资本市场金融科技创新试点（北京）项目公示表

填报时间： 2021 年 5 月 26 日

一、项目概览	1.1 项目编号	BJ-SD-202114
	1.2 项目名称	基于零售业务敏捷化的云原生架构实践
	1.3 项目类型	金融服务类
	1.4 项目简介	中金公司正在推进全面数字化转型，将在零售业务板块率先实现业务敏捷化落地，并与腾讯成立了科技子公司为零售业务提供金融科技服务。为了更好支持业务数字化，中金财富构建了基于云原生的基础架构组件及研运一体化平台，实现更加完善、更加智能的零售云生态。主要达成以下三个方面的目标： 1）满足数字化转型和全敏捷业务落地对云原生架构和敏捷交付框架的要求。根据公司转型和数字化战略需要，需要更加敏捷化的基础设施、应用组件及交付架构支撑更加业务快速变化和实现，进一步提升公司数字化能力； 2）支持公司向互联网科技公司转型，在合规可控的前提之下，快速嫁接金融科技子公司技术能力、互联网思维及客群导入，帮助公司成为具有互联网基因的金融科技公司； 3）做好信创准备，采用信息技术应用创新解决方案，为应用和基础设施信创奠定基础。
	1.5 创新性描述	平台基于云原生架构，赋能中金零售业务的数字化发展，为业务提供快速集成产品的创新能力，提高多团队协作效率，以金融科技创新推动财富管理业务规模化、数字化、敏捷化；该项目的创新主要包括以下四点： 1、云平台解决方案应用创新：基于腾讯公有云实践的专有云（TCE）解决方案在证券经营机构首次整体落地，根据证券业务技术特征和管控要求进行了本地化改造，形成了行业化的解决方案。 2、云原生应用创新：基于 TCE 平台之上构建的云原生解决方案包含了服务注册发现、负载均衡器、故障发现和自我修复、服务滚动升级和在线扩容等能力，探索新技术在证券机构如何支持业务应用的快速实现。 3、可信解决方案：在行业率先采用的满足信创要求的全栈私有云解决方案，包含了可信的分布式数据库（TDSQL）、云原生平台

		（TKE）、大数据套件（TBDS）等组件及配套的监控、安全防护及管理、负载均衡等多项技术落地实施。 4、金融科技生态及敏捷转型落地试点创新：作为开展全面数字化转型的行业经营机构，以及首家成立科技子公司的券商，项目试点可以为监管提供借鉴和思路，为行业其他经营机构提供参考。
	1.6 应用价值描述	公司定位于构建开放共享的云服务平台，提供持续稳定高效的云服务，成为推动效率变革和动力升级的重要驱动力。该云原生架构在高可用保障、费用优化、安全管理、DevOps 等方面的能力均有显著提升。 一、业务及技术价值 1、实现“按需索取”的计量管理能力，可清晰梳理各个维度的资源占用，有效进行 IT 资源的调配和管理。 2、云原生组件：除基础的虚拟云主机之外，也能提供原生前端负载、云中间件、云数据库等应用层的能力支持，便于业务侧架构规划和使用，降低开发和部署成本，有效支持企业级 IT 架构的升级和业务创新。 3、高可用保障：从云平台本身到云产品实例均考虑原生高可用实现，并承诺从机房容错域到地域容错域不同级别的 SLA，供业务部署选型。实现了安全统一管理，提升了整体云原生架构的安全合规水平。 4、推进 DevOps 敏捷交付，实现弹性伸缩。提供自动扩展、容器平台等能力，可实现基于资源维度的弹性扩展和回收，保障业务的波峰敏捷扩容和波谷冗余资源回收。不可变基础设施封装和运行保障业务敏捷迭代更新，使得 IT 服务体系能够有效支撑业务的创新与发展，更快地响应业务需求，快速推出创新产品。 二、行业探索价值 数字化转型已经成为了行业趋势，成立科技子公司或者与互联网公司深度合作实现快速嫁接互联网能力，寻求业务突破发展是行业经营机构的共同探索的话题，中金公司零售业务线基于业务敏捷化的云原生架构实践是公司与互联网科技公司协作探索，为技术与业务协作提供了基础支撑，对行业未来数字化转型及业务敏捷化实践有较好的借鉴意义。
	1.7 试点目的描述	该项目支撑公司数字化转型和敏捷业务的后台技术支撑，将互联网技术架构在敏捷、开放、高伸缩性方面的优势与证券公司原有技术架构的稳定、安全的优势进行了有机融合，实现了包含私有云、容器云以及公有云在内的混合 IT 基础设施的统一管控，同时在自助化服务交付、云服务计量计费等方面进行了优化和改进，使得基于云原生架构的 IT 服务体系具备了较高水平的运营能力，以科技引领业务创

