织、机构为责任主体的代码贡献者越多则优先考虑。	开源基础软件、开源组件。
3	应评估说明文档的数量、质量等支持情况。	查看文档。	a）文档的数量宜多不宜少。 b）官方网站中的说明文档、帮助文档文字的数量宜多不宜少。 c）文档含有图例、代码示例，简单易懂，与开源软件关联度越强则优先考虑。	开源基础软件、开源组件。
4	应评估文档覆盖范围。	查看文档。	核查官方网站中的文档覆盖范围，文档覆盖范围越全则优先考虑。	开源基础软件、开源组件。
5	应评估开源软件技术发展路线是否清晰。	查看文档。	在社区、官方网站等渠道有开发规划等信息公示，开源软件的技术发展路线越清晰则优先考虑。	开源基础软件、开源组件。

表 4　行业支持情况评估内容表（续）

序号	评估项	评估方法	示例	适用对象
6	应评估是否有中文支持。	查看文档。	具有中文版本的说明文档且及时更新，相关的开发工具、管理工具和运维工具的中文支持情况越多则优先考虑。	开源基础软件、开源组件。

6.2.5　功能特性

不同软件用于解决不同场景的特定问题，其功能特性也不相同，对于功能的评测应结合具体场景进行，功能特性评估内容见表5。

表5　功能特性评估内容表

序号	评估项	评估方法	示例	适用对象
1	应评估该开源软件的核心功能。	查看文档。	核心功能满足评测场景的功能需求。	开源基础软件、开源组件。
2	应评估该开源软件功能覆盖是否全面。	查看文档。	开源软件的扩展功能丰富，可满足应用需求。	开源基础软件、开源组件。

6.2.6　安全性

初步筛选阶段安全性重点考查已暴露的漏洞情况，安全性评估内容见表6。

表6　安全性评估内容表

序号	评估项	评估方法	示例	适用对象
1	应综合评估开源软件的安全漏洞数及等级。	查看文档。	a）结合开源软件关注度、发行时间（年数）对开源软件安全漏洞数进行综合评估。可将已暴露的安全漏洞数/（开源软件分支数×发行时间）的值作为评判依据，宜低不宜高。 b）已暴露的安全漏洞等级宜低不宜高。	开源基础软件、开源组件。
2	应评估开源软件已暴露安全漏洞的修复情况。	查看文档。	核查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（例如CVE）已被修复或不会触发。	开源基础软件、开源组件。
3	应通过代码扫描评估该开源软件安全情况，应保证代码扫描后无严重安全漏洞或高危安全漏洞。	a）查看文档。 b）测试系统。	核查是否有代码扫描记录，并进行代码静态扫描，保证扫描后无严重安全漏洞或高危安全漏洞。	开源基础软件、开源组件。

表6　安全性评估内容表（续）

序号	评估项	评估方法	示例	适用对象
4	应评估开源软件自身安全机制。	查看文档。	a）安全漏洞修复时效性高，可快速修复。 b）安全漏洞反馈渠道清晰。	开源基础软件、开源组件。
注：本文件中的测试系统指利用专业工具，通过对目标系统的扫描、探测等操作，使其产生特定的响应等活动，通过分析响应结果，获取证据以证明开源软件的基本要求、性能、安全性是否得以有效实施。				

6.2.7　可靠性

重点考察开源软件自身或者结合其他开源软件的高可用性，在出现故障时是否具备自动故障切换能力和容错能力，可靠性评估内容见表7。

表7　可靠性评估内容表

序号	评估项	评估方法	示例	适用对象
1	应评估该开源软件故障处理能力。	a）查看文档。 b）测试系统。	a）验证不同场景下，开源软件自动切换的能力。 b）开源软件出现故障后具备可以快速恢复的功能。	开源基础软件、开源组件。
2	应评估该开源软件的容错能力。	a）查看文档。 b）测试系统。	在部分节点宕机后仍可提供服务。	开源基础软件、开源组件。
3	应评估开源软件的故障修复时间。	a）查看文档。 b）测试系统。	故障恢复时间宜短不宜长。	开源基础软件、开源组件。
4	应评估开源软件自身的数据恢复能力。	a）查看文档。 b）测试系统。	开源软件在故障下可保证数据一致性和防止数据丢失。	开源基础软件、开源组件。
5	应评估开源软件的运行状态监控能力。	a）查看文档。 b）测试系统。	监控指标可覆盖系统运行状态。	开源基础软件、开源组件。

