内网的众多资源系统进行对接，这些系统存在不确定的风险，数据接口不尽相同，及时的获取相关技术规范以及对接口的测试存在不确定风险，内部及组织管理上的风险包括项目众多的干系人在需求上的变化及冲突、干系人与团队的沟通、团队成员间的冲突、团队骨干成员工程师的可能离职等。

3.定性风险分析

定性风险分析主要是对已识别的风险进行优先级排序，等级、类别、概率和影响性质的评估，我首先通过风险概率及影响评估，建立风险概率及影响矩阵来确定各个风险的优先级等属性。同时对风险数据本身进行质量评估，最后更新风险登记册。例如，该项目的安全接入是最主要的技术风险，我从一开始便进行了识别分析，并有针对性的制定了应对计划，获得了某市局领导的肯定。

4.定量风险分析

定量风险分析则是对风险对项目总体目标的影响进行量化分析，即确定风险的影响值。在该过程中，我通过敏感性分析，预期货币价值分析等分析和建模技术，进一步量化了各类风险的影响，最后再次更新和细化了风险登记册。例如，对于外部风险，我将需要配合接入测试的公司分类，分别进行影响的量化分析，根据龙卷风图，对影响最大的因素提早接入沟通，取得了不错的效果。

5.规划风险应对

规划风险应对是对经过定性、定量分析之后的风险登记册进行分析，进一步确定风险的应对措施。在本项目中，项目干系人分布在全市各地，沟通风险较大，在制定风险应对计划时，针对干系人众多的问题，我计划积极协调市局信息中心，通过在公安内网搭建“项目的 BBS”的方式公布项目的进展及各项目状态报告。针对安全接入的技术风险，我计划采取监控和审计措施来应对。

6.实施风险应对

实施风险应对就是执行商定的风险应对计划的过程。针对沟通风险较大的问题，我积极协调市局信息中心，通过在公安内网搭建“项目的 BBS”的方式公布项目的进展及各项目状态报告，搭建用户与项目组的沟通平台，全局民警通过该 BBS 可以随时与项目组进行交流和互动，务实高效的汇集了他们的问题，并及时反馈，最大限度地降低了项目干系人众多产生的巨大沟通风险。针对安全接入的技术风险，我要求技术团队重点监控短时间内大量获取敏感数据、访问频次异常、非工作时间获取敏感数据等异常调用、异常访问行为进行实时分析。并且我们对接口访问、数据调用等操作进行完整日志记录，并持续开展安全审计。

7.监督风险

在项目开发的全过程，我还始终重视对已识别的风险进行充分的监控，同时也不断收集和识别新出现的风险。组织项目团队定期进行风险评审，分析项目剩余的应急储备与残留风险的匹配程度，充分进行预留管理。

经过 1 年的开发，该项目顺利一次性上线运行成功，移动端系统与服务器端平台运行良好，一线民警反馈软件系统稳定，界面友好，功能实用，故障率低。在公安实战中，达到应用要求，提高了警务工作的效率，极大方便了一线民警的工作，这些成绩的取得是和良好的项目风险管理分不开的。在项目早期我们制定了切实可行的项目风险管理计划，在项目开始和进行中充分发动项目成员对可能的风险进行充分的识别，然后邀请项目组内外的风险专家对识别的风险进行充分的分析，制定切实可行的应对措施，为风险应对预留预算，并且将风险监控的工作落实到人，做到风险件件有人盯，措施条条有落实。

当然，我们的项目风险管理工作也不是十全十美，也存在一些不足，如：（1）进行风险分析的基础数据的积累还不够，需要根据专家的经验，据此进行的定性和定量风险分析的依据不是很可靠；（2）风险管理的意识在项目成员中的宣贯还不到位，一些成员的风险意识不强，