司库视角下的供应商履约风险智慧防控研究

肖宁安　毛杰　薛颖卓　张冬

摘　要：资金风险防范是大型企业司库管理的核心职能，而供应商违约风险始终是司库风险管理领域备受关注的传统难题。鉴于当下供应商履约风险防范领域存在的场景匮乏、手段不足等困境，本文运用通用人工智能大模型技术，通过拓展数据资源、设计算法模型、搭建智慧平台、强化闭环管控四项创新举措，提出构建供应商履约风险智慧化防控体系的全新工作思路，为国内大型企业提供参考与借鉴，助力企业司库管理体系更好发挥“价值守护者”的作用。

关键词：司库风险管理；客商履约风险；人工智能大模型；智慧风控；闭环管控
中图分类号：F275　**文献标志码：**A　**文章编号：**1003-286X(2025)18-0036-04

健康的供应商生态体系是大型企业的重要战略资源和核心竞争力。本文基于大型企业的司库管理视角，深入研究供应商履约风险防控的创新思路与实现路径，为企业筑牢司库风险管理安全屏障提供切实可行的解决方案。

一、业务痛点

（一）风险识别难度大

影响供应商有效履约的因素较多，并且问题往往隐藏较深，需要企业全面了解供应商的财务、业务、舆情等信息，但企业普遍缺乏深入识别此类风险的手段。部分企业订阅了第三方机构提供的客商征信评估在线服务，但存在评估方法不透明、评估内容不全面、量化指标难解释等不足，只能作为人工评价的辅助参考，实际作用比较有限。部分企业将已经出现实际履约问题的供应商列入黑名单，严控对黑名单企业的付款，这种做法属于“亡羊补牢”式防控，难以主动预判供应商的风险隐患。

（二）风控运营效率低

部分企业在付款前采用人工逐条排查风险的方式控制供应商履约风险，作业效率较低、审查时间较长，并且很难满足大型企业对资金支付的时效性要求。部分企业在司库系统的支付流程中嵌入了“黑名单止付”“关键字预警”等简单且僵化的预警规则，缺乏自动化、智能化工作手段，资金管理人员需要花费大量精力将有风险客商及时加入黑名单、无风险客商快速移出黑名单，需要调阅业务财务单据来理解付款的业务背景，从而评估付款单据出现敏感关键字带来的风险，工作强度较大。

（三）闭环控制措施少

部分企业的供应商履约风险防范存在管控滞后的问题，风险管控节点主要集中在司库的资金支付环节，未能有效前置至业务发起和财务审核阶段，这种“前端放任、末端卡控”的管理模式导致整体业务流程效率不足，容易引发基层单位的抵触。同时，部分企业的司库管理人员虽然能够识别风险并发出预警，但由于缺乏精准的风险诊断能力和协同处置机制，难以确保付款单位及时根据预警处置到位，使得风险防控的实际效果存在不

