会计信息化环境下的会计风险及其防范

文/祝学明

几年来，随着经济的发展，现代信息技术的发展和应用超出了常规的想象。然而，就在会计实现电算化的同时，风险也在不断加大，经济犯罪频繁发生，会计领域的计算机犯罪案件也呈上升趋势，犯罪分子可以在短短一、两年甚至几个月，就侵吞国家财产几百万、几千万，给国家，单位资产造成了巨大的损失。会计电算化面临主要的风险来自何方呢？如何防范呢？可归结为以下几点：

一、财务软件配置中存在的风险及防范

财务软件配置是会计电算化信息系统建立的重要环节。目前的配置方法主要有两种：一是购买，二是开发。这项工作的好坏将直接影响电算化的开展质量，对会计信息的真实与否也起着重要作用。在实际配置中安全隐患随处可见。

1、购买方式

目前许多单位包括高校在购买软件时，往往喜欢买最先进的产品，而忽视了单位自身的情况和需要。现在的软件市场上新概念很多，如网络财务软件、会计信息化软件、在线财务软件、会计决策软件等，这种只听冠名追求高档而忽视软件配置的基本要求的做法，一方面不符合最佳效率原则的要求，导致资源浪费。另一方面往往带来软件适应性差，初始参数设置难度大，软件运行环境要求高，操作复杂，对会计人员技术要求高等问题，稍有闪失，安全系数会大大降低。故单位在购买财务软件推行电算化时，应该重点注意：该软件必须通过有关机构的评审，软件的技术指标应满足企业的需求，符合企业特殊核算的要求和行业特性以及发展的需要，能保证会计数据安全可靠，不易被破坏和泄密，操作方便，通俗易懂，简单好学，售后服务好，能及时提供日常维护、版本升级和软件再开发。

2、开发方式

不管是自行开发、委托开发或是联合开发，大多数单位都是采用生命周期法。这种方法将软件工程学和系统工程的理论和方法引入软件配制开发中，将软件开发的全过程视为一个生命周期，严格地划分为系统调查、系统分析、系统设计、系统程序、系统测试、系统运行与维护六个阶段，使软件开发分阶段分步骤地进行，强调软件开发的全过程。由于这种方法结构严谨，逻辑性强，技术要求高，实际研制中常出现一些致命问题：系统分析和设计人员不能充分了解系统状况和用户需求，可行性分析报告不符合实际，数据流程图混乱，输入与输出信息模糊不清，文件调查表不够具体，软件需求说明书不全面，程序设计说明书不清晰，系统测度不完整，程序错误不能及时发现，对系统开发工作不能有效地组织和控制等，直接导致开发出的软件质量下降，安全系数降低。要解决上述问题，系统开发人员必须充分熟悉生命周期法的基本步骤，并严格分阶段、分步骤进行，同时要明确规定每个阶段的任务、原则、方法、工具和形成的文档资料，开发人员之间要相互沟通，保证每个阶段之间相互协调。

二、实际操作中存在的风险及防范

会计软件都有一套相对完整的授权、审批和密码保护功能，充分发挥它的作用，可以让我们在公布信息的同时较好地保护会计系统。但有些单位却把SYSTEM的密码在财务内部公开，这是一种非常危险的做法。如果他们的会计信息网络化的公开了，那么任何人都可以通过SYSTEM用户来控制会计网络系统，会计信息无限制地被浏览已是“小事”，更严重的是破坏科目体系和对账数据，使系统瘫痪。还有一种情况就是操作员之间相互公开自己的密码，相互无原则的信任，而信息会随着人与人之间的交流而传播，所以很难免不会把这些密码告诉非操作人员，这也会造成会计信息的无限制被浏览、丢失等情况。另外还有因操作制度不完善，权限管理不严密，安全措施不全面，缺乏有效的监督而导致玩忽职守的现象时有发生。防止因操作不当带来的安全隐患，重要的是做好以下工作：要保护计算机设备，防止各种非法指定人员操作计算机及财务软件，保证机内的程序和数据的安全；明确规定上机操作人员对会计软件的操作工作内容和权限，对操作密码要严格管理，定期更换操作员的密码；密码是限制操作权限，检查操作人员身份的一道防线，管理好每个人的密码，对整个系统的安全事关重要。杜绝未经授权人员操作会计软件，防止会计人员越权使用软件操作人员离开机器时，应执行相应的命令退出会计软件，否则密码的防线就会失去作用，会给无关人员操作留下机会；根据单位的实际情况，由专人保存上机操作记录，记录操作人、操作时间、操作内容等并与软件中的“日志管理”相比较，开展日志审计。

