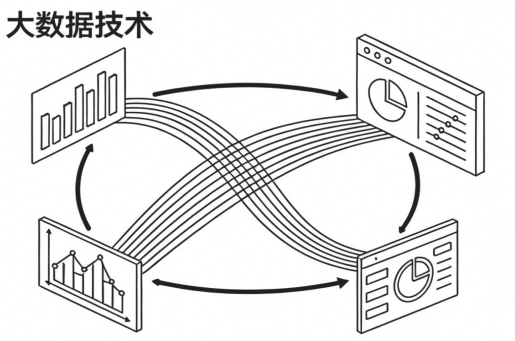
基于大数据的组织内部控制协同研究

文丨 范丽娟

在数字经济时代，大数据技术深刻改变组织运营模式与管理架构。传统内部控制体系中，各要素处于相对独立运作状态，部门间协调依靠人工沟通，难以应对复杂风险场景。大数据技术创造的数据流动条件、智能分析能力和实时监测手段，为内部控制协同提供技术支撑，控制要素间关联关系从机械配合转变为有机融合。不过，“数据孤岛”、权责模糊及技术依赖等问题制约着协同效能的提升。



（配图由 AI 生成）

大数据重构内部控制协同基础

数据流动突破控制边界约束

传统的内部控制体系是依托层级分明的组织结构的，控制信息按照固定层级和职能通道来传递，部门和部门之间形成了非常显著的数据隔阂。借助大数据分布式存储及实时传输的特性，业务数据在产生阶段就能实现跨部门自由流通，这大大减少了控制主体获取信息所耗费的时间，还打破了空间方面的束缚。数据湖平台汇集了财务运营、供应链等多来源、多样化的数据，各控制环节能够直接从这个集中信息库提取所需依据，这样有效规避了传统控制活动因信息不透明产生的问题。不管是风险评估、授权审批，还是绩效评估工作，都能够基于全面的数据集来开展，部门职能划分对控制效果产生的负面影响也随之降低。数据流动具备高效、直接的特点，为跨部门合作提供技术支撑，控制信息获取方式从过去的逐级汇报转变为平台化自主调取。

智能算法支撑协同决策形成

协同决策需要多个控制主体在信息共享的基础上达成一致判断，传统决策模式里各部门基于局部数据形成碎片化结论，决策协调依靠反复沟通并请上级进行裁决。机器学习算法通过训练历史控制数据来识别不同控制要素间的关联规律，从而为协同决策提供量化方面的依据。预测模型结合宏观经济指标、行业波动数据和组织运营参数，生成风险概率分布图谱，让财务、审计、业务等部门在统一风险评估框架下制定控制策略。深度学习算法模拟复杂业务场景下的控制效果，来评估不同协同方案的成本收益比，智能算法将分散的控制知识转化为可计算的决策模型，推动协同决策从经验驱动转向数据驱动。

实时监测促进多主体联动响应

内部控制能不能有效发挥作用，关键在于控制主体对风险事件的反应速度，以往监控主要依靠定期报告和抽样审查，使得风险暴露与采取控制行动之间常有延迟。大数据时代各类传感器、日志记录系统和交易平台，不断生成庞大的实时数据流，流式计算技术能即时对这些数据进行清理和特征提取。异常检测算法可在极短时间内完成风险警示，一旦发现风险，警示信息会通过工作流引擎即时传送给相关控制主体，进而激活预先设定的协同应对流程。比如监测到资金出现异常流动时，财务、内审及业务部门会同时收到警报通知，各团队依照自身职责马上开展核查、冻结、上报等同步管控动作，这种基于事件触发的联动方式能保证多个控制主体在风险发生第一时间迅速形成合力。

内部控制协同机制构建

横向协同的跨部门数据共享机制

构建跨部门数据共享机制要解决数据所有权和使用权分配冲突的问题。可建立数据资产登记制度来明确各业务单元产生数据的权属关系，同时制定分级授权规则，以界定不同控制主体对共享数据的访问范围和操作权限。元数据管理系统需统一各部门的数据定义标准，从而消除因业务术语差异导致的语义冲突，以此确保财务科目、客户编码、产品分类等关键控制维度在全组织范围内保持一致。数据交换接口

采用标准化协议，让各部门通过 API 接口向共享平台推送控制相关数据，敏感数据经过脱敏处理后再开放给协同方，横向协同的实现依赖于数据从部门私有资源向组织公共资产的转化。

