

数字化背景下穿透式风险防控体系建设路径研究

邱剑斌 杨柳春 钱煜州

宁波市永能电力产业投资有限公司 浙江 宁波 315100

摘要：数字化浪潮深刻改变了风险形态与传播方式，传统条块分割、事后应对的风险防控模式已难以应对复杂多变的风险挑战。穿透式风险防控作为一种纵向到底、横向到边、深度到本质的新型治理理念，成为破解风险隐匿化、跨界化、传染化难题的有效路径。本文系统分析了数字化背景下风险防控面临的新挑战，构建了穿透式风险防控的理论框架与技术支持体系，从顶层设计、数据治理、系统建设、流程再造四个维度提出了建设实施路径，为构建适应数字时代的风险防控体系提供理论参考与实践指导。

关键词：数字化背景；穿透式风险防控；体系建设路径；风险管理

引言：随着大数据、人工智能、区块链等数字技术的深度应用，经济社会运行方式发生深刻变革，风险形态也随之演变。风险呈现隐蔽化、加速化、跨界化等新特征，传统以条块分割、事后应对为主的防控模式面临严峻挑战。穿透式风险防控强调突破层级壁垒、部门界限和表象迷雾，实现对风险源头的精准识别与全过程管控，成为数字时代风险治理的重要方向。

1 数字化背景下风险防控面临的挑战

1.1 数字化带来的风险新特征

数字化深刻重塑了风险形态。首先是风险隐蔽化，算法黑箱、数据操纵等问题使风险难以被传统手段察觉，风险源隐藏在数字系统深处。其次是风险传导加速化，单一风险点可通过数据链、资金链快速传导至整个系统，引发链式反应。再次是风险边界模糊化，跨界经营、线上线下融合使传统监管边界被打破，监管真空地带大量存在。最后是风险影响放大化，网络效应使局部风险迅速演变为系统性风险，舆论叠加效应进一步放大风险的社会影响。这些新特征要求防控体系必须实现从静态到动态、从单点到全域、从被动到主动的根本转变。

1.2 传统风险防控模式的局限性

传统风险防控模式的局限性日益凸显。其一，信息碎片化与数据孤岛突出，各部门数据壁垒严重，难以形成全景式风险画像。其二，事后被动应对为主，侧重于应急处置，缺乏事前预警和事中干预能力，错失最佳防控时机。其三，条块分割与协同不足，面对跨界风险时呈现“铁路警察各管一段”的困境，跨部门协同机制不健全。其四，技术手段滞后，依赖规则引擎和阈值告警，难以识别复杂隐蔽的异常模式^[1]。其五，穿透能力不足，难以穿透复杂的组织架构和资金链条，风险源头被多层包装掩盖。这些局限性倒逼风险防控体系必须进行

根本性重构。

2 穿透式风险防控体系的理论框架

2.1 穿透式风险防控的核心逻辑

穿透式风险防控的核心逻辑可概括为“三个穿透、四个环节”。三个穿透是指：纵向穿透，突破行政层级限制，从宏观顶层直达微观末梢，实现全链条追踪溯源；横向穿透，打破部门职能壁垒，贯通业务全流程，实现跨领域协同防控；深度穿透，透过表象直达本质，识别隐藏的真实风险源，揭示复杂关联关系。三个穿透构成防控的立体维度，确保风险无处遁形。四个环节构成防控的完整闭环：风险识别，及时发现潜在风险点；风险评估，进行量化分析和等级评定；风险预警，分级发布预警信息；风险处置，化解风险并跟踪效果。穿透式防控的根本目标是实现从被动应对向主动预防转变、从单点防控向系统治理转变、从事后处置向全周期管理转变。

2.2 穿透式风险防控体系的构成要素

穿透式风险防控体系由四大核心要素构成。组织层是体系的骨架，需建立权责清晰的防控组织架构，设立统筹协调机构，形成纵向贯通、横向联动的组织体系。制度层是规则基础，需建立健全覆盖全流程的规章制度，明确法律授权、操作规程和问责机制，为防控提供法治保障。数据层是信息底座，需建设统一共享的数据资源体系，打通数据壁垒，建立标准规范，确保数据完整性、准确性和时效性。技术层是工具支撑，需集成大数据、人工智能、区块链、物联网等先进技术，构建智能化风险监测预警平台。四大要素相互依存、相互支撑，共同构成穿透式风险防控体系的完整架构^[2]。

