XXXXXX有限公司信息安全管理体系审核案例

推荐机构：广州赛宝认证中心服务有限公司
认证领域：信息安全管理体系审核
审核时间：2022年12月14日—12月16日
审核人员：段沛鑫

一、 案例背景

随着金融业对信息安全监管要求的不断提升，XXXXXX有限公司正积极加强信息安全能力建设，以适应行业发展要求，控制潜在风险。

二、 审核过程介绍

案例主要过程：经过初步访谈审核员了解到，该公司目前信息系统的建设主要依赖外包开发，针对外包开发的安全管理也是其面临的痛点。

审核员首先关注近期是否发生有外包安全事件，随即了解到企业为防止外包人员泄露公司源码，购买有Github等开源代码平台信息泄露告警服务。审核员抽查报告记录时发现，该公司源码曾多次被外包人员泄露至开源代码平台，针对多次发生泄露的情况，处理人员仅是每次通知相关外包商进行删除处理，无后续其他措施。

审核员继续了解发现，该公司外包开发人员在开发过程大量利用开源/第三方组件，故需要经常使用开源代码平台。审核员进一步关注公司针对开源/第三方组件的安全控制问题，公司开发人员表述目前暂没有控制。

综合上述情况，审核员认为公司在外包开发的管理上存在不足，针对已知的信息泄露风险没有及时采取有效措施处理，在外包开发管控过程上也存在缺失。故根据上述情况开具两项一般不符合，并建议

公司重视信息安全事件的复盘并举一反三建立后续防范措施，深入梳理外包开发控制流程，切实加强外包风险控制。

三、 客户收益（增值效果）

企业管代和信息安全负责人均表达了对案例中不符合项的认同，认为将企业在外包开发安全管理过程中存在的漏洞展现了出来，并提出了合理化建议。企业后续发布了开源代码管理规范，并建立了相关安全检测机制；加强了互联网信息泄露检测力度，建立了针对事件的通报跟踪机制。

