信息系统环境下的审计模式

杭州电子科技大学财经学院　陈静然

【摘要】本文首先介绍了信息系统环境下的新审计模式，然后从信息系统审计、系统数据审计、系统外审计三个方面对其进行具体分析，最后提出运用新审计模式需注意的事项。

【关键词】信息系统环境　信息系统审计　系统数据审计　系统外审计

财政部于2006年2月15日发布的中国注册会计师执业准则是满足时代需要的必然结果。笔者认为传统的审计模式已无法应对新的信息系统环境，必须构建新的审计模式。

一、信息系统环境下的新审计模式简介

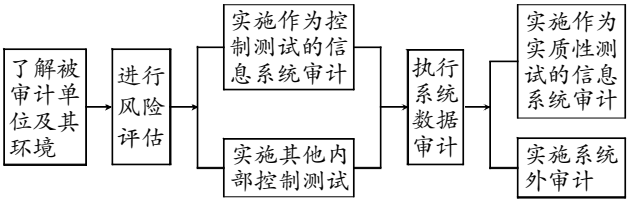
1. 三类审计程序。从内容上说，信息系统环境下的审计应分为三部分，即信息系统审计、系统数据审计和系统外审计。前两者属于依赖信息系统的审计，后者属于非依赖信息系统的审计。三者互相支持，互为补充，只有三者结合才能在信息系统环境下构筑固若金汤的审计防线。

（1）信息系统审计是对被审计单位信息系统进行审计，也称IT审计或IS审计。发达国家已在该领域作了大量的理论研究和实践，国际信息系统审计协会已经制定了信息及相关技术的控制目标。

（2）系统数据审计是面向系统中电子数据的审计，主要目的在于寻找解决问题的线索。在会计电算化和信息集成化、网络化的时代，审计针对的是数据而不仅是账套、报表、财务数据，更有大量的业务数据，有些学者认为信息系统环境下的审计本质就是数据审计。

（3）系统外审计并不直接针对信息系统，也不依赖信息系统或由信息系统产生的数据，而是用函证、盘点、观察、询问、核对、查阅等传统审计方法，对在系统数据审计或信息系统审计中确定的重点领域和发现的问题通过获取信息系统外的证据进行核实。

2. 信息系统环境下新审计模式为：



二、信息系统审计

合法的软件程序、合理的处理规则和对非法处理进行有效控制，是信息系统提供客观、完整的信息的关键要素。因此，信息系统审计的重点就是功能模块的实现与处理规则、数据流的算法与合法性、控制的执行与效率。如果能证明被审计单位信息系统的设计、运行是合法、合理且有效的，将减少系统外审计的工作。

1. 对系统软件和应用软件的测试。包括数据测试法、受控处理法、平行模拟法、程序编码检查法、程序比较法、嵌入审计程序法等。软件测试对发生额的验证较为有效，因此在审计利润表和科目借贷方发生数时应被重点运用。

2. 对信息系统内部控制的测试，通常用于控制测试。信息系统内部控制可分为一般控制和应用控制。一般控制普遍适用于某一单位的信息系统，为每一应用系统提供控制环境。一般控制审计包括：①对组织管理控制的审计；②对系统环境安全管理控制的审计；③对数据货源管理控制的审计；④对系统运行管理的审计；⑤对系统升级、更换控制的审计。应用控制从技术角度对信息系统进行控制，不同的应用系统有不同的控制要求。应用控制审计包括：①对输入控制的审计，如审核职责分工、接触控制、操作权限控制、系统的核对控制以及系统输入的程序化控制；②对处理控制的审计，如审核处理的操作控制、处理条件的检查与控制、处理结果的正确性、完整性、未被重复性控制以及错误控制；③对通信控制的审计，如审核加密通信、数字签名、确认应答与超时重传、自动纠错机制等；④对数据库控制的审计，如用户的身份确认控制、数据库的存取控制、保密控制、完整性控制、并发控制、恢复控制；⑤对输出控制的审计，如测试输出操作的控制、输出条件的检查、输出数据的正确性、完整性、安全性控制、格式控制、及时性和异常处理控制。

3. 对信息系统后台设置的审计。既可用于控制测试，也可用于实质性测试。后台设置工作不同于前台终端机操作，一般经授权后由系统维护人员在系统后台实行，内容包括业务处理的原则、步骤、各种参数、系数设置、计算模式和算法设置、数据库衔接设置、数据库修改等。被审计单位的许多会计估计和会计政策都会采取后台设置的方式实施，而这正是舞弊的重要手段之一。这种舞弊隐蔽性强，能起牵一发而动全身的功效。审计人员应检查后台设置的合法性、合理性，查阅记录后台操作、修改的计算机日志或纸质内部控制文档，询问系统维护人员，以获得相关线索。在验证截止认定时，要检查系统日期的更新情况。

进行信息系统审计时必须考虑实际运行的系统可能与测试时的系统不同。如果只在期中某段时间采用针对舞弊的系统程序,而在期末改为正常的系统,审计人员不一定能发现问题。对此,可通过对连续期间数据的仔细分析来发现异常,也可实行突击检测。把最源头最可靠的原始数据输入审计软件,以运行出的财务结果与被审计单位的账表核对,也是相对有效的检测方法。

