教育数据不出域的智能治理框架与跨域流通应用实证研究

罗屿冰
上海市大数据中心，上海 200003

摘要
针对敏感数据在一体化市场中的跨域流通与安全平衡难题，推导出一套通用的“双重跨域”治理模式，并在教育数据上开展实证研究。首先，在项目间维度上，设计基于LLM与few-shot提示工程的动态审计模块，通过对技术文档的智能化分析，实现治理经验与合规逻辑的跨项目复用，确保原始隐私文档不出域。其次，在项目内维度上，构建“信任、能力、效能”递进式指标体系，量化评估多主体间的数据配置效率与安全水平。实证结果显示，提出的教育数据治理框架能有效识别项目全生命周期中的合规风险点，显著提升治理效能。该框架为敏感数据跨域流通提供了“经验可复用、数据不出域”的智能化监管路径。

关键词
全国一体化数据市场；数据跨域流通；数据不出域；大语言模型；TCE评价模型

中图分类号：G434 文献标志码：A doi：10.11959/j. issn. 2096-0271.2026057

Intelligent governance framework and empirical research on educational data: balancing cross-domain circulation and on-premise security

Luo Yubing
Shanghai Municipal Big Data Center, Shanghai 200003, China

Abstract
To address the dilemma of balancing cross-domain circulation and security protection for sensitive educational data within an integrated data market, this paper proposes an intelligent governance framework characterized by a "dual-domain" perspective. First, on an inter-project dimension, an innovative dynamic auditing module based on large language model (LLM) and few-shot prompt engineering is designed. By performing intelligent analysis of technical documentation, the module enables the cross-project reuse of governance experience and compliance logic, ensuring that original privacy documents remain within their respective domains. Second, on an intra-project dimension, a progressive "trust, capability, and effectiveness" (TCE) indicator system is constructed to quantitatively evaluate data allocation efficiency and security levels among multiple stakeholders. Empirical results demonstrate that the framework effectively identifies compliance risks throughout the project lifecycle and significantly enhances governance

performance. This framework provides a deployable, intelligent regulatory pathway for the cross-domain circulation of sensitive data, achieving the goal of "reusable experience with data remaining on-premise".

Key words
national integrated data market, cross-domain data circulation, data on-premise, large language model, TCE evaluation model

0 引言

全国一体化数据市场的培育与建设，要求数据要素实现“供得出、流得动、用得好、保安全”的目标[1-2]。然而，作为涉及公共利益与个人隐私的典型敏感要素，教育数据面临更独特的治理挑战：其涉及大量未成年人敏感信息，受《中华人民共和国未成年人保护法》与《中华人民共和国个人信息保护法》的双重严格约束；数据的使用目的高度依赖于具体的教学与管理情境，合法利用的边界极易模糊。因此，教育数据的流通必须严格遵循“可用不可见”的原则，确保“数据不出域”[3-5]。因此，如何在全国一体化数据市场中平衡好“数据跨域流通”的效率要求与“数据不出域”的安全要求，是当前数据治理面临的重要挑战。

现有实践揭示出两个治理缺口。①治理经验的跨项目复用缺口。传统的项目管理经验（沉淀在需求、设计、运维等文档中）因涉及敏感数据逻辑，难以在不同的教育信息化项目（如项目A到项目B）之间被安全、高效地复用。这种项目评审经验“不出域”的困境导致评审经验无法复用，项目启动和合规审查成本居高不下。例如，在某教育协同项目中，由于缺乏统一可复用的治理机制，高校与外部机构的跨域协作的合规审查耗时近数月，不仅效率低下，还存在人工审核误判、敏感隐私数据越权访问等风险隐患。②项目内流通与安全评估缺口。由于缺乏动态、量化的微观治理工具与评价体系，单个复杂项目（如跨学校、跨部门项目）的数据流通利用水平及隐私保护水平难以被有效评估，数据要素价值难以被充分释放。

近年来，大语言模型（large language model，LLM）在自然语言处理领域的突破，为解决上述难题提供了新机遇。LLM通过少样本（few-shot）学习机制[6]从少数专家样本中泛化出审计能力，从而实现对非结构化文档的自动化跟踪与风险识别[7-8]。这为在数据不出域的前提下实现治理逻辑的跨项目流通提供了技术支撑。

本文从理论层面提炼了通用的双重跨域治理模式，即横向的治理逻辑跨域与纵向的数据流转跨域，构建了兼顾经验复用与合规评价的智能化治理范式，并在教育数据上进行了实证研究。

（1）管理经验的跨项目智能化复用（项目间维度）。针对不同教育信息化项目间隐私壁垒导致的治理经验“孤岛”问题，本文提出了基于本地化LLM的动态审计技术。该技术不触碰项目底层原始数据，仅通过对技术文档语义逻辑的few-shot学习，实现审计专家能力在异质化项目间的低成本迁移，达成“治理逻辑跨域、隐私数据不出域”的目标。

（2）数据流通效能的多维量化评估

（项目内维度）。针对单一项目内跨学校、跨单位数据交互的复杂性，本文创新地构建了“信任、能力、效能”（trust，capability，and effectiveness，TCE）评价模型。该模型填补了传统治理缺乏微观评价工具的空白，能够有效测算项目内各主体间数据流通的合规水平与价值创造效能，为项目优化提供精准指引。本文的贡献在于突破了传统安全治理中物理隔离即安全的逻辑，提出了一种“逻辑可通、物理隔离”的解耦范式，通过LLM的语义解析能力，将抽象的合规制度转化为项目级的执行逻辑，填补了宏观数据法规与信息化项目执行之间的技术验证空白。

1 相关研究

1.1 全国一体化数据市场下的数据跨域流通与安全博弈

全国一体化数据市场的核心在于实现数据要素在全国范围内的自由流动与高效配置[1-2]。然而，作为涉及公共利益与个人隐私的高敏感要素，教育数据的流通陷入典型的安全与价值对立悖论：一方面，实现教育现代化需要跨地区、跨部门的数据流通；另一方面，法律合规性要求数据的使用必须坚持隐私数据不出域[3-5]。现有的《关于构建数据基础制度更好发挥数据要素作用的意见》及其“三权分置”框架提供了制度保障，并且文献[9]基于保护动机理论对我国数据流通趋势的分析指出，相关机制与合规要求正在逐步完善。但在执行层面，缺乏一种能在隐私数据不出域前提下验证跨域过程合规的智能化手段，这导致市场主体因担忧安全风险而产生“不敢转”现象。这种智能化手段的缺乏成为一体化市场建设的瓶颈。

