《大模型金融应用技术规范》
（征求意见稿）编制说明

一、项目背景

当前，大模型已成为 AI 技术发展前沿和产业发展热点，以大模型为代表的人工智能技术正迅速发展迭代，更智能、更通用、更开放、多模态的大模型不仅是当前 AI 技术发展前沿热点，也是加速人工智能与各行业深度融合的新路径。随着“两个规定一个办法”等相关人工智能治理政策及生成式人工智能相关国家标准的陆续发布，基于生成式人工智能的公共服务类大模型应用得到了有效治理，但大模型金融应用的技术需求、应用风险及行业生态具有较大差异，金融机构在初期探索和大模型金融应用过程中，普遍面临算力不足、开发人员经验缺乏、训练数据难以跨域融合、系统优化不足、应用效果不佳、安全合规风险增加等挑战，虽然《Q/BCTC 0003-2024 大模型金融应用评价规范》《T/SAIAS 019—2024 金融大模型应用测评指南》等大模型金融应用标准已陆续发布，相关行业标准及团体标准也在研制过程中，但由于缺少从底层算力、训练数据、模型能力、系统组件、服务平台再到上层应用，以大模型金融应用系统作为研制对象的通用技术规范作为指引，导致各金融机构在大模型金融应用探索过程中，重复投入较大成本及时间进行大模型金融应用系统验证和经验积累，为此，制定《大模型金融应用技术规范》，进一步明确大模型金融应用系统的

技术要求，保障大模型金融应用效果，成为缓解上述瓶颈、护航金融行业高质量、智能化发展的关键举措。

深圳作为全国信息产业重镇和中国式现代化的开路先锋，高度重视人工智能产业的发展。2022 年 9 月 9 日，深圳出台和实施了我国首部人工智能产业专项立法《深圳经济特区人工智能产业促进条例》，2023 年 5 月 31 日，深圳正式印发了《深圳市加快推动人工智能高质量发展高水平应用行动方案（2023—2024 年）》（后简称《行动方案》），构筑起“一条例、一方案、一清单、一基金群”的人工智能高质量发展和高水平应用的政策体系，积极打造国家新一代人工智能创新发展试验区和国家人工智能创新应用先导区，努力创建人工智能先锋城市。其中，《行动方案》中提出要推进“千行百业+AI”，鼓励金融、商务、工业、交通等行业企业基于人工智能技术对现有生产、服务和管理方式进行升级。

本标准对资源池、金融优化训练数据、金融大模型、系统组件、服务平台以及应用提出核心技术要求，构建一个安全、可信的大模型金融应用系统，推动金融机构基于标准化路径，快速部署、安全集成与灵活调用大模型金融应用。这不仅将有助于提升金融服务的智能化水平与运营效率，更能强化风险控制与合规保障，降低全行业，特别是中小金融机构拥抱前沿技术的试错成本与安全风险。本标准立足于深圳金融与人工智能深度融合的产业优势，是深圳作为人工智能先锋城市，在人工智能治理与金融科技创新交叉领域先行先试的重要举措。

二、工作简况

（一）任务来源

根据深圳市市场监督管理局于2024年1月27日发布的《关于开展2024年深圳市地方标准制修订计划项目征集工作的通知》，深圳国家金融科技测评中心作为金融科技领域的第三方专业测评机构，结合大模型、数安个保等方向的长期研究与积累，为破解大模型金融应用的共性安全、合规与发展难题，提出了《大模型金融应用技术规范》深圳市地方标准制修订计划项目建议书。

经深圳市市场监督管理局公开征集、专家论证等程序，2024年4月7日，深圳市市场监督管理局下达《2024年深圳市地方标准计划项目任务的通知》，《大模型金融应用技术规范》等195项深圳市地方标准予以立项。

（二）主要起草过程

1. 立项论证与筹备阶段（2024年1月至4月）

本阶段核心任务是完成标准的前期论证与立项程序。2025年1月，项目牵头单位深圳国家金融科技测评中心有限公司联合北京银联金卡科技有限公司、蚂蚁科技集团股份有限公司专家成立标准预研组，基于各机构前期研究及调研成果，进行了大模型金融应用标准需求分析。基于分析结果，于2024年3月完成《深圳市地方标准制修订计划项目建议书》的编制与提交，并于2024年4月获得深圳市市场监督管理局正式立项。

