
GOTC 2023
全球开源技术峰会
THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE
OPEN SOURCE, INTO THE FUTURE
「软件定义汽车」专场
极氪汽车开源合规体系建设实践分享
吴慧康 2023年05月28日

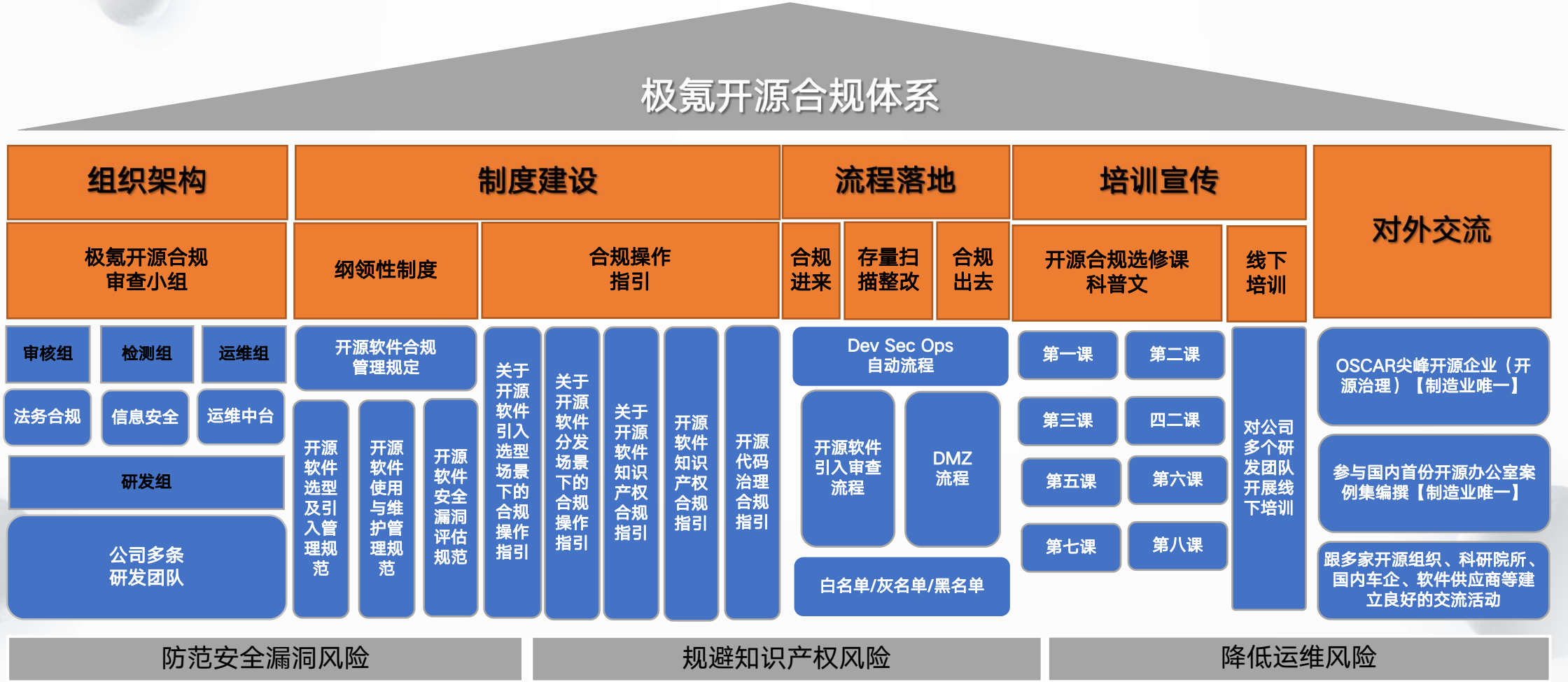
GOTC

极氪 ZEEKR

全球开源技术峰会
THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

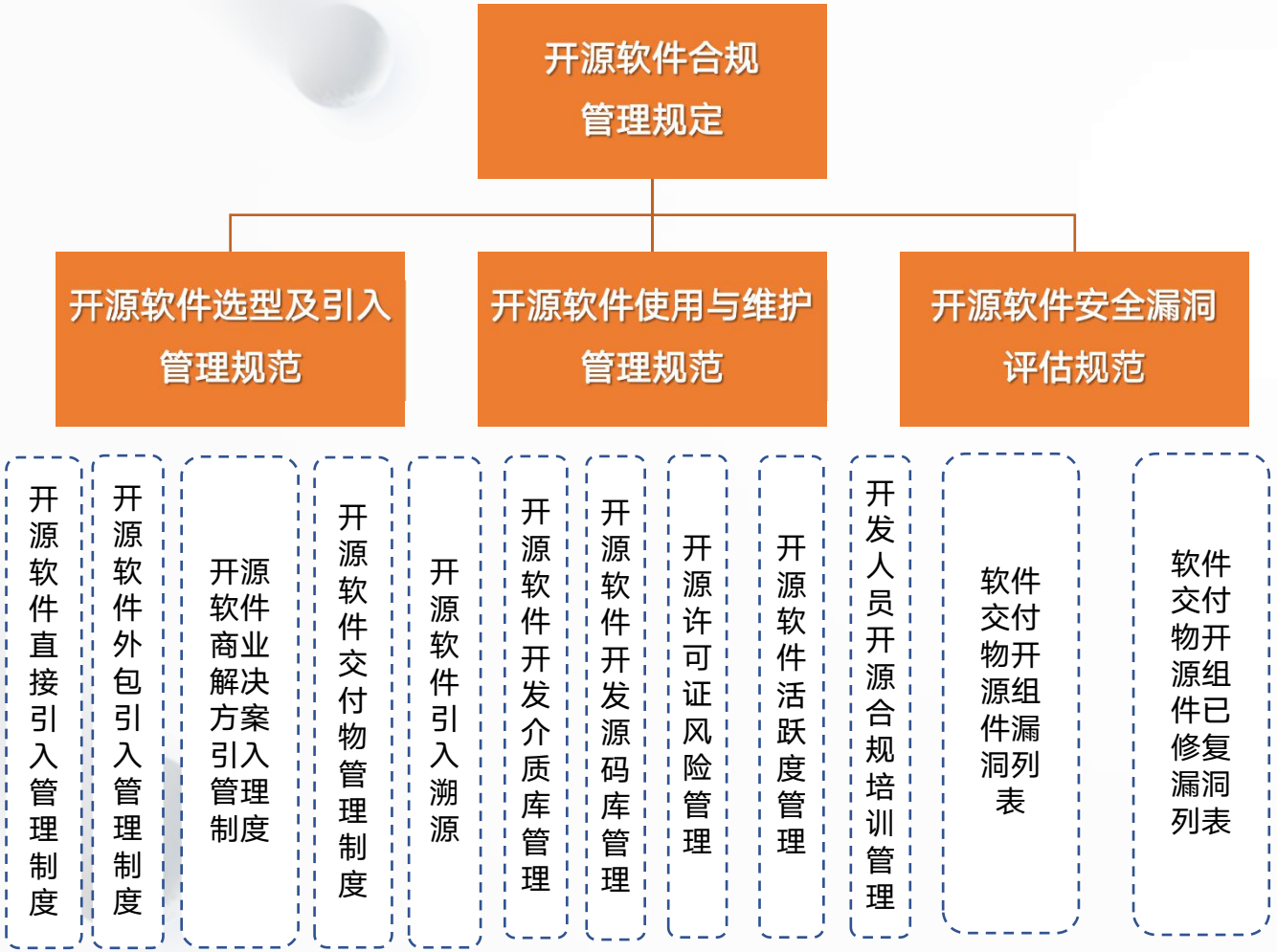
OPENSDV

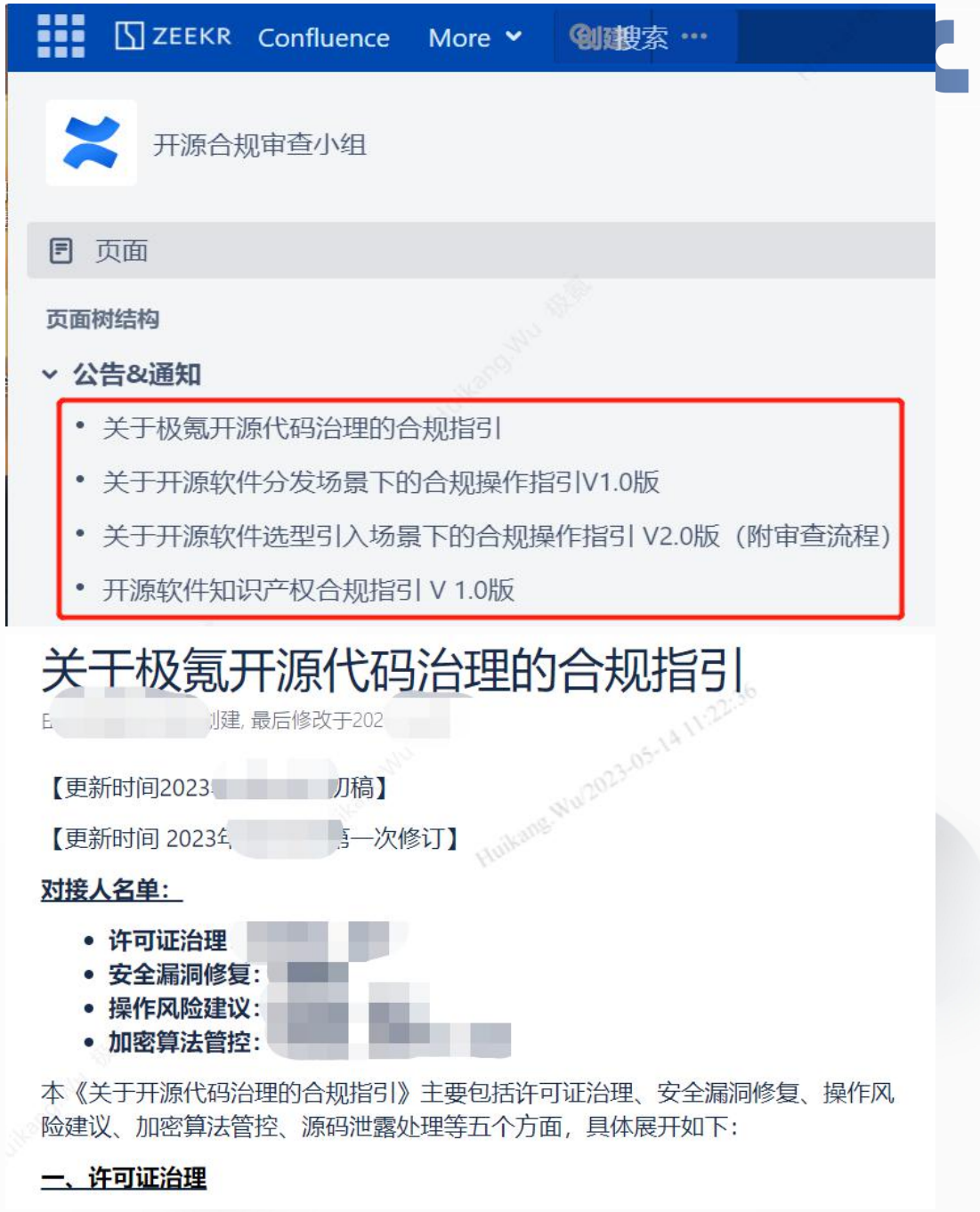
概要总览


极氪开源合规体系
组织架构
制度建设
流程落地
培训宣传
对外交流
极氪开源合规
审查小组
纲领性制度
合规操作
指引
合规
进来
存量扫
描整改
合规
出去
开源合规选修课
科普文
线下
培训
审核组
检测组
运维组
法务合规
信息安全
运维中台
研发组
公司多条
研发团队
开源软件合规
管理规定
开源
软件
选型
及引
入管
理规
范
开源
软件
使用
与维
护管
理规
范
开源
软件