纵向协同的层级信息穿透机制

层级信息穿透机制把传统逐级汇报信息传递方式摒弃掉，保证控制信息在组织纵向架构里实现双向透明流动。数据仓库技术将基层操作数据和高层决策数据融合在一起，构建出从交易明细到战略指标的多维度关联体系，让管理层能够穿透汇总报表直接追溯到具体业务事项控制细节。权限管理体系按照岗位职责设置差异化数据访问层级，赋予高层管理者跨部门、跨层级的数据查询能力，同时允许基层执行者获取跟自身职责相关的上级控制要求及决策依据。信息穿透机制极大提升了控制指令的传达效能，战略目标分解、风险偏好设定、合规要求部署等高层决策，借助数字化工作流系统精准传递到执行层。

动态协同的风险响应联动机制

风险联动响应体系依靠风险动态监测能力和应急预案数字化支撑。机构按照自身业务属性和风险类别，提前构建覆盖财务运营合规等多维度应急处理路径，还把各责任主体权责边界、响应时效及协作要求转化为结构化执行模板，风险监控平台通过实时采集内外部信息流，利用智能分析技术捕捉风险信号，自动调取对应联动策略并激活跨部门协作流程。此体系采用并行运作模式，相关方在收到风险提示后同步落实防控措施，协同系统即时共享处置进展情况，同时 AI 算法通过持续分析过往风险案例响应数据，动态优化联动机制的启动条件。

协同障碍消解的实现路径

“数据孤岛”的治理方案

异构系统和部门壁垒造成了“数据孤岛”现象。治理工作要技术整合与组织改革同时推进，通过运用 ETL 工具来抽取业务系统当中的数据，经过标准化处理以后，将其存入企业数据平台，利用主数据管理统一核心业务对象的标识，消除因编码差异而引发的数据割裂状况。依靠数据治理委员会进行跨部门的协调工作，它负责数据标准的制定、质量考核及共享争议的裁决工作，以此打破部门对于数据资源的垄断局面。把数据共享纳入到部门绩效考核体系当中，“数据孤岛”治理实际上是在重构数据流通的规则，技术手段能降低数据整合成本，制度则可以调整利益的分配格局。

权责模糊的界定机制

在大数据时代，控制活动自动化、协同化，让传统岗位职责界限不再清晰，所以权责划分机制需顺应数字化控制场景作出调整。组织要构建包含数据录入、算法运算、结果输出及人工复核等环节的端到端控制流程图，以此清晰界定每个节点的责任主体与决策权限。对于算法主导的控制决策，需确立人机协同的责任分配框架，算法开发团队负责模型的准确性，业务部门负责参数的配置，内控部门承担监督与验证职责，借助数字化授权系统，完整记录每笔业务的审批轨迹和决策依据，构建无法篡改的责任追溯链条。协同控制环境中实施集体决策时，引入贡献度量化体系，依据数据质量、响应速度、决策影响权重等因素，合理分配协同成果的责任比例。

技术依赖的平衡策略

过度依赖技术应用可能会让人工判断能力下降，还会埋下系统性风险方面的隐患。平衡的办法是把技术赋能和人工监督进行有机结合，在常规、高频且规则明确的控制活动当中，要充分发挥自动化系统的高效性，来减少人工干预，对于涉及重大资金、复杂判断及战略影响的控制决策，必须要保留人工审核与否决权，以避免算法偏差引发控制失误。组织需要制定技术应急响应预案，当核心系统出现故障时，能够立即启动手工替代流程，以此确保控制活动不会中断。定期开展技术脱离演练，既可以检验控制人员在系统失效时的应急处理能力，又能够防止相关技能出现退化。技术伦理审查机制要评估算法决策的公平性与透明度，杜绝“算法黑箱”现象损害利益相关方的权益。人才培养要兼顾数据技能和业务判断能力的同步提升，培养既精通技术工具，又具备风险洞察力的复合型控制人才。平衡策略的核心是明确技术的工具属性，即技术系统服务于控制目标，而不是替代控制职能。人与技术在协同控制中形成互补而非替代关系，进而保障组织在技术变革中始终保持稳健的控制能力。

结束语

大数据技术给组织内部控制协同提供了前所未有的实现条件，横向数据共享机制、纵向信息穿透机制及动态风险联动机制，一起构成协同运行框架。协同效能的提升涉及组织架构调整、业务流程重构及人员能力培养等多方面变革，组织需要在战略层面进行统筹规划，并在执行层面持续改进，最终达成风险防控与价值创造的有机统一。

作者简介：范丽娟 新天智汇能源科技（雄安）有限公司

责任编辑：孙姗姗　**投稿邮箱：**zhouhl@staff.ccidnet.com