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 18 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）

☐ **辅导公示** （对于通过辅导申请的项目，《公示表》将在项目公示阶段对社会公开，标*项目可酌情填写，或填“暂无”、“不适用”）

一、项目基本信息	**1.1 申报单位**（以重要性为序逐行列明单位营业执照上的全称）	**1.1.1 牵头申报单位：** 国泰君安证券股份有限公司
		1.1.2 联合申报单位 ： 杭州默安科技有限公司 北京微步在线科技有限公司
	1.2 项目名称	面向攻击溯源的行业威胁情报共享解决方案
	1.3 项目类型（可多选）	☐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	（试点项目应用业务领域、主要功能、提供的服务、解决的问题等。） **一、 应用业务领域** 目前证券行业各机构的安全建设水平和防御能力参差不齐，特别是在威胁情报的建设与应用上各自为营，呈现竖井式发展。面对攻击者针对同类目标发起的关联攻击或者更具隐蔽性 APT 攻击，行业各机构很难借助于孤岛式的情报数据来判断攻击者的攻击手段、攻击路径、攻击目标及攻击范围等上下文关联信息，难以有效的进行攻击者画像，进而导致行业各机构在面对攻击时缺少主动的威胁溯源能力。 因此，本项目拟构建面向攻击溯源的行业威胁情报共享体系，通过“一套机制、一个中心”打通行业威胁情报共享通道，结合多源威胁情报信息数据的采集上报，利用机器学习算法关联分析出具备行业特色的攻击溯源情报，打造行业级情报知识库并实时共享给行业各机构，进行威胁预警、攻击溯源的工作，打破安全防御的孤岛和竖井，提升“一点威胁感知、情报共享联防”能力，探索建立基于威胁情报共享的行业安全生态圈。

		二、 主要功能/服务 在行业威胁情报共享体系中，一套机制：基于威胁情报共享体系进行多种类的攻击溯源情报共享，进行威胁报告的上传下达以及威胁通报管理；一个中心：以情报中心节点为核心，针对情报数据进行统一运营，以保障情报数据的时效性、准确性和丰富性；威胁情报体系以平台为载体，情报中心节点进行情报采集、交换、共享和管理，各情报分节点进行本地情报的生产、上传、情报接收及与现有安全体系全场景应用。 **三、 解决的问题** **四、 建立行业溯源威胁情报知识库** 通过多源、多维度的威胁情报采集以及各机构自己生产的私有情报，在威胁情报中心进行智能关联分析，根据影响范围、攻击频率、是否恶意、攻击行为等计算出威胁值，生产出具备高威胁的行业情报，刻画攻击者画像、攻击常用手法、攻击趋势等数据，形成行业在面对攻击溯源所需的情报共享知识库。 **五、 多源渠道情报信息格式统一展现** 将源自专业安全厂商、企业自身、同行业企业、行业监管单位及其他信息渠道获得的网络威胁情报、线索进行关联分析处理，将不同的信息格式进行归并处理，进行不同维度和不同粒度的可视化展现，以统一标准化的情报数据格式进行行业风险预警。 **六、 助力提升行业攻防对抗能力** 行业情报知识库为各机构赋能，通过下发攻击者画像、攻击者常用手法、攻击热点趋势等信息，快速提升各机构的安全防护能力，尤其是对于中小机构，可以快速补齐对于高级威胁的检测、溯源能力，提升其实战水平。在 HW 攻防演练中，可以实时自动化同步各机构发现的 HW 情报，提前处置，降低机构被攻破的概率，提升对抗防护能力。 **七、 构建“一点联动，全网可知”的能力** 建立行业面向攻击溯源的威胁狩猎网，任何机构存在较大的安全事件，都可以将相关攻击者信息、攻击者手法上传到情报中心平台，根据监管的相关要求，隐去涉及机构信息后将该信息同步共享给其它机构，实现“一点威胁、情报共享、全网感知”。
	***1.5 数据应用**	（试点项目使用的数据来源，应区分内/外部数据，区分公开/私有数据，明确数据主体、采集方式、数据规模、数据分类、安全级别、数据共享和融合应用安排等。） 为构建行业各机构之间的威胁情报共享能力，提升攻击溯源能力，需要构建情报数据的“上传下达”通道，“上传”需要包括多元化情报与线索数据的采集，“下达”包括多元化情报数据的共享。按照《证券期货业数据分类分级指引》JR/T 0158-2018，数据分类主要为日志类数据，安