安全
漏洞
评估
规范
关于
开源
软件
引入
选型
场景
下的
合规
操作
指引
关于
开源
软件
分发
场景
下的
合规
操作
指引
关于
开源
软件
知识
产权
合规
指引
开源
软件
知识
产权
合规
指引
开源
代码
治理
合规
指引
Dev Sec Ops
自动流程
开源软件
引入审查
流程
DMZ
流程
白名单/灰名单/黑名单
第一课
第二课
第三课
四二课
第五课
第六课
第七课
第八课
对公司
多个研
发团队
开展线
下培训
OSCAR尖峰开源企业（开源治理）【制造业唯一】
参与国内首份开源办公室案例集编撰【制造业唯一】
跟多家开源组织、科研院所、国内车企、软件供应商等建立良好的交流活动
防范安全漏洞风险
规避知识产权风险
降低运维风险

1. 组织架构（OSPO）

2. 制度建设


开源软件合规管理规定
开源软件选型及引入管理规范
开源软件使用与维护管理规范
开源软件安全漏洞评估规范
开源软件直接引入管理制度
开源软件外包引入管理制度
开源软件商业解决方案引入管理制度
开源软件交付物管理制度
开源软件引入溯源
开源软件开发介质库管理
开源软件开发源码库管理
开源许可证风险管理
开源软件活跃度管理
开发人员开源合规培训管理
软件交付物开源组件漏洞列表
软件交付物开源组件已修复漏洞列表


