XXXXXX 股份有限公司审核案例

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：2021 年 12 月 9 日—12 月 11 日
审核人员：段沛鑫

一、案例背景

XXXXXX 股份有限公司是一家致力于大数据应用服务产品的软件企业，随着数据安全法的颁布，数据安全成为信息安全领域的新热点，公司产品作为支撑政务数据应用的载体，将会面临更多的挑战。

二、审核策划

针对该企业业务的特点，审核组将审核的重点锁定在企业针对数据软件类项目实施过程中的信息安全管理情况，分为三个小组开展审核，由审核组长对企业在产品、项目信息安全管理方面进行深入的审核。

三、审核过程

在 12 月 9 日审核开始当天，爆发了“Apache Log4j 存在任意代码执行漏洞”，该漏洞可以导致未取得身份认证的用户，可以从远程发送数据请求输入数据日志，轻松触发漏洞，最终在目标上执行任意代码造成数据泄露。这一漏洞由于破坏力强，影响范围大，业内各大权威机构都第一时间进行了重大风险提示预警。

审核员针对此项热点情况，对企业的应急响应情况进行检查，但却未发现企业采取任何措施对公司各项目进行影响处置，安全弱点的报告和应急处理环节存在缺失。

综合上述情况，审核员认为公司在安全事态情报的应急响应方面存在不足，针对突发安全事件缺少应急机制，难以应对项目活动中突发的信息安全风险。针对上述情况开具一般不符合项“现场未能提供针对近期爆发的热点安全事态 Apache Log4j2 远程代码执行漏洞进行报告及应急响应的记录”，并建议公司利用其在使用的禅道项目管理平台上建立信息安全应急事件处理情况的跟踪机制，以及针对产品安全开发生命周期管理进行导入学习。

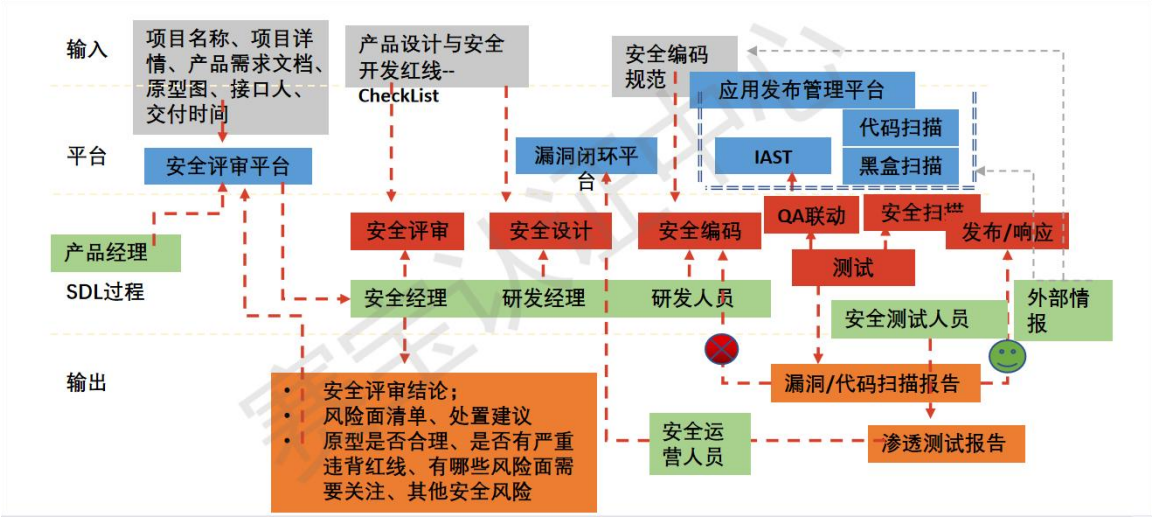

图 1. 改进建议

四、客户增值效益

通过本次审核帮助企业发现了其在日常管理环节中项目应急安全事件响应方面存在的漏洞短板和风险隐患，并通过开具不符合项，促进企业对业内较为先进主流的安全开发管理经验进行学习，引导企业在项目信息安全及产品开发安全上深入改进，帮助企业在信息安全管理流程上进行优化改造。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，认为将企业在项目信息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，降低了企业在项目实施过程中风险事件发生的可能性。

图 2. 企业收益