		全级别为二级，数据规模预估为 20 万条。 **一、 多元化情报与线索** 为了使情报信息发挥最大价值，需要进行多元化的信息采集。主要来源为： 1) 内部情报（高价值精准情报） 由国泰君安证券内部产生的情报，或是由监管机构、第三方提供的针对国泰君安的真实威胁情报。主要是采集现有的相关安全系统、网络设备、业务系统提供的信息化数据，具体如下： ➢ 基于设备产生的日志数据:NDR、EDR、沙箱、SoC、SIEM 等安全系统数据，以及网络设备、业务系统日志数据。 ➢ 资产数据:利用探针等技术获取来自信息资产、网络流量的相关安全信息， 如漏洞信息、IP 数据包信息、行为信息、特征信息等。 ➢ 基于已有的安全知识库的数据:包括漏洞库、病毒样本库、安全事件库、黑客组织库、设备指纹库等。 ➢ 蜜罐蜜网:利用部署的蜜罐密网系统，捕捉相关威胁攻击信息数据。 ➢ 情报命中数据/产出情报：本地情报命中的告警日志及本地生产出的情报数据。 2) 外部情报（作为情报线索） 通过外部或共享方式获取到的威胁情报，可以作为线索判断是否在机构内部已经发生过类似攻击或作为预测是否将会发生类似攻击。 ➢ 专业厂商多维度威胁情报数据（如默安、微步在线等厂商）; ➢ 开源威胁情报数据; ➢ 监管单位; ➢ 其它（如社区、自媒体等）。 **采集的情报数据类型和内容：** 1) 攻防者设备指纹信息（设备指纹：是一种攻击者电脑设备指纹识别技术，通过特定的算法将操作系统、浏览器、IT 设备行为、HTML5 WebGL 等特征融合计算出攻击者的 IT 设备指纹信息。IT 设备指纹虽具有可追溯性和不可抵赖性，但非传统意义上的人体生物信息） 2) IP 信誉 3) IOC 4) CVE、NVD、CNVD、CNNVD、CWE、NVD 等漏洞情报 5) Hash 6) MD5 7) URL 8) Domain

		9) SRC 为了增强情报数据的安全管控，会分别对网络指标、PCAP数据包、钓鱼邮件样本、系统、网络以及应用程序的日志等情报信息进行相关字段的脱敏或去标识化。 **二、 采集方式** 1) 通过威胁狩猎技术采集攻击者设备指纹信息与威胁信息； 2) 通过流量分析技术采集威胁信息； 3) 通过终端分析技术采集威胁信息； 4) 通过邮件分析与溯源技术采集攻击样本与相关信息； 5) 机器人通过安全社区自动爬取； 6) SRC、Syslog或第三方API采集。 **三、 情报融合分析** 要使情报发挥决策性作用则需要有高价值情报作为依据，因此需要对获取到的海量情报做深度融合性分析。 利用ATT&CK、钻石等模型，结合现有情报进行碰撞、去重、去伪、规则匹配与AI技术等深度关联分析，发现与预测潜在攻击行为，并对之进行溯源分析攻击链等威胁信息。全面覆盖基础设施信息、攻击者设备指纹、漏洞、战术、技术手段、过程与APT等不同层面的威胁情报。 基于威胁、被攻击资产重要程度等维度，结合情报来源、上下文分析进行研判，定义威胁等级，为后续处置提供优先级依据。 **四、 面向攻击溯源的威胁情报交换与共享** 建立本地化威胁情报平台，提供情报汇聚、分析、检索与协同等能力。通过共享机制对行业机构间的情报平台进行情报信息的交换与共享，以使情报可以发挥联防联控的功效。 1. 共享的情报数据内容： 机构单位在发生攻击事件时对攻击者进行溯源取证时需要的相关信息，如攻击设备指纹、攻击者画像、攻击者使用的Domain、IP、URL等。 2. 情报共享方式： 支持API调用、KAFKA读取以及导入方式等多种情报共享方式。 1) API对接 通过情报平台API接口能够实现行业、机构间的情报交换与共享。此方式需要制定API标准，保持接口一致。 2) KAFKA读取方式 通过KAFKA方式进行威胁情报数据交换和共享。此方式需要统一KAFKA读取标准，保持接口一致。

