

深圳市标准化协会团体标准

《大模型金融应用技术规范》编制说明

一、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。

根据国家市场监督管理总局的统一部署，自 2025 年 7 月起，深圳市停止发布地方标准，2026 年 1 月 22 日经发函与深圳市市场监督管理局沟通确认，《大模型金融应用技术规范》由深圳地方标准项目转为团体标准项目。2026 年 2 月 10 日，经深圳市标准化协会批准，对《大模型金融应用技术规范》团体标准予以立项。

（二）起草单位

深圳国家金融科技测评中心有限公司作为本标准牵头单位，负责标准总体策划、组织协调、技术路线统筹、文本编制和报批材料准备等工作。

深圳市标准化协会作为本标准的发布和归口机构，负责审核团体标准材料、组织征求意见、技术审查、发布等环节工作，进一步保障标准内容质量及流程充分性。

深圳市金融科技协会作为服务数字金融的专业组织，向会员单位征集参编单位，引入多家金融领域机构积极参与标准研制工作。

北京银联金卡科技有限公司、中国平安人寿保险股份有限公司、中国农业发展银行总行、交通银行股份有限公司深圳分行、招商证券股份有限公司、深圳前海微众银行股份有限公司等金融机构及金融科技相关单位，结合银行、证券、保险等场景提供业务需求、应用实践和条款建议。

深圳壹账通智能科技有限公司、山证科技（深圳）有限公司、粤港澳大湾区数字经济研究院、腾讯云计算（北京）有限责任公司单位围绕训练数据、模型能力、系统组件、管控服务平台和应用安全等内容提供技术支撑。

深圳市网安计算机安全检测技术有限公司、北京大成（杭州）律师事务所、中山证券有限责任公司等单位参与标准研讨、意见反馈、条款审核和应用推广建议。

各起草单位组成专项工作组，发挥金融业务、人工智能、网络安全、数据合规、标准化和产业应用等方面优势，共同推进标准编制。

（三）主要起草人

本文件主要起草人包括罗丰、许晋元、董晶、杨波、叶晓聪等人。主要起草人参与了标准需求调研、技术框架设计、资料收集、条款起草、意见处理、专家评审材料准备及报批材料整理等工作。

其中，深圳国家金融科技测评中心有限公司牵头负责标准总体策划、工作组组织协调、标准文本统稿、技术内容把关、征求意见和专家评审意见处理、版本管理及报批材料编制；其他起草单位结合金融业务场景、大模型工程实践、数据安全、网络安全、法律合规、标准化应用等领域经验，参与章节内容编制、技术指标论证、案例和材料提供、修订意见反馈、日常研讨和标准实施建议形成。

二、制定（修订）标准的必要性和意义

近年来，大模型技术在智能客服、智能营销、智能合规、智能信贷、智能投顾、智能理赔等金融业务场景中加速应用，正在推动金融机构业务处理、运营支持、风险识别和客户服务方式发生深刻变化。与此同时，大模型金融应用涉及训练推理资源、金融优化训练数据、模型选型与优化、知识库和工具调用、内容安全、可解释性、运行监控、升级更新等多

个环节，若缺乏统一的技术要求，容易产生数据来源不清、模型输出不可控、业务责任边界不清、生成内容不合规、系统运行不稳定等风险。

制定《大模型金融应用技术规范》，有利于将大模型金融应用从单一模型能力管理扩展到“资源池—数据—模型—组件—平台—应用”的全链路治理，形成面向大模型金融应用设计、开发、部署、运行、管理和评估的系统化技术指导。该标准能够为金融机构开展大模型金融应用提供统一参考，降低中小金融机构技术试错和合规管理成本，促进金融行业在安全、可信、可控的基础上提升智能化服务能力。

深圳具备金融科技产业基础、人工智能应用生态和标准化实践优势，围绕大模型金融应用制定团体标准，能够进一步推动深圳金融科技创新与人工智能治理协同发展，促进金融机构、科技企业、检测认证机构、科研院校和行业组织形成可复制、可推广的技术共识，对提升行业应用质量、保障金融消费者权益和推动相关产业规范发展具有积极意义。

三、主要工作过程

（一）深圳地方标准立项论证与筹备阶段（2024年1月至2024年4月）

本阶段核心任务是完成标准的前期论证与立项程序。2024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

限公司等单位专家成立标准预研组，基于各机构前期研究和调研成果，开展大模型金融应用标准需求分析。基于分析结果，编制组于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。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》作为深圳市地方标准予以立项。