3 数字化背景下穿透式风险防控技术支持体系

3.1 大数据驱动的风险识别技术

大数据技术是穿透式风险防控的基础支撑,其核心价值在于从海量异构数据中提取风险信号、发现异常模式。多源异构数据融合技术可以整合来自不同部门、不同系统、不同结构的数据,包括结构化业务数据、半结构化日志数据和非结构化文本图像数据,通过数据清洗、标准化、关联融合,构建统一的数据视图。风险特征提取与标签化技术通过数据挖掘和统计分析,从原始数据中提取表征风险的关键特征,对主体、行为、关系进行多维度标签化处理,形成可量化、可比较的风险指标。关联图谱分析技术将分散的数据点连接成关系网络,揭示隐藏的资金流向、股权结构、人员关联等复杂关系,使隐藏的风险链条显性化。大数据风险识别能够实现从“人找风险”到“风险找人”的转变,在金融反欺诈、税务稽查、市场监管等领域已取得显著成效。构建大数据风险识别能力,需要建设统一的数据采集平台、建立标准化的数据处理流程、配备专业的数据分析团队,并持续优化风险识别模型。

3.2 人工智能赋能的智能预警技术

人工智能技术使风险预警从规则驱动向数据驱动、从被动响应向主动预测演进。机器学习异常检测模型通过对历史正常行为的学习,建立行为基线,实时监测偏离基线的异常行为,无需预设规则即可发现未知类型风险,特别适用于应对新型、变异风险。深度学习风险预测模型利用神经网络强大的特征学习能力,从时序数据中发现风险演化的规律,预测风险发生的概率和可能的影响范围,为提前干预争取时间窗口。自然语言处理技术可自动解析非结构化的文本信息,如舆情报道、投诉举报、审计报告等,从中提取风险线索,与结构化数据进行交叉验证。知识图谱推理技术将领域专家的知识经验形式化为推理规则,结合图谱中的实体关系进行智能推理,发现逻辑上存在但尚未显性暴露的风险。人工智能预警系统可根据风险等级自动分级推送预警信息,实现差异化的响应策略。建设智能预警体系,需要持续积累高质量标注数据、不断优化算法模型、建立人机协同的审核机制,确保预警的准确性和可解释性。

3.3 区块链保障的可追溯技术

区块链技术以其去中心化、不可篡改、全程留痕的特性,为穿透式风险防控提供了可信追溯能力。数据存证与防篡改机制将风险相关的关键数据(交易记录、操作日志、审批流程等)上链存证,一旦写入即不可篡改、不可否认,为事后审计和追责提供可信证据。智能合约与自动执行技术将规则代码化,当预设条件满足时自动触发风险处置动作,如冻结异常账户、暂停可疑交

易、通知相关人员等,减少人为干预的时滞和偏差。在供应链金融领域,区块链可实现对底层资产的穿透式监管,从核心企业信用传递到多级供应商融资,全链条可追溯、可验证。多方安全计算与隐私保护技术解决了数据共享与隐私保护之间的矛盾,使不同机构在不暴露原始数据的前提下协同完成风险分析。“数据可用不可见”的特性为跨域风险防控提供了技术基础。基于区块链的风险追溯体系能够有效解决传统模式下“信息不对称、追溯成本高、证据易灭失”等痛点,构建起可信、高效、低成本的风险防控新范式^[3]。

3.4 物联网赋能的实时感知技术

物联网技术将风险感知能力延伸至物理世界的末梢,实现对人员、设备、环境状态的实时监测。边缘计算与实时采集技术将计算能力下沉至靠近数据源的网络边缘,支持毫秒级的数据采集和处理,对工业设备运行状态、环境参数、人员位置等实现连续不间断监测。设备指纹与身份认证技术为每台接入设备分配唯一标识,通过行为分析识别异常设备,防止伪造设备接入和非法控制。时空大数据分析技术将物联网采集的位置数据、轨迹数据与环境感知数据相结合,可发现异常聚集、非法入侵、危险行为等风险事件。在安全生产领域,物联网感知系统可实时监测危险源状态,一旦参数超限即自动报警并联动处置;在金融领域,物联网可监测抵押物状态、企业经营状况等物理信息,与金融数据交叉验证。建设物联网感知体系,需要统筹规划感知终端的布局,建立统一的设备接入标准和数据规范,构建安全可靠的通信网络,并配套建设智能化的分析平台,实现从“看得见”到“看得清”再到“看得远”的能力跃升。

4 穿透式风险防控体系建设的实施路径

4.1 顶层设计:构建穿透式防控的制度框架

顶层设计是穿透式风险防控体系建设的先导和保障。首先,需要完善法律法规体系,明确穿透式监管的法律地位、适用范围和权限边界,解决“谁来穿、穿什么、怎么穿”的根本问题,赋予监管部门穿透访问数据的法定权限,明确相关主体配合监管的法定义务。其次,建立跨部门协同机制,设立多部门参与的统筹协调机构,定期召开联席会议,共享风险信息,协同开展风险处置,消除“各管一段”的体制弊端。再次,制定统一的标准规范体系,包括数据标准、接口规范、风险分级标准、处置流程规范等,为体系建设提供统一的技术语言和操作准则。最后,建立激励约束与问责机制,将穿透式防控成效纳入绩效考核,对履职不到位的严肃问责,对积极探索创新的给予正向激励。顶层设计应坚持

