

防范电子式审计证据审计风险的建议

常启军 李婉婷 底萌妍

信息技术背景下审计职能从“以事后监督”为主向“以预测、控制、评价为主”转变。目前,在信息化审计工作建设过程中,电子式审计证据的运用仍存在一定问题。本文主要从控制风险以及检查风险为切入点,提出了大数据审计中应对以上风险的相关建议,以实现大数据审计工作整体规划和动态控制,增强审计工作的科学性和合理性,从规模导向的粗放审计向价值导向的精细化审计转变。

(一) 做好内部控制评估,防范控制风险

审计单位可以提前通过询问、观察、检查等方式了解被审计单位信息系统硬件设施配备、软件系统安装的情况。随后,加强系统流程的穿行测试,验证系统内部控制逻辑。模拟被审计单位业务,并且将该业务形成的数据投入被审计单位信息系统中进行测试,检验由被审计单位系统形成和输出的电子式审计证据是否真实有效。从信息系统流程的内部环境、风险评估、控制活动、信息与沟通、内部监督五大要素进行全方位评价。

同时,审计过程中应该重点关注电子式审计证据的增加、修改、删除、归档、审核等不相容职务授权是否存在交叉或重叠,信息系统处理电子式审计证据时不相容职务是否满足分离需求,避免因“一人多权、一人多职”影响电子式审计证据的真实与完整。

大数据审计要将系统性、多维性、动态性结合,并且要有效串联被审计

单位内部信息系统,揭示企业经营管理中的薄弱环节。实现对被审计单位财务、业务系统的可衡量安全指标进行跟踪,对异常情况深度挖掘,夯实对信息系统内部控制的实质管控。通过对被审计单位信息系统内部控制的分析,可以实现大数据审计的及时纠偏和监督优势,提高电子式审计数据的精准性,避免因被审计单位系统粗糙从源头影响电子式审计证据的质量。

(二) 提升新型专业胜任能力,降低检查风险

1. 加强审计取证,证据多维整合。运用大数据技术和云平台收集精度高、应用性强的审计证据是保证大数据审计有效实施的关键所在。要将结构化审计证据与非结构化审计证据相互关联,通过文本情感分析、语音识别、图像视频分析等技术提供更多被审计单位相关信息。例如通过被审计单位公告、财务报告、会议记录、董事会决议、合同文书、新闻报道、互联网媒体信息等,提取计算机可以识别的文本并进行情感分析;采用神经网络的语言识别功能将会议、访谈的音频转为可识别文本,通过自动处理识别存在的舞弊迹象,评估和应对舞弊风险,为审计意见发表提供支持;运用图像处理技术,从仓库监控视频中识别存货数量、质量、所有权等信息,助力传统审计的实地盘点,提升审计工作效率。

同时,向事前引导和预警、事中审计与控制延伸,做到全程动态关联

审计。运用聚类分析、关联分析、比较分析、整体趋势分析、预测分析等技术准确把握企业的发展动态,以维度体系为基础进行审计疑点分析,针对性地找出风险与问题所在。实现大数据审计证据逐步向下挖掘分析的目的,帮助审计人员按需求将海量数据进行分类管理,并有针对性地进行跟踪。大数据背景下,要实现单一审计转向整合审计、结果导向转为过程导向、事后评估转为事前预警的目标。

2. 加强关联审计,求证横向联动。电子式审计证据的取证要打破传统审计的内部边界,实现多方“联动协同、互求互证、信息共享”。仅来自于被审计单位内部信息系统的电子式审计证据可靠性不足,要发挥互联网平台、云计算技术特有优势,消除“电子式审计证据孤岛”现象。若一种电子式审计证据来源所陈述的事实与多方来源的陈述相同,则加强了审计证据的可靠性;若基于多方信号源采集的信息不尽相同,甚至出现相互矛盾或不相符的情况,就需要对异常情况重点关注、深度挖掘,夯实大数据环境下电子式审计证据的实质性管控。同时,要加强企业内部信息系统与外部供应商、客户、银行、税务局等信息系统互通互证,使企业同一业务存在多向信息流,构建良好的大数据审计软环境。联动协同可以使多方信息源互为印证,倍数增长电子式审计证据的可靠性。

3. 明确审计核心,职责专攻协同。