（二）起草工作组组建与标准草案研制阶段（2024年4月至2025年1月）

标准立项后，在深圳国家金融科技测评中心有限公司组织协调下，编制组启动参编单位组建和任务分工工作，邀请人工智能、金融业务、数据安全、网络安全和标准化领域专家共同参与起草，形成标准起草工作组。工作组在前期调研基础上，围绕大模型的通用能力、金融知识能力、安全合规和性能效率等内容开展草案研制，形成《大模型金融应用技术规范》（草案稿）。

2025年初，以DeepSeek为代表的新一代大模型技术取得突破性进展，并在金融行业催生大量实质性、系统化应用案例。工作组经内部论证认为，产业关注重点已由单一“模型能力”拓展至“大模型金融应用”的系统构建与治理，原草案在规范对象、覆盖范围和前瞻性方面需要调整。为此，

工作组将核心规范对象由“金融大模型”调整为“大模型金融应用”，以更好支撑金融机构在设计、开发、部署、运行、管理和评估过程中的安全合规与应用治理需求。

（三）标准重构与征求意见稿形成阶段（2025 年 2 月至 2025 年 8 月）

为提升标准内容的前瞻性、行业代表性和落地可行性，工作组在标准重构阶段进一步扩大参编单位范围，于 2025 年 3 月和 5 月通过公开渠道发布参编单位征集通知，并依据产业代表性、技术实力和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金融机构、科技企业、检测认证机构、法律服务机构、科研院校和行业组织等多类主体。

在新一届工作组框架下，编制组围绕大模型金融应用技术框架重新组织标准内容，形成覆盖资源池、金融优化训练数据、金融应用大模型、系统组件、管控服务平台和大模型金融应用等环节的技术要求。深圳国家金融科技测评中心有限公司牵头组织多轮研讨、实地调研、意见征集和文本修订，邀请行业专家、典型金融机构和科技企业对技术内容开展集中评议，最终形成《大模型金融应用技术规范（征求意见稿）》。

（四）公开征求意见阶段（2025 年 11 月至 2025 年 12 月）

2025 年 11 月至 2025 年 12 月，深圳国家金融科技测评中心有限公司面向社会公开征求意见，共收到 4 条反馈意见。

标准工作组对反馈意见逐条研究处理，采纳 3 条，未采纳 1 条，并根据处理结果对标准文本进行修改完善。

（五）地方标准转团体标准立项阶段（2026 年 1 月至 2026 年 2 月）

根据国家市场监督管理总局统一部署，自 2025 年 7 月起，深圳市停止发布地方标准。2026 年 1 月 22 日，经深圳国家金融科技测评中心有限公司提出申请并与深圳市市场监督管理局沟通确认，《大模型金融应用技术规范》由深圳地方标准项目转为团体标准项目。2026 年 2 月 10 日，经深圳市标准化协会批准，《大模型金融应用技术规范》团体标准予以立项。

（六）团体标准公开征求意见与送审稿形成阶段（2026 年 2 月至 2026 年 4 月）

2026 年 2 月 12 日至 2026 年 3 月 14 日，深圳市标准化协会向社会公开征求意见。标准工作组基于反馈意见对标准范围、章节结构、术语定义、引用文件、技术要求和表述规范性等内容进行修订完善，形成《大模型金融应用技术规范（送审稿）》及配套送审材料。

（七）专家评审及报批稿形成阶段（2026 年 4 月至 2026 年 6 月）

2026 年 4 月 30 日，深圳市标准化协会组织召开团体标准专家评审会，评审专家对标准送审稿、编制说明及配套材

料进行了审查。专家认为编制组提交的文档规范、齐全，符合评审要求，标准的编制是必要和及时的，并围绕规范性引用文件、章节合并、术语定义、数据和模型要求、知识库与风险验证库、智能体安全管理、处理性能指标及全文表述规范性等方面提出修改意见。标准工作组会后逐条研究处理，形成《专家评审意见汇总处理表》，共处理 49 条意见，其中 43 条采纳、6 条未采纳；未采纳意见均在备注中说明理由。

根据专家评审意见处理结果，标准工作组对标准文本进行了系统修改：新增第 5 章“技术框架”，删除与核心技术要素关联度较低的附录 A，将“大模型金融应用处理性能要求”合并至第 11 章，调整“服务平台要求”为“管控服务平台要求”，补充缩略语和参考文献，规范“金融应用大模型”“金融大模型”等术语，完善数据、模型、系统组件、管控服务平台、应用准入、安全管理、运行监控和性能评估等要求，并同步修改编制说明，形成报批稿。