1.2 治理范式的演进：从静态指标到项目级微观智能化治理

传统的项目治理理论（如PMBOK或敏捷治理）侧重于任务的完成，而非数据要素价值的合规流转。在一体化市场建设的“五统一”要求下，治理范式正经历从人工审计向智能化协同监管的演进历程。有研究指出，数据跨域流通的信任基础不仅依赖于隐私计算等底层技术，还依赖于对流通逻辑（即技术文档、业务规则）的实时审计。文献[10]提出数据社会化视角下的“五位一体”安全治理框架，强调了多维度的安全管控机制。然而，由于教育数据具有多主体参与（如教育主管部门、学校、劳动力市场等）、长周期流转以及教学/管理双用途高度交织的生命周期特征，传统的静态指标评价（如DCMM）难以捕捉数据在跨主体、长周期动态流通中的合规演化与用途变异，因此亟须引入能高效处理合规证据的智能化框架[11-12]。为解决传统的宏观监管面临的“看得见管不到”困境，数据要素的合规流通应以单个信息化项目为微观治理单元，通过对项目全过程文档的逻辑对齐，确保宏观安全红线在微观执行层面不走样。

1.3 LLM在流通与安全平衡中的技术耦合性

LLM为解决数据跨域流通与不出域安全的矛盾提供了新路径。在一体化市场中，监管需要极强的规则对齐能力。LLM通过few-shot学习将复杂的行业合规标准转化为自动化的审计逻辑。近期研究也开始探索大模型在强合规领域的自动化应用，文献[9]验证了LLM在金融审计中进行自动化监管合规审查的有效性。LLM部署在数据流出的边缘侧（不出域本地化部署），却能

通过语义比对确保数据用途符合跨域协议要求，从而成为平衡数据要素的跨域流通效率与不出域安全红线的关键技术支点[13-14]。

2 教育数据不出域智能治理框架与评价模型构建

本文构建的“双重跨域”模式是一种高敏感数据（如教育、医疗、人社数据等）在全国统一大市场中流通的理论范式。理论上，数据要素流通过程伴随着物理边界安全与逻辑流通需求之间的内生博弈。针对这一矛盾，本文将其解耦为两个跨域维度。

（1）治理逻辑的横向跨域（项目间维度），提炼为知识提取+逻辑复用理论范式。针对不同建设主体间的经验孤岛与隐私壁垒，该模式利用智能化手段（如LLM）将包含敏感信息的非结构化技术文档抽象为通用的合规特征与管控规则，实现了实体原始数据物理不出域、治理经验与逻辑全网跨域。

（2）数据流转的纵向跨域（项目内维度），提炼为“信任、能力、效能”博弈理论范式。在单一复杂业务链（如跨部门协同）中，将信任底座、技术支撑能力与最终流通价值进行量化解耦。

这种通用的双重跨域模式突破了传统安全治理中网络物理跨域即风险的观念，将治理逻辑的可信跨域作为前提，为各垂直行业敏感数据在一体化市场中的审查与流转提供了普适性的底层理论架构。

2.1 整体治理框架设计

针对教育数据要素流通中存在的隐私敏感度高、多主体利益博弈复杂以及全生命周期文档监管缺失等问题，本文提出了一种新型治理框架（如**图1**所示）。该框架的核心在于从两个维度进行治理：一是“横向复用维”，即利用基于LLM的智能文档审计方案（intelligent document auditing module，IDAM）捕捉不同项目（如A校与管理机构所属的不同平台系统）在全生命周期中产生的文档知识，实现审计能力的跨项目沉淀；二是“纵向评价维”，即利用TCE评价模型对当前项目内部各参与主体间的数据流转进行实时测算。该框架将两者结合，构成了工具赋能治理、指标衡量成效的闭环。

在该框架中，隐私文档被严格界定为非结构化技术文档（如数据库设计说明书、API接口规范、核心脱敏规则文档等），包含教育领域敏感数据结构、表设计、接口权限、用户真实数据样例以及跨系统数据流转的具体技术细节。针对此类文档，本文设计的“不出域”治理策略遵循安全与效能平衡的原则，既确保原始隐私文档物理不出域，又保障合规审查逻辑能够跨域流通，具体体现在：①物理环境隔离，所有隐私文档的向量化存储与LLM推理过程均严格限制在项目所在的安全内网（域内）进行本地化部署，阻隔与外部公网连接；②治理逻辑流通，跨域共享与复用的并非文档原文数据，而是经过本地LLM脱敏和抽象化后的合规判定逻辑与风险特征模型。

其中，TCE评价模型将教育数据流通项目管理视为一个动态的反馈闭环，如**图2**所示，信任底座层负责守住隐私数据不出域的底线，能力支撑层负责提升流通的上限，而效能应用层则是两者博弈后的最优解。**图2**还阐述了TCE评价模型与IDAM之间的关系，前者为后者提供结果反馈与案例补充，后者利用前者信息对项目进行全生命周期动态审计。

