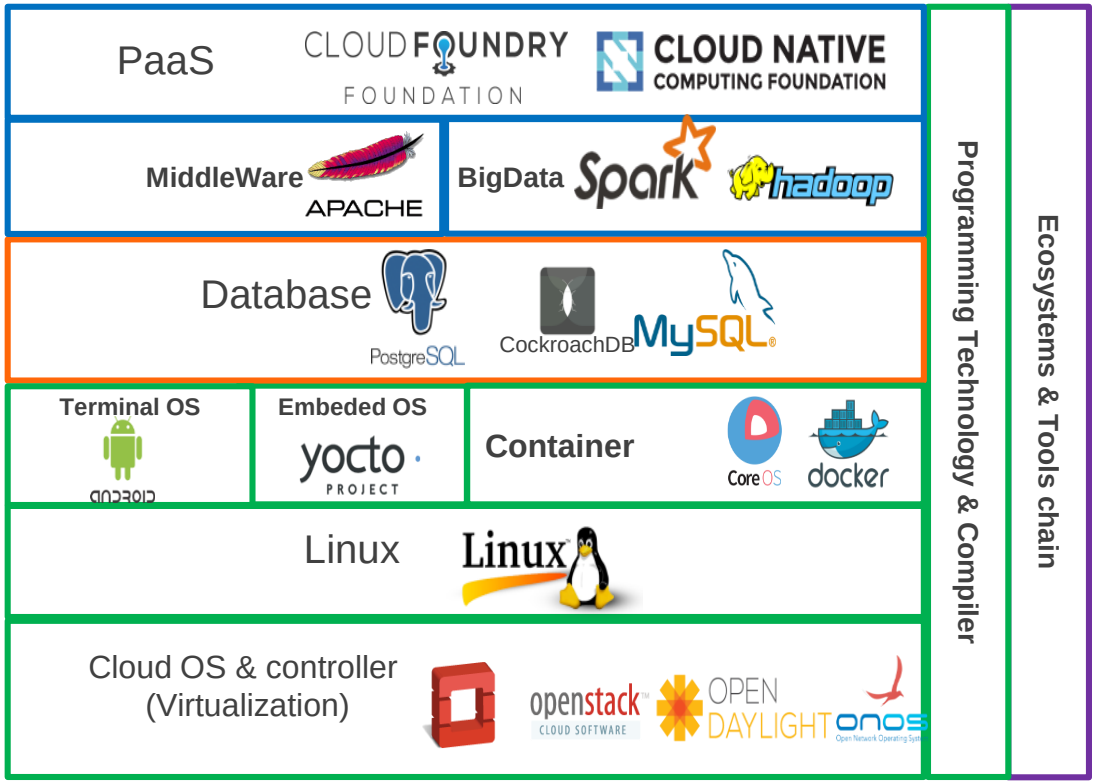
浦发银行开源治理分享

杨欣捷

2019年7月

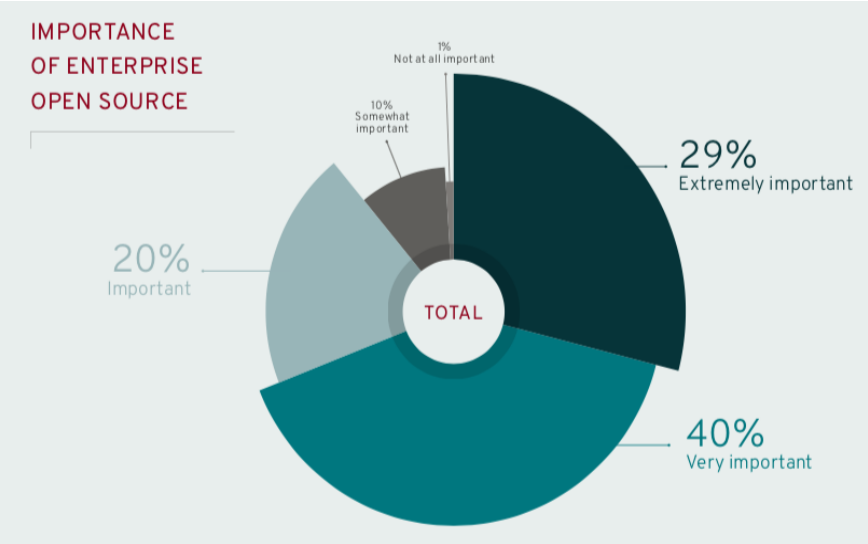
1.1 背景: 开源技术

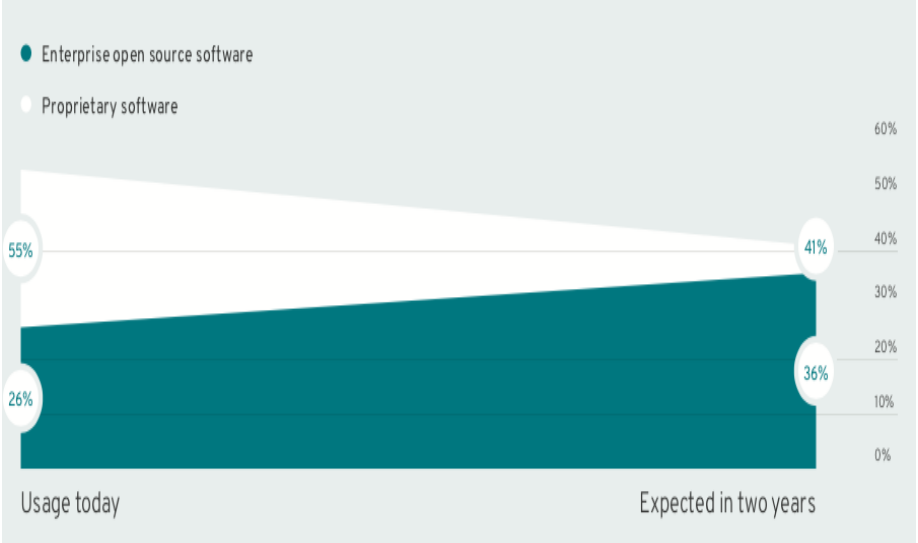


- 山寨商业软件-->引领技术创新
- 生产方式-->生态竞争
- 个人兴趣-->企业和商业
- 开源软件吞噬世界

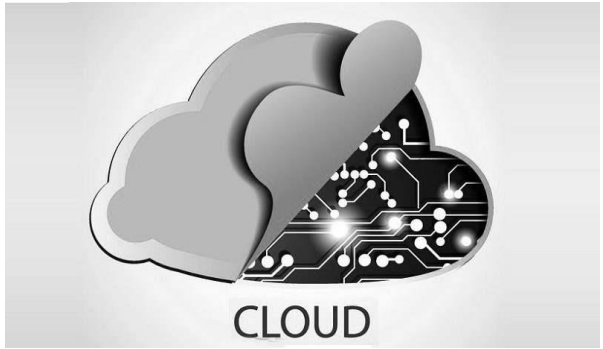
1.1 背景: 开源技术

RedHat的报告，开源软件在企业战略中的重要性，开源软件使用率趋势





1.1 背景: 开源软件相对商业软件的优势（技术角度）



生态优势，云服务市场越来越大，云服务一般基于开源软件。

开源软件很多源于大型互联网公司，这些公司比商业软件公司更懂得客户需求，他们自己就有最好的客户场景。

技术高速发展，快速适应市场的大背景下。架构选型中开发人员的话语权越来越大。一般情况下，预算不在开发人员手里，所以倾向于选择开源免费的软件。

1.2 背景: 开源软件的经济学悖论

分工悖论

- 市场分工推动经济发展，经济发展的结果也必然是市场分工的细化。