		新，从而推动证券公司进入财富管理的新时代，为行业进行零售业务敏捷化提供有价值的参考。具体包括以下几个方面： 1、从云原生技术角度考虑，除基础的虚拟云主机之外，也能提供原生前端负载、云中间件、云数据库等应用层的能力支持，便于业务侧架构规划和使用，降低开发和部署成本。 2、构建云原生体系基础平台，推进 DevOps 敏捷交付。提供自动扩展、容器平台等能力，可实现基于资源维度的弹性扩展和回收，保障业务的波峰敏捷扩容和波谷冗余资源回收。不可变基础设施封装和运行保障业务敏捷迭代更新。 3、从高可用保障角度，从云平台本身到云产品实例均考虑原生高可用实现，并承诺从机房容错域到地域容错域不同级别的 SLA，供业务部署选型。 4、在管理角度，在合规的前提下将部分平台权限（如创建、修改、回收）下放，前移到业务侧，在一定程度上弱化流程，提升资源交付效率，保障业务敏捷；以租户形式隔离不同组织架构的资源对象及账户权限管理体系，实现资源可靠管理。
	1.8 牵头申报单位	中国国际金融股份有限公司
	1.9 联合申报单位	中国中金财富证券有限公司
二、项目基本信息	**2.1 功能服务**	该项目支撑公司数字化转型和敏捷业务的后台技术支撑，主要功能包括： 1）提供一站式的敏捷弹性伸缩的基础设施，为业务发展提供必要的、可自助式管理的计算、存储等 IT 资源支持； 2）提供全栈云原生能力落地支撑，建立更加开放的技术平台，支持应用向云原生架构的演进； 3）实现统一的零售业务应用发布与运维管控，在满足合规可控前提下，支持科技子公司交付应用的横向灵活部署； 4）适用于全敏捷业务的开发运维一体化交付框架，实现多团队快速交付和协同； 5）充分整合金腾科技的互联网能力与金融机构的业务能力。
	2.2 技术应用	为满足公司对数字化转型的要求和敏捷化的业务需求，需要如下技术： 1）具备完善的云计算基础设施，包括基于云计算技术，构建计算及存储资源池，实现可弹性伸缩的计算及存储资源，覆盖 IaaS、PaaS、安全管理、运营运维等多个领域云能力的开放共享云平台；

		2）拥有分布式数据库及大数据套件，能够支持分布式部署的TDSQL，集群 Cache 节点 Redis，包括分布式存储系统、管理节点、离线计算引擎等的大数据套件（TBDS）。以数据为核心的云管控架构，在合规前提下具备整合互联网能力； 3）拥有丰富的中间件及相关套件：MQ/Kfaka 消息队列服务、TKE 容器服务；建设开源工具链的研运一体化（DevOps）平台，支持全敏捷业务下多团队并行与跨团队便捷协作，实现对质量、源代码安全等管控； 4）采用 DevOps 研发运维一体化体系，包括研运流程、工具链、度量平台等，支持研发效能提升和质量管控。采用信息技术应用创新解决方案，为应用和基础设施信创奠定基础。
	2.3 数据应用	数据来源：项目使用数据主要为公司内部数据； 采集方式：数据 ETL 采集； 数据规模：现有数据 5T 左右，根据未来承载业务类型规模逐步扩大 数据分类：按照公司数据分级分类要求进行划分，主要包括客户数据、系统数据、业务数据等； 安全级别：按照公司数据分级分类要求进行划分为 4 级； 数据共享：不提供对外部单位的数据共享； 融合应用安排：作为基础资源为应用提供基础支撑；
	2.4 服务对象与渠道	目前主要是中金财富及金融科技子公司（金腾科技）内部研发运维人员
	2.5 业务规模	预期用户数量：提供给 IT 研发及运维人员使用，预期用户 200 人左右 资产数额：非业务类型项目； 交易数额：非业务类型项目；
	2.6 预期效果	通过项目建设，实现相对完备的云服务能力，满足不同需求用户的上云需求，可根据业务发展需求实现云服务的定制和扩展，支持满足未来公司用户持续扩展的性能容量需求和服务水平要求，同时建立敏捷交付体系，实现各业务形态数字化团队的安全快速交付，提供满足监管架构合规性要求的安全管控体系。 **使用成效：** ➢ 提供敏捷可扩张的基础设施 ● 为业务发展提供必要的计算、存储等 IT 资源支持； ● 为业务创新的快速实现奠定基础架构和应用组件的基础，提升数字化能力，满足业务智能化、数字化转型需要； ➢ 统一零售业务应用发布与运维管控： ● 支持业务应用交付； ● 支持金融科技子公司交付应用的横向部署，快速嫁