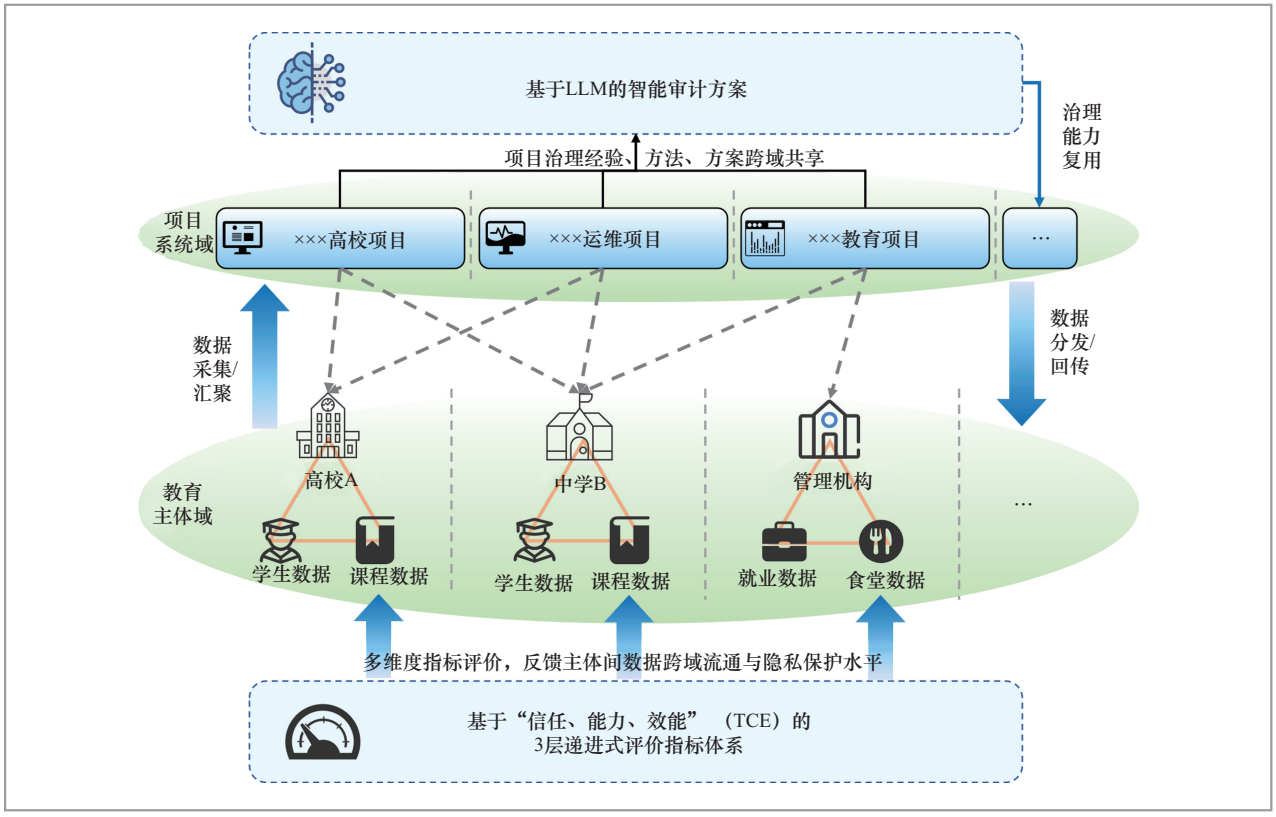

图1 整体治理框架

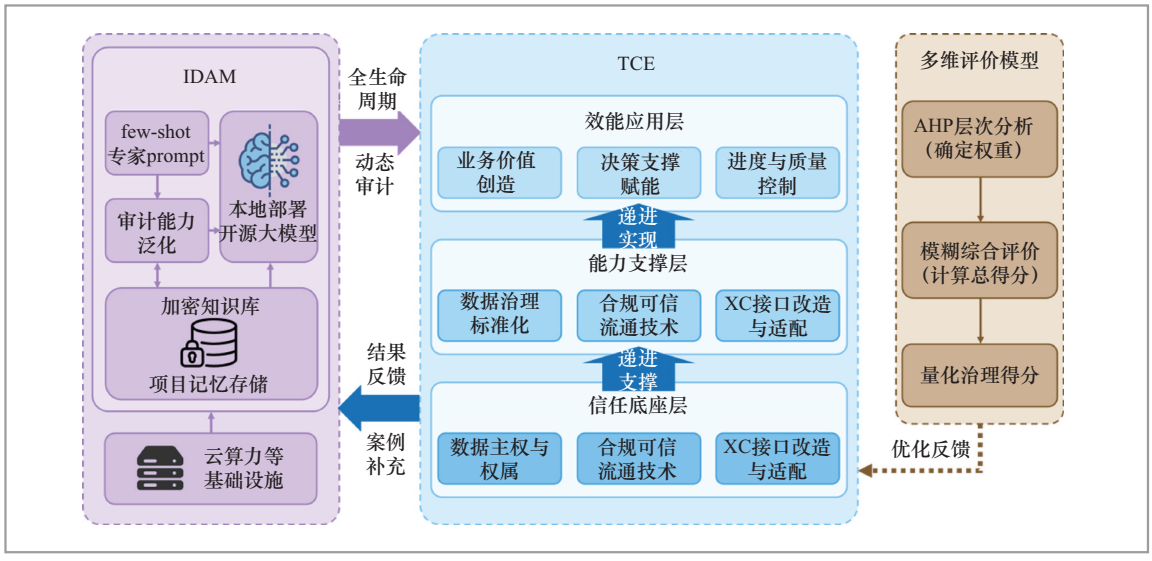

图2 TCE评价模型与IDAM的协同机制

2.2 基于TCE的评价模型

TCE模型包含3个层级：①信任底座层，解决“敢不敢流”的问题，通过隐私计算与权属界定，守住隐私数据不出域的底线；②能力支撑层，解决“能不能流”

的问题，侧重标准统一与信创适配，确保跨域协作的技术兼容性；③效能应用层，解决“流得好不好”的问题，关注业务价值创造与决策支持的量化反馈。

相较于传统项目管理核心指标，本文系统性地在TCE模型中融入了反映智能化治理水平的评价因子，提出了五维评价指标体系（见**表1**）。针对项目文档的全生命周期管理，五维评价指标体系增加了“文档一致性覆盖率”与“审计自动化率”等关键指标。

层次分析法（analytic hierarchy process，AHP）确定权重：构建判断矩阵$\boldsymbol{P}$衡量各维度间的相对重要性，其中n为判断矩阵的阶数。

$$\boldsymbol{P}=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \quad (1)$$

判断矩阵的构建基于德尔菲法，邀请了多位来自教育行政管理部门、大数据中心监管方及信息化项目管理的资深专家，采用1–9标度法对**表1**中的五维评价指标进行成对重要性比较打分。专家组一致认为数据治理能力、可信流通支撑、合规安全保障、项目实施效果与价值创造效益在一体化市场建设中相互制约且同等重要。汇聚专家打分构建判断矩阵$\boldsymbol{P}$，计算特征向量得到各指标的归一化权重$\boldsymbol{W}$并进行一致性检验。若一致性比率$CR<0.1$，则满足一致性要求，说明权重设定具有科学性与合理性。