ZEEKR Confluence More 创建 搜索
开源合规审查小组
页面
页面树结构
公告&通知
关于极氪开源代码治理的合规指引
关于开源软件分发场景下的合规操作指引V1.0版
关于开源软件选型引入场景下的合规操作指引 V2.0版（附审查流程）
开源软件知识产权合规指引 V 1.0版
关于极氪开源代码治理的合规指引
【更新时间2023 初稿】
【更新时间 2023年 第一次修订】
对接人名单：
许可证治理
安全漏洞修复：
操作风险建议：
加密算法管控：
本《关于开源代码治理的合规指引》主要包括许可证治理、安全漏洞修复、操作风险建议、加密算法管控、源码泄露处理等五个方面，具体展开如下：
一、许可证治理

3. 选型策略

“新&稳定”

遵循成熟可靠、兼顾性能、社区活跃的原则，重点考虑许可证和安全漏洞的风险等级，兼顾软件来源、活跃度、社区规范度等多种因素。

开源许可证分类表

许可证类型	宽松型（允许型）	弱传染型（弱互惠型）	传染型（互惠型）	强传染型（AGPL）	未知型&非认证&通用型	限制性第三方专有
	MIT	代码项目开放（Coin-OR - CoinUtils 1.0.2）	GPL2.0/3.0	AGPL3.0/3.0+	unknown	Basic Proprietary Commercial
	BSD	Eclipse许可证（EPL1.0/2.0）	Sun GPL2.0（带路径异常）			NVIDIA Customer Use License
	WTFPL	CDDL1.0/1.1				Server Side Public License1.0
	Apache2.0	Mozilla公共(MPL)				Elastic License 2.0 (ELv2)
	木兰2.0	LGPL2.1/3.0				
	艺术许可证	Microsoft 相互				
	ISC					
	Microsoft 公共					
	Zlib-Libpng					
外部项目	无	高（源代码、静态链接）、中（动态链接）	高（源代码、静态链接、动态链接）	高（源代码、静态链接、动态链接、独立进程）	高（源代码、静态链接、动态链接）	中（源代码、静态链接、动态链接等）
Saas项目	无	低（源代码、静态链接、动态链接）	低（源代码、静态链接、动态链接）	高（源代码、静态链接、动态链接、独立进程）	高（源代码、静态链接、动态链接）	中（源代码、静态链接、动态链接等）
内部项目	无	无	无	无	高（源代码、静态链接、动态链接）	中（源代码、静态链接、动态链接等）
开源项目	无	无	无	无	高（源代码、静态链接、动态链接）	高（源代码、静态链接、动态链接）