		接金腾科技技术与运营能力； ➢ 构建金融科技生态与云原生能力： ● 通过云平台建设，加快公司向云原生架构的演进，建立更加开放的技术平台； ● 为公司中台化架构落地提供技术基础，支持业务与技术能力的整合和输出。 ➢ 满足数据管控的合规要求： ● 建立满足合规要求的管控区域，构建满足等保合规要求的云化基础设施； ➢ 敏捷交付体系： ● 建立一套统一的敏捷交付体系，支持公司各业务形态数字化团队的安全快速交付，实现业务与 IT 的深度融合； ● 建立一套统一研发管理体系，支持各敏捷团队的敏捷协同； ● 建立一个全生命周期度量平台，不断优化改进，适应数字化转型需要。
	2.7 已获专利、认证或奖项	无
三、依法合规原则评估	**3.1 涉及的业务场景是否由持牌机构提供**	是
	3.2 是否违反现行法律法规和监管规定	否
	3.3 分析及结论： 比照技术规范和相关合规要求，该项目在合规安全报障方面做了如下布置： 1、平台提供的各项安全控制措施和安全防护技术，如 VPC、云防火墙、基于安全组的访问控制、边界防护、WEB 应用防护、安全运营中心等，均按照等级保护三级基本要求进行配备，且提供了基于等级保护三级基本要求的安全配置核查能力，协助安全管理人员对主机层面安全合规进行核查。 同时，在平台落地实施过程中，特制了满足等级保护三级基本要求的操作系统镜像，虚拟机生成后，安全配置项默认满足三级等保要求，并默认安装专业版主机安全软件。 2、平台采用私有云方式部署，所有软硬件和功能组件均落地在公司数据中心，系统产生和处理的数据均在公司数据中心内部保护和流转，满足监管部门对于物理机房、敏感数据落地和保护的要求。 3、对于有信息隔离墙要求的信息系统，目前暂不考虑在平台上部署，继续采用传统数据中心的隔离方式。 综上所述，该系统建设满足当前合规性要求，能保障业务系统正常运行。	
四、有序创新原则评估	**4.1 是否侧重于大数据、云计算、人工智能、区块链等新一代信息技术对资本市场各类业务的科技赋能**	是

	4.2 是否以服务实体经济、提升市场效能、强化合规风控、增强监管能力、保障金融安全为应用导向	是
	4.3 是否有助于稳妥推动新一代信息技术在资本年市场的落地实施，促进资本市场的数字化发展	是
	4.4 分析及结论： 公司建立的云原生架构系统，有利于实现自助服务、运营分析、弹性伸缩及敏捷化、计量计费、容器管理等核心 IT 管理能力，为实现 IT 服务化转型奠定了基础。 1、将与业务灵活性相关联的权限下放给用户，结合公司敏捷转型的部落组织架构，为每个部落创建了独立的账号体系，实现各敏捷团队业务快速部署上线，资源弹性收缩，后台运营体系做到粗中有细，对关键权限、安全漏扫等集中管理； 2、为实现集团战略全面数字化转型和敏捷落地，将私有云采用公有云的模式对内全面输出，随时随地落地自己的想法，真正做到 IT 赋能业务。	
五、风险可控原则评估	**5.1 是否已有效识别相关业务合规、系统安全、数据安全风险**	是
	5.2 是否不存在重大风险隐患或已充分做好相应风险防范和补偿安排	是
	5.3 是否不存在发生系统性风险的隐患	是
	5.4 分析及结论： 该系统除了提供满足等级保护三级基本要求的安全域划分、传统访问控制、边界防护、WEB 应用防护、带外运维审计、数据库审计等安全功能外，针对当前网络安全应急演练常态化的趋势和高级持续威胁的形势，提供了更专业、基于云原生的安全技术特性。 首先，在网络访问控制层面，基于零信任的思想，使用云原生的分布式防火墙和，实现基于安全组的细粒度网络访问控制，突破传统基于 IP 加端口的控制方式，将控制落实到主机级别。 其次，在主机安全方面，基于长期积累的海量威胁数据，利用机器学习为主机操作系统提供黑客入侵检测和漏洞风险预警等安全防护能力，包括密码破解拦截、异常登录提醒、木马文件查杀、高危漏洞检测等安全功能和行为审计、漏洞管理、资产管理等安全运营支持。 第三，在高级威胁检测方面，集成沙箱分析技术、网络入侵检测技术、流量解析和行为建模技术、溯源分析技术等，应用先进机器学习和行为分析算法，并搭载威胁情报，对未知威胁行为和失陷主机等进行精准识别和溯源分析。 最后，在安全运营层面，提供云原生的统一安全运营与管理平台，提供资产自动化盘点、互联网攻击面测绘、云安全配置风险检查、合规风险评估、流量威胁感知、泄漏监测、日志审计与检索调查、安全编排与自动化响应及安全可视等能力，实现事前安全预防，	