- 为何开源业态中，**非软件公司为何投入大量资源研究和开发基础软件**?

分享悖论

- 人类本性是追求个人利益最大化。
- 为何开源业态中，**大量的个人无偿分享其劳动成果?**

开源经济也是人类经济活动的组成部分，

不会脱离经济学基本规律

1.2 背景: 开源业态的经济学悖论

分工悖论的解释

- 在信息充分流动的条件下，市场**最终**会达到供需平衡（达到稳定态）
- 互联网时代，**产品更新速度跟不上市场需求的变化**
- 开源社区利用互联网直接打通了需求和供给，产品能够第一时间捕捉到市场的实际需求，利用各种社区资源迅速实现需求
- **社会分工原则并未打破，只是市场模型并未处于稳定态**

没有顶级IT实力的传统企业，拥抱开源，实际就是在**自身有限的IT资源**和**力求快速应对市场需求**的一个妥协。

- **应对市场的速度：**
  自主开发>开源>商业产品
- **IT人力投入：**
  自主开发>开源>商业产品

1.2 背景: 开源业态的经济学悖论

分享悖论的解释

- 仅靠自身力量不足以维持产品长期的竞争力
- 引入社区力量降低开发成本
- 用极低的成本迅速占领市场，提供商业化订阅和支持服务
- 相比于商业软件许可方式，这是一种低投入低营收的商业模式