		3） 明文导入方式 通过明文的方式将行业情报导入证券机构本地的情报平台节点进行使用。 **五、 情报查询** 1） 在线查询 基于设备指纹、IP、URL、MD5、Hash、域名、邮箱和行业等信息提供在线情报查询功能。 2） API 查询 基于 API 方式提供威胁情报的查询，通过 ID、密钥访问对应接口，以 json 或 xml 等格式获取情报信息。 3） 订阅推送方式查询 通过订阅方式对行业内或订阅类型的威胁情报与威胁态势进行推送。 4） 社区方式 通过社区形式进行威胁情报的分享与讨论。 **六、 处理与安全自动化编排能力** 应建立威胁自动化处置能力，如对接相关自动化处置平台对精准关键威胁进行自动化处置或通过相应流程及时的对威胁进行手工处置。
	***1.6 实施计划**	（项目研发、测试、上线等各主要阶段时间节点及进度安排。试点申报项目应已完成研发、测试等主要工作，已经在生产环境实际运行或具备在被允许试点之日起一年内上线运行条件。针对分期建设开发的项目，应注明各期或版本的主要内容和日程安排，远期目标可作为单独项目后续另行申报。） **一、 方案制定和设计阶段 1 个月** 进行充分的项目调研分析，设计平台基础架构，试点系统目标和分析模型，包括定义平台的软硬件、网络的组成和非功能需求，定义系统目标和功能，设计系统的输入和输出接口。在调研、研讨中不断完善、细化方案。进一步落实资金，推进实施。 **二、 项目详细设计及平台基础架构搭建 2 个月** 进行项目的详细设计、方案细化，软硬件采购部署，物理平台和网络架构搭建完成。 **三、 平台各系统功能开发 6 个月** 根据需求，实现主要技术平台的搭建和测试，数据的整理、清洗、预处理和存储，实现模型的定义、配置和运行。完成各系统的开发和测试工作，配合用户使用进行最终结果的优化和确认。

		四、 各系统联调和数据系统接入功能开发 2 个月 各系统联调、数据对接，反馈和测试结果，结合实际业务运行状况进一步优化调试。测试设备之间联通性、时效性、安全性。 **五、 试运行及检查验收阶段 2 个月** 系统正式进入试运行阶段，在此过程中，通过不断的改进系统完善各项功能，核查系统运行稳定性，并最终通过检查验收。
	1.7 面临的困难及解决思路	（试点项目研发过程中可能或已经面临的各类困难，包括但不限于技术、业务、人力、资金、合规、风控等方面，以及后续解决的方向和思路。） **一、 多源威胁情报数据格式规范化问题** 与运维监控中通过 ELK 方式实现 SIEM 安全信息与事件管理最终形成 SOC 运营的模式相似，多源情报关联分析模型的实现方式也将会面临相类似的数据聚合问题。 数据导入本身非常简单，但由于数据来源不同，格式不同等原因，数据规范化导入过程将会面临挑战。威胁情报多源异构的数据特点使得现有数据表达规范和通信传输协议不能在威胁情报共享中直接使用，无法有效地进行威胁情报的表达和传输。 基于结构化的规范情报描述标准和固定的传输协议可降低参与情报共享机构、存储库进行情报交换和数据格式转化的成本，提高所交换情报的效率和准确性，同时简化参与方的连接管理，促进各成员资源共享、协同交流。 解决思路：通过前期调研，预选出高价值情报源，分批次、阶段实现情报采集与格式规范化。 **二、 保障在有限的带宽下确保上报数据的一致性、完整性和可用性** 数据传输带宽较小，并且存在专线和互联网等多种通信链路。需要确保在复杂的通信链路下，上报数据不重复、不遗漏、不短缺，并且确保上报数据不间断、高可用。 解决方案：对各类型定时上报的数据进行压缩，并且对传输数据链路进行加密，确保安全数据的上报；对每条上报的数据都加入一致性和完整性奇偶校验码，确保数据中途不被修改或恶意篡改；对于相同数据重复上报的问题，每个情报节点会对数据进行去重处理，确保上报数据一致、完整且唯一；利用 Kafka 队列缓存技术，能够确保并发极限时无法处理的数据通过队列进行有序上报，避免数据丢失。 **三、 情报采集源众多，需解决快速部署难点** 项目实施交付涉及大量内容，包括安全设备接入、数据标准化映射、网络连通测试、数据多向上传等，并且实施机构众多，

