如何在软件开发生命周期中管理引入的开源组件

朱贤曼

极客时间 | 企业版 × InfoQ

DTDS
全球数字人才发展线上峰会

建设面向未来数字化全局的人才梯队

2022 年 8 月 9 日 · 线上

入局·链接

扫码预约直播

使用开源软件有哪些风险

开源软件免费、无采购成本、能缩短产品开发周期，但蕴藏潜在风险

安全风险

运维风险

开源许可证合规风险

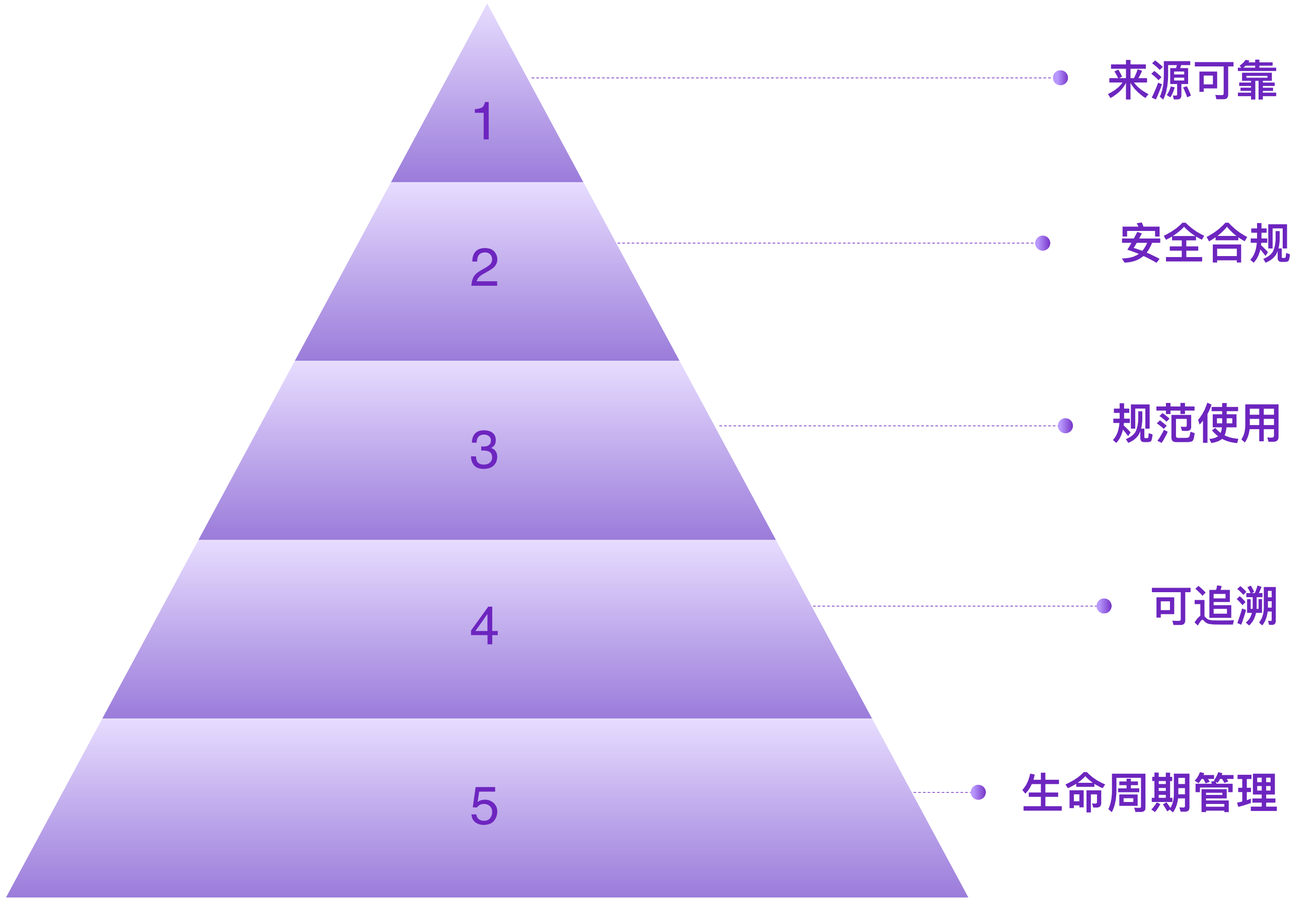
供应链风险

出口管制合规风险

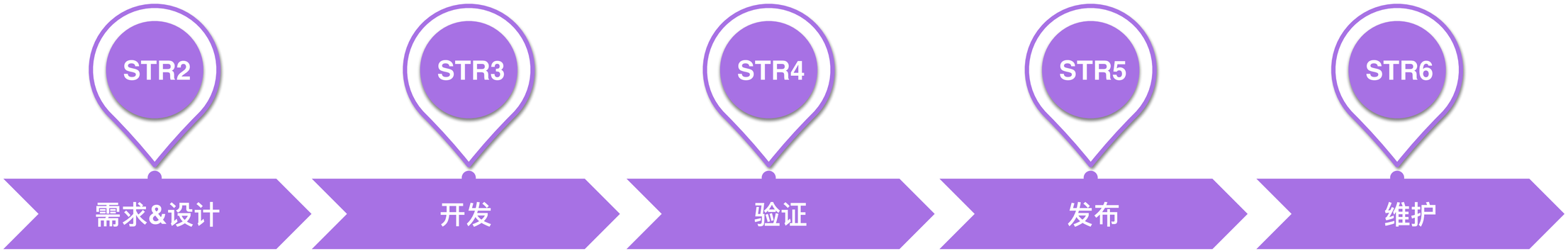
专利侵权风险

商标侵权风险

从哪些方面来管控风险



基于 SDL 的开源合规治理



业务 + 安全 + 法务 + OSPO	SE + 开发	测试 + 开发	PM + SE / 开发	运维PM + 开发
• 开源风险评估 • 选型&入库 • 使用申请 • BIS 备案	• SCA工具扫描及治理 • Notice 集成 • 使用申请更新	• 开源合规测试 • Notice 更新 • 准出校验	• FSR • 开源分发 • 应急响应计划	• 漏洞跟踪和处理 • 生命周期维护 • 应急响应

IT基础设施 开源软件库、开源源码库/制品库、DevOps工具链、项目管理系统、PDM产品数据系统、版本控制系统、故障跟踪系统……

需求 & 设计阶段 — 选型评估