模糊综合评价法计算总得分：针对评价过程中的主观性，定义评价向量$\boldsymbol{R}_i$。设评语集为$V=\{v_1,v_2,v_3,v_4,v_5\}$（即优、良、中、可、差）。将专家打分与LLM预审得分进行加权融合，得到模糊关系矩阵$\boldsymbol{R}$。最终综合评价结果$\boldsymbol{S}$为：

$$\boldsymbol{S}=\boldsymbol{W}\cdot\boldsymbol{R}=\left(w_1,w_2,\cdots,w_n\right)\cdot\begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nm} \end{pmatrix} \quad (2)$$

表1 五维评价指标体系

治理维度	二级指标	指标说明	权重分配建议
数据治理能力	一数一源落实率	消除重复数据源的核心字段占比	0.12
	数据标准覆盖率	符合教育行业标准的数据元占比	0.08
可信流通支撑	隐私计算应用率	采用安全多方计算/沙箱环境的场景占比	0.10
	信创适配度	系统核心组件国产化部署比例	0.10
合规安全保障	审计自动化率	利用LLM等手段实现的自动化技术文档质量及数据流通合规性检查评分	0.11
	授权管理完备度	基于角色的访问控制(role-based access control,RBAC)/基于属性的访问控制(attribute-based access control,ABAC)动态权限配置的覆盖度	0.09
项目实施效果	文档一致性覆盖率	在启动、中期、结项文档中需求覆盖与修正的一致性	0.15
	进度控制偏差率	实际工期与计划工期的偏离程度	0.05
价值创造效益	决策效率提升度	数据流通前后报表生成周期的缩减效率	0.10
	跨部门业务协同率	支撑跨校、跨部门协同业务的成效	0.10

其中，n和m分别代表评价指标（维度/因素）的总数量及评语集（评价等级）的总数量。

得到综合评价结果$\boldsymbol{S}$后，再通过去模糊化处理（如最大隶属度法或加权平均法），得出项目治理水平的最终量化得分。

2.3 基于LLM的智能审计方案

在传统教育数据项目管理中，技术文档（如需求、设计、运维文档等）的审计过度依赖人工专家，存在主观性强、跨阶段追溯难等问题。本文提出基于LLM的智能审计方案IDAM，借助LLM的长文本处理与逻辑推理能力，从微观治理视角实现数据不出域与跨域流通的动态平衡。

IDAM模块采用“本地化部署+知识增强存储”的架构设计：①在风险隔离层，为实现数据不出域的流通目标，LLM采用本地化、沙箱化部署模式，切断外部公网调用，确保数据使用环境（如开源的Llama-3或Qwen系列的本地推理版本）安全；②在加密记忆模块中，项目的历史文档通过向量化处理存储在本地向量数据库中，确保了知识资产的安全性。

2.3.1 全生命周期动态审计机制

动态审计的核心在于其随项目全生命周期（立项、开发、测试、运维等）的演进而持续迭代。不同于传统的期末一次性静态合规检查，IDAM模块通过监测项目管理系统或代码仓库的文档更新状态，以事件驱动或人工干预的方式实时触发审计任务。模型会根据项目当前所处阶段的特征，动态组装上下文提示词与审查基线，实现对数据流转风险的早期预警。IDAM基于长文本理解能力实现了从项目立项、开发到验收的纵向追踪：①一致性回溯审计，自动对比《中期检查报告》中提出的整改意见与《结项验收申请书》中的实际修订内容，识别遗漏风险；②需求覆盖度计算，基于提示词工程提取《需求规格说明书》中的核心功能点，并与《测试用例》及《运维手册》进行匹配，计算需求覆盖度。

$$R_{\mathrm{cov}}=\sum_{i=1}^{n}S\left(D_i,E_i\right)/n,\ S\left(D_i,E_i\right)\in[0,1]\quad(3)$$

其中，n为合规需求总数，$S\left(D_i,E_i\right)$为经LLM语义比对后的需求D_i与实施证据E_i的一致性得分。

为了实现式（3）的自动化求解，本文设计了结构化的Prompt模板（如**图3**、**图4**所示）。该模板强制LLM输出标准化的JSON数据结构，将非结构化的自然语言文本转化为计算机可处理的逻辑布尔值（即结构化输出中的risk_flag）。其中，字段alignment_score直接映射为式（3）中的参数$S\left(D_i,E_i\right)$。通过Python脚本批量调用该Prompt模板，系统能够实时计算当前项目阶段的文档一致性覆盖率，并将risk_flag为true的条目自动推送到风险预警看板，实现了从“定性文本审计”到“定量指数评估”的范式转变。

本文的Prompt设计遵循“角色、任务、输入、约束”结构化框架。首先，设定大模型为数据要素监管专家以激发其专业领域的先验知识；其次，明确进行跨域合规性比对的核心任务；再次，提供标准化的需求与证据片段作为分析的上下文；最后，严格定义数据不出域的判定底线与规范的JSON输出格式。

为验证该Prompt设计方法的有效性，本文对比了无约束基础提示与本文设计的结构化少样本提示在审计任务中的差异。实验观察表明，基础提示往往产生冗长且缺乏确定性的定性描述，难

```
# Role & Task
你作为数据要素监管专家，负责审计“全国一体化数据市场”下的教育数据合规性。请对比【需求】与【证据】，判定方案是否在跨域应用的同时，严守“数据不出域”底线。
# Input Data
[需求]: REQ-085: 跨部门精准资助业务，要求原始数据严禁出域，必须采用隐私计算（可用不可见）。
[证据]: 接口文档显示采用 HTTPS 加密传输密文包，但目标端（民政）拥有私钥并解密还原明文。
# Constraints
核心逻辑：传输加密不等于数据不出域。若原始数据在接收方解密复现，即视为“违规出域”。
审计标准：必须满足隐私计算范式。若不达标，得分直接为 0。
```

图3 基于LLM技术文档审计的结构化Prompt模板示例

```
{
  "analysis": "合规要求采用隐私计算实现‘可用不可见’，但实施证据表明数据在目标端解密复现，本质为‘明文出域’。HTTPS 加密仅保障传输安全，未满足数据不出域的管控要求，存在严重合规风险。",
  "alignment_score": 0,
  "risk_flag": true
}
```