		涉及大量组织间沟通协调工作，所以需要从安装、采集、数据转化、上报等环节实现自动化“一键实施”，缩短实施周期，摆脱对大量人力的依赖。 解决方案：生成软件自动化安装包，执行“一键安装”；提前分配采集端口，对于需要采集的数据进行“一键采集”；对于采集数据格式的范式化处理，通过预置字段映射和字段提取转化插件进行“一键转化”；对于需要上报的数据支持 API、Kafka 等多种技术进行“一键上报”。 **四、 多源威胁情报数据关联分析挑战** 多源威胁情报数据关联分析，将多线索关联分析并以高价值情报的形态呈现，发挥出决策性作用，就必需使情报具备真实、可用的特性。因此如何保证关联分析结果的价值，就是必须要面对、解决的重要问题。 解决思路：通过分析威胁情报相关模型，结合现有情报分析、匹配、关联等方式，实现攻击行为预测与发现等能力，并对其进行威胁分析。 **五、 情报源格式或内容变更风险** 多源情报除内部情报以外，将从第三方不同组织、不同数据采集方式作为线索进行汇总分析。在后续长期运营过程中，各机构发布信息格式，如情报字段等均可能存在变化导致接口失效等问题。 解决思路：通过定期人工维护更新，以及情报平台增加手工模板导入等方式解决该问题。 **六、 情报数据泄露风险** 威胁情报在本质上是高度敏感的，尤其是经过关联分析后产生的精准情报；运营者本地及数据传输过程中存在的泄露风险，以及共享者在不同的信任边界内操作，可能产生的信任问题导致隐私问题。如果威胁情报处理不当或泄露，可能会对情报来源组织造成不利影响；更有可能会受到攻击者的进一步利用，造成其声誉受损，进而导致收入损失。因此共享数据的隐私保护方法也是建设威胁情报共享平台需要重点解决的问题。 解决思路：威胁情报共享在用户群体和服务类型以及共享内容结构上都存在差异，需要根据服务、数据类型和结构的不同进行优化和重建；除在建立本地平台及交互过程保障数据安全防护外，还需在平台设计初期规划情报鉴权、实现信息分级别共享保护，防止情报泄露。

	1.8 专利、认证或奖项	（项目所获得的专利、认证或奖项的名称、时间及颁发单位等主要信息。） 无。
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**（本表所称证券期货相关业务指受到中国证监会及其派出机构或相关自律组织认可并进行监管的业务，业务资格取得方式不限于行政审批、备案、登记等）： 证券经纪；证券自营；证券承销与保荐；证券投资咨询；与证券交易、证券投资活动有关的财务顾问；融资融券业务；证券投资基金代销；代销金融产品业务；基金投顾业务；为期货公司提供中间介绍业务；股票期权做市业务；中国证监会批准的其他业务。
		2.1.2 本次申报项目业务场景涉及的业务资格： 不适用。
	2.2 现行法律法规和监管规定符合情况 （对与项目应用场景相关的业务法规和技术规范符合情况进行梳理分析，是否存在违反禁止性规定的情形）	**2.2.1 证券监管部门的相关法规及符合情况**（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）： 经梳理分析，本项目不存在违反证券监管部门相关法规的情况。
		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（要求同上）： 经梳理分析，本项目不存在违反行业协会、交易所等自律组织相关规范的情况。
		2.2.3 国家或其他管理部门的相关法规及符合情况（要求同上）： 经梳理分析，本项目不存在违反国家或其他管理部门相关法规的情况。
	***2.3 出具合规评估意见的机构、评估时间及评估结论**	**2.3.1 评估机构名称**（公司合规部门或第三方专业机构）： 国泰君安证券股份有限公司法律合规部
		2.3.2 出具时间（如包含有效期的请注明）： 2022 年 1 月 18 日
		2.3.3 评估结论（最终结论） 根据现有方案描述，本创新试点项目方案总体风险可控。 《中华人民共和国网络安全法》第三十九条：国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享。