2. 核心参编单位组建（2024年4月至5月）

标准立项后，在深圳国家金融科技测评中心的组织协调下，迅速启动了参编单位的组建工作。定向邀请了数位在人工智能和金融领域具有较强经验积累及标准化专家作为核心参编人员，共同组建了第一届标准起草工作组。工作组明确了分工、制定了工作计划，为后续的草案编制工作奠定了组织基础。

3. 标准草案研制与迭代阶段（2024年5月至2025年1月）

编制组在前期充分调研与分工基础上，基于标准项目建议书的范围和主要技术内容，以大模型为对象，重点围绕大模型的通用知识与能力、金融知识与能力、安全与合规、性能效率四个部分进行修订完善，最终形成《大模型金融应用技术规范》（草案稿）。到 2025 年 2 月，以 DeepSeek 为代表的新一代大模型技术取得突破性进展，并迅速在金融行业催生了大量实质性、系统化的应用案例。这一重大技术变革使得产业焦点从“大模型能力”本身转向了“应用系统”的构建与治理。工作组经过内部论证与分析，原有的草案稿在规范对象、覆盖范围和前瞻性上已无法满足产业快速发展的实际需求。为此，工作组做出战略性决策：对标准进行重构，将核心规范对象从“金融大模型”调整为“大模型金融应用系统”，以有效降低金融机构在大模型金融应用系统开发建设、部署及应用运维过程中的安全合规风险，切实提升大模型金融应用效果及治理水平。

4. 进一步征集参编单位（2025年2月至2025年5月）

由于标准的核心规范对象已由“金融大模型”战略性调整为“大模型金融应用系统”，这一重构深刻改变了标准的技术侧重点、覆盖范围和关键风险点。为了确保标准内容的前瞻性、行业代表性和落地可行性，工作组决定在标准重构阶段进一步扩大参编单位范围，于2025年3月及5月分两次，通过官方公众号等渠道公开发布征集通知，并依据产业代表性、技术实力以及参与意愿等维度对申报单位进行综合评议，参编单位进一步拓展至四十多家，涵盖银行、证券、保险等金融机构、科技企业及科研院校。新成员的加入，为标准注入了宝贵的实践视角。

5. 形成标准草案稿（2025年4月至2025年7月）

在新一届工作组的框架下，以“大模型金融应用系统”为对象，经过多轮研讨，重新搭建了标准框架并对标准框架进行了多个版本的修订，最终标准内容涵盖资源池要求、优化数据要求、模型要求、模型系统组件要求、服务平台要求、任务处理能力要求、任务处理安全要求以及任务处理性能要求8大章节，各机构依据自身优势分头撰写，深圳测评中心牵头拜访多家金融机构，实地考察金融机构大模型金融应用效果及痛点，先后组织召开了多次标准研讨会及修订意见征集、进行了深入研讨及多轮修订，逐步完善最终达成了技术共识，并邀请行业专家、典型金融机构、科技企业为代表，对标准内容开展了集中评议，形成《大模型金融应用技术规范（草案稿）》。

6. 公开征求意见并形成送审稿（2025年8月至2026年1月）

基于专家反馈意见，对标准草案稿内容进行修订，进一步形成公开征求意见稿并于2025年11月24日至2025年12月25日公开征求意见，根据公开征求的反馈意见进行具体条款修订，进一步完善标准内容，于2026年1月22日形成标准送审稿。

7. 转化团体标准阶段

2026年2月9日，深圳国家金融科技测评中心有限公司向深圳市标准化协会提出团体标准转化申请，并提交“深圳市标准化协会团体标准制修订立项申请书”。2026年2月10日，通过深圳市标准化协会官方网站发布“关于批准团体标准《大模型金融应用技术规范》立项的通知”，本标准作为团体标准予以立项。

三、主要内容的依据以及与国内领先、国际先进标准的对标情况

1. 主要内容的依据

《大模型金融应用技术规范》的编制，旨在为金融机构安全、合规、高效地应用大模型提供系统化的技术指导。其主要内容的依据可归纳为以下两个方面：

（1） 政策法规依据

本标准依据参考的主要政策法规包括《互联网信息服务算法推荐管理规定》《生成式人工智能服务管理暂行办法》《互联网信息服务深度合成管理规定》以及《人工智能生成合成内容标识办法》，结合金融领域大模型应用特点及风险，明确了大模型金融应用中的生成内