作者简介：肖宁安、毛　杰、薛颖卓，中国交通建设集团有限公司；
张　冬，国家电投集团财务有限公司。

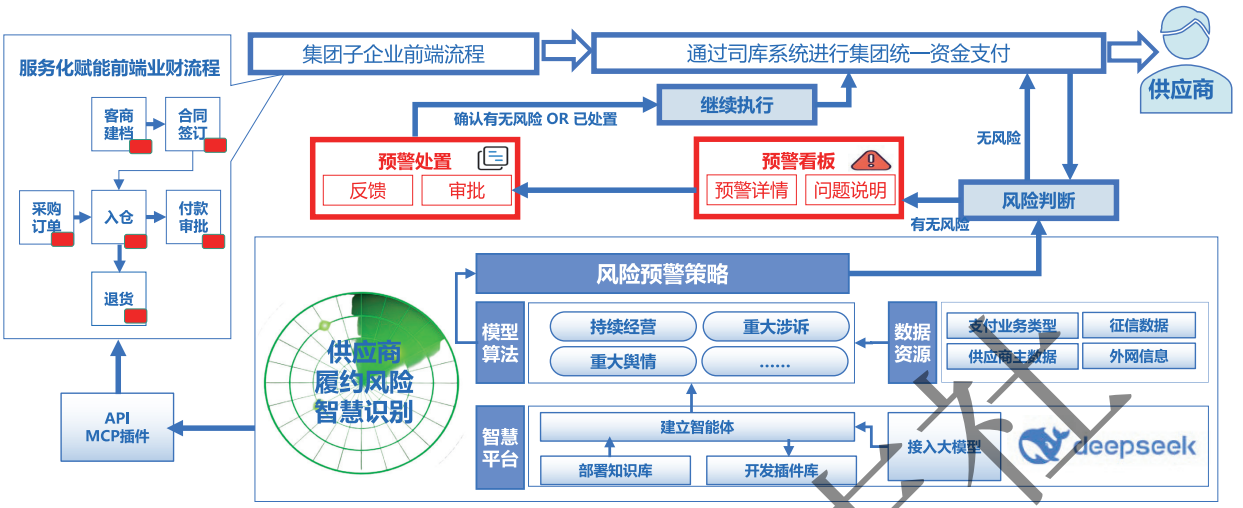

图1　供应商履约风险智慧防控方案

确定性。

二、创新方案

基于企业司库管理的实践经验和人工智能技术的研究成果，本文创新性地提出供应商履约风险的智慧化防控方案（见图1），突破传统的“人工逐项审查＋固化简单规则”的思路，通过风控理念创新和人工智能技术赋能，聚焦拓展数据资源、采用算法模型、搭建智慧平台、强化闭环管控四项创新举措，在供应商履约风险的识别精度、运营效率、控制闭环等方面实现新的突破，全面提升企业司库管理的智慧化水平与风险防控能力。

（一）拓展数据资源，从“经验依赖”进化为“数据驱动”

创新构建客商风险数据湖，从内部业财和外部生态两个角度发力，将识别供应商履约风险的依据从“依赖个人经验”进化为“数据精准驱动”。一是向企业内部业财要资源。摆脱“司库支付只能是企业内部网银”的传统思路，从上游的ERP（企业资源计划）、财务共享、客商主数据等系统获取资金支付相关的业务信息，包括付款用途、付款类型、预算科目、收款客商等重要内容，从而结合供应商的风险特征进行综合风险评估，例如，高危客商提供长周期服务项目，无履约保函的大额首付款即为高风险；高危客商提供食品原料属于高风险；高危客商提供低质保要求的普通物资，且当前付款为质保金尾款，则风险相对较低。二是向企业外部生态要资源。通过外部数据服务厂商接入社会化大数据，包含外部企业的工商注册、司法诉讼、行业评级、舆情风险、票据或债券逾期等底层数据，在企业内部进行存储，为智慧算法模型提供丰富的数据资源支持。

（二）采用算法模型，从“人工审批”进化为“算法识别”

摆脱人工逐项审批的效率局限，突破“自开发人工智能小模型”的传统思路，创新运用通用人工智能大模型技术，设计持续经营、重大涉诉、重大舆情等风险识别算法模型，加工内外部大数据，深度挖掘、量化识别影响供应商高质量履行的隐藏风险，将供应商履约风险识别的手段从人工审批进化为算法识别。

1. 设计持续经营风险算法模型。使用大模型智能分析工商注册、重要资质、财务健康等信息，为供应商赋予持续经营风险特征标签。一是读取知识库。让大模型读取供应商主数据、外部征信数据、预设提示词等本地知识库文档。二是定义重要资质。通过预设专用提示词文档，要求大模型按照供应商类型自动梳理出影响其履约能力的资质证书类型。三是执行风险评估。通过执行预设专用提示词文档，根据供应商的工商注册是否有效、重要资质证书是否有效、财务健康度是否突破红线（重点评估资产负债率、经营活动现金流净值）、税款是否拖欠等条件，要求大模型评估供应商履约风险。四是更新风险值。由大模型调用司库系统，为每家供应商自动设置或动态更新1至5级持续经营风险特征标签。

2. 设计重大涉诉风险算法模型。使用大模型自动评估企业主体和董监高人员的诉讼信息，为供应商赋予重大涉诉风险特征标签。一是读取知识库。让大模型读取供应商主数据、外部征信数据、预设提示词等本地知识库文档。二是筛选诉讼类型。通过预

组织范围	业务属性				风险特征			预警策略
	合同类型	付款类型	付款用途	关键字	持续经营	重大涉诉	重大舆情	
全部单位	原材料采购	预付10%	材料采购	……	=5	=5	>4	阻断+经办人确认
XX公司	工程服务	首付30%	工程付款	基建	=5	>4	=5	阻断+财务总监确认
……	……	……	……	……	……	……	……	……