		《关键信息基础设施安全保护条例》第二十三条：国家网信部门统筹协调有关部门建立网络安全信息共享机制，及时汇总、研判、共享、发布网络安全威胁、漏洞、事件等信息，促进有关部门、保护工作部门、运营者以及网络安全服务机构等之间的网络安全信息共享。 本试点项目主要通过面向攻击溯源的威胁情报数据进行收集、归类和关联分析，并以共享机制实现行业机构间的威胁情报信息交换与共享，达到安全攻击威胁有效溯源的联防联控效果，符合法律和条例相关监管精神。但在威胁情报数据共享的机构单位中，各方需遵守《中华人民共和国个人信息保护法》相关要求对个人信息进行保护。综上，同意该项目申报资本市场金融科技创新试点项目。
三、有序创新原则评估	3.1 技术创新情况	（试点项目所使用的新兴技术及为业务赋能的基本原理，与传统技术方案相比的价值体现。涉及多项技术应用的，可逐条列明，同时注明多项技术的融合应用原理与价值。） **一、基于攻击者画像的知识图谱构建威胁关联分析能力** 基于攻击者画像构建模型，实现多元威胁情报数据的自动采集、融合、关系抽取、质量评估，以及关系型数据库威胁情报向图数据库的自动转换和构建，基于图谱进行威胁的深入关联分析，产出高质量情报数据，为攻击溯源提供有价值的线索。 **二、基于情报信息敏感度与私密度标签化的多元共享交换与跟踪技术** 通过对情报中攻击目标 IP、URL、登录凭证、被攻击单位等相关敏感信息进行标签化处理，通过标签化技术可以实现哪些敏感信息元数据在进行情报共享前需先进行改写，以此最大限度降低情报中的敏感度。通过对行业、来源渠道等标签定义情报类型、级别，并根据情报级别标签来控制可共享的内容、行业、范围。 **三、通过跨机构、跨行业、跨地域的共享交换机制探索行业安全生态圈建设路径** 威胁情报的多源与共享需要共同建立和遵守共享规则，通过规则定义成员单位所能读取的情报级别，同行业的单位与其他成员单位能够读取的情报因有所区别。同时还需要对情报共享情况进行记录，对各单位读取情报的行为进行审计。 在相关监管机构的指导下，通过持续开发情报中心管理功能、输入/输出 API 接口和情报数据规范，推动与行业机构、第三方单位战略合作，打通情报数据链、丰富情报数据源，实现跨机构、跨行业、跨地域多源情报的采集和共享，探索构建行业安全生态圈，形成网络安全情报数据的快速共享和协同联动机制。

	3.2 技术领先优势	（项目技术应用、业务模式、工作流程等属于首创还是对同业做法有显著改进；所用技术先进性衡量指标及相对其他同业做法的主要优势，如：算法、技术路线、设备平台等方面。） **一、结合基于浏览器多点存储的防篡改标记终端设备与机器学习分析的跨浏览器设备识别技术** 基于设备指纹（设备指纹：是一种攻击者电脑设备指纹识别技术，通过特定的算法将操作系统、浏览器、IT 设备行为、HTML5 WebGL 等特征融合计算出攻击者的 IT 设备指纹信息）技术开发的威胁情报平台，支持对国泰君安发起攻击的攻击者进行设备指纹收集和归并，同时也支持对下属分/子公司上送的同类攻击者情报进行分析归并。 基于设备指纹定位的攻击者信息，可依据相同的设备指纹对不同的攻击源 IP 进行归并，设备指纹的生成条件依赖几十个维度，如操作系统信息、硬件信息（如声卡、网卡）、浏览器版本等等，通过加权算法进行计算最终形成高精度的设备指纹，相比传统通过单一 IP 信息进行定位攻击者的方式，设备指纹技术的定位更加精准可靠。 传统的攻击者情报是割裂的，同一个攻击者更换 IP 后会识别为新的攻击源，通过设备指纹技术可实现对攻击者更换 IP 后的同一性判断，同时依据相同的设备指纹可进一步对不同子单位收集到的攻击者进行设备指纹碰撞，形成攻击情报关联性，互相补充完善攻击者画像。 **二、基于多重算法控制产出情报质量** 1）权重统计法 为可信度得分，B 为基准值，目前默认为 20 分，N 为当天报警次数，W 为 TIP 内配置的数据源权重比。 $S_n=(B_1+\frac{SUM(N_1+...+N_{30})}{100})\times W_1+...+(B_n+\frac{SUM(N_1+...+N_{30})}{100})\times W_n$ 2）行为统计法 S 为可信度评分，W 为 TIP 内配置的日志数据源权重比，C1 为日志源 1 内该标签的可信度等级，目前 C 分为 1、2、3、4，级别越高数值越大。E 为对不同设备的初始分数，目前为 E=20 分。 $S_n=E_1*C_1*W_1+...+E_n*C_n*W_n$ 3）情报分析法 D 为基础值目前设定为 20 分；H 为攻击活跃度，取值为 0-1 之间，当云端有明确情报确认该 IP 有过攻击行为则取值为 1；F 为攻击行业范围，当该 IP 攻击过 2 个行业以上，且取值为 1，

