信息系统审计内容分析

吴沁红(博士)

(北京师范大学经济与工商管理学院 北京 100875)

【摘要】本文从信息系统构成要素、信息系统生命周期和信息系统管理三个维度入手,综合分析了信息系统的逻辑结构,构造了信息系统审计内容的基本框架,并对信息系统审计的内容与审计目标进行阐述。

【关键词】信息系统审计 审计内容 审计目标

信息系统审计在我国还是一项新型审计业务,开展这项业务,必须准确概括信息系统审计的内容。本文描述了信息系统的逻辑结构,并对信息系统审计的内容与审计目标进行了阐述。

一、信息系统的逻辑结构

信息系统是以信息基础设施为基本运行环境,由人、信息技术设备和运行规程组成,通过信息采集、传输、加工处理和存储,以企业战略竞优、提高效率为目标,支持企业高层决策、中层控制和基层运作的集成化人机系统。信息系统有其产生、发展、成熟、消亡或更新的过程,信息系统在使用过程中,随着生存环境的变化,需要不断维护、修改,当它不再适应企业发展要求时就会被淘汰,由新系统替代老系统。在信息系统的生命周期中,必须对信息系统进行严格管理与控制,并对信息系统实施审计,只有这样才能保证信息系统的有效运作。信息系统审计的对象是被审计单位的计算机信息系统。为全面分析和准确定位信息系统的审计内容,首先应全方位地了解信息系统的逻辑结构,从信息系统构成要素、信息系统生命周期和信息系统管理三个维度来描述信息系统的逻辑结构。

从信息系统构成要素来看,信息系统是由硬件平台、软件平台、应用系统、数据文件、人和运行规程组成的。其中:硬件平台和软件平台为信息系统提供了基本运行环境;信息系

2. 评估特定的管理舞弊审计风险。

(1)评估财务报表层次的重大错报风险。一般来说,公司治理结构的效率与公司战略风险、经营管理风险成反向关系。对公司治理状况的评价对于注册会计师来说也是意义重大的,因为财务报表层次的重大错报风险很大程度上源于薄弱的公司内部治理环境,合理地评价被审计单位的公司治理状况有助于注册会计师评估被审计单位财务报表层次的重大错报风险。

(2)评估各类交易、账户余额、列报认定层次的重大错报风险。管理舞弊导致各类交易、账户余额、列报认定层次的重大错报风险,必然会对上市公司的财务状况产生影响,进而带来的是财务指标的异常。在对上市公司财务指标的评价中,可将其分为盈利能力指标、营运能力指标、偿债能力等指标。

3. 应对管理舞弊导致的重大错报风险的措施。

(1)总体应对措施。①提高注册会计师的独立性和专业胜任能力。会计师事务所应当根据管理舞弊导致的重大错报风险的评估结果,分派具备相应知识和技能的人员。②在选择进一步审计程序的性质、时间和范围时,应当考虑采取下列措施:第一,对通常由于风险程度较低而不会做出测试的账户余额实施实质性程序;第二,调整实施审计程序的时间,使之有别于预期的时间安排;第三,运用不同的抽样方法;第四,对不同地理位置的多个组成部分分别实施审计程序;第五,以不预先通知的方式实施审计程序等。

(2)针对管理舞弊导致的列报认定层次重大错报风险实施的审计程序。在普通的审计程序之外,管理舞弊导向审计中还应当借鉴国外常用的延伸性审计程序:①在一日之内或近期突击盘点两次现金。②对供应商及客户进行调查,以发现虚构的供应商及客户。③对特别函证支票的二次背书进行审查。④实施管理舞弊审计询问程序。⑤对被怀疑对象财产净值的追踪分析。⑥跟踪支出分析。这种分析类似于财产净值分析,是将正常的收入同所有的支出进行比较。

(3)针对管理层凌驾于控制之上的风险实施控制。管理层凌驾于控制之上的风险属于特别风险。注册会计师针对该特别风险应当实施的审计程序包括:①测试日常会计核算过程中做出的会计分录以及为编制财务报表做出的调整分录是否恰当。②复核会计估计是否有失公允,从而是否可能产生管理舞弊导致的重大错报。③对于注意到的、超过正常经营过程或基于对被审计单位及其环境了解显得异常的重大交易,了解交易的合理性。