- 个人通过软件许可方式获利运作成本高，前期投入大，周期长
- 开源工作成果有利于快速提升个人知名度和“身价”

开源并没有打破经济学的理性人假设，只是**改变了软件的获利模式。**

1.2 背景: 开源业态的经济学悖论

1

由此可见，开源业态的特点能解释分工悖论和分享悖论。

不仅如此，正是这些特点，决定了即便是传统行业，

要想快速应对互联网时代瞬息万变的市场需求，必须积极拥抱开源技术

2

对于传统企业，拥抱开源，获得更快速灵活的应对需求能力的同时，

意味着整体IT投入的加大

开源的价值更多体现在“开源”上，而非“节流”上

1.3 背景: 开源与风险

从软件商转移给了用户

专利	著作权	许可证	收费
维护	服务	质量	安全

1.4 背景: 开源使用风险案例(1)(2)

软件来源：非可靠来源的开源软件，被植入后门，造成重大数据泄漏

事件概述：

2012.1月，中文版开源软件putty、WinSCP、SSH Secure被发现有后门，有后门的软件都来自非官方授权的中文打包分发网站。

造成的影响：

后来泄漏出的数据表明，有1万多个服务器帐号被泄露。

软件许可：未遵循版权约定，被起诉

事件概述：软件自由法律中心起诉三星等违法GPL的企业

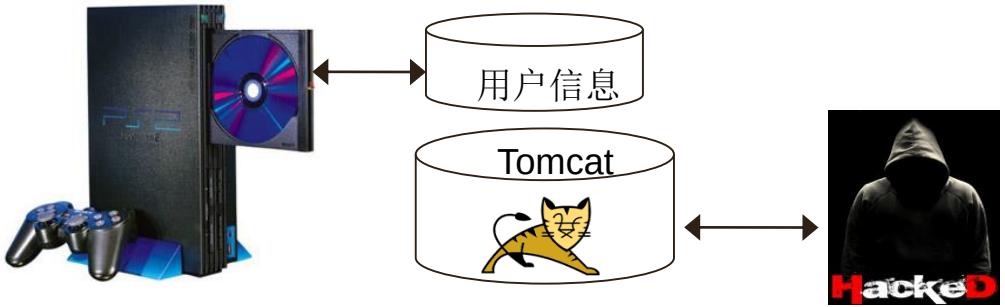
2009年12月，软件自由保护组织 (SFC) 与 软件自由法律中心(SFLC) 宣布对违反GPL的企业采取法律诉讼，这些企业大部分都是消费类电子产品，其中包括全球500强的三星电子。被列入被告的企业还有百思买集团，三星电子美国，西屋电子，JVC美国，西部数据，台湾合勤科技，以及其它违反GPL2的电子设备。这些消费类电子产品使用了Busybox，并经SFLC索取代码仍不愿开源，故被起诉到纽约南区法院。

1.4 背景: 开源使用风险案例(3)

生命周期管理：PlayStation因Tomcat没有修复漏洞，丢了用户信息

- **事件：2011年5月，Sony公开承认**，有黑客通过非法手段从PlayStation网络用户数据库中**窃取了超过7000万个人用户资料**。更令索尼网络游戏用户担心的是，**1000万个人信用卡账号**也存在遭窃可能。

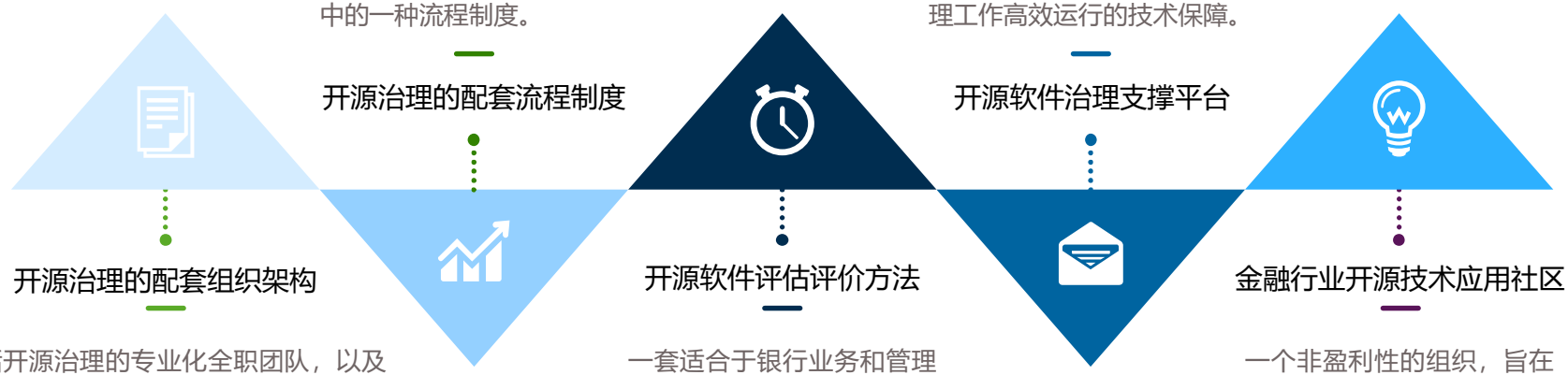
原因：使用老版本Tomcat，没及时与社区版本同步，黑客通过公开的漏洞击破PlayStation用户系统。