图4 结构化输出示例

以直接提取用于量化评估的分值，而且对“解密复现等于明文出域”等复杂业务逻辑的误判率较高。而采用上述结构化框架并结合专家案例后，模型输出的标准JSON的解析成功率提升约30%，对隐蔽合规风险的识别准确率也提升了约25%。这证明结构化且约束明确的Prompt是保障大模型在严苛合规审计场景下可靠输出的关键要素。

2.3.2 基于few-shot的专家能力泛化

IDAM利用少样本提示技术，将项目评审专家的审计经验转化为模型的优秀提示词。向模型展示3~5个典型的“文档错漏分析”案例（如系统架构设计不合规、安全性要求缺失等），使LLM能够低成本迁移至不同类型教育信息化项目的审计中。IDAM模块构建了一个在数据不出域前提下的“逻辑流通走廊”，通过审计技术文档的一致性，确保跨域流通的业务意图在技术实现上不触碰安全红线，从而在原始数据不可见的情况下，保障流通逻辑的可信与可控，实现了在治理层面上安全与效率的统一。

3 跨域流通应用实证：上海市教育数据要素治理量化实践

3.1 案例背景：一体化市场中的教育领域“样板节点”

本文以教育综合管理决策系统（升级改造）项目为实证对象。该项目是上海参与全国一体化数据市场建设、探索教育数据跨域流通的典型案例，项目架构如图5所示。其形成的治理范式与智能化工具，可为全国一体化数据市场提供垂直领域的监管尺度统一化的微观参考。

该项目涉及全市数百所学校（不同主体、不同系统）的数据向市级中枢的归集与流通。其核心挑战是如何在保障学生隐私“不出校/不出中心”的前提下，实现全市教育治理业务的“跨域协同”。该项目积累了500余份技术文档，构成了“市场监管审计”的仿真语料库。

3.2 基于TCE模型的流通管理实践与效能分析

在TCE模型的指导下，该项目从主体协同、数据汇聚、链路流通3个维度推进教育数据跨域治理，结果如图6所示。（1）信任层协同：如图6（a）所示，项目构建了覆盖市属高校（44.0%）、区教育局（19.0%）、直属单位（19.0%）、两委处室（17.9%）的多主体协同治理体系，筑牢了跨域流通的信任底座。（2）能力层支撑：如图6（b）所示，项目完成中职、托幼、学生等五大业务领域数据全量汇聚，累计超5 476万条，为跨域流通提供了坚实的数据支撑。（3）效能层释放：如图6（c）