	事中事件监测与威胁检测，事后响应处置的一站式、可视化、自动化的云上安全运营管理。		
六、业务风险控制机制	项目具有相对完备的安全管控和审计组件，配备严格的管控流程和权限管理机制，满足等保及监管要求。 1、针对权限配置导致的潜在威胁，要求安全管理人员严格遵循最小化原则配置对云上资源的访问控制策略；同时，基于长期积累的海量威胁数据，利用机器学习为主机操作系统提供黑客入侵检测和漏洞风险预警等安全防护能力； 2、运维人员利用自动化工具时刻监控告警和事件通知等机制，确保对容器应用运行时安全的关注，对敏感数据根据等级保护三级基本要求采取对应的密钥加密机制，保证数据在传输和落盘链路上的数据安全性； 3、及时修复安全漏洞和进行版本更新，避免恶意攻击者利用容器安全漏洞入侵应用内部，同时提高员工的安全防护意识。		
七、技术安全保障机制	云平台上线前，已启用云平台不同层级的安全防护。网络层通过防火墙、安全组和网络 ACL 限制边界访问；主机层通过主机安全提供实时防护，对主机操作系统进行全面、符合等保三级的安全基线检查；应用层通过 WAF 提供应用智能防护。同时，利用 TCE 平台 SOC 的安全运营能力，在监控中心实现全平台安全事件的监控和运营。		
八、投资者保护	**8.1 客户投诉渠道**	内部项目，不涉及到投资者相关事项。	
	8.2 投诉处理机制		
	8.3 风险补偿机制		
	8.4 项目退出机制		
九、申报单位基本信息	**9.1 牵头申报单位**	**9.1.1 单位名称**	中国国际金融股份有限公司
		9.1.2 单位类型	证券公司
		9.1.3 统一社会信用代码	91110000625909986U
		9.1.4 注册地址（办公地址）	中国北京市朝阳区建国门外大街 1 号国贸大厦 2 座 27 层及 28 层
		9.1.5 持有金融牌照情况	公司经营范围包括：（一）人民币特种股票、人民币普通股票、境外发行股票，境内外政府债券、公司债券和企业债券的经纪业务；（二）人民币普通股票、人民币特种股票、境外发行股票，境内外政府债券、公司债券

			和企业债券的自营业务；（三）人民币普通股票、人民币特种股票、境外发行股票，境内外政府债券、公司债券和企业债券的承销业务；（四）基金的发起和管理；（五）企业重组、收购与合并顾问；（六）项目融资顾问；（七）投资顾问及其他顾问业务；（八）外汇买卖；（九）境外企业、境内外商投资企业的外汇资产管理；（十）同业拆借；（十一）客户资产管理；（十二）网上证券委托业务；（十三）融资融券业务；（十四）代销金融产品；（十五）证券投资基金代销；（十六）为期货公司提供中间介绍业务；（十七）证券投资基金托管业务；（十八）经金融监管机构批准的其他业务
		9.1.6 试点项目涉及的业务牌照	非业务类型项目
		9.1.7 工作分工	
		9.1.8 单位简介	中国国际金融股份有限公司（中金公司，601995.SH，3908.HK）是中国首家中外合资投资银行。凭借率先采用国际最佳实践以及深厚的专业知识，我们完成了众多开创先河的交易，并深度参与中国经济改革和发展，与客户共同成长。我们的目标是成为一家具有全球影响力的世界级金融机构。 自 1995 年成立以来，中金一直致力于为客户提供高质量金融增值服务，建立了以研究和信息技术为基础，投资银行、股票业务、固定收益、资产管理、私募股权和财富管理全方位发展的业务结构。凭借深厚的经济、行业、法律法规等专业知识和优质的客户服务，中金在海内外媒体评选中屡获“亚洲年度最佳投行”“中国最佳投资银行”“最佳销售服务团队”“最具影响力研究机构”“最佳企业社会责任”等殊荣。 2015 年，中金在香港联交所主板成功挂牌上市。2017 年，中金与中国中金财富证券有限公司（简称“中金财富证券”，原中国中投证券有限责任公司）的战略重组完成，中金财富证券成为中金的全资子公司。本次交易使公司规模显著扩大，综合实力进一步提升，将实现对大、中小企业及机构、个人客户更为深度的覆盖，构建更为均衡的一二级市场业务结构。2018 年，中金成