6.2.8　兼容性

可通过查看文档的方式评估开源软件的兼容性，例如开源软件对不同硬件的兼容性、对不同操作系统的兼容性。

6.3　终选评估要求

6.3.1　安全性

终选阶段安全性重点考查安全机制方面的支持情况。安全性评估内容见表8。

表8　安全性评估内容表

序号	评估项	评估方法	示例	适用对象
1	应评估是否具备鉴权功能。	a）查看文档。 b）测试系统。	对外直接提供服务、接口调用服务的开源软件，具备密码登录等访问控制功能。	开源基础软件。
2	应评估是否支持加密通信。	a）查看文档。 b）测试系统。	a）在远程运维通信过程中采用校验技术或密码技术保证数据的完整性。 b）采用密码技术对敏感通信内容或整个通信报文进行加密，保证数据的保密性。 c）加密算法和密钥长度是否符合国家密码管理部门及行业主管部门要求。	开源基础软件、开源组件。
3	应评估是否支持集成外部认证插件。	a）查看文档。 b）测试系统。	对外部插件具有认证功能则优先考虑。	开源基础软件。

6.3.2　可靠性

终选阶段可靠性重点考察外部开源软件长时间无故障运行的能力，系统可在极限情况下长时间稳定运行，保证业务成功率以及执行效率，可靠性评估内容见表9。

表9　可靠性评估内容表

序号	评估项	评估方法	示例	适用对象
1	应评估开源软件的稳定性，评估其无故障运行的能力。	测试系统。	根据系统的重要性设置差异化可靠性评估指标。例如对于实时重要信息系统，测试系统在极限情况下至少稳定运行24小时，核查监控指标是否正常。	开源基础软件、开源组件。

6.3.3　性能效率

终选阶段性能效率重点考查在实际压测环境下开源软件的TPS、QPS、平均响应时间、最大响应时间、最大并发数、服务调用成功率、时间标准差、CPU使用率、内存占用率、带宽占用及I/O情况，性能效率评估内容见表10。

表10　性能效率评估内容表

序号	评估项	评估方法	示例	适用对象
1	应评估该开源软件的TPS是否满足预估需求。	a）查看文档。 b）测试系统。	a）查看软件说明文档声明的测试场景下TPS数值。 b）在业务需求场景下测试系统，在满足预估需求的情况下，TPS数值越高则优先考虑。	开源基础软件、开源组件。

表 10　性能效率评估内容表（续）

序号	评估项	评估方法	示例	适用对象
2	应评估该开源软件的QPS是否满足预估需求。	a）查看文档。 b）测试系统。	a)查看软件说明文档声明的测试场景下的QPS。 b)在业务需求场景下，系统并发查询交易信息，交易信息查询吞吐率越大则优先考虑。	开源基础软件、开源组件。
3	应评估该开源软件的平均响应时间是否满足预估需求。	a）查看文档。 b）测试系统。	a)查看软件说明文档声明的测试场景下的平均响应时间。 b）在业务需求场景下，平均响应时间越短则优先考虑。	开源基础软件、开源组件。
4	应评估该开源软件的最大响应时间是否满足预估需求。	a）查看文档。 b）测试系统。	a)查看软件说明文档声明的测试场景下的最大响应时间。 b）在业务需求场景下，最大响应时间越短则优先考虑。	开源基础软件、开源组件。
5	应评估该开源软件的最大并发数是否满足预估需求。	a）查看文档。 b）测试系统。	a)查看软件说明文档声明的测试场景下的最大并发数。 b）在业务需求场景下，最大并发数越大则优先考虑。	开源基础软件、开源组件。
6	应评估服务调用成功率是否满足预估需求。	a）查看文档。 b）测试系统。	a)查看软件说明文档声明的测试场景下的服务调用成功率。 b）在业务需求场景下，服务调用成功率越高则优先考虑。	开源基础软件、开源组件。
7	应评估响应时间标准差是否满足预估需求。	a）查看文档。 b）测试系统。	a)查看软件说明文档声明的测试场景下的响应时间标准差。 b）在业务需求场景下，响应时间标准差越小则优先考虑。	开源基础软件、开源组件。
8	应评估主机CPU使用率是否满足预估需求。	a）查看文档。 b）测试系统。	a)查看软件说明文档声明的测试场景下的主机CPU使用率。 b） 在业务需求场景下， 主机CPU使用率越低则优先考虑。	开源基础软件、开源组件。
9	应评估内存占用率是否满足预估需求。	a）查看文档。 b）测试系统。	a)查看软件说明文档声明的测试场景下的内存占用率。 b）在业务需求场景下，内存占用率越低则优先考虑。	开源基础软件、开源组件。
10	应评估带宽占用是否满足预估需求。	a）查看文档。 b）测试系统。	a)查看软件说明文档声明的测试场景下的带宽占用。 b）在业务需求场景下，带宽占用率越低则优先考虑。	开源基础软件、开源组件。