主要参考文献

1. 王泽霞. 论风险导向审计发展创新——管理舞弊导向审计.会计研究,2004;12

2. 赵德武,马永强.管理层舞弊、审计失败与审计模式重构——论治理系统基础审计.会计研究,2006;4

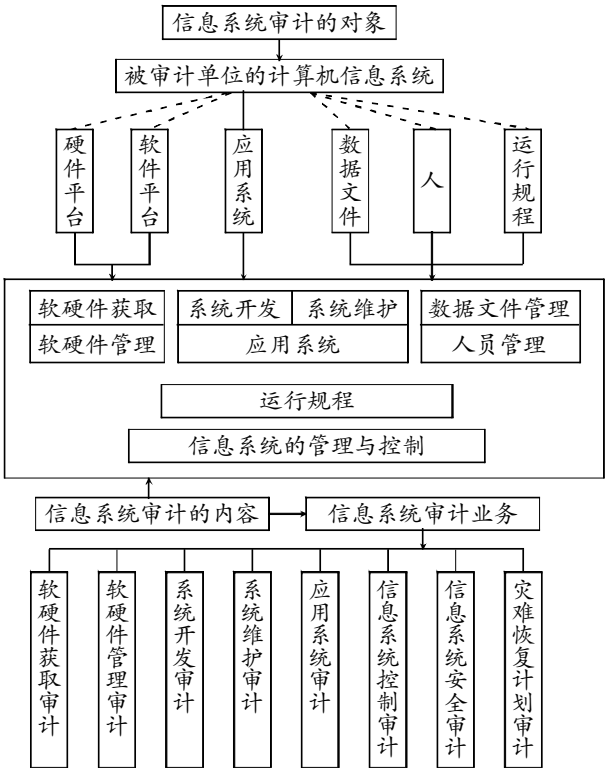
统在安装软硬件平台后，还需要选购或开发符合企业管理需求的应用系统;安装软硬件平台和应用系统后,为支持系统的日常运行,必须组织基础数据文件并将其存放到计算机中;人不仅是信息系统的组成元素,而且是信息系统使用者;运行规程规定了信息系统本身的运作规则，所有信息系统使用者都应遵守运行规程。

从信息系统生命周期来看，信息系统的生命周期可划分为系统规划、系统分析、系统设计、系统实施、系统运行和系统维护六个阶段。其中系统规划、系统分析、系统设计、系统实施这几个阶段属于系统开发阶段。

从信息系统管理来看，对信息系统的管理与控制活动伴随信息系统生命周期的始终。信息系统管理的内容包括系统规划与组织管理、系统开发管理、系统实施管理和系统日常运行管理四个方面，主要是通过一系列健全有效的规章制度和管理规程的有效执行实现的。

二、信息系统审计内容的基本框架

本文从信息系统构成要素、信息系统生命周期和信息系统管理三个维度，通过信息系统的逻辑结构综合分析信息系统审计内容的基本框架,如下图所示:



信息系统审计内容的基本框架

信息系统审计内容涵盖信息系统生命周期的各个阶段，从信息系统生命周期维度来看，信息系统审计的内容既涉及系统开发审计又涉及系统运行审计和系统维护审计。

信息系统审计的对象是被审计单位的计算机信息系统，涉及构成信息系统的各个要素，从信息系统构成要素维度来看，信息系统审计不仅要对信息系统软硬件平台的获取与管理进行审计,还要对应用系统进行审计,并对信息系统的人员管理、数据文件管理、运行规程及其执行情况进行审计。

信息系统管理不仅涉及对信息系统构成要素的管理,而且要对信息系统生命周期各个阶段进行管理，它是保证信息系统有效运行的重要条件，包括一系列管理规程和内部控制制度。从信息系统管理维度来看,信息系统审计是对信息系统各项构成要素的管理控制措施和对系统生命周期各个阶段的管理控制措施是否健全有效进行审计，也就是对信息系统的各项内部控制进行审计。在信息系统运作过程中,信息系统安全管理和灾难恢复计划是信息系统安全运行与持续运作的重要保障，因此信息系统安全审计和灾难恢复计划审计也是信息系统审计的内容。

三、信息系统审计的内容与审计目标

1. 软硬件获取审计。审计目标为:①确定被审计单位的软硬件获取政策是否合理;②确认企业是否按照相应的软硬件获取政策取得软硬件;③确认所获取的软硬件是否满足企业的需求。

2. 软硬件管理审计。审计目标为:①确定被审计单位的软硬件使用与管理政策是否合理;②确定所使用的软件是否经过授权;③确定被审计单位是否创建软硬件管理计划。

3. 系统开发审计。审计目标为:①确定各项系统开发活动是否完全遵循既定的政策与规划;②确定系统开发的各个阶段是否都经过严格审核与批准确认;③确认系统文档是否准确完整,便于审计和维护活动的开展;④确认系统实施前是否经过全面测试,而不存在重大错误和舞弊;⑤确认系统开发过程是否实施了有效的全面质量控制。

4. 系统维护审计。审计目标为:①确定是否有维护计划,系统是否按照维护计划进行了维护；②确认是否存在未经授权擅自修改或更改系统的问题；③确定维护工作是否保护了应用程序,使程序库不受非法访问;④确定系统维护后是否经过充分测试；⑤确定是否对每一次维护工作都有详细的记录,系统维护后文档资料是否及时更新。

5. 应用系统审计。审计目标为:①确定应用系统的各项处理功能是否有效；②确认应用系统的控制是否健全有效；③确认应用系统是否得到及时正确的维护。

6. 信息系统控制审计。审计目标为:①确认信息系统的各项控制措施是否健全;②确认信息系统的各项控制措施是否得到有效执行。

7. 信息系统安全审计。审计目标为:①确认被审计单位的各项信息系统安全控制措施是否健全;②确认信息系统的安全控制措施是否得到有效执行;③确认被审计单位的信息系统安全策略与程序是否能最大限度地降低信息系统的安全风险。

8. 灾难恢复计划审计。审计目标为:①确认灾难恢复计划是否适应企业的要求,灾难恢复计划的实施是否可行和有效;②确认相应资源包括数据和设备是否做好了备份;③评估异地存储及其安全性;④确认灾难恢复计划测试结果是否达到预定的目标。○