# 信息安全测评服务项目立项报告

1. **项目名称**

信息安全测评服务项目

1. **项目必要性及可行性**

eMAS2.0项目和再·型-地震巨灾模型2.0项目，作为对外提供服务的信息系统，面临的信息安全风险更高，监管对这类系统的安全要求也更高。eMAS2.0项目的苹果交易场景更是涉及资金流动，为保证交易资金安全、为提高该类系统安全性及稳定性，防止来自外部的非法访问和恶意攻击，有效预防信息安全风险的发生，需要对相应的业务系统开展渗透测试、代码审计等专业安全评测。渗透测试、代码审计等安全评测是专业安全公司的常规外包服务主要内容之一，这些专业安全公司组建了成熟的、专业能力强的技术团队，长期服务于各大金融机构。

1. **项目主要内容**

**渗透测试：**渗透测试是指由信息安全工程师利用安全工具并结合实践经验，同时采用各种攻击技术对系统进行非破坏性质的侵入测试和模拟黑客攻击。这种测试方法可以非常有效的发现最严重的安全漏洞，尤其是与全面的代码审计相比，其更高效。渗透测试主要包括：信息收集类（互联网可收集到高价车定价系统的敏感信息），配置管理类（HTTP方法测试、应用管理界面测试、信息泄露等），认证类（用户枚举、密码猜解、密码重置测试等），会话类（cookie测试、会话固定测试等），授权类（URL越权、路径遍历、业务逻辑、文件下载测试等）、数据验证类（SQL注入、跨站脚本、代码注入、URL跳转、文件上传测试等）、系统应用漏洞（溢出、0day漏洞等）等。

**源代码安全审计**：源代码安全审计以发现应用程序编码过程中造成的安全漏洞为目的， 通过源代码静态分析工具，对已有的代码进行扫描、分析，并对导致安全漏洞的错误代码进行定位和验证，然后提供补救建议。

**安全加固：**安全加固是针对系统脆弱性采取的一种有效的安全手段，可以提高系统抵御外来的入侵和蠕虫病毒袭击的能力，缩小影响范围，使被测系统可以长期保持在高度可信的状态。为了减小和避免安全加固操作对操作系统、数据库、应用系统和网络设备的影响，在加固方案设计和加固实施过程中会遵循标准性、规范性、可控性、整体性、最小影响等原则。主要包含主机和应用系统安全加固两个方面。

1. **实施计划**

预计启动时间：2019年8月

预计完成时间：2019年9月

1. **采购方式**

拟采用单一来源的方式采购

1. **预算安排**

项目预算：本项目总预算合计10万元人民币，包括eMAS2.0平台和再·型-地震巨灾模型2.0两个项目，拟从“电子设备运转费”中调剂支出，不超电子设备运转费总预算。