企业信息系统内部控制审计的发展策略

谈江辉

（三峡大学科技学院经济管理学部，湖北宜昌 443000）

【摘要】对企业信息系统内部控制的有效性和健全性进行审计是现代审计工作的新内容，信息系统内部控制审计对审计方式、审计参与者、审计环境的要求都比较特殊，也是审计适应经济发展的特殊产物。本文从审计目标和审计内容方面论述了构建企业信息系统内部控制审计框架体系的关注要点，通过案例的形式分析了实施企业信息系统内部控制审计的流程和审计重点，并在此基础上提出了完善信息系统内部控制审计的策略。

【关键词】信息系统；框架体系；内部控制审计

信息化是现代企业的普遍特征，因此对企业的信息系统进行内部控制审计是现代审计不可或缺的重要工作内容之一。内部控制是企业管理的核心工作，企业生产、销售、财务、人力、合同等各项工作的顺利进行都与内部控制的健全性和有效性密不可分，因而目前许多大型优势企业都建立起了适合本身生产经营特点的信息系统。

信息系统的稳定运行是建立在严密的内部控制制度基础之上的，对信息系统的安全、可靠、稳定等方面进行审计评价构成企业内部审计工作的新课题。对企业信息系统内部控制进行审计可以找到系统设计和运行过程中的薄弱环节进而对其进行弥补与完善，提高企业信息系统的使用效率，从而保障各项数据资料的真实性和完整性，防止非法入侵系统数据库及人为篡改数据的情况发生。这对于强化企业信息系统的运营效果，提高企业管理水平都是大有裨益的。

一、构建企业信息系统内部控制审计的框架体系

（一）框架体系的基础——企业信息系统内部控制审计的目标

1. 保障企业经营目标的顺利实现。企业的所有控制活动的目的都是保障企业经营目标的实现，对信息系统内部控制的审计也是为实现企业目标服务的。企业信息系统内部控制审计旨在通过审计促进信息系统合理、高效地运行，从而保证企业价值最大化这一经营目标的实现。所以，企业信息系统内部控制审计的框架体系的建立要始终围绕这一目标而展开，设计的审计方法和程序也应以企业目标为基础。

2. 促进企业资产安全，提高资产使用效率。企业信息系统的设计和实施是在管理层的督导下建立起来的，其目的是保证企业资产的高效使用，促使资产的保值增值。一个内部控制制度不健全的信息系统难以保证数据的安全及资产的有效利用，可能会给企业带来无法弥补的损失。所以，对企业信息系统进行内部控制审计是以促进企业资产安全及提高其使用效率为目标的。

3. 促使企业信息系统依法稳定运行。企业建立信息系统必须在法律规定的框架内合法运行，在内部控制制度的设计上也应体现法律、政策规定的主旨特点。信息系统内部控制制度的制定要体现法律思维，信息系统是企业运营的中心，各项经济活动都在这一系统中得以记录，企业经营活动的过程和成果都会依托信息系统体现出来。可见，信息系统内部控制审计体系的目标是保证企业信息系统依法稳定运行。

（二）框架体系的内容——企业信息系统内部控制审计的内容和方法

企业信息系统内部控制审计是对构成内部控制制度的各项程序和规定进行检查和评价。信息系统内部控制审计有着不同于其他内部控制审计的构成内容，如：检查企业信息系统是否建立起内部控制措施，内部控制措施的设计是否得当，各项内部控制制度是否得到有效执行，以及针对信息系统的内部控制制度设计与实施是否存在风险等。在审计实务中，可以把信息系统内部控制审计的内容分为一般控制审计及应用控制审计两大部分，两者的具体内容及审计方法详见下页表。

通过下页表可以看到，企业信息系统内部控制审计是围绕着一般控制及应用控制而进行的，内部审计人员在对信息系统内部控制实施审计之前，应做好充分的前期准备工作，通过风险评估发现关键控制点，把有限的人力安排到影响系统安全的关键控制上，通过发生频率确定抽样样本，通过穿行测试记录详细测试步骤，从而得出正确的审计结论。