			功完成引入腾讯作为战略投资者。2020年，中金在上海证券交易所主板成功挂牌上市。 中金总部设在北京，在境内设有多家子公司，在上海、深圳、厦门、成都、杭州、济南设有分公司，在中国大陆28个省、直辖市拥有200多个营业网点。公司亦积极开拓海外市场，在中国香港、纽约、伦敦、新加坡、旧金山、法兰克福、东京等国际金融中心设有分支机构。凭借广泛的业务网络及杰出的跨境能力，中金能够为客户提供全方位的金融服务。 秉承“植根中国，融通世界”的理念，通过境内外业务的无缝对接，中金将持续为客户提供一流的金融服务，协助客户实现其战略发展目标。
	9.2 联合申报单位 1	**9.2.1 单位名称**	中国中金财富证券有限公司
		9.2.2 单位类型	证券公司
		9.2.3 统一社会信用代码	91440300779891627F
		9.2.4 注册地址（办公地址）	注册地址：深圳市福田区益田路与福中路交界处荣超商务中心A栋第18—21层及第04层01、02、03、05、11、12、13、15、16、18、19、20、21、22、23单元 办公地址：深圳市福田区益田路6003号荣超商务中心A栋第04层、第18—21层
		9.2.5 持有金融牌照情况	填报要求同上。 证券业务许可范围：证券经纪；证券投资咨询；与证券交易、证券投资活动有关的财务顾问；证券承销与保荐；证券自营；证券资产管理；融资融券；证券投资基金代销；代销金融产品
		9.2.6 试点项目涉及的业务牌照	非业务类型项目
		9.2.7 工作分工	
		9.2.8 单位简介	中国中金财富证券有限公司（原中国中投证券有限责任公司，以下简称“中金财富”或“公司”）是由中国

			建银投资有限责任公司（以下简称“中国建投”）在购买原南方证券相关证券类资产的基础上，以中国建银投资证券有限责任公司的名称成立的一家全国性、综合类证券公司，成立时间为 2005 年 9 月 28 日，注册地为深圳，初始注册资本为 15 亿元人民币。 根据国务院有关批复精神及财政部[财金函（2009）77 号]文件精神，从 2008 年 12 月 31 日起，公司股权从中国建投划转至中央汇金投资有限责任公司（以下简称“中央汇金”），中国证监会于 2010 年 8 月核准公司股东变更，公司于 2011 年 4 月 2 日完成工商变更。 2009 年 7 月，经中国证监会批准，公司注册资本增至 25 亿元。 2011 年 9 月，经中国证监会批准，公司注册资本增加至 50 亿元。 2011 年 11 月，经中国证监会及国家工商总局批准，公司名称变更为“中国中投证券有限责任公司”。 2016 年 11 月 4 日，中国国际金融股份有限公司（以下简称“中金公司”）与中央汇金签订股权转让协议，通过受让中央汇金所持中投证券 100%股权设立子公司。中国证监会于 2017 年 3 月 6 日核准本次交易事项，公司于 2017 年 3 月 21 日完成工商变更，成为中金公司全资子公司。 2017 年 11 月 3 日，经股东决定，公司注册资本增加至 80 亿元,公司于 2017 年 12 月 5 日完成工商变更。 2019 年 9 月，经中国证监会及国家工商总局批准，公司名称变更为“中国中金财富证券有限公司”。
十、其他补充事项			

十一、其他申报材料清单	材料名称	出具单位（部门）	时间（时效）

十二、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（北京）项目过程中，所提供的一切申报材料信息真实、准确和完整，本单位承诺承担与此相应的法律责任。 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. 申报项目不存在违法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。 单位（公章） 法定代表人（签字）： 2021 年 11 月 10 日

证券章

附页：联合申报单位承诺

项目名称	
联合申报单位承诺1	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（北京）项目过程中，所提供的一切申报材料信息真实、准确和完整，本单位承诺承担与此相应的法律责任。 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. 申报项目不存在违法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。 单位（公章） 法定代表人（签字）：高涛 2021 年 11 月 10 日