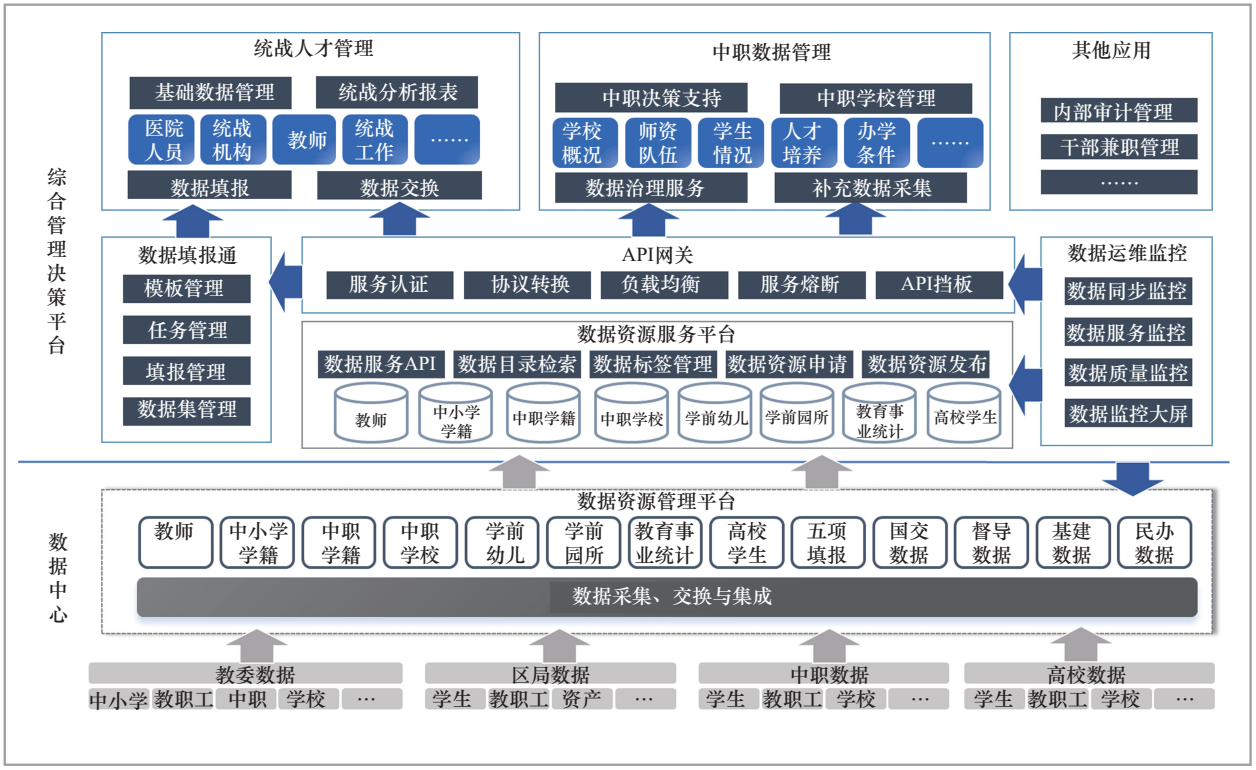

图5 市级教育系统升级改造项目架构

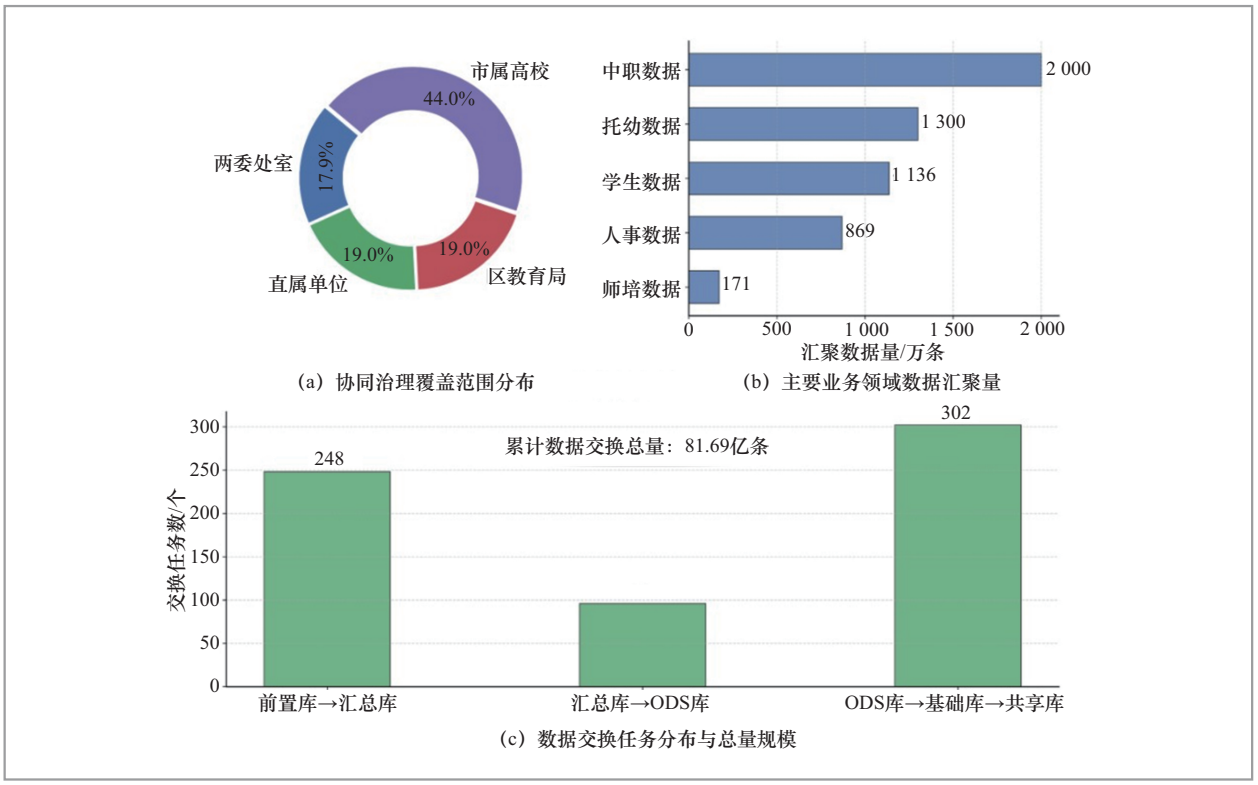

图6 多维度教育数据流通管理实践与效能分析

所示，项目搭建全链路数据交换体系，涵盖三大流通环节共646个交换任务，累计完成数据交换81.69亿条，显著提升了数据要素配置效能。

3.3 LLM驱动的数据要素治理创新与实证发现

在全国一体化数据市场中，各地、各校文档格式异构性强，人工审计难以实现统一监管尺度。审计实验显示，经LLM自动化对比《需求规格说明书》与《测试报告》发现，约15%的跨域数据交换点在设计与实现阶段存在语义偏离。LLM审计模块在不接触底层原始数据的前提下，通过扫描“治理链路”深度识别安全外泄或流通阻断风险，以逻辑层统一监管替代传统数据层直接审计，显著降低合规成本，并为垂直领域监管尺度统一提供微观技术支撑。

受教育政务内网算力与隐私限制，实验选取无风险样例文档模板，采用3款主流国产大语言模型（GLM、DeepSeek、Qwen同级别模型）开展云API对比测试。对比的目的在于：通过多模型横向验证LLM在教育数据治理场景下的适配性，量化不同模型在指令遵循、合规推理及资源消耗层面的表现，为实际部署选型提供量化决策依据。

在教育数据治理真实场景中的初步对比测试中，各模型表现的定性分析如下：①GLM系列在中文政务与教育领域专业词汇的理解上表现出良好的语义对齐能力，但在处理包含复杂接口逻辑的超长技术文

档时，推理时延相对较高；②DeepSeek系列展现出极强的逻辑推理与代码级规则解析能力，在结构化Prompt与思维链引导下，在跨域数据流转中的细粒度合规漏洞检出方面表现优异，而且显存占用控制较好；③Qwen系列在长上下文支持与综合表现上最为均衡，不仅能准确识别“数据不出域”“可用不可见”等特定治理策略风险点，而且在few-shot场景下的上下文稳定性强，响应速度满足动态审计的实时性需求。

3.4 基于项目经验参数的IDAM模块与传统审计流程对比

实验以一份约500页的技术方案文档为标准审查对象，调研结果见**表2**。根据实际项目经验及调查问卷反馈，传统审查通常需要3位专家分别独立阅读，每位专家平均耗时3.0 h；在IDAM方案中，模型自动分析平均耗时约20 min，约70%的报告仍须进入人工复核环节，复核时由两位专家参与，每位专家平均耗时约25 min。专家成本按照上海地区事业单位工程师年薪20万元、年有效工时2 000 h折算为100元/人时。

IDAM模块与传统审计流程的直接量化对比结果见**表3**，在保守取值条件下，IDAM相对于传统流程表现出显著优势。首先，在审查周期上，传统流程完成一份报告平均需要180 min，而IDAM的平均周期约为37.5 min，下降79.2%。周期时间按模型自动审查+进入复核报告的期望复核时间计算，且默认复核专家可并行工作。其次，在人工投入上，传统方式单份报告约需9.0人时，而IDAM约需0.58人时，减少93.5%。进一步按100元/人时折算，单份报告的人力成本由900元降至58.3元，降幅达到93.5%。

在准确率方面，考虑到当前缺少全量标注样本，采用专家调查问卷反馈的区间及其中值进行保守估计：传统方式的问题识别准确率约为75%～80%，IDAM约为88%～92%。若取区间中值，则IDAM较传统流程提高约12.5%。这表明，大模型在长文档解析、跨章节证据关联和隐含风险定位方面，相较于单纯关键词搜索与人工抽检，更易保持审查的一致性与高覆盖度。

