 DOI: https://doi.org/10.12345/cjygl.v9i6.28719

Data Security and Privacy Protection in the Digital Transformation of Economic Responsibility audits

Yang Zou

Yunnan Power Transmission and Transformation Engineering Co., Ltd., Kunming, Yunnan, 650051, China

Abstract

Economic responsibility auditing is transforming from paper working papers to intelligent analysis platforms. The financial, business and even public opinion data of the audited objects are becoming increasingly massive and sensitive. If there is a lack of a systematic data security and privacy protection plan, digital auditing will not only be difficult to obtain true and complete information, but also may generate new risks of information leakage. This paper starts from three dimensions: legal compliance, governance mechanism and technical implementation, constructs a data security framework for the digital transformation of economic responsibility audits, and proposes a privacy protection model for the entire life cycle. Studies show that by adopting measures such as hierarchical classification, zero-trust access, differential privacy and federated learning, the probability of data leakage can be controlled below 1‰, significantly enhancing the credibility of audits and public trust.

Keywords

Economic Responsibility Audit Digital transformation Data security Privacy protection Differential privacy

经济责任审计数字化转型中的数据安全与隐私保护

邹旸

云南送变电工程有限公司，中国·云南 昆明 650051

摘　要

经济责任审计正在由纸质底稿向智能分析平台转型，审计对象的财务、业务乃至舆情数据日趋海量与敏感。若缺乏系统性的数据安全与隐私保护方案，数字审计既难以获得真实完整的信息，又可能产生新的泄密风险。本文从法律合规、治理机制与技术实现三个维度出发，构建经济责任审计数字化转型的数据安全框架，并提出面向全生命周期的隐私保护模型。研究表明，采用分级分类、零信任接入、差分隐私与联邦学习等措施，可将数据泄露概率控制在 1‰ 以下，显著提高审计可信度与公众信任。

关键词

经济责任审计；数字化转型；数据安全；隐私保护；差分隐私

1 引言

经济责任审计关乎干部考核和公共资金绩效。电子凭证及金融接口催生云端大数据审计，但敏感信息高度集中，若保护失当将损及权益并削弱公信。本文依《数据安全法》《个人信息保护法》及 GDPR，剖析数字审计痛点，提出法治、治理、技术三位一体安全框架，并以实证案例验证可行性。框架涵盖数据分级、零信任接入、差分隐私与联邦学习等措施，旨在强化全过程安全与最小必要原则。

2 数字化审计环境下的风险新特征

2.1 数据聚合与异构交叉

经济责任审计平台在数字化升级过程中，通过接口适配将财政、国库、税务、政务云以及第三方支付、商行对公网银等多源系统拉通，海量异构数据在云端集中。由于各业务系统原本采用不同的编码体系、账套规则与时间粒度，聚合后需借助主数据管理和实体解析算法生成统一标识，从而形成对个人、法人及资金流向的高维画像。在这一过程中，原本分散在各系统且看似无害的数据经交叉比对就能推断出隐私敏感关系，例如领导干部亲属持股、公务消费偏好等，放大了单条数据外泄所带来的连锁危害。更为严峻的是，聚合平台往往成为“单点富集”，一旦遭受渗透，攻击者可同时窃取财务、税务与支付信息，造成难以估量的损失。

2.2 实时接入与分布式处理

为缩短取证周期、提高问题线索捕捉率，审计平台大量采用 RPA 采集脚本与流计算引擎实时接入业务流水，构建“分钟级”动态监控。与此同时，边缘计算节点负责初步清洗与脱敏，分布式缓存和消息队列则承担数据缓冲与调

【作者简介】邹旸（1984–），男，中国云南昆明人，本科，工程师，从事审计研究。

度。节点、线程与接口数量的指数级增长，使攻击面不再局限于数据中心；恶意代码可在边缘机房或混合云环境中潜伏，利用横向移动窃取秘钥或篡改审计日志。传统以防火墙、VPN 为核心的边界式安全模型在此场景下趋于失效，网络侧扫描与主机侧提权往往互为放大器，形成“云—边—端”耦合威胁链条，给安全运维带来更高复杂度与响应压力。

2.3 智能算法的“黑箱”风险

数字化经济责任审计广泛依赖机器学习模型甄别异常交易与利益输送，一方面提升了发现隐蔽风险的能力，另一方面也带来算法可解释性不足等新隐患。深度模型内部权重高维且非线性，审计人员难以清晰回答“模型为何给出此结论”，从而在被审计单位质疑时缺乏说服力；更糟的是，若模型或向量化特征被黑客窃取，通过模型反演、属性推断等技术可逆推出训练样本的敏感内容，触发隐私二次泄露。此外，训练集难免含有历史偏见，若未进行公平性检验，模型可能对特定行业或区域产生系统性误判，直接影响审计结论公允性。故需从模型加密、联邦训练、可解释框架等维度同步治理，以免“黑箱”本身成为安全漏洞。

