信息系统审计风险

薛富平

在信息化浪潮席卷全球的今天，信息技术在极大地促进企业创新、提升企业核心竞争力的同时，也带来了不容忽视的风险。信息系统审计是降低这一风险的有效制度与方法。比照传统审计风险概念，可以将信息系统审计风险定义为：信息系统可能有重要错误，但信息系统审计师未发现已发生的错误，并做出了错误结论的风险。美国注册会计师协会发布的第39号审计准则公告建立了审计的风险模型，将审计风险分为固有风险、控制风险和检查风险。信息系统审计风险也可以分为固有风险、控制风险和检查风险。

一、信息系统审计风险的特征和表现

1. 固有风险。是指假设不存在相关的内部控制的情况下，发生重大错误的风险。固有风险的存在与审计无关，其发生是由于企业性质和所采用信息系统的特性所决定的。主要表现在信息系统的脆弱性方面：(1)电子数据的不可见性。在磁介质上记录的数据肉眼看不到，很容易被滥用、篡改和丢失，且不留蛛丝马迹。(2)数据的大量集中和高速处理。信息系统实现的功能与系统数据都高度集中在数据中心或信息中心，一旦数据中心或信息中心遭到破坏其后果不堪设想。在高速、大量的信息处理过程中，如果出现错误或疏忽，也会立即造成巨额的损失。(3)原始数据的录入存在错漏的可能性。在信息系统处理环境中，大量的初始信息仍靠人工录入，由于数据量庞大而且分散，输入错误出现的概率比较高；(4)计算机犯罪。信息处理过程中防护措施比较薄弱，使得图谋舞弊者容易获得可乘之机。

2. 控制风险。是指有内部控制制度，但无法预防、及时发现或纠正重要错误的风险。控制风险与内部控制制度执行的有效性有关，与审计无关。主要表现在：(1)信息访问的技术性暴露。信息系统采用技术不先进、访问技术设置不充分，会引起整个系统的技术性暴露。主要表现在对网络、操作系统、数据库及应用系统四个层面的数据和软件的操作上。(2)未经授权的访问。进入信息系统的逻辑访问都有适当的访问安全级别，超范围授权就会出现未授权的访问或超权限的访问，对企业的信息资源造成人为泄露。(3)职责不分离。在企业内部虽然都制定了职责分离的有关制度，但在实践中由于人员数量的限制，往往出现一个人负责多个关键职位的情况，使内部控制实质上处于失效状态。(4)网络监控失效。对网络的广泛使用，使通过网络传输的信息很容易被窃听、追踪和非法使用。(5)信息流和业务流的不一致。信息处理和业务传递缺乏有效的控制手段，往往出现业务处理资料和系统处理数据的不一致性，可能引起企业决策失误。(6)业务流程重组。在追逐利益和效率的过程中，企业纷纷进行业务流程重组，但是很可能失去一些关键的控制环节，加大了系统运行的控制风险。

3. 检查风险。是指信息系统审计人员由于采用了不恰当的测试程序，未能发现已存在的重大错误的风险。检查风险与审计师有关，是审计师利用审计模型计算出来的，它能满足可接受的审计风险。当可接受的审计风险一定时，固有风险与控制风险越大，检查风险越高。主要表现在：(1)未能识别出系统的关键环节和重要的信息资产。如企业的销售环节，财务核算信息和数据备份等。(2)利用测试数据对系统进行测试时，很难保证恰当的程序都被检查。(3)开发模拟程序来处理生产数据以测试生产系统时，加大检查成本和时间，反而加大了检查风险。(4)系统更新换代，使得测试系统失去时效性，不仅测试没意义，而且浪费时间，误导对信息系统的审计评价。(5)参与系统开发的人员来执行信息系统的检查。在审计人员缺乏的情况下，往往出现让参与系统开发的人员来执行信息系统的检查和测试，检查风险将会很高。

二、形成信息系统审计风险的原因

1. 信息处理的虚拟化、网络化。在信息处理环境中，海量的信息都存储在磁盘或磁带上，肉眼无法看到信息处理的轨迹，也发现不了线索。而存储在磁盘上的数据很容易被修改、删除、隐匿和转移，又无明显的痕迹。信息的传递以网络的形式乾地，在传输过程中存在被窃听、篡改的可能性。

2. 捕捉证据的动态化。信息系统是一个很大的综合性的系统，每天都要进行大量的业务核算和动态分析，供管理层次决策参考。因此审计人员必须在系统处运行中进行取证，增加取证难度，也存在一定的审计风险。

3. 内控制度的复杂化。在信息系统中，特别是互联网的运用，使得企业内部控制的技术和方法发生了很大的变化，大部分控制措施都是以程序的形式建立在信息系统中，肉眼无法觉察，在很大程度上依赖于计算机处理。在实际操作中，内控环境的复杂性以及内部控制的局限性也使舞弊行为有机可乘。