教训：使用Tomcat作为“基础设施”，没有投入Tomcat开源社区后续的跟踪。

2 开源治理的内容

开源治理体系是一套帮助浦发银行安全、合规、可靠、高效地评估和使用开源软件、管理开源资产、把控开源软件使用中的安全风险的方法论和实践。主要包括5部分内容：



开源治理的配套组织架构

包括开源治理的专业化全职团队，以及在开源软件使用全生命周期中涉及的，来自于架构、开发、运维、安全、法务等部门的成员。

开源治理的配套流程制度

将开源治理要求嵌入到浦发银行现有信息系统项目建设中的一种流程制度。

开源软件评估评价方法

一套适合于银行业务和管理特点的开源软件评估评价方法，用于指导开源软件在银行的引入和选型。

开源软件治理支撑平台

一个用于支撑开源软件治理的平台系统，是整个开源治理工作高效运行的技术保障。

金融行业开源技术应用社区

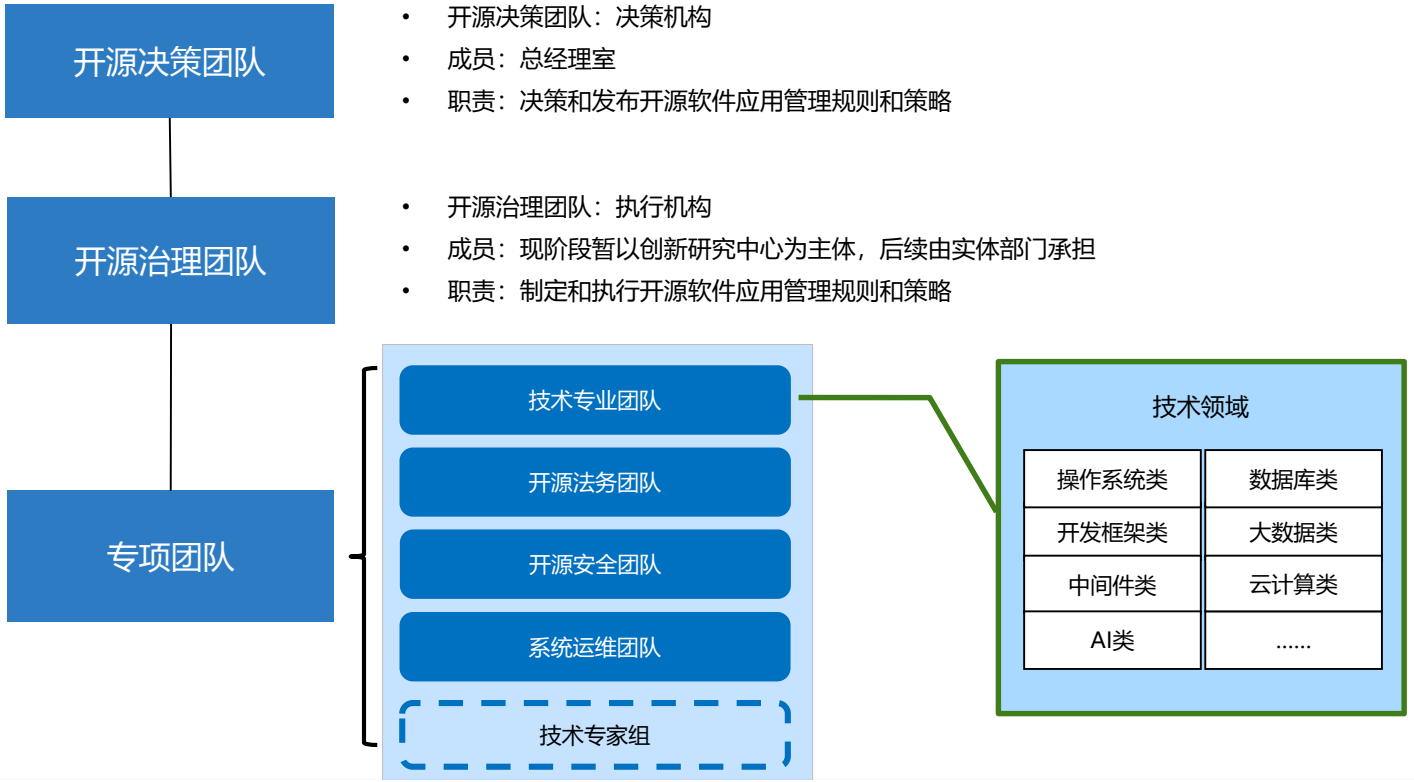
一个非盈利性的组织，旨在通过信息共享，推动开源技术和软件在金融行业内安全可靠的使用。

