Account information system under network environment

Internal control

浅谈网络环境下会计信息系统的内部控制

田 宏（成都 四川省电力公司物资部 610061）

摘要：本文探讨网络环境下会计电算化系统的新变化、新特点，提出相应对策，使网络会计信息系统的内部控制不断创新。

关键词：会计信息系统 会计电算化

近年来，随着计算机技术和网络通信技术的发展，网络化会计信息系统的日趋普及，在单机系统下，一方面诸如计算错误之类的技术性问题得到解决，另一方面又出现了传统手工会计系统所没有的新问题。而网络的广泛应用在很大程度上弥补了单机电算化系统的不足，使电算化会计系统的内部控制更加完善，同时也对它提出了新的要求。内部控制的作用在于促使企业有效率地达成经营目标，提供可靠的财务报表与信息，并确保一切程序符合相关的法令与规章。就网络环境而言，企业交易的处理与相关作业程序都必须依赖良好的计算机信息系统，因此信息系统内部控制的好坏，将直接影响企业的营运与发展。本文将结合作者的实践经验探讨网络环境下会计电算化系统的新变化、新特点，并提出相应对策，使网络会计信息系统的内部控制体系不断创新。

1 单机会计电算化系统中内部控制的缺陷

由于计算机具有工作自动化、控制程序化、存储数字化等特点，传统的单机电算化系统在提高会计工作效率的同时也带来了内部控制上的新问题，具体表现在：

(1) 会计业务缺乏有效牵制。由于计算机的自动高效使工作人员减少，各种手续都被合并到一起由计算机统一执行，从而不能像手工方式那样相互牵制，成为内控隐患。

(2) 电算化系统的主体是计算机软件，因此其内部控制也更加依赖于程序的质量。一旦程序中存在严重的问题，便会危害系统安全。而会计人员对计算机专业知识所知较少，很难及时发现这些漏洞，致使系统会多次重复同一错误，扩大损失。这也是手工会计系统不会遇到的问题。

(3) 电算化系统下权限分工的主要形式是口令授权。口令存放于计算机系统内而不是像印章那样锁在箱子里或带在主人身上，因此一旦被人偷看到或窃取到便会带来隐患。

以上几点是单机电算化会计系统在内控方面的主要问题。它们是由电算化系统自身特点所决定的，在单机系统下只能通过加强人员教育等方式进行预防，难以彻底解决。

2 网络技术的发展对电算化会计系统内部控制的影响

(1) 网络构成要素的复杂性使得系统安全控制的难度加大。计算机硬件、软件、人员和各种规程等构成各种网络组织的基本要素，由于硬件配置不合理、软件功能欠完善、系统操作失误、内部管理人员的非法访问及来自外部的恶意攻击等原因，网络组织的各个层面临着严重的安全威胁。错综复杂的网络结构使得系统安全问题日益突出，安全控制的难度将进一步加大。

(2) 网络数据处理的集中性使得传统的组织控制功能减弱，网络的应用大大减少了人工输入环节，数据访问和数据交换都通过应用服务器进行。网络计算机集成化处理促使传统手工会计中制单、复核、记帐等不相容岗位相互牵制制度的效力逐步削弱，传统的组织控制功能弱化。

(3) 网络环境的开放性使得会计信息失真的风险加剧。从信息的取得渠道看，其来源具有多样性，有可能导致审计线索紊乱；从信息传递的方式看，大量信息通过网络通信线路传输，有可能遭受非法的拦截、窃取和篡改；从信息的存储形式看，信息大都以电子数据的形式存储，肉眼难辨认，易被修改、删除、隐匿、转移和伪造且不留痕迹。网络系统的开放性和动态性加大了审计取证难度，加剧了会计信息失真的风险。