表 10　性能效率评估内容表（续）

序号	评估项	评估方法	示例	适用对象
11	应评估I/O情况是否满足预估需求。	a）查看文档。 b）测试系统。	a）查看软件说明文档声明的测试场景下的I/O情况。 b）在业务需求场景下，I/O数值越小则优先考虑。	开源基础软件、开源组件。

6.3.4　兼容性

兼容性包括硬件兼容性、操作系统平台兼容性、数据库兼容性、开源软件版本之间的兼容性，以及编程语言的兼容性、协议兼容性、同一运行环境的其他组件兼容性、开源软件与国产操作系统兼容性，兼容性评估内容见表11。

表11　兼容性评估内容表

序号	评估项	评估方法	示例	适用对象
1	应评估硬件兼容性。	a）查看文档。 b）测试系统。	查看文档并进行系统测试，核查开源软件的运行是否对硬件有特殊要求，例如服务器型号的要求。	开源基础软件、开源组件。
2	应评估操作系统的兼容性。	a）查看文档。 b）测试系统。	a）开源软件支持在多个操作系统上兼容。 b）在不同的操作系统上无需重新编译。	开源基础软件、开源组件。
3	应评估数据库兼容性。	a）查看文档。 b）测试系统。	核查是否支持多种数据库，数据库支持种类越多则优先考虑。	开源基础软件、开源组件。
4	应评估开源软件版本之间的兼容性。	a）查看文档。 b）测试系统。	升级后的版本与升级前版本在系统间数据交互的参数、格式等方面未发生变更。	开源基础软件、开源组件。
5	应评估编程语言的兼容性。	a）查看文档。 b）测试系统。	兼容主流开发语言接口（例如JAVA、C++等）。	开源基础软件、开源组件。
6	应评估协议兼容性。	a）查看文档。 b）测试系统。	支持主流协议（例如TCP、HTTP等）。	开源基础软件、开源组件。
7	应评估与同一运行环境的其他软件的兼容情况。	a）查看文档。 b）测试系统。	同一运行环境下，可兼容存在依赖关系的其他软件。	开源基础软件、开源组件。
8	应评估开源软件与国产操作系统的兼容性。	a）查看文档。 b）测试系统。	在国产操作系统上功能正常，运行稳定。	开源基础软件、开源组件。
注：1.JAVA是1种计算机编程语言，被广泛用于开发各种应用程序和网络应用程序，包括网站后端、客户端应用程序等。 2.C++是1种计算机编程语言，被广泛用于开发系统软件、应用程序、驱动程序和游戏等，具有高性能、可移植性、灵活性等优点。				

6.3.5　可维护性

可维护性即维护人员对该开源软件进行维护的难易程度，具体包括理解、改正、改动和改进该软件的难易程度，可维护性评估内容见表12。

表12　可维护性评估内容表

序号	评估项	评估方法	示例	适用对象
1	应评估代码可读性，例如评估是否使用模块划分、代码注释使用情况等。	a）查看文档。 b）统计工具。	a）应使用模块化设计。 b）代码的注释量不低于5%。	开源基础软件、开源组件。
2	应评估运维复杂性。	查看文档。	a）紧密耦合组件宜少不宜多。 b）应支持一般故障自动化处理，无需人工介入。 c）开源软件的配置简单。	开源基础软件、开源组件。
3	应评估在线变更能力。	a）查看文档。 b）测试系统。	关键配置参数支持在线变更。	开源基础软件、开源组件。

