云原生产业大会 2021 CLOUD NATIVE INDUSTRY CONFERENCE
2021/05/26 × 中国 / 北京
原生蓄力 云领未来

企业开源安全可信供应链治理实践分享

中兴通讯股份有限公司　　项曙明

CAICT 中国信通院

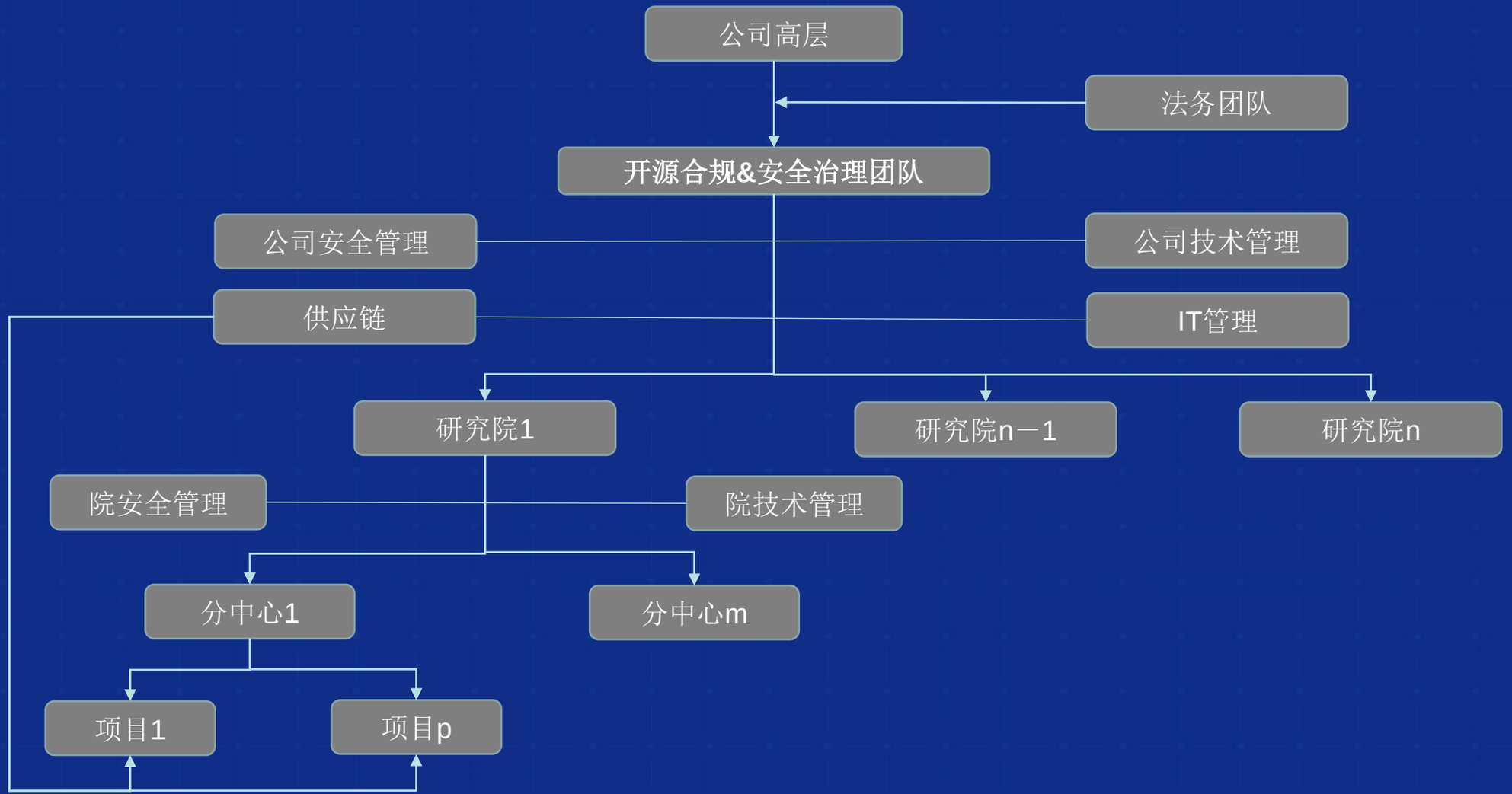
治理实践要点分享

- 领导的支持是任何过程改进成功的首要条件（获取支持）
- 其次结合企业实际需要，明确开源治理目标（去哪里？）
- 结合实际，寻求和组建合适的企业治理机构（团队）
- 识别涉及组织哪些部门、流程和工具（范围）
- 对上述范围进行现状分析，找出不足与差距（在哪里？）
- 输出可行的治理计划，按计划推进治理实践（项目化运作）
- 外部环境和要求是治理过程的推进器（外力）
- 构建组织开源治理能力（可复制）