3 开源治理的四个维度


软件来源
1
开源软件实体必须来自官方社区，防止实体被第三方篡改，植入后门或病毒。
合法合规
2
在使用开源软件过程中，必须严格遵从开源软件许可证的规定，避免开源法务风险。
安全漏洞
3
安全漏洞，开源软件漏洞必须快速、及时地修复，降低产品被攻击的可能性。
生命周期
4
开源软件必须有明确的引入和退出机制，以降低维护成本，降低安全保障的难度。

4.1 开源治理的方法—组织架构和制度

一、设置组织架构及相应职责：围绕工作目标结合各职能部门进行构建，做到人责权匹配



- 开源决策团队：决策机构
- 成员：总经理室
- 职责：决策和发布开源软件应用管理规则和策略

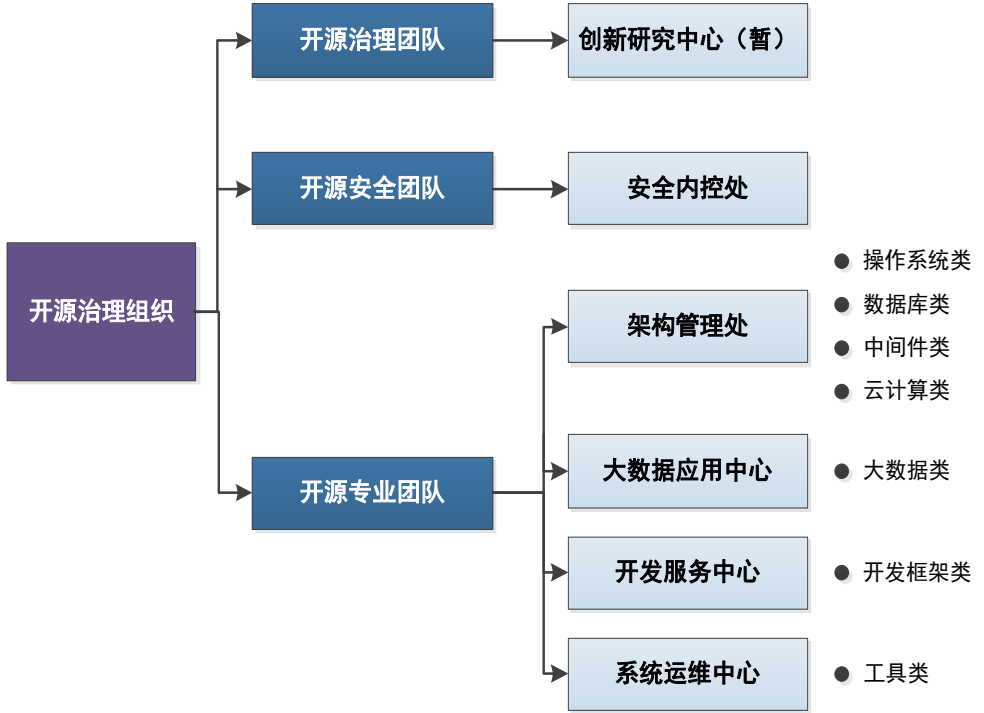
- 开源治理团队：执行机构
- 成员：现阶段暂以创新研究中心为主体，后续由实体部门承担
- 职责：制定和执行开源软件应用管理规则和策略