容安全要求、内容标识要求、可解释性要求、管理要求等内容。

（2） 标准依据

本文件的起草严格遵循标准化工作导则的要求，按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定进行，确保了标准的结构清晰、逻辑严谨。在具体标准内容上主要依据《GB/T 35273 信息安全技术 个人信息安全规范》《GB/T 45225 人工智能 深度学习算法评估》《GB/T 45288.1 人工智能 大模型 第 1 部分：通用要求》《GB 45438 网络安全技术 人工智能生成合成内容标识方法》《GB/T 45654 网络安全技术 生成式人工智能服务安全基本要求》《GB/T 45674 网络安全技术 生成式人工智能数据标注安全规范》《JR/T 0171 个人金融信息保护技术规范》《JR/T 0221 人工智能算法金融应用评价规范》并引用了上述标准中的部分条款内容，参考文献包括《GB/T 9813.3-2017 计算机通用规范 第 3 部分：服务器》《GB/T 45288.2-2025 人工智能 大模型 第 2 部分：评测指标与方法》《GB/T 45288.3-2025 人工智能 大模型 第 3 部分：服务能力成熟度评估》《JR/T 0197-2020 金融数据安全 数据安全分级指南》。

2. 与国内领先标准的对标情况

本《大模型金融应用技术规范》与国内其他已发布或在研的标准形成了互补和协同关系，共同构成了金融大模型应用的规范体系，其中现有国内大模型金融应用在研及已发布的主要标准如下：

序号	标准名称	标准性质
1	数字金融 人工智能大模型技术应用安全规范	行业标准
2	证券期货业基础大模型选型评估指引	行业标准
3	大语言模型金融应用技术要求	团体标准
4	大语言模型金融应用评测规范	团体标准
5	金融大模型应用测评指南	团体标准
6	大模型金融应用评价规范	企业标准

（1） 标准对标情况

现有国内相关标准多数以大模型为对象进行研制，本标准聚焦于“大模型金融应用系统”，覆盖了资源池、数据、模型、系统组件、服务平台、应用六大核心环节。覆盖面更广、系统性更强，旨在解决应用系统全生命周期的技术问题，尤其突出了金融专业知识库、安全合规工具等系统组件的设计要求。

3. 与国际先进标准的对标情况

本标准在治理理念和技术要求上，与国际先进的 AI 治理和金融科技规范保持高度一致，并体现了中国标准的系统性和前瞻性。

（1） 风险管理

国际上多强调 AI 系统的风险分级管理和合规性。本标准在优化训练数据、金融大模型、大模型金融应用等关键环节进一步明确了来源选择、准入控制、安全管理及维护具体要求，确保了大模型金融应用全生命周期过程中，具备可控、可信和可追溯的安全合规机制。

（2） 可解释性

本规范基于现有大模型金融应用情况，进一步对大模型输出内容的可解释性提出了具体要求，规定在大模型金融应用准入过程中，需

要对输出内容的可解释性进行合理评估，确保决策过程的透明可信，这与国际先进标准关于可信赖 AI 的要求保持同步。

（3） 系统完整性与前瞻性

在系统构建方面，本标准全面覆盖了“算力－数据－模型－系统－平台－应用”的完整链路，提出了易于理解、具体可操作的技术规范，本标准聚焦于大模型金融应用落地，填补了在大模型金融应用系统构建层面上的技术规范空白，展现了中国在金融科技标准化领域的前瞻性。

四、主要条款的说明以及主要技术指标、参数、试验验证的论述

1. 主要条款说明

本规范主要条款的设计围绕金融业务对大模型应用的专业性、安全性、高性能三个核心需求展开。

基础设施保障（章节 5、6）： 章节 5“资源池要求”针对大模型对异构算力的巨大需求，提出了资源调度和管理要求，是应用得以实施的硬件基石。章节 6“金融优化训练数据要求”强调金融优化训练数据的安全性和质量，提出优化训练数据在内容、数据结构、文件格式、多样性等方面与大模型金融应用处理场景一致等条款，为金融大模型对齐及训练提供基本条件。