3 网络会计系统内部控制的主要内容及其对策

3.1 组织与管理控制

(1) 适当的职责分离。这就是设置网络管理中心，由网管中心全盘规划，合理布局，采取措施确保各工作站、终端和人员之间适当的职责分离；

(2) 优化配置人力资源。良好的人力资源管理政策对于企业内部控制的顺利实施起着关键性的作用。因此要制定措施，确保人力资源的合理利用；

(3) 发挥内部审计的作用。通过内部审计部门对网络会计系统信息的质量和完整性进行独立和公正地监督与评价，有利于系统内部自我约束、自我激励机制的建立与健全。

3.2 系统开发控制

系统开发控制是为保证网络会计系统开发过程中各项活动的合法性和有效性而设计的控制措施，它应贯穿于系统规则、系统分析、系统设计、系统实施和系统运行测试与维护的各个阶段。其主要内容包括如下：

(1) 明确开发目标，制定项目管理计划，进行项目的可行性研究与分析；控制开发进度，监督开发质量，检查各功能模块设置的合理性及程序设计的可靠性，提高系统的可审性。

(2) 利用网络在线测试的功能，检验整个系统的完整性，并应对非法数据的容错能力、系统抗干扰能力和发生突发事件的应变能力以及系统遭遇破坏后的恢复能力进行重点测试；做好人员和设备等资源的整合配置以及初始数据的安全导入，保证新旧系统的转换有序进行。

(3) 一旦发现网络系统各类软件可能存在安全漏洞，应立即进行在线修补与升级，并将所有与软件修改有关的记录报告及时存储归档。

3.3 日常操作系统管理控制

(1) 制定上机操作规程。主要包括软硬件操作规程、作业运行规程和用机时间记录规程等。

(2) 加强系统人员的操作管理。人作为系统主体是网络发展的基本动力和信息安全的最终防线，人员操作管理的重点是权限控制。系统管理员被赋予超级用户管理权限，主要负责系统硬、软件的管理维护和网络资源分配，操作人员应按照被授予的权限严格作业，不得越权接触系统，以避免人为因素或操作不当给操作系统带来不必要的损失和风险。

(3) 建立计算机资源访问授权和身份认证制度。即明确每个用户的安全级别和身份标识，并分别定义具体的访问对象。

(4) 建立安全稽核机制。对系统操作的事件类型、用户身份、操作时间、系统参数和状态以及系统敏感资源进行实时监控和记录，进行必要的权限设置，以便能够对各种不同的权限进行用户识别和远程请求识别。

(5) 设置安全检测预警系统，实时响应和报警，阻断非法的网络连接，对事件涉及的系统实施进一步跟踪，创造一种漏洞检测与实时监控相结合的安全模式。

3.4 网络系统安全控制

(1) 硬件设备安全控制。硬件设备安全主要涉及计算机机房环境和设备的技术安全要求。应制定网络计算机机房和设备和管理制度、岗位职责和操作规程，严格禁止无关人员接触系统，专机专用；计算机机房应充分满足防火、防潮、防尘、防磁和防辐射及恒温等技术要求，关键性的硬件设备可采用双系统备份。

(2) 系统软件安全控制。严格控制系统软件的安装与修改，对系统软件进行定期的预防性检查，系统被破坏时，要求系统软件具备紧急响应、强制备份、快速重构和快速恢复的功能。

(3) 系统入侵防范控制。为了防止非法用户对网络会计系统的入侵，应采取设置防火墙，身份认证和授权管理等安全技术，用以限制外界对主机操作系统的访问；用以隔离开局应用系统与外界访问区域之间的联系，限制外界穿过访问区域对网络应用系统服务器尤其是对会计数据库系统的非法访问；加强原有的基于帐户和口令的控制，提供授权访问控制和用户身份识别。

4 结束语

综上所述，随着网络技术的逐渐成熟与完善，会计信息系统的内部控制体系将发生深刻的变化。只有清楚地意识到这些变化，才能适应社会的发展，建立完备的、崭新的会计体系。会计专业人员如何体察此种趋势，培养相关的能力，发挥专业服务功能，应是值得重视的课题。