4. 审计人员知识结构的单一化。实施信息系统审计，审计人员除了要有专业的审计、会计知识外，还必须掌握一定的信息系统知识和计算机应用技术。实际上，审计人员的知识结构比较单一，熟练审计和会计知识的多，懂信息技术的少，审计人员作出的审计结论有可能偏离被审计单位信息系统的实际。

三、信息系统审计风险的防范措施

综上，信息系统审计风险有其特有的表现形式，形成信息系统审计风险的原因也比较复杂。信息系统审计师在审计时，要持应有的执业谨慎，并采取适当措施，使审计风险控制在可接受的水平上。

1. 降低固有风险措施。管理层对固有风险的认识是降低固有风险的关键，所以要和被审计单位有关人员通过座谈的

强化事业单位内部会计控制制度的认识

■/刘月华

内部会计控制是指各单位为提高会计信息质量,保护资产的安全完成,确保有关法律法规和规章制度的贯彻执行等制定和实施的一系列控制方法、措施和程序。近年来,我国一系列法规性文件,对单位内部会计控制的重要性以及建立与完善单位内部会计控制制度的迫切性,都作了明确的阐述。随着市场经济的逐步完善,林业事业单位资金来源呈现出多渠道、多层次、多元化,为了确保各项资金的安全运行就必须建立一整套完整的内部监控机制,所以如何加强林业事业单位内部控制职能及其作用的认识显得尤为突出和重要。

一、建立权责明确、管理科学的单位内部控制组织体系,是实现内部会计控制的基础。

内部会计控制涉及单位内部与会计工作相关的各项经济业务,以及与这些经济业务相关的不同岗位,是会计制度。设计合理的单位内部控制的组织结构,建立不同层次的管理责任体系,是实施单位内部会计控制的基础。

(一)建立合理的单位内部控制的框架体系,并赋予其更为丰富的管理内涵。

设计合理内控组织体系,使内部会计控制工作能够深入开展,不仅约束单位内部涉及会计工作的所有人员,而且涵盖涉及会计工作的各项经济业务及相关岗位,以确保会计资

方式,充分了解被审计单位的信息化环境。通过了解识别出固有风险,制定出相应的策略和机制。一般采取的措施是:(1)加强信息资产管理。信息资产应采用表单管理,使所有的信息资产都在可控状态中。(2)强化内外部安全控制机制。对信息数据的使用和存储建立有效的控制机制,降低信息数据被滥用、篡改和丢失的可能性。(3)建立安全的运行环境。为了保护企业信息的安全传递,建立一个相对开放且安全级别较高的专用局域网,合理设置多层加密关口和防火墙。(4)加强数据输入控制。在系统设计中设定限制性输入和复核机制,保证有效数据输入准确无误。

2. 降低控制风险的措施。控制风险是由内部控制制度不健全或执行内控制度不严造成的。可以采用以下措施:(1)正确分配访问和操作权限,及时管理和维护权限分配表。用户要定期修改自己的密码,管理人员要及时删除解雇员工的权限和口令,动态监视是否有超权限访问或操作的行为。(2)建立严格的职责分离、轮岗和休假制度。职责分离,避免一个员工操作多岗位给企业带来的风险;轮岗制度最能发现一个人长期操作积累的错误和风险;休假给企业一个全面检查员工在职时有无工作弊端的机会。(3)建立安全的网络监控机制,减少来自外部的风险。一是建立外部连接的用户的身份认证机制,保证只有授权用户才可以录陆访问。二是建立强制性的路径,对使用者的终端机和网络服务器之间的路径加以控制。三是远程诊断端口的保护。

3. 降低检查风险的措施。要降低检查风险,要求审计人员在充分了解被审计单位的业务流程和信息流程的基础上有效的识别出各个风险点。主要措施有:(1)识别出重要信息资产。从管理部门索要一份详细的信息资产列表,进行分类。一是按类型归类,如分为数据与文档、书面文件、软件资产、实物资产和人员等,二是根据敏感性及重要性进行定性分级,可以分为高、中、低或其他级别。(2)确定合理的检查顺序。按重要性原则依次进行下列检查:一是对信息系统防范犯罪控制的检查;二是对信息系统实体的检查;三是对信息系统安全管理控制机制的检查;三是对数据网络安全的审查,四是对财务核算数据的核对检查。(3)改进审计手段。选择有效的审计软件和进行科学抽样,尽量减少因审计手段使用不当引起的风险。对系统进行测试时,测试技术很多,应根据审计成本和审计重要性原则选择不同的方式进行。

参考文献

[1]《CISA REVIEW MANUAL 2005》,By Marios Damianides, Michael J. Aparkinson, Information System And it And Control Association.

[2]胡克瑾著《IT审计》,电子工业出版社。

[3](美)Jack J. Champlain著《审计信息系统》(张金城,李海风等译),清华大学出版社。

[4]傅元略,庄明来著《计算机审计》,上海人民出版社。

[5]孙强,陈伟,王东红著《信息安全管理》,清华大学出版社。

[6]余玉苗主编《审计学》,清华大学出版社。

◇作者单位:审计署兰州特派办金融处

◇责任编辑:闫树北