信息系统内部控制审计内容及方法

审计项目		审计内容	审计方法
一般控制审计	组织规划控制审计	是否建立信息管理部门,各部门是否明确其权责,是否建立信息管理战略并定期评估风险	发放调查问卷、查阅企业制度规定
	开发变更控制审计	信息系统的开发和决策方式是否符合制度规定,生命周期中的编程设计、测试是否有控制规定,系统程序的变更流程是否有制度并遵照执行	查询变更申请单、外包服务合同等,自行开发的查阅会议记录,访谈相关人员
	安全管理控制审计	是否建立了信息系统安全管理制度,是否建立用户管理、访问认证、逻辑访问的权限认证等内控制度并认真执行	查阅用户管理台账,调取系统访问记录、用户权限变更申请单等资料,询问安全管理人员,对他们的个人能力进行评价
	运行维护控制审计	企业是否建立数据备份制度、上机培训制度,企业是否有系统的帮助平台以对数据监控和错误更正	检查数据备份是否及时完整,定期培训的实施周期。询问使用人员帮助平台是否实用
应用控制审计	输入控制审计	信息系统输入控制的授权制度是否明晰,系统是否对输入数据的合理性和完整性进行自动检测	按发生频率确定抽样规模,并进行穿行测试。例如,重复执行相同订单编号时系统的反应
	处理控制审计	信息系统数据是否得到及时正确的处理,财务、人力、采购、销售等子系统是否按照业务特点及逻辑规则设计程序,系统是否提供了自动处理的功能	检查相关记录、询问业务人员、观察操作程序、必要时重复执行。例如:高出50 000元的采购订单是否在提交前得到主管的审批,固定资产折旧是否由财务软件自动计算并生成凭证
	输出控制审计	系统数据输出是否有控制程序,对数据输出范围和期间是否设置了输出限制和审批流程,系统是否自动识别例外情况并提供更改建议,检查系统处理结果的完整性和正确性	与系统输出结果使用人员面谈,采取平行模拟方法检查系统输出控制。例如,系统是否自动生成银行存款余额调节表,采购单价及成本变动的例外报告等
	系统和数据管理接口控制审计	企业信息系统中财务、人力、销售等子系统之间的数据接口和共享设置是否正确,兼容程度是否符合监管要求	采取重复执行、物理查看等方法。例如,电子商务系统中的销售数据被编译并导入财务ERP系统中,Excel数据通过数据库导入技术导入财务系统中

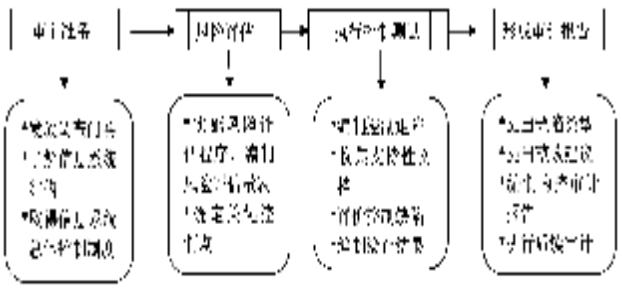
二、A公司信息系统内部控制审计的现状及存在的主要问题

(一)A公司信息系统内部控制的基本情况

A公司是我国知名的食品连锁企业,成立于20世纪80年代,产销量一直居国内领先水平,去年的产量更是达到了1 300万吨,销售收入近3亿元。A公司为总部部门及各分公司建立起了0A信息系统办公管理平台、财务用友NC网络软件、人力资源管理系统、审计信息系统等多个信息系统,使公司的资产管理、财务管理、采购管理、销售管理全部实现信息化。在此基础上,公司还建立起一系列的内部控制制度,用于规范信息系统的操作。

(二)对A公司实施信息系统内部控制审计

1. A公司信息系统内部控制审计流程图及审计重点。审计部决定对公司信息系统内部控制的设计与运行实施审计,审计部组成了有IT顾问专家参与的审计组,绘制了信息系统内部控制审计流程图如下:



A公司信息系统内控审计流程图

审计组根据A公司的生产管理情况制定了详细的调查问卷,并于审计入场前进行发放。调查问卷由三部分组成:信息系统清单,包含财务、采购、销售、人力资源等五大系统;信息系统复杂程度评估;结论。

由于信息系统自身的特点,决定了其内部控制审计的重点不在纸质的规章制度上,而在于以不同程序形式编排在操作系统中的各项控制。例如:财务用友NC系统中,对于凭证生成后的自动检查程序设定了编码的逻辑取值范围、编号重复性检查、借贷方金额相等、制单和审核人员不同等程序,用于检查输入控制中的违规操作。据此,审计组设计了内部控制审计的重点即电子数据的管理部门。由于其他业务部门的操作停留在输入层面,而系统程序和开发维护等都在数据管理部门,所以审计组设计了以数据管理部为核心、辐射其他职能部室的审计工作重点,重点对信息系统的安全性和可靠性进行评价和测试。

审计组在执行审计测试的过程中,根据关键控制点编制了控制矩阵,从信息系统的软硬件配置、数据通讯的安全加密情况、数据库的访问与修改编辑等内容着手,进行控制测试,寻找审计线索。例如,针对数据通讯的安全性能设计的测试,可以抽取一组财务会计数据进行传输,通过其他子系统的接入模块检查输入数据是否失真,是否被其他系统正确接收。对于非正常请求状态下的数据库访问,通过是否设置了密钥以及接入异常生成日志,进而对非正常访问进行持续监控,以保持系统安全。审计组

通过上述程序，对A公司信息系统内部控制做出了评价。

2. A公司信息系统内部控制存在的主要问题。审计组认为A公司信息系统内部控制的目标能够围绕企业经营目标而设定，基本保证了资产的安全性。在控制方式上，A公司对信息系统内部控制作了十六项制度规定，分别是：数据管理部与其他部门的职责权限；信息系统数据通讯制度；系统输入输出制度；数据库开发和维护制度；硬件设备管理制度等几大方面。审计组通过认真审查，提出了三个方面的缺陷认定，分别是组织规划方面、安全维护方面、应用控制方面。

