附件 3

资本市场金融科技创新试点（上海）
项目公示表

填报时间：2022 年 1 月 21 日

☑试点公示 （对于通过试点申请的项目，《公示表》将在项目公示阶段对社会公开）

一、项目基本信息	1.1 申报单位	1.1.1 牵头申报单位： 上交所技术有限责任公司
		1.1.2 联合申报单位 ： 奇安信科技集团股份有限公司
	1.2 项目名称	证券行业供应链安全管理中心研究与实践
	1.3 项目类型	□金融服务□科技产品□业务辅助□合规科技□监管科技 ☑行业平台☑行业基础设施 □其他(需补充说明)：_____
	1.4 应用场景	软件供应链已经成为网络空间攻防对抗的焦点，直接影响关键基础设施和重要信息系统安全。我国在软件供应链安全方面的基础比较薄弱，国家、各行业尚未建立成熟的软件供应链安全管理中心。本项目为建设证券行业供应链安全管理中心，中心包含三大能力，分别为供应链安全入网能力、供应链安全检查能力、供应链安全监测能力，通过安全能力的建设，形成常态化的供应链安全管理机制，为行业关键基础设施、重要证券公司提供检查能力，保障证券行业常见交易软件、行情软件等软件应用，使其具备安全性，实现对供应链攻击的攻击发现和预警，整体提升证券行业的软件供应链安全管理的水平。
	*1.5 数据应用	本项目建设的证券行业供应链安全管理中心为检测行业内应用软件，数据来源为外部供应商提供的应用软件、证券公司自研的应用软件。
	*1.6 实施计划	本项目已完成研发、测试等主要工作，具备在被允许试点之日起一年内上线运行条件。
	1.7 面临的困难	软件供应链上频发的由于缺乏管理引起的安全事件使得安

	及解决思路	全人员和管理者有理由认为这些管理方式并没有得到彻底地执行，或者管理方式本身存在问题。如何探索更有效且可行的软件供应链管理方法，设计相关流程和工具，制定评价指标，并以技术标准的形式推行，是证券行业供应链管理中的重大难题。
	1.8 专利、认证或奖项	开源检测组件获得奖项： 第二十三届中国国际高新技术成果交易会优秀产品奖； 供应链安全治理系统获得奖项： 赛迪颁发的 2020-2021 年度新一代信息技术创新产品； 代码检测组件获得专利： 一种基于序列化中间表示的源代码云检测系统及方法； 一种基于静态分析技术的源代码检测系统及方法； 一种用于检测数组越界缺陷的方法及系统； 一种基于序列化中间表示的源代码分布式检测系统及方法； 一种用于检测与内存空间释放相关的缺陷的方法及系统；
二、依法合规原则评估	*2.1 涉及的业务场景是否由持牌机构提供	2.1.1 申报机构已取得的证券期货相关法定业务资格名称： 不涉及
		2.1.2 本次申报项目业务场景涉及的业务资格： 不涉及
	2.2 现行法律法规和监管规定符合情况	2.2.1 证券监管部门的相关法规及符合情况： 本项目不存在违反禁止性规定的情况，包括但不限于账户实名、资金安全、公平交易、个人信息保护、可控数据跨境流动、反洗钱、网络安全等。
		2.2.2 行业协会、交易所等自律组织的相关规范及符合情况： 本项目不存在违反禁止性规定的情况，包括但不限于账户实名、资金安全、公平交易、个人信息保护、可控数据跨境流动、反洗钱、网络安全等。
		2.2.3 国家或其他管理部门的相关法规及符合情况： 本项目符合国家《网络安全法》、《关键信息基础设施安全保护条例》； 本项目符合行业《关于规范金融业开源技术应用与发展的意见》、《证券期货业移动互联网应用程序安全检测规范》；
	*2.3 出具合规评估意见的机构、评	2.3.1 评估机构名称： 公司合规部门