6.3.6　可扩展性

可扩展性主要包括分布式系统下节点的水平扩展、动态扩展及代码扩展能力，可扩展性评估内容见表13。

表13　可扩展性评估内容表

序号	评估项	评估方法	示例	适用对象
1	应评估水平扩展能力。	a）查看文档。 b）测试系统。	支持大规模集群和水平扩展。	开源基础软件、开源组件。
2	应评估动态扩展能力。	a）查看文档。 b）测试系统。	支持动态扩容和动态缩容。	开源基础软件、开源组件。
3	应评估代码扩展能力。	a）查看文档。 b）测试系统。	优先选择定制开发改动量小、代码扩展性好的开源软件，例如微内核加插件式设计思想的软件具有比较好的代码扩展性。	开源基础软件、开源组件。

6.3.7　易用性

易用性描述了开源软件的学习成本、安装和部署的难易程度等。易用性评估内容见表14。

表14　易用性评估内容表

序号	评估项	评估方法	示例	适用对象
1	应评估使用开源软件的学习成本。	查看文档。	应用案例充分且质量良好、重要场景包含完整的示例代码，能够较快熟练操作。	开源基础软件、开源组件。
2	应评估安装和部署的难易程度。	a）查看文档。 b）测试系统。	支持图形化安装部署、一键脚本安装部署等方式，安装和部署简易。	开源基础软件、开源组件。

7 开源软件维护评估

7.1 自主可控程度分级

为保证金融业信息系统运行稳定、可控，在开源软件维护过程中，金融机构应根据开源软件的自主可控程度将开源软件进行分类管理，根据其对主营业务的影响程度分为简单使用类开源软件、深度使用类开源软件与定制开发类开源软件。

a）简单使用类开源软件：可搭建环境，且功能可正常使用。

b）深度使用类开源软件：在满足简单使用类开源软件要求基础上，掌握开源软件容灾容错机制、实现原理、核心算法等重要内容。

c）定制开发类开源软件：在满足深度使用类开源软件要求基础上，熟悉代码实现、设计思路，通过定制开发能够较好地满足平台需求。

在开源软件维护阶段，应至少满足简单使用类开源软件的要求。

7.2 简单使用类开源软件维护

简单使用类开源软件维护评估内容见表15。

表15 简单使用类开源软件维护评估内容表

序号	评估项	评估方法	示例	适用对象
1	应评估开源软件是否正常运行且满足需求。	a）查看文档。 b）测试系统。	搭建环境后开源软件正常运行，功能与说明文档一致，核心功能支持业务需求。	开源基础软件、开源组件。
2	应对开源软件进行漏洞修复及补丁升级。	查看文档。	a）具备漏洞定期扫描和修复的记录。 b）生成漏洞扫描报告或现场进行漏洞扫描。 c）根据漏洞等级及时修补。	开源基础软件、开源组件。
3	应建立指标定期监控机制。	查看文档。	a）对开源许可证、功能特性、安全性、可靠性和性能效率、产品活跃度等方面建立监控策略。 b）建立相应的监控机制，对上述指标内容进行监控并形成监控记录。 c）对于产品活跃度监控指标发生变动，或产品版本不活跃的开源软件进行进一步评估。	开源基础软件、开源组件。
4	应通过软件制品仓库对开源软件进行管理。	查看文档。	开源软件源码以及升级（补丁）包应保存在软件制品仓库，并提供统一访问地址。	开源基础软件、开源组件。
5	应形成统一的开源软件目录清单，并进行定期维护、更新和发布。	查看文档。	核查文档，形成统一的开源软件目录清单，进行定期维护、更新和发布，并有相应的记录。	开源基础软件、开源组件。