建立准入机制，从源头把控风险，是安全左移的重要举措，其中开源软件选型是关键活动之一

	技术生态	开源许可证	安全	生命周期
考量因素	• 功能/性能满足程度 • 架构的高可用性、先进性和可靠性 • 兼容性 • 易用性 • 行业应用范围	• 许可证条款、附加条款 • 专利陷阱 • 历史诉讼案例	• 已知安全漏洞 • 历史版本漏洞 • 历史漏洞处理情况	• 成立时间 • Star/Fork/Watching • 贡献者/PR • 版本更新频率

开源软件库

开源同源

- 官网同源
- 内网同源
- 版本同源

功能

- 开源软件库、许可证库、漏洞库、黑名单、台账
- 入库、使用申请、更新和退出
- 漏洞推送

开源软件库

运营

- Owner机制
- TMG / 专家评审团
- 分级审核机制

需求 & 设计阶段 — 风险评估 & 使用申请

开源风险评估

依托开源合规库，进行开源风险评估

- 输入：开源合规调查问卷
- 输出：风险项/合规需求
- 准出条件：所有新项目/新增需求均已完成开源风险评估

开源软件使用申请

依托开源软件库，进行使用申请

- 先申请，后使用
- 从开源软件库申请

使用申请关注的信息

- 基本信息
- 使用信息

开发阶段 — 开源扫描 & 义务履行

规范使用

- 从开源软件库中引入
- 架构解耦
- 配置解耦
- 保留原始版权、许可证
- 禁止故意绕过工具检查
- 禁止代码片段引入
- 整包使用，不修改
- Patch 管理