三、系统数据审计

1. 采集数据,它是数据审计的前提和基础,具有明确的选择性、目的性和可操作性。既可从终端查询下载,也可从后台数据库直接取得。不同的目的应采取不同的取得方式。

2. 数据转换、清理和验证。数据转换不仅是语法层次的问题(即将意义相同但形式不同的数据转换成所需要的形式统一的数据),还是语义层次的问题(即要识别原始数据的含义和各个表、字段之间的关系)。数据清理和验证的目的在于去除干扰,提高数据质量,检查所采集数据的真实性、完整性。账表、账账、账证核对的机械工作主要在该阶段完成。

3. 建立审计中间表,以解决因范式分解造成的信息分裂问题,因数据日的不同造成的垃圾数据问题,因数据结构变化造成的审计分析模型难以复用问题,因利用外部关联数据引发的信息整合问题。

4. 多维分析,把握总体,锁定重点,撰写数据分析报告。多维分析的方法有切片、切块、旋转、钻取、挖掘等,以发现趋势和异常。

5. 建立个体模型,内外关联,筛选分析数据。可以利用法律规章的具体规定、数据间的勾稽关系、业务逻辑与流程、内外数据关联、审计经验和专业判断等建立个体分析模型。

6. 延伸落实,运用信息系统审计和系统外审计取证。

系统数据审计的六个步骤是一个完整的体系,不同的审计任务中可能具体运用的方法有多有少,但是没有哪个步骤可以省略。还应看到,系统数据审计主要在于分析既定结果的数据的合理性,但难以解释数据在信息系统中变化的过程。系统数据审计需要采集的三个主要数据库,具体为凭证库、科目库和期初余额库。要对这些数据进行完整性、有效性的验证,将通过审计软件运行出的报表与被审计单位的报表进行核对。但是,凭证库里的每个数据在系统中如何形成、是否被正确处理,则必须依靠信息系统审计中的软件测试来验证。

四、系统外审计

无论被审计单位信息系统是否值得信赖,审计人员都应开展系统外审计。

1. 审查从外单位取得的外部证据。信息系统数据容易被篡改,但由于被审计单位在实际业务中通常还是使用真实的凭据,因此从被审计单位的客户、供应商、银行等直接获取的证据较可靠,这些证据包括发票、对账单、收付款凭证、询证函、合同、订单等。

2. 通过盘点、观察等手段审查实物流动状况。进行信息系统舞弊所花费的人工、时间成本较低,而以操纵实物流动进行舞弊则费时费力,实务中较少见。因而,盘点实物和观察生产经营过程,能获取较可靠的证据,而不至于被信息系统中的数据迷惑。

3. 审查内部证据中被审计单位信息系统之外的证据。除非故意为之,信息系统能够做到所有电子化数据的账证、账账和账表一致。审计人员应通过各种途径获取被审计单位信息系统之外的证据(如内部管理资料、账外记录、会议记要等),并与信息系统数据核对以发现问题。

4. 应重视对普通员工的询问。普通员工往往不知道舞弊操作的背景,容易透露事情真相。而询问知情的管理层,则可能被误导并促使管理层消除有关证据。

五、运用新审计模式需注意的事项

1. 以下这类舞弊需重点依靠系统外审计来发现。如信息系统造假一条龙,即制造虚假交易或没有商业实质的交易,以及将某类交易故意按照其他类型交易处理,而一旦进入信息系统后则一切处理走正常操作程序。对这种从输入环节开始的管理层舞弊和串通舞弊,信息系统审计往往显得无能为力,只能依靠系统外审计。

2. 应特别关注信息系统中的手工处理环节。大量审计案例表明信息系统中的手工处理是进行舞弊的重要方式,因此对期中尤其是期末出现的大批或大额的手工冲销分录、不涉及具体业务的会计科目之间的转账调整分录应重点审核。另外,通过分析软件的功能模型或数据组织模型,可发现软件是否提供支持系统非法处理或违法处理的功能。如某些系统的"反记账"和"反结账"功能就能为无痕迹修改历史账表提供方便。审计人员还应关注对系统自定义功能的使用是否合理。

3. 随着审计技术的发展,三类审计程序的某些部分可能相互替代。如在电子商务环境下,传统审计中涉及的许多原始凭证就是信息系统各业务模块中的数据,因此原始凭证与记账凭证的部分核对工作可在信息系统审计中完成。再如,函证将逐渐被内外数据联网取代。系统数据审计中利用共享信息库,做到内外数据关联,从而印证被审计单位内部数据的可靠性,在相当程度上能取代函证。例如,利用从银行获取的电子数据,从税务部门获取的对方开具的发票,对照被审计单位原材料库存的电子数据,能验证应付账款的完整性和真实性。目前我国的政府审计正在大力发展联网审计,并力图将工商、税务、金融等行业信息和审计历史信息进行整合,构建一个具有丰富信息资源的审计共享信息库。

4. 新审计程序模式仍有局限性。例如仍无法有效应对故意运用不合理的会计估计这类舞弊,虽然通过对以前会计估计和相应实际数据的比较分析,能在一定程度上判别会计估计是否合理。

主要参考文献

1. 郭宗文,张红卫,胡仁昱.计算机审计.北京:清华大学出版社,2005

2. 苏运法,袁小勇,王海洪.计算机审计.北京:首都经济贸易大学出版社,2005

3. 张金城.计算机系统控制与审计.北京:北京大学出版社,2002