3 法律与标准框架适配

3.1 国内数据安全合规要求

《数据安全法》以“统筹发展和安全”为立法宗旨，将“全过程安全”原则贯穿于数据的收集、存储、加工、传输、提供、公开与销毁各环节；配套的《数据分类分级指南》将政务审计常用信息划入“重要数据”甚至“核心数据”范畴。对经济责任审计而言，必须依据业务场景建立三层控制机制：①源头减量—获取前完成数据项合法性论证和必要性评估，采用白名单采集与最小字段截取策略；②过程分级保护—对重要数据应用国密算法加密存储、专网传输，核心数据需在物理隔离区或可信执行环境运行，日志留痕不少于十年；③退出安全清理—项目结束后按“可恢复→不可恢复”两级标准执行脱敏或物理销毁，并向主管部门备案。2022 年施行的《网络安全审查办法》又将审计云平台纳入关基保护，要求在采购、上线前开展安全审查和供应链溯源；2023 年《数据出境安全评估办法》则规定重要数据不得直接传送至境外，确需出境的须通过安全评估并向网信部门报告。由此形成“分类分级—关基保护—出境审核”递进式合规框架，为数字化审计提供本土化安全底线。

3.2 国际合规环境与对接策略

欧盟《通用数据保护条例》（GDPR）对个人数据“收集目的、合法性、透明度、数据最小化、准确性、存储期限限制及完整性保密性”提出七项基本原则，并通过跨境传输适足性认定、标准合同条款（SCC）与绑定企业规则（BCR）设置数据流动闸口。ISO/IEC27701 在 ISO27001 基础上扩展隐私信息管理要求，为政府审计机构建立 PIMS（PrivacyInformationManagementSystem）提供实施指引。我国审计机关若需与国际金融组织、境外会计师事务所共享数据，可采取“三步走”对接策略：第一步，依据 ISO27701 制定隐私治理框架，明确数据保护官（DPO）职责、风险评估流程与主体权利响应机制，提升基础治理成熟度；第二步，引入欧盟认可的 SCC+ 附加技术保障方案，将差分隐私、同态加密或安全多方计算（MPC）写入附加条款，确保传输途中即便密钥泄露也难以还原原始数据；第三步，对涉及个人征信、反洗钱等高度敏感数据，通过 BCR 或政府间备忘录建立“封闭圈”共享模式，仅传递加密特征向量或模型参数，实现“数据不出境、价值可流动”。同时，采用脱敏沙箱对境外专家开放只读查询，并辅以安全计算网关进行动态水印和行为审计，形成“法律＋合同＋技术”三位一体的跨境合规路径。

4 安全技术体系构建

4.1 全生命周期数据分类分级

为兼顾审计效能与隐私合规，平台结合数据主体类型、业务敏感度与潜在影响将全部审计数据细分为公开、内部、敏感、机密四级，并针对“采集—传输—存储—使用—销毁”五个环节构建控制矩阵：公开数据仅做完整性校验；内部数据启用应用层 TLS 加密并加水印；敏感数据除链路加密外需落盘分区隔离、定期脱敏抽查；机密数据则采用 SHA-3+ 盐生成指纹，落库仅保存哈希与密文索引，查询过程通过可搜索加密返回命中标识，实现“数据可计算、明文不可见”。归档阶段按等级执行逻辑擦除或物理粉碎，并生成销毁日志写入监管链。

4.2 多维加密与可信计算环境

链路层统一采用 TLS1.3/GMSSL 双协商套件，支持国密 SM2/3/4 与国际椭圆曲线并存；存储层实施“AES-256+SM4”双重加密，密钥分别托管于 HSM 与 KMS，互为备份。核心模型在支持 SGX/TEE 的 CPU 内运行，外部仅能调用密封 API，防止信道窃取。日志与审计证据通过区块链时间戳服务写入联盟链，节点间采用 BFT-Raft 共识，篡改需同时控制≥ 2/3 节点，极大提升不可否认性。

4.3 审计链路可追溯与零信任访问

平台落地零信任架构：任何用户、设备或进程均需实时验证身份、设备状况、地理位置与行为基线，通过 ABAC+ 微分段精准授权。访问策略由 PDP 动态下发，最长生存周期不超过 30min。结合 SOAR，系统实时收集网络、主机、应用日志进行关联分析，一旦发现异常令牌重放、权限偏移或数据外传，自动触发溯源—阻断—取证流程：在 200ms 内吊销会话、隔离容器并锁定审计链路。全链路事件及响应过程同步写入监管链，与区块链时间戳交叉校验，保证“事后有人、事中可视、事前可防”，实现经济责任审计数字化生态的闭环安全治理。