开源扫描

- SCA工具扫描
- SBOM生成
- SCA 工具嵌入到 CI/CD

问题整改

- 风险分析、整改计划
- 安全漏洞修复
- 合规治理

义务履行

- Notice 集成
- 开源分发准备
- 修改说明

验证阶段 — 开源测试

测试计划

- 测试计划
- 测试用例

测试执行

- Notice 集成测试
- 开源分发准备工作验收
- 其它义务履行情况验收
- 漏洞修复情况验收

准出校验

- 使用申请和 SBOM一致
- 高风险问题处理完成
- Notice 集成测试通过
- 开源分发准备就绪

发布阶段 — 开源发布

执行FSR，审核各项开源合规活动是否已执行完成，做好开源发布准备，并制定应急响应计划

开 源 发 布

主动开源

贡献整个项目

- 开源合规治理
- 确定许可证
- 其它相关审查
- Notice、分发说明

主动回馈社区

- 开源范围
- 编译通过
- 其它相关审查

被动开源

- 开源范围审核
- 不包含第三方专有代码
- 不包含公司商业秘密和其它敏感信息
- 出口管制审查
- 提供符合许可证要求的源码

维护阶段 — 漏洞跟踪和修复

漏洞收集

- 内部漏洞库
- SCA工具

漏洞跟踪和验证

- 快速定位
- 漏洞验证和分析
- 漏洞分发
- 产品漏洞预警

漏洞修复

- 临时紧急措施
- 源码补丁
- 跟随社区升级
- 现网产品漏洞修复支持

建立持续跟踪机制，根据应急响应流程和漏洞修复协作机制，完成漏洞跟踪和修复

维护阶段 — 生命周期管理

及时升级到最新稳定版本

- 定期维护开源软件库
- 及时跟随社区升级

制定明确的退出机制和流程

- 定期维护黑名单
- 及时退出

IT系统支撑和工程能力建设

- 提供完善的IT系统支撑和较强的工程能力
- 溯源及自动化管理

极客时间App — 数字人才的专属学习空间

Geekbang.

极客时间

- 极客时间是**数字人才**的专属学习空间，有近**200+**体系课和**1400+**技术视频。为学员提供系统化、场景化、工具化和游戏化的学习服务
- 极客时间课程涵盖：前端/移动、计算机基础、后端/架构、AI/大数据、运维/测试等**十多门**技术学习版块
- 在极客时间可以学习各**大厂CTO**及阿里**P8**级以上技术大牛**独家技术修炼心法**，更有技术大牛直播，面对面帮你解决技术难题

更多精品好课

下载免费领取7天学习卡

17 条学习路径，补足能力短板

由浅到深，由易到难，从垂直深耕到触类旁通

后端工程师 20+ 门课程 43.4w 人已学习	架构师 20+ 门课程 41.5w 人已学习	前端工程师 15+ 门课程 25.6w 人已学习
运维工程师 15+ 门课程 21.6w 人已学习	计算机基础知识 10+ 门课程 21.5w 人已学习	Go 工程师 15+ 门课程 18.6w 人已学习
测试工程师 15+ 门课程 22.9w 人已学习	Java 工程师 20+ 门课程 31.2w 人已学习	Python 工程师 15+ 门课程 23.9w 人已学习

名师出高徒

1000+ 大牛独家心法，站在巨人的肩膀上不走弯路

李运华
前阿里资深技术专家（P9），《从 0 开始学架构》专栏作者

“《从 0 开始学架构》我写了 3 年，很荣幸能成为 5.8 万程序员的架构入门选择，今年又重新梳理了一遍，把我认为旧的内容替换掉，新的思考写成加餐。之后会继续花时间完善内容和回复评论区疑问，每个观点都是我当下的认知，期待你和我同频。”

想一想，我该如何把这些技术应用在工作实践中？

THANKS