

ICS 点击此处添加 ICS 号

CCS 点击此处添加 CCS 号

团 体 标 准

T/QGCML XXXX—XXXX

金融行业智能体设计规范

Design Specification for Intelligent Agents in the Financial Industry

XXXX – XX – XX 发布

XXXX – XX – XX 实施

全国城市工业品贸易中心联合会 发 布

前 言

本文件按照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》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由 提出。

本文件由全国城市工业品贸易中心联合会归口。

本文件主要起草单位：

本文件主要起草人：

金融行业智能体设计规范

1 范围

本规范适用于金融行业智能体的设计、开发、部署及运维，涵盖智能客服、智能投顾、智能风控、智能合规等应用场景，确保智能体在业务场景中的高效性、安全性及合规性。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 35273-2020 《信息安全技术 个人信息安全规范》
JR/T 0171-2020 《个人金融信息保护技术规范》
ISO/IEC 27001:2013 《信息技术 安全技术 信息安全管理体系要求》

3 术语和定义

本文件没有需要界定的术语和定义。

3.1

金融智能体

基于人工智能技术，具备环境感知、策略生成、自我校验及人机协作能力的自动化决策系统。

3.2

分层架构

将智能体系统分为基础工作流层与动态智能体层，实现风险隔离与效能提升。

3.3

认知降维

将复杂业务逻辑封装为功能明确、接口简洁的“认知单元”，降低智能体决策难度。

3.4

可解释性

智能体输出附带可读的决策依据，支持人类监督与审计。

4 设计原则

1. 架构分层

基础工作流层：固化高频、高确定性的操作，如支付清算中的账务核对、风控系统中的黑名单筛查。

动态智能体层：处理需要灵活响应的场景，如财富管理中的个性化方案生成、信贷审批中的风险评估。

关键节点：在动态智能体层设置人工确认机制，确保重要决策的人为把控。

2. 工具生态

认知降维设计：将复杂业务拆解为独立工具，每个工具仅暴露必要参数，并嵌入业务规则的自然语言解释。

自解释性输出：工具输出附带决策依据，如风险评估工具标注影响评分的关键因子（如近期交易频率异常、资产负债比波动）。

3. 成本效能

价值密度优先：深耕细分场景，建立可复用的能力模块，避免追求“全能型”系统。

认知成本纳入评估：包括错误决策的修正成本、过度自动化导致的客户信任损耗、系统黑箱引发的监管沟通成本等隐性指标。

技术投资回报率（TI-ROI）模型：包含直接成本（算力、开发投入）、风险成本（错误率×总操作次数×单次错误损失）、机会成本（资源错配导致的业务损失）。

5 功能要求

1. 环境感知

实时数据采集：从金融机构内外部获取与业务相关的数据，包括客户信息、交易记录、市场数据等。

监管文件解析：自动捕捉监管文件的关键变更，及时调整业务策略以确保合规运营。

2. 策略生成

个性化方案生成：根据客户风险偏好、资产状况和市场趋势，动态调整投资组合或信贷方案。

风险评估与预警：建立风险评估模型，对客户信用风险、市场风险、操作风险等进行评估，并实时预警潜在风险。

3. 自我校验

多维度合规检查：在执行交易前自动触发合规检查，确保交易的合法性和安全性。

决策质量评估：定期评估智能体输出的质量，根据反馈进行改进。

6 安全与合规

1. 数据安全

数据加密：对敏感数据进行加密处理，确保数据在传输和存储过程中的安全性。

访问控制：实施严格的访问控制策略，确保只有授权人员能够访问敏感数据。

2. 系统安全

抗攻击能力：具备较强的抗攻击能力，防止恶意攻击导致的数据泄露或系统瘫痪。

安全审计：从数据输入到决策输出的全链路留痕，捕获决策过程中的关键推理节点，满足监管审计要求。

3. 合规性

监管政策应对：建立合规性检查机制，确保智能体系统符合金融监管要求。

合规性评估：定期对智能体系统进行合规性评估，及时发现并整改合规问题。

7 运维与优化

1. 运维工具

自动化运维：构建完备的端到端的自动化ITOM运维工具体系，提高运维效率。

监控与预警：实时监控智能体系统的运行状态，及时发现并处理异常情况。

2. 持续优化

模型迭代：定期评估智能体模型的性能，根据业务需求和数据变化进行模型迭代和优化。

反馈机制：建立用户反馈机制，收集用户对智能体系统的意见和建议，持续改进系统性能。