四、标准原则/依据和主要内容

（一）标准原则

1. 科学性原则

本标准在编制过程中，首先坚持科学性原则。在方法论层面，本文件严格按照 GB/T 1.1—2020《标准化工作导则》的要求进行编制，确保标准整体结构规范、逻辑严谨、表达清晰。在内容依据方面，标准充分结合国家政策法规与已有

国家标准体系，例如个人信息保护规范、生成式人工智能安全要求以及金融领域相关标准，确保技术要求来源可靠、体系完整。

2. 实用性原则

在实用性方面，本标准紧密围绕金融机构实际应用需求展开。首先，在规范对象上，从传统的“模型能力”转向“大模型金融应用系统”，使标准直接服务于应用落地，而非停留在模型层面。

其次，在内容覆盖上，本标准覆盖了从资源池、训练数据、模型能力，到系统组件、管控服务平台及应用的完整链路，能够支撑金融机构从建设到部署再到运维的全过程，并且结合了头部金融机构及互联网厂商的实际工程经验。

3. 先进性原则

在先进性方面，本标准在理念和技术要求上均对标国际先进水平。

在治理理念上，标准强调风险分级管理、安全可控以及合规性要求，在数据、模型及应用各环节明确提出来源控制、准入机制以及安全管理要求，与国际 AI 治理框架保持一致。

在技术体系上，本标准不仅关注模型能力，更聚焦应用系统构建，涵盖“算力—数据—模型—系统—平台—应用”的全链路架构，强调系统工程在实际应用中的作用。

（二）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》。

（三）标准主要内容

1. 主要条款说明

本文件规定了大模型金融应用的资源池要求、金融优化训练数据要求、金融应用大模型要求、系统组件要求、管控服务平台要求和大模型金融应用要求，适用于开展大模型金融应用活动、利用大模型处理金融业务的金融机构，为大模型金融应用的设计、开发、部署、运行、管理和评估提供技术指导。

标准正文共设置 11 章。第 1 章明确标准适用范围；第 2 章列明规范性引用文件；第 3 章界定大模型训练推理资源、金融优化训练数据、生成合成数据、准入控制、金融应用大模型、基础大模型、金融大模型、人工智能体、关键词库、安全风险验证库等术语；第 4 章规定 RDMA、API、MCP、TTFT、TPOT、E2E Latency、QPS、TPS 等缩略语；第 5 章新增大模型金融应用技术框架，说明资源池、金融优化训练数据、金融应用大模型、系统组件、管控服务平台和大模型金融应用之间的关系；第 6 章规定资源池要求，包括大模型训练推理资源、资源虚拟化和调度策略要求；第 7 章规定金融优化训

练数据要求，包括通用要求、来源要求、准入控制和维护要求；第 8 章规定金融应用大模型要求，包括基础大模型选择、金融大模型优化、金融大模型安全管理、部署运行和升级更新要求；第 9 章规定系统组件要求，包括接口协议、知识库、标识工具、关键词库、安全风险验证库、沙箱、记忆系统、编排工具、推理引擎等要求；第 10 章规定管控服务平台要求，包括平台功能和安全管理要求；第 11 章规定大模型金融应用要求，包括准入控制、安全管理、运行、升级更新和处理性能要求。

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“应根据大模型金融应用类型建立合理的准入基准，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。在大模型金融应用评价指标方面，提出“应根据大模型金融应用类型使用合理的评价指标，通过多个指标进行综合分析以发现金融应用处理缺陷，例如分类任务指标可包括准确率、召回率、精确率、F1 分值等”，以避免单一指标造成的评价不充分。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、TPOT、E2E Latency、吞吐量（QPS/TPS）等指标，以满足金融业务对实时性、高并发、低延迟的极端要求。

五、产业化情况和预期的经济效果

《大模型金融应用技术规范》以大模型金融应用为对象，对资源池、金融优化训练数据、金融应用大模型、系统组件、管控服务平台以及大模型金融应用提出核心技术要求，能够为金融机构构建安全、可信、可控的大模型金融应用提供标准化路径。标准实施后，有助于金融机构提升智能客服、智能营销、智能合规、智能信贷、智能投顾、智能理赔等场景的建设效率和治理水平，强化数据安全、模型安全、内容安全、运行稳定性和合规管理能力，降低行业特别是中小金融机构应用大模型技术的试错成本和安全风险。