问题导向、目标导向和结果导向相统一。

4.2 数据治理：打造统一共享的数据底座

数据是穿透式风险防控的核心资产，高质量的数据治理是体系有效运行的基石。（1）建立统一的数据标准体系，明确各类风险数据的定义、格式、编码规则和质量要求，解决数据异构问题，实现跨系统数据的语义贯通。（2）构建数据采集与质量管理机制，明确数据源主体责任，建立数据质量监控和追溯体系，确保数据的完整性、准确性、及时性和一致性，对缺失和异常数据建立补录修正流程。（3）建设数据共享交换平台，打破部门间数据壁垒，实现风险相关数据的按需共享和有序流动，遵循“最小够用”原则，严格管控数据访问权限。（4）建立数据安全与隐私保护体系，对数据进行分级分类管理，对敏感数据实施加密存储、脱敏展示、审计追踪，确保数据全生命周期安全可控。数据治理应坚持“一数一源、一源多用”原则。

4.3 系统建设：搭建智能高效的技术平台

技术平台是穿透式风险防控体系的物理载体，其建设水平直接决定体系效能。风险监测预警系统是平台的核心模块，集成大数据分析和人工智能算法，对多源数据进行实时监测和智能分析，自动识别异常模式并生成预警信号。系统应具备规则引擎与机器学习双引擎驱动能力，兼顾已知风险的快速识别和未知风险的主动发现。风险态势感知系统通过可视化技术将抽象的风险数据转化为直观的态势图景，实现风险全景“一屏统览”，支持钻取式分析，从宏观态势逐级下钻至微观详情。风险处置指挥系统实现预警信息的自动推送、处置任务的智能派发、处置进度的实时跟踪，形成“发现-研判-处置-反馈”的业务闭环，支持多方协同会商和应急指挥调度^[4]。评估反馈优化系统对体系运行效果进行持续评估，收集处置结果反馈至前端模型，形成“监测-预警-处置-评估-优化”的闭环迭代。系统建设应采用模块化、微服务架构，支持根据业务需求灵活扩展，避免“重复建设、信息孤岛”。

4.4 流程再造：实现全链条闭环管理

穿透式风险防控的核心在于实现从“被动应对”到

“主动预防”、从“分段管理”到“全链条闭环”的流程再造。风险识别流程优化，改变传统依赖人工报送和定期排查的模式，建立基于数据驱动的自动化风险扫描机制，实现7×24小时不间断监测，变“定时体检”为“实时监护”。风险评估模型建设，建立定量与定性相结合的风险评估模型，根据风险发生概率和影响程度进行综合评级，为差异化防控提供依据。评估模型应具备自学习能力，基于历史处置结果持续优化。风险预警分级处置，根据风险等级设置不同级别的预警和响应机制，低风险自动记录持续关注，中风险推送提示信息并建议关注，高风险立即触发报警并启动应急响应。处置完成后进行效果评估和案例归档，为模型优化提供经验输入。流程再造需要配套建立相应的组织架构和岗位职责，确保新流程有人执行、有人监督、有人优化。

结束语

数字化背景下，风险防控体系建设面临前所未有的挑战与机遇。穿透式风险防控通过纵向穿透层级、横向穿透壁垒、深度穿透表象，为破解风险隐蔽化、跨界化、传染化难题提供了有效路径。本文系统分析了数字化带来的风险新特征和传统防控模式的局限性，构建了穿透式风险防控的理论框架，明确了组织、制度、数据、技术四大构成要素，提出了大数据、人工智能、区块链、物联网等技术支撑体系，并从顶层设计、数据治理、系统建设、流程再造四个维度阐述了实施路径。统筹推进协同发展，方能有效应对数字化时代的风险挑战。

参考文献

- [1]陈尚聪,刘安英,胡玉环.全周期穿透式管理视角下政府采购风险防控长效机制研究[J].中国现代教育装备,2025(15):1-4,8.
- [2]杨帆.穿透式监管背景下电力企业资金链全流程管控体系构建[J].中国电子商情,2026,32(2):52-54.
- [3]王延田.基于穿透式管控的集团级制度体系建设实践路径研究——以中国能建为例[J].企业改革与管理,2025(12):6-8.
- [4]李素楠.穿透式监管背景下国有企业内部控制建设研究[J].知识经济,2026(6):62-65.