合规、安全、可信供应链治理目标

开源风险类别		开源引入风险分析	治理范围&目标
1、知识产权及合规风险	1.1、许可证合规风险	1、不遵守开源许可证要求 2、为了满足许可证要求，被迫开源 3、引入的多个开源软件许可证不兼容	1、项目组使用开源软件时符合许可证合规要求 2、确保项目核心代码的安全，不会被动开源 3、确保开源许可证解读、合规治理的最佳实践等能在公司内进行有效共享共创，提升合规治理效率 4、能够优选到外部社区最佳（业界知名度高、质量好、活跃度高、有大公司支撑、没有木马病毒、没有官司、不会导致专利侵权）的开源项目
	1.2、知识产权风险	1、开源许可证本身知识产权界定不清晰 2、开源代码中知识产权风险的应对	
	1.3、开源规则变化风险	开源软件遵循许可证存在变化 ——JAVA、Oracle基础开源版收费 ——MonogoDB AGPL变成SSPL对云服务影响	
2、安全风险		1、安全漏洞和缺陷治理与应对 2、如何安全透明、可信地使用开源 3、如何快速响应开源CVE漏洞、选型、运维、同源	1、确保项目版本发布时使用到的开源软件没有已知漏洞、或者其已知漏洞已经被关闭 2、确保项目已发布版本中若新增开源漏洞时公司具备开源软件安全风险应对的能力 3、构建公司产品、解决方案能够在较短时间内解决开源软件安全问题的能力
3、EAR合规风险		1、识别不清 2、未遵循EAR法条 3、组织如何有效管控？	1、识别所有项目使用的开源软件是否受EAR管辖 2、确保所有受EAR管辖的开源软件已完成BIS备案 3、公司层面统一管理、统一备案，全生命周期管控

开源供应链风险管理机构&涉及部门



规范建设与产品研发过程融合

规范建设

1. 《开源软件管理规范》
2. 《开源软件EAR合规管理规范》
3. 《第三方软件（组件）管理规范》
4. 《供应商网络安全认证管理规范》
5. 《软件外包供应商合规一体化认证评定表》
6. 《产品安全管理》、《产品安全质量红线》
7. 《HPPD产品研发配置管理规范》
8. 《软件服务 / 项目外包管理规范》

与产品研发、经营过程融合

1. 规范融合：《高效产品开发（HPPD）总则》［原有规范基础上增加使用开源软件合规管控的规范要求，纳入研发项目全过程］
2. 过程融合：研发管理、配置管理、质量管理、CI / CD、DevSecOps
3. 经营融合：商机管理、产品管理、研发量管理、供应链管理、售后运维管理融合
4. 工具融合：开源扫描、安全管控、项目管理、配置管理、编译构建、合规管控、供应链管理、运维售后等工具链的融合、优化与贯通

治理实践探索

- 引入专业扫描工具，确保摸清开源使用情况、了解合规&安全风险 ——开源BOM清单
- 许可证治理
  - Top许可证统一解读与守护，优先完成xGPL许可证开源软件的合规治理，确保代码安全、降低经营风险【MonogoDB、MySql、JDK合规使用指导】
  - 共享共创、开源COP、沙龙、最佳实践、FAQ等形式输出不同场景下的合规指引
  - 法务进行解读、咨询、治理实践合规性确认
  - 逐步延申至文件级合规、兼容性合规、豁免条款等深层次合规治理
- 开源同源
  - 三个层次的同源：官网同源、内源同源、版本同源
  - 构建**企业开源库**、统一拉取、集中守护、共享共创、同源构建
  - CI/CD融合、Devsecops、安全左移
- EAR治理
  - 输出统一规范与指引、组建管控团队
  - 公司统一集中管理开源软件BIS备案清单、E化管理
  - 软件构成要素表

治理实践探索

- 安全治理
  - 开源软件BOM清单：直接引用、间接引用
  - 源码治理
    - ✓源码治理管控：摸清开源使用方式（解耦完整、解耦衍生、耦合衍生、片段）、合规治理&安全治理平衡
    - ✓官网同源、版本同源
  - 直接依赖
    - ✓使用最新无CVE漏洞的版本
- 安全应对
  - 配置管理、局点版本管理
  - E化工具支撑
  - 快速响应，闭环处理
- 第三方代码（供应链）管理
  - 强化第三方代码管理：ECCN码、分发说明、协议约束
  - 工具扫描
  - 外包管控
  - ODM/OEM
- Devsecops探索、安全左移
  - 版本构建安全管控：Xray、Hub插件试点
  - 扫描策略管理应用+自研工具管控+Devops融合
  - 引入管控、IDE、CI/CD过程管控
  - 不同组织层级设置不同的管控要求

云原生 产业大会
2021 CLOUD NATIVE INDUSTRY CONFERENCE
2021/05/26 × 中国 / 北京
原生蓄力 云领未来

THANKS!

CAICT 中国信通院