		单个行业为 0.5 ； C 为可信度，75-100 分 $S = D*H + (C-75)*H + D*F$ 4）频率统计法 S 为可信度得分，AN 为近 N 分钟的的攻击总数，计算攻击 IP 在过去 10 分钟时间内的攻击频率，逐步加强该 IP 的威胁分数，统计 10 分钟内总次数比上一个 10 分钟次数的增长比，增加对应的分数。 $S_n = S_{n-1} * (A_N - A_{N-1}) / (A_{N-1} - A_{N-2})$ **三、基于知识图谱的融合与推理构建统一的威胁情报全景图** 威胁情报中心内置智能威胁分析引擎，依托大数据和机器学习技术，能够从海量数据中整合显示黑客信息及行为详情。引擎通过大量训练数据学习各种攻击模式的内在特征，形成独特的威胁分析模型，提供准确、全面的威胁分析。 通过关联来自企业自身的攻击“情报”和来自外部共享的“线索”分析详细记录攻击者的设备指纹信息，进而知道攻击者的其他攻击行为，攻击手法，攻击对象，对攻击上下文的了解，能更加全面的掌握攻击者的真实目的。 **四、基于多重维度自动评估情报源质量** 基于多维度设置权重对各情报源进行动态评分，作为判别情报质量的依据，多维度评估系统包含情报的准确性、及时性、丰富性、差异性、来源比例、类型比例、命中比例及其他定制维度。
	3.3 服务对象与渠道	（试点项目上线后的预期服务对象，区分内/外部，区分机构/个人；涉及个人投资者的，应详细描述获客渠道、服务方式、适当性要求等；试点单位应按照风险可控原则合理确定服务投资者范围、规模和适当性要求等。） 1） 内部：企业本身及分子机构； 2） 外部：监管机构以及在相关监管机构指导下，跨证券、期货、基金等机构参与情报共享的单位。
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**（应结合试点项目特点，描述试点项目上线后可能面临的业务风险，包括但不限于市场风险、信用风险、流动性风险、操作风险、合规风险、舆情风险等）： 1） 硬件环境系统宕机或网络中断，导致无法对外提供服务。 2） 外部供应商关键成员变化，调离项目，导致项目进度和质量得不到保证。
		4.1.2 风险监测机制（应描述如何采取措施及时发现和准确评估上述业务风险，针对各类风险分别列举）： 1） 建立容量管理监测机制，设置监控阈值，一旦有系统宕机或

		网络中断，能及时预警和发现。 2) 及时提供产生风险原因、影响范围等数据，协助风控合规部门评估风险范围。
		4.1.3 风险控制措施(应描述如何采取措施防控上述业务风险，针对各类风险分别列举)： 1) 定期（周会）和不定期的与项目组人员进行沟通，使得信息能及早得知； 2) 确定后备人员，并安排适当的培训； 3) 通过良好的项目文档、项目组成员之间的定期沟通，使工作不依赖于个人。
		4.1.4 应急预案(应描述如若上述业务风险发生将如何采取有效措施尽可能降低或消除负面影响)： 根据国泰君安证券网络与信息安全事件应急预案，制定本项目的日常运营应急预案，定期制定相应应急演练计划、按计划定期开展应急演练，并做好相关记录。
	4.2 技术风险防控	**4.3.1 技术风险点**(应结合试点项目特点，描述试点项目可能存在的技术风险，包括但不限于网络安全风险、数据安全风险等)： 试点项目可能有以下的技术风险点： 1) 网络安全风险 网络中断的风险；非法网络访问的风险。 2) 数据安全风险 数据丢失的风险；数据泄露的风险。
		4.3.2 风险监测机制(应描述如何采取措施及时发现和准确评估上述技术风险，针对各类风险分别列举)： 针对以下的技术风险点建立风险监测机制： 1) 网络安全风险 建设网络监控系统，实时监测网络的中断、阻塞、入侵等。 2) 数据安全风险 定期对数据记录介质进行故障检测；记录数据访问日志；对敏感数据的批量操作设置预警。
		4.3.3 风险控制措施(应描述如何采取措施来防控上述技术风险，针对各类风险分别列举)： 1) 网络安全风险 已建立安全运营体系，能够持续针对网络安全事件进行检测、分析、响应和应急处置；并通过防火墙、入侵检测等设备和手段，阻止非法网络访问；通过DDoS防护服务、多数据中心、多线路接入等方法提供网络链路可用性保证。