综上，在教育数据不出域的智能治理场景中，IDAM相较于传统以规则检索和人工抽检为主的审计方式，具有更高的长文档审查效率、更低的人力投入以及更高的一致性识别能力。这一结果进一步支撑

表2 量化对比所采用的项目经验参数与口径说明

参数项	传统流程	IDAM流程	备注
标准审查对象	500页技术方案		两类方法处理的报告规模相同
专家人数配置	3位专家	3位专家复核	IDAM仅在高风险报告上触发复核
单专家平均审查时长	~3.0 h	~25 min	后者仅包含复核时长
模型自动审查时长	—	~20 min	含解析、检索、推理与摘要输出
人工复核比例	100%	70%	按专家经验给出
人工成本单价	100元/人时		按20万元/年、2 000 h/年折算
问题识别准确率	77.5%(经验区间75%～80%)	90%(经验区间88%～92%)	准确率为专家经验估计中值

了本文关于规则兜底+模型增强治理范式的应用价值判断。

3.5 综合评估结果与管理价值讨论

采用AHP–模糊综合评价法对教育综合管理决策系统（升级改造）项目进行量化评估，结果见**表4**。通过TCE模型与LLM审计的耦合，教育综合管理决策系统成功在“数据不出域”的严苛安全约束下，实现了高效的“跨域业务协同”。这种“微观治理”的成功，为全国一体化数据市场中“行业垂直领域”统筹流通与安全提供了可复制的技术路径。

图7为不同学校数据治理达标情况与办学质量的关联分析图：横轴为学校在数据完整性、准确性、一致性等核心维度的达标项目数（4~10项），纵轴为对应学校的办学质量评分，图中拟合直线的拟合优度$R^2 = 0.84$，表明两者呈显著正相关——学校数据治理达标项目数越多，办学质量评分越高。该结果直观验证了项目落地的“一数一源”数据治理机制，通过系统性提升学校数据质量，有效赋能办学水平提升，充分体现了本项目数据治理方案的实践价值与管理效能。

表3 IDAM模块与传统审计流程的直接量化对比结果

指标	传统流程	IDAM流程	变化幅度
问题识别准确率	77.5%	90%	+12.5 %
平均单份审查周期	180 min	37.5 min	−79.2%
单份报告人工工时	9.0人时	0.58人时	−93.5%
单份报告人力成本	900元	58.3元	−93.5%

4 结束语

针对全国一体化数据市场建设，本文依托“信任、能力、效能”递进逻辑构建TCE评价模型，并创新性地利用本地化LLM构建智能审计模块，实现了从“数据流转监管”向“逻辑穿透监管”的范式转变。该框架坚持“数据不出域、逻辑跨域流动”，在上海教育项目中达到了80%的审计自动化率，并精准识别合规偏离，为平衡敏感数据安全与要素配置效率提供了可复制的智能化路径。未来将通过检索增强生成技术增强审计权威性，推动本文提出的治理范式在超大规模与异质化场景下的工程化落地。

表4 教育系统升级项目五维量化评估结果

评价维度	得分	等级	关键指标
数据治理能力	92.1	优秀	【一数一源落实率】基本达标，重复数据源核心字段去重成效显著； 【数据标准覆盖率】达95%（制定68项元标准），符合教育行业数据标准要求
可信流通支撑	76.3	中等	【隐私计算应用率】仅约35%，为维度核心短板； 【信创适配度】满足系统核心组件国产化部署比例要求
合规安全保障	88.5	良好	【审计自动化率】达80%（政策规则引擎生效），LLM驱动的自动化技术文档与数据合规审查能力达标； 【授权管理完备度】实现RBAC/ABAC动态权限配置全覆盖，访问控制体系完善
项目实施效果	85.2	良好	【文档一致性覆盖率】达标，项目启动、中期、结项全流程文档需求覆盖与修正一致性符合规范； 【进度控制偏差率】为−5%（较计划提前2周），项目进度管控成效良好
价值创造效益	83.7	良好	【决策效率提升度】较高，数据流通后报表生成周期大幅缩短，中职学校管理成本下降40%； 【跨部门业务协同率】显著提升，跨校、跨部门协同业务支撑成效突出，数据不一致问题减少70%