从产业化角度看，本标准有利于促进金融机构、金融科技企业、模型服务商、系统集成商、检测认证机构和科研院所围绕统一技术要求开展产品研发、系统建设、符合性评估和应用推广，推动形成大模型金融应用的工具、平台、评测和服务生态。标准立足深圳金融与人工智能深度融合的产业优势，对深圳在人工智能治理和金融科技创新交叉领域先行先试、形成可复制推广的行业经验具有积极作用。

六、国内外相关研究依据、技术标准

（一）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

标准对标情况：

现有国内相关标准多数以模型能力、应用安全或评测方法为重点，本标准聚焦大模型金融应用，覆盖资源池、金融优化训练数据、金融应用大模型、系统组件、管控服务平台和大模型金融应用等核心环节，并通过新增技术框架章节说明各环节之间的关系。与现有标准相比，本标准更强调系统工程和全生命周期治理，突出知识库、标识工具、关键词库、安全风险验证库、沙箱、记忆系统、编排工具、推理引擎以及管控服务平台等支撑能力，对金融机构落地建设具有较强补充作用。

（二）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，与国际人工智能治理和金融科技规范强调的风险管理、透明可信、安全可控、持续监测等要求保持一致，并结合我国生成式人工智能治理和金融行业监管要求形成适用于金融机构落地实施的技术规范。

1. 风险管理

本标准在金融优化训练数据、金融应用大模型、系统组件、管控服务平台和大模型金融应用等关键环节提出来源控制、准入控制、安全管理、维护更新和监控记录要求，确保大模型金融应用具备可控、可信、可追溯的治理机制。

2. 可解释性和可信应用方面

在可解释性和可信应用方面，本标准要求在大模型金融应用准入过程中对输出内容准确性、可解释性、安全性和处理性能进行评估，并对输入内容审查、输出内容使用、输出内容监控和人工智能体安全管理提出要求，体现了可信人工智能在金融业务场景中的应用要求。

3. 系统完整性与前瞻性

在系统完整性与前瞻性方面，本标准全面覆盖“资源池—数据—模型—组件—平台—应用”的完整链路，提出便于理解和实施的技术要求，填补了大模型金融应用系统构建和治理层面的标准化空白。

七、重大意见分歧的处理依据和结果

标准研制过程中未出现无法协调的重大意见分歧。对公开征求意见和专家评审意见，标准工作组均按照“逐条研究、充分论证、协调一致、说明理由”的原则进行处理。专家评审阶段共形成 49 条处理意见，其中 43 条采纳、6 条未采纳；未采纳意见主要涉及人工智能体定义是否调整、准确率评估方法是否在本标准中展开、处理性能是否设置统一最低阈值、基础大模型选择准确率与应用准确率的区别、公正性是否另设条款、大模型是否按参数量划定边界等内容。

对未采纳意见，工作组结合现行国家标准、行业共识和金融机构应用差异进行了说明：人工智能体定义与相关国家标准计划征求意见稿保持一致；准确率评估方法和性能阈值受金融机构业务类型、算力条件、模型能力和应用场景影响较大，不宜在本标准中设置统一公式或最低值；输出内容可解释性评估中已包含决策公平性解释要求；现行国家标准和行业标 准尚未按参数量明确大模型边界。上述处理结果已在《专家评审意见汇总处理表》中列明，标准文本也已根据采纳意见完成相应修改。

八、贯彻深标协标准的要求和措施建议

为确保《大模型金融应用技术规范》得到有效贯彻和落地，建议采取以下措施。

（一）组织宣贯与专业培训

面向金融机构、金融科技企业、模型服务商、系统集成

商、检测认证机构和相关行业组织开展专题宣贯和技术培训，重点解读标准中的技术框架、资源池、金融优化训练数据、金融应用大模型、系统组件、管控服务平台、大模型金融应用准入控制、安全管理、运行监控和处理性能要求，帮助相关主体准确理解和执行标准。

（二）推动试点与示范应用

选取具有代表性的金融机构和业务场景开展标准应用试点，围绕智能客服、智能合规、智能信贷、智能投顾、智能理赔等场景验证标准的科学性、适用性和可操作性，形成可复制、可推广的建设方案、管理流程和符合性案例，带动行业规范应用。

（三）建立符合性评估和持续改进机制

推动建立标准实施后的符合性评估机制，围绕标准要求进一步明确评估方案、测试指标、证据材料和判定准则，为金融机构自评估、第三方测评和项目验收提供依据。根据大模型技术发展、金融监管要求和应用实践变化，持续收集标准实施反馈，适时开展标准复审和修订。

九、其他应予说明的事项

无。