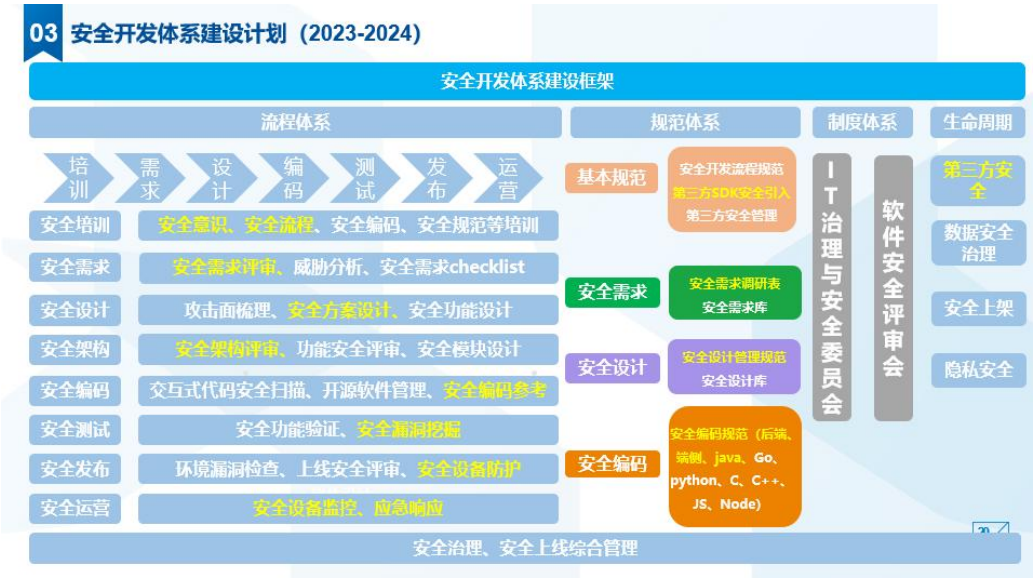

图 1. 安全开发体系建设计划

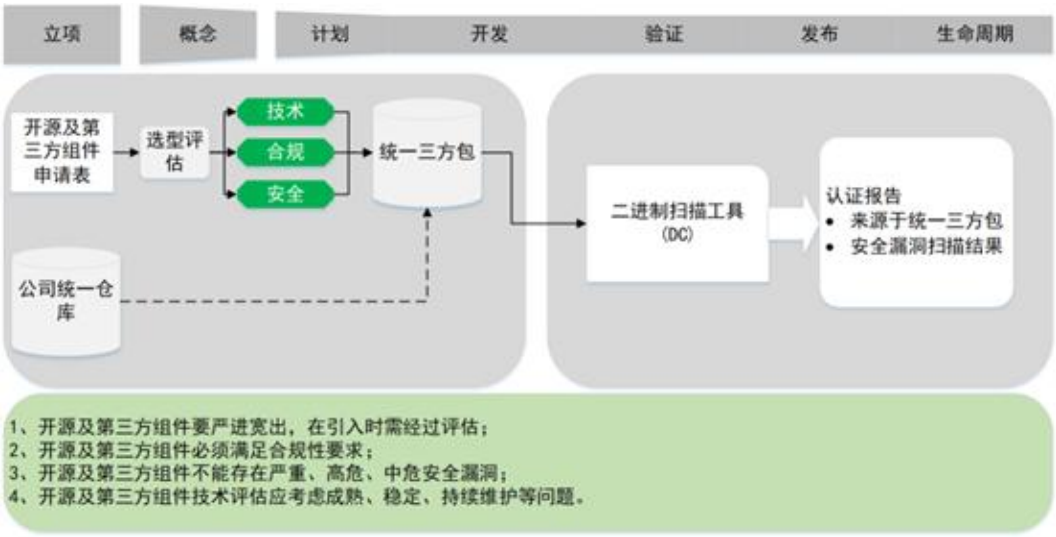

图 2. 完善开源及第三方组件管理

阶段	名称	形态
总体规范	软件供应链安全管理办法	文档
源头治理阶段	开源软件库构建咨询服务	服务（输出报告）
	开源软件私库规范、软件采购安全规范	文档
	开源软件入库安全检测（静态扫描、动态测试、成分分析、渗透测试）	SAST、IAST、SCA、渗透测试服务
签署合同阶段	供货商安全审查标准	文档
	采购软件安全治理规范	文档
	软件采购安全需求分析指南、安全需求设计知识库	文档
	安全需求分析与安全设计报告	STAC(输出报告)
开发阶段	软件的开源安全编码规范、软件的开源安全测试规范	文档
	开发环境和工具安全管理规范	文档
	驻场开发人员安全管理规范	文档
	开源软件安全测试用例	文档
	软件的开源组件安全检测	SCA、漏洞管理平台（输出报告）
交付阶段	软件交付安全管理规范	文档
	软件交付安全检测（静态扫描、动态测试、成分分析、渗透测试）	SAST、IAST、SCA、漏洞管理平台、渗透测试服务
上线/发布阶段	软件部署环境安全规范	文档
	部署环境安全检测（主机暴露面检测、主机基线检查、容器安全检测）	DAST、CWPP、容器安全平台（展示、输出报告）
运行阶段	软件运营安全规范	文档
	发布环境安全监测（互联网暴露面检测、容器安全检测）	DAST、容器安全平台、漏洞管理平台（展示、输出报告）
	开源软件漏洞监控（开源组件成分分析、应急响应）	SCA、应急响应服务
	运行环境日常运营（关基保护、等级保护咨询）	服务
	敏感码泄漏监测	巡哨（展示、输出报告）
培训	开源软件库构建、威胁建模方法、编码规范、漏洞讲解等，贯穿整个流程	面授培训、培训教材、培训总结

图 3. 软件供应链全生命周期控制