图2　算法模型评估结果转化为预警策略规则

设专用提示词文档，要求大模型自动归纳出影响供应商履约能力的诉讼关键字，例如债务违约、破产清算、资产冻结、税务异常、偷税漏税、股权质押、合同纠纷等，暂时排除现阶段影响程度较低的劳动争议、环保处罚、商业贿赂等诉讼。三是执行风险评估。由大模型自动分析供应商的企业主体和董监高人员的诉讼信息，按照固定阈值（例如累计30项、累计涉诉金额超注册资金的10%、同比新增超40%等）或数量（同类供应商的前10名）评估供应商履约风险。四是更新风险值。由大模型调用司库系统，为每家供应商自动设置或动态更新1至5级重大涉诉风险特征标签。

3. 设计重大舆情风险算法模型。使用大模型量化评估舆情的传播范围、情感强度、影响力度、恢复难度，为供应商赋予重大舆情风险特征标签。读取知识库，让大模型读取供应商主数据、预设提示词等本地知识库文档。搜索外部媒体，通过预设专用提示词文档要求大模型自动进行联网搜索信息、社交媒体信息检索，从而获得外网的最新舆情素材。评估传播范围，使用大模型自动扫查监测负面舆情覆盖80%以上主流媒体（含境外媒体），社交媒体+行业专属媒体声量占比需要超过60%。评估情感强度，要求大模型自动评价负面情感，例如隐含情感倾向（如讽刺、隐喻等）。影响力度评估，要求大模型通过网络影响力传播模型，重点识别和评估客户维权、金融机构挤兑、监管部门调查、食品安全、质量事故等风险。恢复难度评估，要求大模型识别和评估涉事后多次声明未能平息舆论、政府协调债务重组等风险。更新风险值，根据传播范围、情感强度、影响力度、恢复难度四个象限的评估成果，由大模型调用司库系统，为每家供应商自动设置或动态更新1至5级重大舆情风险特征标签。

4. 转化形成供应商风控策略。为避免每次付款调用大模型造成的时间延迟，提升预警的可解释性，需要将算法模型对供应商的评估结果转化为结构化、灵活可配置的预警策略规则（如图2所示）。

维护预警策略规则需要在定期评估的基础上不断优化并做好个性适配。一是定期评估。考虑到大型企业供应商数量较多，可以由人工智能大模型根据合同金额、类型、活跃度对供应商进行分类评估，按照50%每日评估、30%隔日评估、其余部分每周评估的原则，动态更新供应商的风险特征标签。二是优化策略。根据预警规则的实际执行结果，通过大模型主动识别“长期未预警”“误报率大于10%”等“问题规则”，经过司库运营人员确认后进行规则更新或停用，不断提升预警精度。三是个性适配。考虑到不同业务类型、不同生命周期的基层单位的管理方式不同，将针对不同单位设置差异化的预警策略，从而适配基层单位的个性化风控需求。

（三）搭建智慧平台，从“手动筛查”进化为“无人值守”

为了让通用人工智能大模型能够安全高效地在企业内部使用，无需每次人工录入提示词即可自动按预设流程执行，具备自动调用系统接口、读取本地文档、理解专业知识的“无人值守”运行能力，需要在企业内部搭建一套适用的智慧技术底座。本文按照“接入大模型、部署知识库、建立插件库、开发智能体”的思路，为企业构建专用的智慧风控技术栈。一是接入大模型。本地化部署通用人工智能大模型，提升模型运行的稳定性和数据的安全性。同步接入低配置蒸馏模型、其他品牌通用大模型作为备用，形成多模型协同的工作机制，共同为风险算法模型提供底层强大的通用算法能力支持。二是部署知识库。通过RAG（检索增强生成）技术建立向量知识库，让人工智能大模型“回答问题前先查资料”，读取和分析业务经验、白名单、公司制度、客商名单库、风险处