7.3 深度使用类开源软件维护

深度使用类开源软件维护评估内容见表16。

表16　深度使用类开源软件维护评估内容表

序号	评估项	评估方法	示例	适用对象
1	应满足简单使用类开源软件的维护要求。	参考7.2评估方法。	参考7.2示例。	开源基础软件、开源组件。
2	应评估开源软件服务高可用能力。	a）查看文档。 b）测试系统。	a）掌握开源软件核心算法、高可用实现方式，当部分节点故障时，确保数据一致且不丢失。 b）形成部分节点故障时的恢复方案。	开源基础软件、开源组件。
3	应评估开源软件所依赖的服务出现版本更新或故障（或部分故障）对开源软件的影响。	查看文档。	形成开源软件的依赖服务清单，对该类服务出现版本更新或故障（或部分故障）所可能造成的影响进行分析，制定对应的应急预案。	开源基础软件、开源组件。
4	应评估开源软件出现故障时对业务造成的影响。	查看文档。	形成开源软件故障时的应急预案并建立相应的持续优化机制。	开源基础软件、开源组件。
5	应评估开源软件重要指标阈值设置与告警及处置机制情况。	a）查看文档。 b）测试系统。	a）可使用监控工具对开源软件的主要功能、性能、业务数据进行监控并设置阈值，依据设定的阈值（或默认阈值）实时告警。 b）可建立超出阈值的应急处置预案。	开源基础软件、开源组件。
6	应评估开源软件的可监控功能。	查看文档。	可通过搭建监控运维平台，以自动化脚本方式实现对开源软件自身故障数据监控与处理。	开源基础软件、开源组件。
7	应评估开源软件故障解决能力。	查看文档。	可通过源码分析等方式确定问题产生的原因并形成解决办法。	开源基础软件、开源组件。
8	应持续评估重要开源软件出现版本更新等变化时对现有系统的影响。	查看文档。	出现缺陷、安全漏洞及社区更新（例如功能架构改变、开源许可证更新）时，可及时完善应急处置方案。	开源基础软件、开源组件。
注：重要开源软件指在核心链路中一旦出现故障影响较大的开源软件。				

7.4　定制开发类开源软件维护

定制开发类开源软件维护评估内容见表17。

表17　定制开发类开源软件维护评估内容表

序号	评估项	评估方法	示例	适用对象
1	应满足深度使用类开源软件的维护要求。	参考7.3评估方法。	参考7.3示例。	开源基础软件、开源组件。

表17　定制开发类开源软件维护评估内容表（续）

序号	评估项	评估方法	示例	适用对象
2	应评估开源软件的核心技术掌控程度。	a）人员访谈。 b）测试演练。	技术人员熟悉开源软件的实现思路、容错容灾机制、底层数据流向、存储方式、计算原理等核心内容。	开源基础软件、开源组件。
3	应评估开源软件的持续优化能力。	a）查看文档。 b）人员访谈。 c）测试系统。	根据使用过程中开源软件出现的问题与不足，分析、掌握每个功能的缺点、性能瓶颈，梳理可优化项，对开源软件持续优化。	开源基础软件、开源组件。
4	应评估开源软件产品化能力。	查看文档。	持续完善定制开发的开源软件功能、性能，梳理功能需求，将其封装为产品，对外提供服务，并不断提供技术支持和技术迭代更新，探索产品化输出。	开源基础软件、开源组件。
注：1.人员访谈指与被测系统或产品有关人员进行交流、讨论等活动，获取相关证据，了解有关信息。 2.测试演练指结合测试场景的搭建，通过模拟实际应用场景、灾难环境等，从基础知识、代码审查、性能测试、安全测试到应急响应测试等层面，对处置方式、效率、有效性等进行综合评估的过程。				

8　开源软件退出评估

对于开源软件当前版本已无法满足功能、性能需求，或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，应进行退出评估。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。开源软件退出评估内容见表18。

表18　开源软件退出评估内容表

序号	评估项	评估方法	示例	适用对象
1	应评估开源软件退出机制。	查看文档。	开源软件的退出应经过评审并制定退出计划，退出计划应至少包含可行性分析、对现有业务及系统的影响、升级或更换的软件调研分析及其生效日期的提示。	开源基础软件、开源组件。
2	应评估开源软件的升级具备兼容性。	a）查看文档。 b）测试系统。	升级后版本与退出的版本在参数、功能等方面均可兼容。	开源基础软件、开源组件。
3	应评估开源软件在升级后开源许可证的变化。	查看文档。	开源许可证如发生变化，应按照6.2.1进行重新评估。	开源基础软件、开源组件。
4	应评估更换的开源软件。	参考6评估方法。	应按照6进行重新评估。	开源基础软件、开源组件。

9 证实方法

查看金融业信息系统中所应用的软件清单或台账，对于种类与本文件一致的开源软件，是否有按照本文件的评估项，在引入、维护、退出等阶段形成评审记录及操作记录等信息。

参 考 文 献

[1] GB/T 40473—2021（所有部分） 银行业应用系统 非功能需求
[2] JR/T 0140—2017 中小银行信息系统托管维护服务规范