制定开源治理的规范及制度

《浦发银行开源软件应用管理技术要求》

《浦发银行开源软件应用管理规程》

组建开源治理体系配套团队



4.2 开源治理的方法—流程体系

二、建设流程体系：开源软件引入、评估、使用、漏洞持续评估

来源可靠 | 许可遵从 | 生命周期管理 | 版本推荐 | 开源软件应用台账 | 安全漏洞管理

开源软件引入和使用评估

- 项目使用开源软件前必须先从开源软件管理平台申请引入，软件仓库中介质都来自社区或供应商官方渠道
- 申请时必须通过开源软件引入评估
- 系统投产前必须通过代码和二进制扫描，确保所有软件都通过申请，介质来源可靠

软件推荐级别管控

- 所有软件版本都有其推荐级别：推荐、可用、禁用
- 开源软件专业团队通过推荐级别维护管理软件生命周期
- 同一开源软件只有一个推荐版本

开源软件配置管理

- 建立结构化开源软件配置库，建立应用系统---开源软件版本---开源软件对应漏洞之间的关系，确保信息可追溯

漏洞收集---通知---修复流程

- 通过内外部安全漏洞信息源等方式获取开源软件漏洞信息
- 建立从漏洞通知到生产系统漏洞修复的全周期管理

设计实施开源治理流程：合理的流程制度保证了开源治理的有效实施

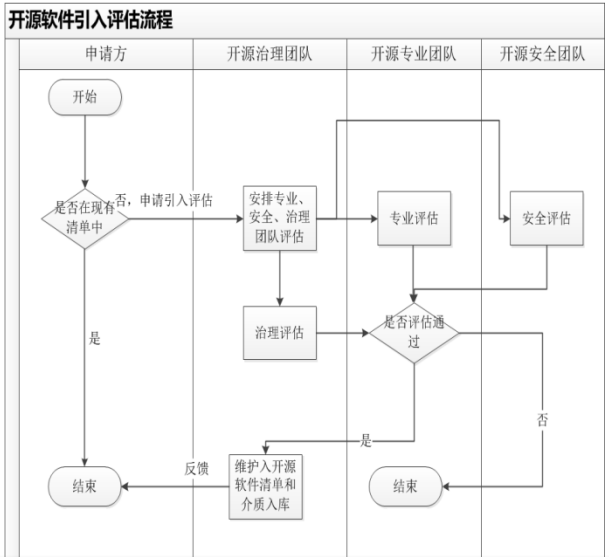
流程体系建设：开源软件引入评估、开源软件使用、开源软件漏洞持续评估

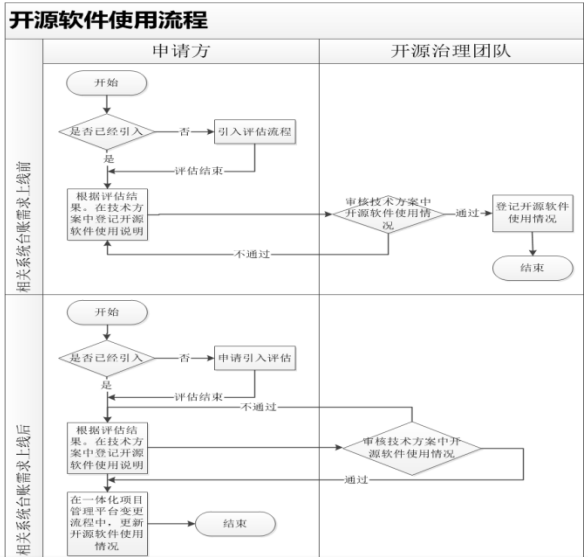
项目立项	方案设计	方案评审	开发测试	投产上线	维护