安全漏洞要求？

操作风险建议？

开源加密算法管控？

4. 供应链管理

◆*动作1：*修改软件采购合同模板，增加开源合规的要求，并修改合规承诺书内容；

◆*动作2：*要求每一个供应商提供开源软件使用情况表或SCA检测报告；

◆*动作3：*引入前，对代码进行SCA扫描。

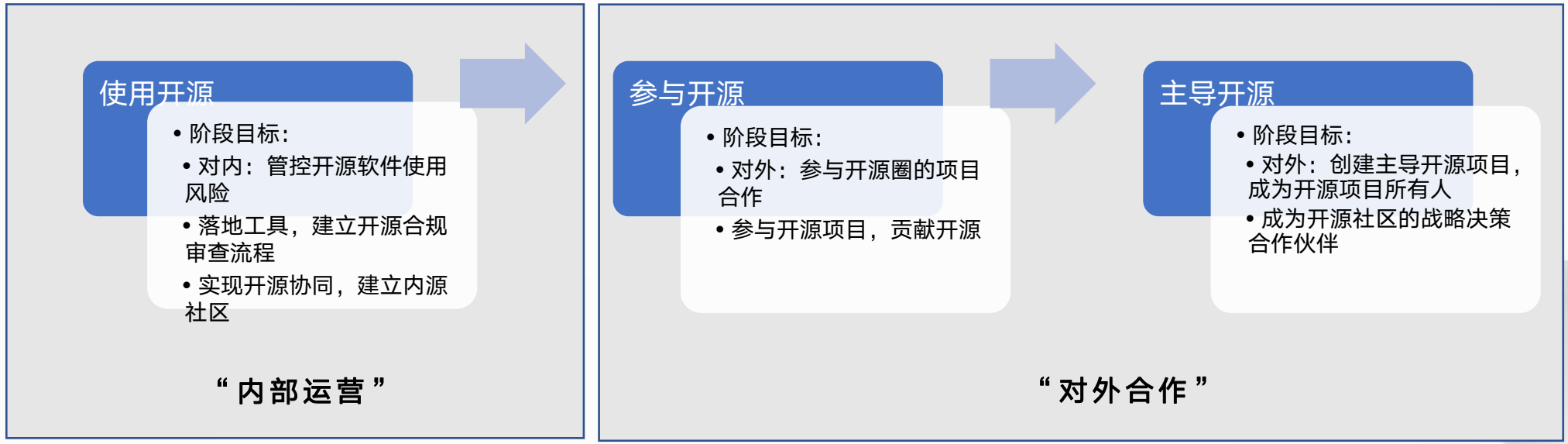
条款落地？

供应商开源软件使用情况汇总表										
公司名称										
项目/产品/服务名称										
开发负责人及联系方式										
开源软件相关信息										
序号	开源软件名称	所使用开源软件版本	软件版本最新更新日期	开源软件官方下载链接	许可证名称	许可证文本链接	著作权声明（可能是单独文档/源码最前面部分）	是否存在Third Party（如Third Party文件夹或Third Party列表，如有请提供链接）	是否对开源软件做出了修改	开源软件使用方式（源码融合、静态链接、动态链接、进程隔离或其他）
1										