	估时间及评估结论	2.3.2 出具时间： 2022 年 1 月 20 日
		2.3.3 评估结论： 无风险
三、有序创新原则评估	3.1 技术创新情况	3.1.1 技术创新情况： 本项目中使用的软件检测技术为业内领先，具体涉及技术如下： 1、构建全面的软件空间测绘数据 软件元素种类多样（数百万）：库文件、代码模块、URL/IP 等。元素依赖关系多元（数千万）：静态依赖、动态依赖、释放生成等。 2、高精准漏洞影响范围评估 提出了高精度的软件模块信息抽取方法，构建了精确到模块级别的漏洞信息库，结合漏洞关联分析方法与软件空间测绘数据，准确检索受到威胁元素影响的软件。 3、开源软件许可协议分析 从项目中识别出开源组件，即提取所有可读文本的字符串，过滤后，一是通过正则表达式匹配，二是通过 hash 匹配，三是通过 ac 自动机算法匹配。识别开源组件的许可协议特征。依据特征，获取许可协议信息。经过遍历项目所有组件相应的许可协议信息，生成许可协议列表，并在任务检测结果页面呈现给用户，列表包括许可协议名称、版本和等级； 4、源代码安全缺陷分析 对源代码进行“编译”，该编译过程可以识别源代码中的函数调用关系、控制流信息、变量别名信息、指针信息、数据依赖关系及接口等要素，进而依据缺陷知识库模块中的策略，对编译信息中的语法、结构、过程、接口进行检查，最终实现源代码安全缺陷及隐患的自动化检查。 5、软件深度分析 静态分析是拆解软件的基本组成，提取软件各个模块的静态依赖关系；动态分析是构建软件运行时依赖的各种元素（例如网络访问）及其动态依赖关系（例如模块加载、文件创建、第三方工具调用）；沙箱分析是尽可能遍历软件执行路径，触发可能的安全隐患和后门，以及满足大批量软件大自动化分析需求。

	3.2 技术领先优势	我国在软件供应链安全方面的基础比较薄弱，国家、各行业尚未建立软件供应链安全管理中心。本项目为证券行业首创，建设行业级软件供应链安全风险分析平台，从证券行业层面建立软件供应链安全风险的发现能力、分析能力、处置能力、防护能力，为行业关键基础设施、重要证券公司提供检查能力，及时发现和处置软件供应链安全风险，整体提升证券行业的软件供应链安全管理的水平。
	3.3 服务对象与渠道	3.2.1 服务对象与渠道： 本项目服务对象为证券公司
四、风险可控原则评估	4.1 业务风险防控	4.1.1 业务风险点： 本项目不涉及业务风险。
		4.1.2 风险监测机制： 不涉及。
		4.1.3 风险控制措施： 不涉及。
		4.1.4 应急预案： 不涉及。
	4.2 技术风险防控	4.2.1 技术风险点： 本项目建设的供应链安全管理中心主要为检测行业内的软件应用，存在大量检测任务并发情况下，供应链安全管理中心性能不足以支撑检测任务顺利进行的情况。
		4.2.2 风险监测机制： 在供应链安全管理中心中建立风险监测机制，实时监测中心性能情况。
		4.2.3 风险控制措施： 本项目可部署在云环境中，利用云计算的特性进行计算资源的动态、弹性扩展，保障中心资源。
		4.3.4 应急预案： 若发生性能不足以满足任务并发的情况，由项目相关负责工程师控制检测任务数量，降低性能不足带来的影响。
	*4.3 投资者保护机制	4.3.1 客户投诉渠道： 上交所服务热线：400-8888-400

		4.3.2 投诉处理机制： 客户投诉意见由呼叫中心受理，并将投诉意见移交至业务部门。业务部门将根据客户意见及时联系客户，进行处理。
		4.3.3 风险补偿机制： 不存在客户损失风险。
		4.3.4 项目退出机制： 课题组为项目建立了完善的项目退出机制，如果由于不可控的风险项目需要退出，会按照退出机制恢复现场环境，销毁项目相关文档。

附页：

牵头申报单位承诺	本单位郑重承诺： 1. 本单位在申报资本市场金融科技创新试点（上海）项目过程中，所提供的一切申报材料信息真实、准确和完整。 2. 申报项目符合依法合规、有序创新、风险可控的申报原则。 3. 申报项目不存在违反法律和行政法规情况，不包含国家秘密信息。 4. 本单位将配合监管部门完成后续评审公示、监督检查或风险处置等工作。 5. 本单位已全面开展合规性评估和内控审计，能够有效保障业务连续性和用户信息安全，保证资金安全。 以上承诺如有违反，愿承担相应责任与后果。 单位（公章） 法定代表人（签字）： 2022 年 1 月 21 日
联合申报单位 1 承诺	本单位郑重承诺： 1. 本单位在申报资本市场金融科技创新试点（上海）项目过程中，所提供的一切申报材料信息真实、准确和完整。 2. 申报项目符合依法合规、有序创新、风险可控的申报原则。 3. 申报项目不存在违反法律和行政法规情况，不包含国家秘密信息。 4. 本单位将配合监管部门完成后续评审公示、监督检查或风险处置等工作。 5. 本单位已全面开展合规性评估和内控审计，能够有效保障业务连续性和用户信息安全，保证资金安全。 以上承诺如有违反，愿承担相应责任与后果。 单位（公章） 法定代表人（签字）： 2022 年 1 月 21 日

（注：联合申报单位如多于 1 家，承诺签章栏请相应增加）