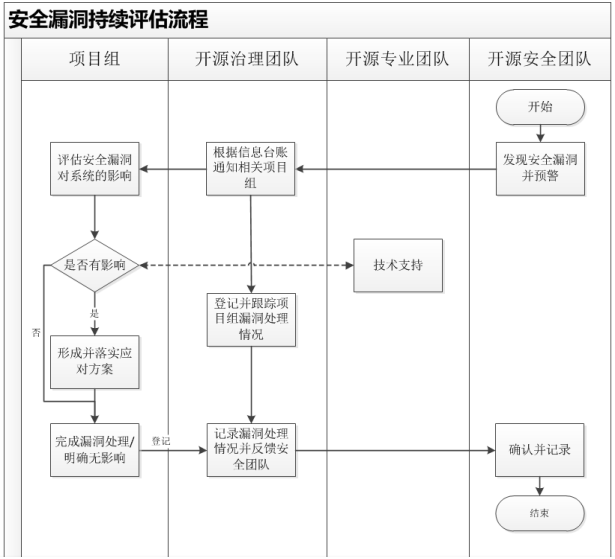
开源软件引入评估

开源软件使用

开源软件漏洞持续评估





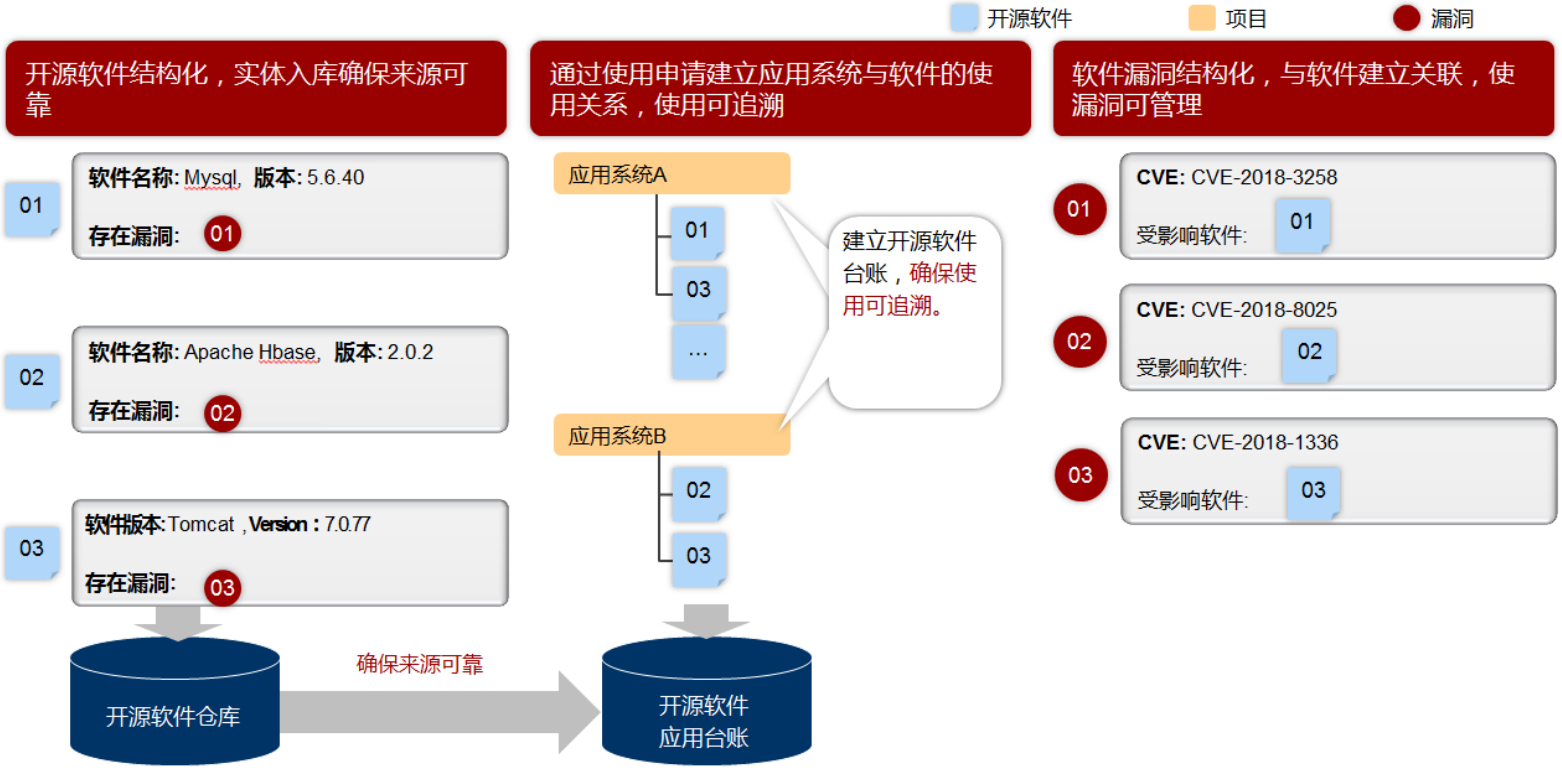


分类	评估项	说明
基本评估要素	许可证类型	评估许可证条款对于我行应用场景的合法性和限制性。
	社区活跃度（健康度）	评估整个开源软件项目的生命力和社区整体质量。
	安全性	评估引入开源软件的代码安全性
	版本评估	评估开源软件版本的生命周期和稳定性
	软件成熟度	评估软件在行业中的使用广泛性以及行业中的专业第三方评价
软件技术评估	功能	针对应用场景，评估软件功能（包括安全功能）的满足度和正确性。
	性能	针对场景的非功能需求，评估软件的处理效率、容量和资源使用率。
	高可用性	针对场景的非功能需求，评估软件的高可用架构的先进性、可靠性和正确性。
	兼容性	对于其他运行环境兼容性评估，如操作系统，监控软件，备份等。
	易用性	对于软件安装部署和维护管理的易用性进行评估。
运维支持情况评估	支持形式	1、是否有商业化支持；2、社区支持具体支持形式。
	商业服务内容及SLA	1、具体可以提供的服务内容；2、SLA承诺，包括响应时间、服务形式等。
	商业服务本地化能力	是否有本地化商业支持团队，本地化沟通及服务。
	我行支持能力	评估我行在使用、维护上的支持能力。

***Reference：E- OSMM (Enterprise Open Source Maturity Model)模型以及华为开源治理的成功经验**

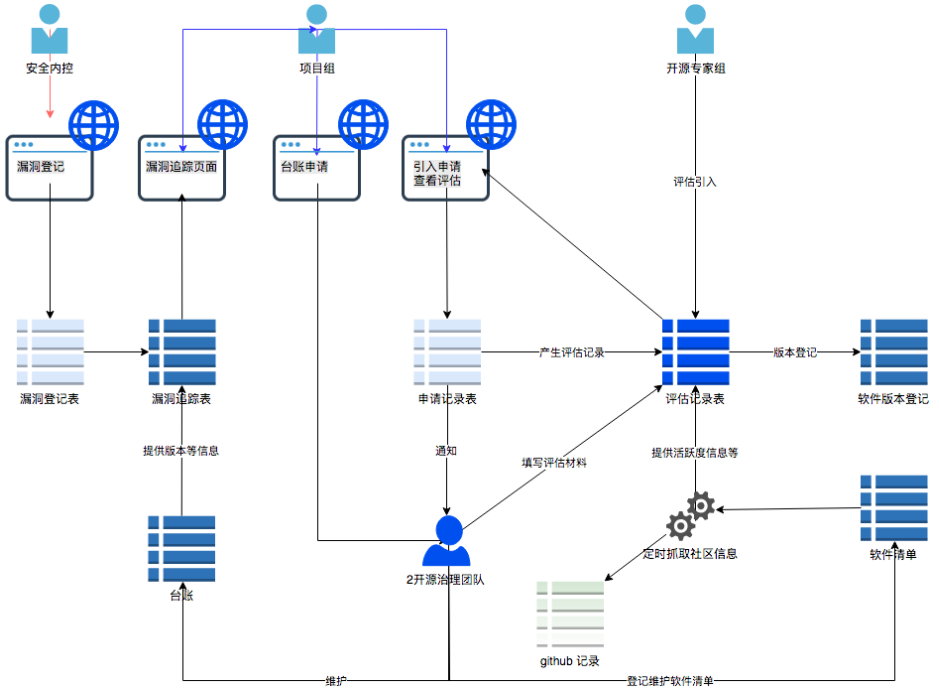