模型与系统核心（章节 7、8、9）： 章节 7“金融大模型要求”规定模型须具备金融专业知识、推理计算和复杂任务处理能力，是实现业务智能化的核心。章节 8“系统组件要求”和章节 9“服务平台要求”是本标准的关键创新点，旨在解决大模型在金融应用中存在的“幻觉”和专业性不足问题。这两章要求系统通过构建金融专业知识库（且知识库内容添加前需进行审核）、专业工具集、安全合规工具等核心组件，并通过服务平台进行统一管理和能力封装，以保障应用结果专业性、严谨性和合规性的关键技术路径。

2. 主要技术指标与参数论述

本规范对技术指标和参数的要求，旨在通过量化指标确保大模型金融应用系统的性能、能力和安全性符合行业最高标准。在大模型生成内容准确率方面，提出“应根据金融大模型应用类型建立合理的准入标准，例如分类任务中非资金类大模型金融应用输出内容准确率应大于 90%，资金类大模型金融应用输出准确率应大于 95%”，强调资金类应用场景需要更加可靠的内容输出，以进一步降低应用风险。在系统组件使用方面，提出“知识库的 token 数量不宜超过 10 万”，以降低知识库 token 数量过大对结果检索和使用的影响，在性能指标方面，主要关注用户体验和系统承载能力，包括 TTFT (Time to First Token）（首字符生成时间）和吞吐量（QPS/TPS），以满足金融业务对实时性、高并发、低延迟的极端要求。

3. 试验验证情况分析

本标准的试验验证工作以“符合性验证”为核心原则，确认是否满足本规范规定的各项技术要求。验证内容涵盖本标准规定的七大部分：资源池要求、金融优化训练数据要求、金融大模型要求、系统组件要求、服务平台要求、大模型金融应用要求以及性能处理要求。验证方法将综合采用多种手段，具体包括：自评估、人员访谈、系统测试、查阅材料等，同时，本标准在制定过程中充分征求并吸纳参编机构尤其是金融机构的意见，具备良好的共识基础，具有较强的推广应用前景。

五、是否涉及专利等知识产权问题

大模型金融应用涉及的技术链条极长，从基础架构、模型训练优化算法，到应用层的 RAG（检索增强生成）框架，以及金融知识图谱的构建方法等，均有可能是国内外机构或公司已申请或持有的专利技术。虽然本标准作为技术规范本身不涉及专利，但其指导的实践过程依赖于这些底层技术。依据标准化工作的通用原则，并参照已发布的行业标准，本文件采取以下原则进行处理：本文件不对可能涉及的第三方知识产权做任何声明和担保，本文件的发布机构不承担识别这些专利的责任。 各金融机构在采用本规范时，应自行负责评估和处理其具体技术实现方案可能涉及的专利风险，并确保合规使用。

六、重大意见分歧的处理依据和结果

在标准研制过程中，最重大的“意见分歧”是关于资源池的虚拟化、分级及调度的要求，原因是各金融机构的算力及应用需求情况不一，头部金融机构具有较多算力和异构资源，通过虚拟化和分级调度能够更合理地进行资源分配，优先保障关键核心业务不受影响，但大部分金融机构仍存在算力规模较小，甚至单卡单机的模式，短期内没有虚拟化及分级调度的需求和必要性。最终处理意见是将强制性条款修改为建议性条款，例如将“应建立任务分级机制，以优先保障关键大模型金融应用不受影响”改为“宜建立任务分级机制，以优先保障关键大模型金融应用不受影响”，以进一步加强标准的适宜性。

七、实施地方标准的措施建议

为确保《大模型金融应用技术规范》这一深圳地方标准能够得到有效贯彻和落地，建议采取以下措施：

1. 组织宣贯与专业培训

组织面向全市金融机构、金融科技公司和相关监管机构的专题宣贯会和深度技术培训。重点解读新标准中关于“大模型金融应用系统”的完整架构、系统组件，以及核心性能与安全指标，确保各方对标准内容的准确理解和有效执行。

2. 推动试点与示范项目建设

选取具有代表性的金融机构和应用场景，开展应用试点和示范项目。通过实际应用检验标准的科学性和可行性，并将成功经验和合规实践总结提炼，向全市金融机构推广，形成“AI+金融服务”的标杆示范应用。

3. 建立符合性评估机制

推动标准应用落地后的规范化评估机制，基于标准要求，进一步明确评估方案及符合性判定准则，形成统一共识用于金融机构自评估及第三方测评机构实施测评，在政府采购或大型项目招标中，将“符合本标准”作为优先条件或加分项，形成市场牵引。