首先，在组织规划方面，由于A公司在信息系统的选择方案评估过程中，没有制定统一流程和评价标准，造成公司总部及下属公司对软件的选择比较随意，公司内各系统软件的品种较多，不利于形成统一的规模化管理，产生投资浪费现象。

其次，在安全维护方面，A公司的变更管理流程设计没有控制到位。例如，A公司设计了正式的和临时的变更管理流程，但并未对其管理范围做出明确规定。由于界限模糊，相关人员大多会利用这一制度上的设计缺陷而采用限制条件较小的临时性变更措施，使系统安全受到威胁。在程序漏洞的维护方面，A公司过度依赖软件公司。例如，财务用友NC系统多次出现登录错误提示及界面乱码，由于软件公司的维修不及时，公司系统管理员又缺乏及时培训，时常造成关键报表时点登录不上系统的情况，给财务管理带来障碍。

最后，在应用控制方面，审计组认为A公司的财务轮岗制度并未得到有效实施。A公司虽然有此项制度，但在执行过程中并未认真贯彻，某些关键岗位职务长期由一人担任，存在舞弊风险。在系统输出管理控制测试中，审计组发现A公司数据输出活动日志丢失。数据库备份文件只存放于数据管理部这一个区域，不利于防范数据丢失的风险，如果发生水火灾害，则可能数据全部丢失，损失无法弥补。

三、完善信息系统内部控制审计的主要策略

1. 在审计线索的搜寻方面。信息系统审计不同于传统审计项目，由于其审计对象是各种电子数据和程序，存在瞬时性和无空间性的特点，因而其审计疑点比较隐蔽，较难发现。由于信息系统对数据的操作存在连续计算的特征，审计时很难随时中断进行控制测试，从而增加了审计线索的寻找难度。

在审计实务中，建议在软件开发设计的初期就进行充分规划，预留审计软件的数据接口，这样可以方便审计人员快速查找到审计需要的资料，迅速找到突破口。除此之外，审计人员还可以利用跟踪技术和嵌入型审计软件进行实时追踪，查找异常记录。上例中，由于A公司没有为审计软件查询信息系统预留接口，使得审计组的审计工作停留在已完成的数据处理范围，只能对存档资料及内部控制制度作出简单的评价，无法实时监督企业日常管理中的突发变动。可见，预留审计软件数据接口在系统组织设计时显得异常重要，它可以帮助信息系统审计人员得出有价值有深度的审计建议。

2. 在审计标准的制定方面。信息系统内部控制审计在我国尚处于发展的初期，在国家层面、企业层面和中介机构层面并没有一个统一的审计标准，审计实践中通常使用的是安全性、可靠性、保密性等定性标准，而这种定性的标准往往是难以准确评判的。所以，标准的缺失和模糊给审计人员造成了主观上的困难，容易形成非客观的评价结论。

我国应借鉴国际上通行的COBIT（信息与控制目标）4.1版，从信息系统的规划组织、交付与维护、获得与实践、运行监控等四个方面制定审计标准，结合我国信息系统内部审计工作的实际，完善信息系统内部控制审计的标准体系，尽早地指导审计实践工作。在设计实施细则中，也可以分为一般控制审计标准和应用控制审计标准。其中，一般控制审计标准主要是从全局的角度出发，从软硬件的配置、人员的选聘、信息系统实施方案等角度制定审计标准。应用控制审计侧重于输入和输出及处理控制标准的制定，主要围绕操作层面建立控制体系审查标准，为审计监督提供政策支持。

四、结束语

随着企业信息化进程的加快，信息化技术已渗透到企业经营管理的各个层面，其在促进企业提高效益、增强管理实力方面的作用不可小视。但由于其技术水平要求较高，管理难度也在逐渐加大，运用不当会存在一定的舞弊风险。因此如何加强监管，充分发挥其积极作用是各级管理者需面对的主要问题。随着企业对信息系统管理质量的关注，对其进行审计并评价内部控制制度的设计和实施上的缺陷是审计工作的新内容，如果从系统建设、人员培训、审计标准等方面实施改进，对今后的信息系统内部控制审计会有很大的促进作用。随着企业经营环境的不断变化，信息系统审计的内容也会与时俱进，期待着有更多审计人才加入研究行列，为信息系统内部控制审计提供宝贵建议。

主要参考文献

李莉.论企业内部控制的风险管理机制[J].企业经济，2012(3).

孙立辉.企业信息系统审计中的内部控制评价[J].审计月刊，2010(3).

岳彦斐.试论会计信息系统内部控制存在的问题和对策[J].财会审计，2011(8).

张效梅，许磊.应用BPM推进企业内部控制建设[J].商业经济，2012(6).