4.3 开源治理—管理平台

三、建设开源治理平台：提供平台级技术支持，提高开源软件管理效能



建设开源软件管理平台

开源治理流程高效可控 → **软件社区信息及时获取** → **开源软件来源可控可溯**



4.4 开源治理—社区共享

浦发银行联合中国信通院发起成立金融行业开源技术应用社区，旨在推动开源技术、产品和产业在中国金融业安全可靠的使用。

参与成员

浦发银行 SPD BANK
CAICT 中国信通院
上海清算所 SHANGHAI CLEARING HOUSE
中国农业银行 AGRICULTURAL BANK OF CHINA
兴业银行 INDUSTRIAL BANK CO.,LTD.
中信银行 CHINA CITIC BANK
上海银行 Bank of Shanghai
上海农村商业银行 Shanghai Rural Commercial Bank
中国人寿 CHINA LIFE
太平洋保险 CPIC
HUAWEI
Tencent 腾讯
BSG

- 定期开源软件技术研究和使用经验沟通会
- 共享开源软件评估评价结果
- 后期知识库和评估评价系统共享
- 开源技术供应商提供专业技术支持

5 下阶段安排

后续计划：

持续优化、全面推广、贡献社区

- 持续优化开源治理平台开发，完善功能和使用体验，引入专业工具扫描开源源码。
- 逐渐在全行全面推广开源治理体系，对接项目管理平台。
- 开源治理体系中增加自研代码输出，贡献社区的相关流程和制度
- 深化社区合作，治理平台开源，社区内部拥抱开源软件生产方式，推进行业标准。

感谢聆听