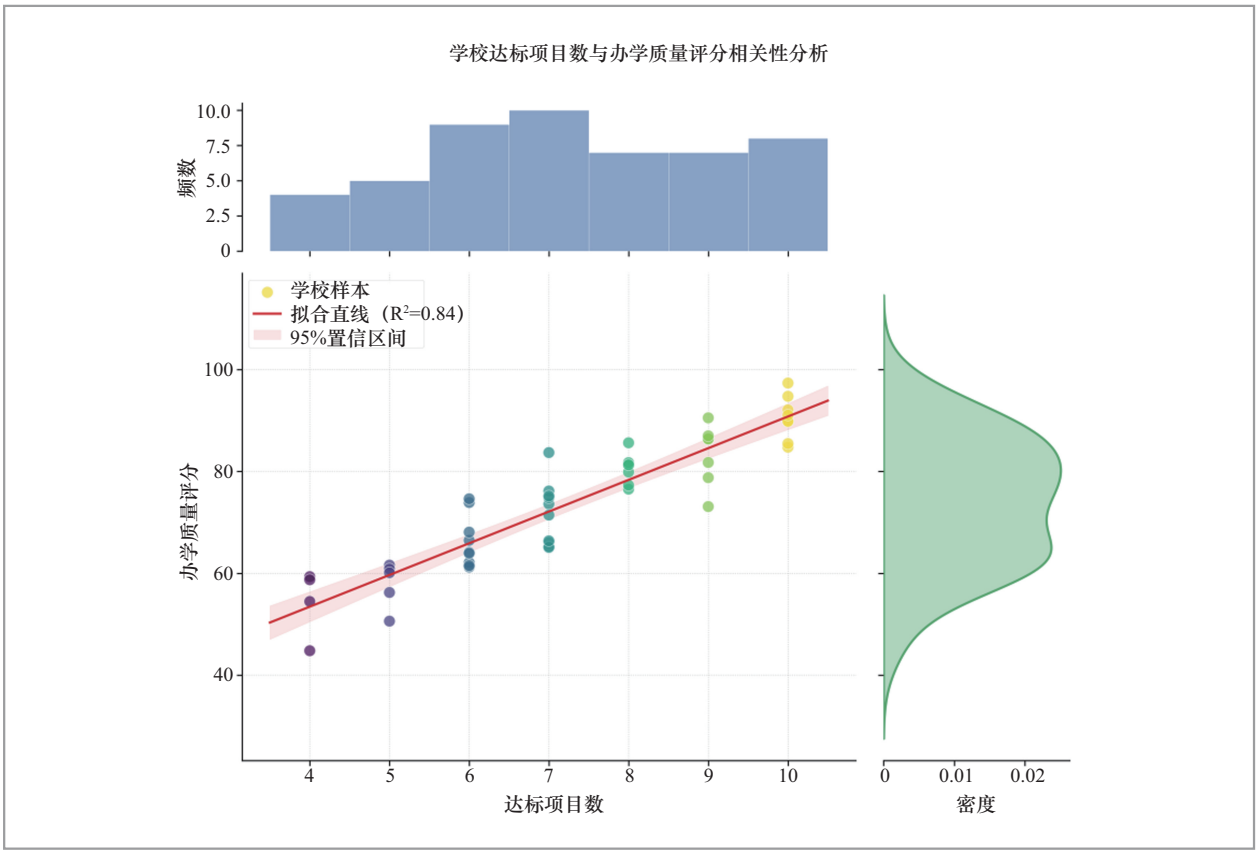

图7 学校归集汇总数据资源质量评估分析

参考文献：

[1] 徐凤敏，王柯蕴. 建设统一数据要素大市场的科学内涵、内在逻辑与政策建议[J]. 西安交通大学学报（社会科学版），2023，43(2)：95-106.
Xu F M，Wang K Y. The construction of the unified national market of data elements：scientific connotation，internal logic，and policy suggestions[J]. Journal of Xi'an Jiaotong University (Social Sciences)，2023，43(2)：95-106.

[2] 郝爱民，任禛，冉净斐. 流通数字化赋能全国统一大市场建设的机理与效应研究[J]. 统计研究，2024，41(4)：40-53.
Hao A M，Ren Z，Ran J F. Research on the mechanism and effects of circulation digitalization in empowering the construction of a national unified market[J]. Statistical Research，2024，41(4)：40-53.

[3] 王涛，张玉平，李秀晗，等. 数据驱动教育数字化转型的信任机制：教育大数据全生命周期隐私增强模型的构建与典型应用场景分析[J]. 现代教育技术，2024，34(3)：28-38.
Wang T，Zhang Y P，Li X H，et al. Trust mechanism for the data-driven education digital transformation：construction and typical application scenario analysis of privacy enhancement model for the full life cycle of educational big data[J]. Modern Educational Technology，2024，34(3)：28-38.

[4] 张君，林小红，耿雨歌，等. 隐私计算+区块链：教育数据伦理研究的新视角[J]. 现代教育技术，2023，33(9)：27-36.
Zhang J，Lin X H，Geng Y G，et al. Privacy computing + blockchain：a new

perspective of educational data ethics research[J]. Modern Educational Technology, 2023, 33(9): 27-36.

[5] 胡新瑞. 数字化转型中教育数据分类分级的治理制度研究[J]. 北京理工大学学报(社会科学版), 2025, 27(2): 215-222.
Hu X R. Research on the governance system of classification and classification of educational data in digital transformation[J]. Journal of Beijing Institute of Technology (Social Sciences Edition), 2025, 27(2): 215-222.

[6] Brown T B, Mann B, Ryder N, et al. Language models are few-shot learners [C]//Proceedings of the 34th International Conference on Neural Information Processing Systems. New York: Curran Associates Inc., 2020: 1877-1901.

[7] Radosky L, Polasek I. Large language models for software documentation: a systematic literature review[PP]. arXiv preprint, 2026, arXiv: 2602.04938.

[8] Pahune S, Akhtar Z, Mandapati V, et al. The importance of AI data governance in large language models[J]. Big Data and Cognitive Computing, 2025, 9(6): 147.

[9] 刘波, 黄科满, 何安珣, 等. 基于保护动机理论的中国数据流通政策机制分析: 政策趋势[J]. 大数据, 2024, 10(6): 121-137.
Liu B, Huang K M, He A X, et al. Analysis of China's data circulation policy mechanisms based on protection motivation theory: policy trends[J]. Big Data Research, 2024, 10(6): 121-137.

[10] 黄科满, 许多, 杜小勇. 数据社会化视角下的数据流通安全治理: 五位一体框架[J]. 大数据, 2024, 10(6): 5-15.
Huang K M, Xu D, Du X Y. Data circulation security governance from the perspective of data socialization: a five-sphere framework[J]. Big Data Research, 2024, 10(6): 5-15.

[11] 靳澜涛. 从"技术治理"到"治理技术":教育治理现代化的重点突破[J]. 现代教育管理, 2021(12): 46-52.
Jin L T. From "technological governance" to "governance technology": key breakthroughs in the modernization of educational governance[J]. Modern Educational Management, 2021(12): 46-52.

[12] Floridi L. AI as agency without intelligence: on artificial intelligence as a new form of artificial agency and the multiple realisability of agency thesis[J]. Philosophy & Technology, 2025, 38: 30.

[13] 周辉, 郭烘佑. 大语言模型安全的技术治理: 对抗测试与评估审计[J]. 西安交通大学学报(社会科学版), 2025, 45(2): 78-88.
Zhou H, Guo H Y. Technical governance of large language models security: red teaming and evaluation audits[J]. Journal of Xi'an Jiaotong University (Social Sciences), 2025, 45(2): 78-88.

[14] Mökander J, Schuett J, Kirk H R, et al. Auditing large language models: a three-layered approach[J]. AI and Ethics, 2024, 4(4): 1085-1115.

作者简介

罗屿冰（1981- ），女，上海市大数据中心工程师，主要研究方向为大数据、项目管理、政务信息化。

收稿日期: 2026-03-25
通信作者: 罗屿冰，ybluo@shanghai.gov.cn