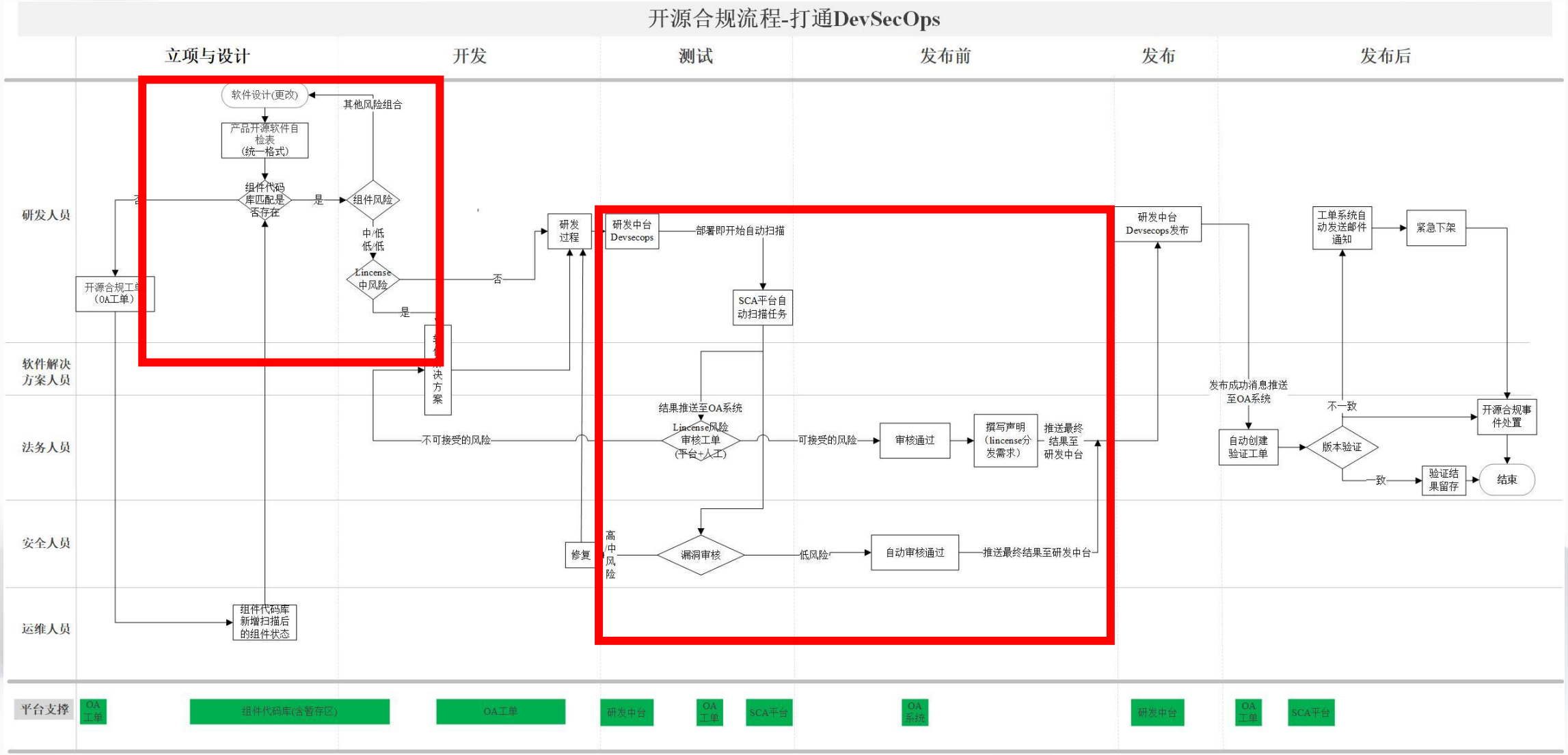
5. 规划设计

开源办公室OSPO

开源三阶段



6. 流程落地


开源合规流程-打通DevSecOps
立项与设计
开发
测试
发布前
发布
发布后
研发人员
软件解决方案人员
法务人员
安全人员
运维人员
平台支撑
软件设计(更改)
其他风险组合
产品开源软件自检表(统一格式)
组件代码库匹配是否存在
否
是
组件风险
中/低
低/低
Lincense中风险
否
是
开源合规工单(OA工单)
研发过程
研发中台Devsecops
部署即开始自动扫描
SCA平台自动扫描任务
结果推送至OA系统
Lincense风险审核工单(平台+人工)
不可接受的风险
可接受的风险
审核通过
撰写声明(lincense分发需求)
推送最终结果至研发中台
修复
高/中风险
漏洞审核
低风险
自动审核通过
推送最终结果至研发中台
组件代码库新增扫描后的组件状态
研发中台Devsecops发布
发布成功消息推送至OA系统
自动创建验证工单
版本验证
不一致
一致
工单系统自动发送邮件通知
紧急下架
开源合规事件处置
验证结果留存
结束
OA工单
组件代码库(含暂存区)
OA工单
研发中台
OA工单
SCA平台
OA系统
研发中台
OA工单
SCA平台

GOTC

THANKS

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

OPENSDV