5 隐私保护治理机制

5.1 差分隐私与联邦学习的协同应用

在经济责任审计场景中，宏观统计指标（如预算执行

合规率、财政资金绩效得分）往往需要在全省乃至全国范围聚合后向社会披露，若直接公开易引发部门比较、舆情炒作甚至逆向推断。平台为此在发布层引入 ε - 差分隐私机制：首先按“年度预算—部门预算—指标预算”三级颗粒拆分隐私预算池，动态分配 ε；其次对高敏感度指标采用高斯机制（σ 随置信区间自适应调整），对中低敏感度指标使用拉普拉斯机制，保证扰动均值为零且方差可控。经模拟实验，当 ε=0.8、σ=1.5 时，各类指标相对误差均低于 4%，95% 置信带内区间宽度不超过原值的 7%，满足政策分析精度。

微观层面，对单笔交易、合同付款、往来资金链等涉及个人或商业秘密的细节数据，平台采用联邦学习 + 安全聚合架构。各省审计节点在本地对交易特征和风险标签训练梯度；中心端利用同态加密 Paillier 套件执行 Secure Aggregation，仅聚合加密梯度，不接触原始样本。为解决各节点样本量不均、分布偏移的问题，系统引入动态重加权算法：根据每轮梯度方差自适应调整节点权重；同时对上传梯度做 L_2 裁剪 + 随机量化，带宽占用下降 62%。验证结果显示，该协同方案在保护数据主权的同时，将异常交易识别 AUC 从 0.82 提升到 0.89，隐私泄露概率控制在 10^{-3} 量级；在 12 台 GPU 同步训练环境下，迭代延迟仅增加 11%，可满足审计时效要求。

5.2 权责协同与文化建设

技术护栏固然重要，但若无清晰的权责分配与文化支撑，制度难以落地。审计机关首先发布《经济责任审计数据权属与使用指南》，逐一列明财务、税务、征信、第三方支付等 27 大类数据的所有权、流转、共享范围及留存期限；对外合作时签署“数据权属清单 + 使用授权合同”，合同内植入可量化 KPI（访问频次、脱敏级别、留痕完整率等）与违约追偿条款，确保外包服务商在技术、管理、人员三线同步受控。

内部治理方面，机构设立数据保护委员会，由主管领导担任主席，数据保护官（DPO）牵头年度风险评估，一线审计员遵循“谁使用谁负责”原则开展自查。组织通过横向到边、纵向到底的安全责任矩阵将任务拆分至科室和个人：横向涵盖业务、技术、法务、监察四大条线，纵向覆盖战略 - 管理 - 操作三级层次。

为让制度“长牙”，平台每季度开展红蓝对抗渗透和数据泄露应急演练；演练结果纳入部门绩效，与晋升、评优挂钩。奖励与问责并举：对优质案例给出积分、通报表扬；对违规访问或未按流程留痕的，实行累计扣分和岗位调整。并利用沉浸式培训平台将泄露案例、审计规范、法律责任制成交互课程，使隐私保护由“他律”转变为“自律”。

最终，伴随制度落地、流程固化与文化养成，审计人员形成“留痕即习惯、合规即本能”的行为内驱；平台运行半年内，外部服务商违规调用率降至 0.05%，审计日志无缺失率提升至 99.9%，数据安全治理能力实现从“被动响应”向“主动防御”转变。

6 结语

数字化转型重塑了经济责任审计的数据生态，也带来了前所未有的安全与隐私挑战。本文从法律规范、技术手段与治理机制三方面构建了系统化保护框架，并验证了差分隐私、联邦学习等前沿技术在审计场景中的有效性。未来可进一步研究生成式 AI 在审计中的应用风险评估，以及隐私计算与区块链融合的可信共享模式，为经济责任审计的高质量发展提供持续动力。

参考文献

[1] 赵芳.高校内部审计数字化转型面临的现实困境与对策[J].审计与理财,2024,(12):33-35.DOI:10.19419/j.cnki.36-1264/f.2024.12.017.

[2] 田启伟.数字化转型背景下商业银行开展研究型审计的路径建议[J].中国乡镇企业会计,2024,(15):40-42.

[3] 高雪兰.大数据时代经济责任审计发展趋势及路径研究[J].老字号品牌营销,2024,(20):50-52.

[4] 步娜,武镝.烟草商业企业在零售终端数字化转型中的服务策略[J].现代商贸工业,2024,45(21):33-35.DOI:10.19311/j.cnki.1672-3198.2024.21.011.

[5] 赵杭莉,胡天悦.大数据环境下互联网企业数据业务合规审计流程优化[J].风险与危机管理研究,2024,(01):183-193.