置经验案例等企业内部材料，使得大模型无需“精确调优”就可以理解专业知识、吃透控制参数。三是开发插件库。基于MCP（模型上下文协议）等通用协议开发API（应用程序编程接口）插件，包括外部信息联网搜索、本地知识库调用、司库系统支付接口、客商主数据存取等，让人工智能大模型可以按需调用内外部系统接口，实现数据资源按需调用、控制策略自动嵌入。四是建立智能体。通过拖拽、设置等低代码方式建立人工智能大模型的工作流程，将各类风险识别模型转化为“有记忆、能规划、会执行”的各项具体系统功能，无需每次人工录入提示词即可自动按预设流程执行。五是完善安全机制。结合人工智能大模型对系统安全性的特殊要求，升级现有的系统安全机制，对知识库文档、API插件、智能体等多个系统对象专门设置安全权限，通过安全专用提示词对智能体的关键流程环节进行安全检查和危险操作禁止声明，从而严格防范信息泄密、越权调用、知识库投毒等安全威胁。

（四）强化闭环管控，从“人工筛查”进化为“无人值守”

通过嵌入化管控支付流程、闭环化在线预警触达、服务化赋能前端流程三类措施，实现风险的识别、预警、处置全周期无死角闭环管理。一是嵌入化管控支付流程。将智慧算法加持下的供应商风控策略嵌入到司库系统的支付流程，对每一笔支付指令进行高效率自动化筛查，一旦命中预设的风控策略，则自动化触发预警。二是闭环化在线预警触达。考虑到大型企业的多元业务、多层管理特点，集团总部难以代替基层单位处理风险。为了充分撬动基层单位的参与度和专业资源，系统自动将风险预警、问题详情、处置排查智能建议等信息形成处置工单，自动发送到相关单位的业务经办人的手机移动端。经办人进行预警确认、问题核实、误报及证明材料反馈后，经过相关单位财务领导审批，司库系统根据反馈结果自动完成资金的止付、暂停、继续执行等操作，并对预警的分布规律、算法准确性、基层单位处置时效等进行在线分析，引导集团总部和基层单位不断完善风险防范手段。三是服务化赋能前端流程。通过API或MCP插件等技术形式，司库系统将风险识别算法转化为标准化在线服务输出能力，供集团内部的ERP、供应链、财务共享等前端业财系统按需调用，司库系统动态接收前端业财系统反馈的风险确认、白名单免检等信息，从而将风险控制能力从后端的资金支付流程，向前推进至集团各单位的供应商招标竞谈、合作签约、合同履约、例行扫查等端到端业务流程环节，实现处处有控制、环环不重复。

三、未来展望

本文提出的大型企业供应商履约风险防控方案，未来还需在三个方面持续优化。一是持续优化算法识别精度。引入更多的数据资源，识别供应商背后的实控人风险，根据预警反馈信息对算法模型进行持续优化和迭代升级，不断提高算法的识别精度和准确性。二是升级构建信用风险中心。一方面，进行场景拓展。增加客户视角的信用风险评估能力，将风险管理的范围从资金支付场景逐步推广至集团各单位的客户授信、定价、催收、资产证券化评级等多个关键业务场景。通过整合供应商和客户的信用风险数据，构建起集团整体的客商画像，为企业全面的风险管理决策提供更加丰富、全面的数据支持和参考依据。另一方面，强化个性适配。紧密围绕子企业和不同业务场景的个性化要求，提供更具灵活性和差异化的算法能力和提示词参数。为部分具备条件的基层单位开发非关键参数自主控制能力，使得基层单位能够在遵循集团整体风险防控策略的前提下，根据自身的实际情况和业务特点，自主对风险评估模型进行适度调整和优化，更好地满足其个性化的风险管理需求，提升基层单位风险防控的积极性和主动性。三是赋能行业信用风险联盟。依托第三方科技企业或行业联盟机构的平台优势，积极汇聚和共享多企业的客商信用风险数据和识别算法。充分运用多方安全计算（MPC）、联邦学习（FL）等前沿的隐私计算技术，确保各企业在数据共享和合作过程中的隐私保护和信息安全，实现数据价值的最大化挖掘和利用，实现生态链视角下的合作共赢，推动行业的健康、稳定、可持续发展。

责任编辑　任宇欣

主要参考文献

[1] 方剑华，赵志刚，赖海联，等. 国家电网司库管理体系建设实践 [J]. 财务与会计，2021，(23)：23-26.

[2] 梁颐姬，李付喜. 对国有企业司库管理体系建设关键要素的思考 [J]. 产业创新研究，2024，(20)：151-153.

[3] 曾丽兰. 司库在企业资金管理中的关键作用 [J]. 今日财富，2024，(34)：101-103.