		2） 数据安全风险 建立数据备份和恢复流程；建立数据分级分类机制，设置数据访问权限和审核流程，遵循最少功能以及最小权限等原则分配信息系统管理、操作和访问权限；通过加密服务，保障通信数据隐私安全。
		4.3.4 应急预案(应描述如若上述技术风险发生将如何采取有效措施尽可能降低或消除负面影响)： 1） 网络安全风险 建立网络故障分级分类及响应机制，针对不同级别和各类的网络故障采取网络隔离、路由、切换等措施。对于项目单位设备突发事故，评估影响范围，并做日志分析，排查问题原因。 2） 数据安全风险 定期进行数据恢复演练，对数据安全风险进行评估，确定影响范围，联系相关干系人进行漏洞风险排除或缓解。
	***4.3 投资者保护机制**	**4.3.1 客户投诉渠道**(接受客户投诉的渠道信息，包括但不限于营业网点地址、通讯地址、电话、传真、电子邮箱、官方网站等)： 1） 通讯地址：上海市静安区南京西路 768 号国泰君安大厦 2） 全国统一服务热线：95521 传真：86-21-38670666 3） 电子邮箱：95521@gtjas.com 4） 官方网站：www.gtja.com
		4.3.2 投诉处理机制(客户投诉受理与处理机制相关内容，包括但不限于受理部门、受理时间、处理流程、处理时限等信息)： 1、国泰君安在收到客户投诉信息后，将基于投诉基础事实，在保护投资者合法权益的基础上与客户积极沟通，充分协商，促进投诉事项的妥善解决。 2、国泰君安评估后认为本单位无法独立处理重大投诉事项，或重大投诉事项涉及多单位业务、需协作处理的，将牵头成立跨单位投诉处理专项小组，召集相关单位协调处理，妥善处置投诉事项。相关单位在本单位职责范围内配合投诉处理工作。 3、国泰君安通过公司客户投诉管理系统持续跟进并录入投诉事项办理进度、调解情况（如有）、诉讼或仲裁情况（如有）等信息，并上传相关留痕材料，直至所涉投诉事项全部处理完毕。 4、如经投诉事项发现本试点项目在机制、流程、运行、系统等方面存在待整改完善之处，国泰君安将牵头及时、妥善地开展投诉后续整改完善工作，与联合申报单位一起制定项目整改方案，并对重要材料予以留痕。

		4.3.3 风险补偿机制(应描述申报单位就本试点项目建立的风险补偿和赔付机制，确保试点项目出现意外风险时能够及时对投资者损失进行合理补偿，降低试点项目的负面影响。对于多个单位联合申报的试点项目，应明确风险补偿责任主体)： 不适用。
		4.3.4 项目退出机制(应描述试点项目因发生特殊情况需终止或下线时的工作安排。项目退出应平稳有序，确保投资者资金和数据安全，最大程度减少对市场的负面影响。退出机制包括但不限于退出触发条件、业务退出安排、技术退出安排等内容)： 如遇不可抗力或其他重大故障导致本试点项目提前终止时，国泰君安与联合申报单位一起制定项目退出机制，在保障用户信息安全的前提下进行系统平稳退出：技术退出。在数据处理方面，按照《网络安全法》等要求，完成数据信息备份，归档和清理在资源回收方面，停止本项目相关的系统资源、服务包括服务器、基础组件等，取消三方网络防火墙权限，关闭合作方网络白名单，确保系统安全稳定退出。

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 18 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 18 日

（注：联合申报单位如多于 1 家，承诺签章栏请相应增加）

联合申报单位 2 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 18 日