三、计算机维护过程中存在的风险及防范

由于计算机技术的迅速发展，利用计算机技术进行犯罪已具有智能化、隐蔽化，发现问题不易查找线索等几个特征，其技术手段也高于防范措施。如国际上虽已广泛采用各种技术防止外部攻击，但黑客、病毒的入侵仍屡屡得逞。全球著名的雅虎等五大网站普遍连续受到黑客攻击，迫使网站停止服务数小时，使企业受到巨大损失。故对那些用会计系统服务器或工作站连接Internet的企业来说，病毒通过互联网和电子邮件入侵会计系统的可能性更大，而会计网络里工作站之间共享功能的开放，为病毒在网络里传播又提供了通道，一旦病毒发作，后果将是很严重的。再加上维护人员缺乏必要的防范意识和措施，对利用计算机犯罪知之甚少，相应的控制措施不多，安全隐患更大。尽管防范上述问题的难度很大，但只要措施得力，仍能保证其尽可能少的发生隐患。单机系统和多机分散系统电算化的单位应尽量做到：系统使用的计算机是专用的，尽量不从事与会计无关的工作，杜绝在财务专用计算机上安装游戏软件；避免使用来路不明的软盘和各种非法拷贝的软件，尽量减少使用软盘的次数，不得以而使用软盘，要先杀毒再使用；系统最好安装上具有高效实时临控功能的防毒软件如KV3000、瑞星等，安装到每台机器上，建立可靠的防护网。网络系统电算化的单位要使用防火墙软件，防火墙是建立在被保护网络周边，分隔被保护网络与外部网络的一种技术手段。为防止社会不法分子对单位内联网的非法进入，可以根据网络系统区域划分的不同，设置多级防火墙。一般分为两类，一类是外层防火墙，用来限制外界对主机操作系统的访问；另一类是应用级防火墙，用来逻辑隔离会计应用系统与外部访问区域间的联系，限制外界穿透防火墙对会计数据库的非法访问。同时也要安装具有高效实时监控功能的防毒软件。

四、会计档案管理过程中存在的风险及防范

会计档案在收集过程中，由于操作人员时间观念不强，没有定期把计算机系统中的所有会议资料备份到磁性介质或光盘上，没有脱离原计算机系统进行保存。一旦因意外或人为错误造成数据丢失或系统被破坏，就不能在最短时间、最小损失下恢复原有的会计资料，电算化系统不能正常工作。会计档案在保管过程中，操作员往往是单备份保存，且保存在电算化系统附近，一旦发生意外，后果不堪设想。又因档案保管人员缺乏必要的物理知识，不懂磁性介质的物理特性，将之接近磁场，备份资料瞬间消失。

正确的做法是：按照财政部颁布的《会计电算化管理办法》的规定，实现会计电算化的单位只要发生新的经济业务，内容经过电算化账务处理后，就应坚持每天备份且要双重备份，即“AB备份法”进行资料的备份，并且备份盘上要注明形成档案时的时间与操作员姓名，同时要分处、分人保管，以防意外事件导致整体资料系统的毁灭与不可恢复性。由于光盘的安全性强、容量大，故备份盘要尽量使用光盘。备份盘应远离磁场，注意“七防”，还应定期进行检查、复制，防止由于磁性介质的破坏而使会计档案丢失，造成无法挽救的损失。经领导同意借阅的会计档案，应严格履行相应的借阅手续，经手人必须签字记录。存放在磁性介质上的会计资料借阅归还时，要做杀毒处理，防止病毒感染。

总之，随着计算机技术的发展，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。近年来，单位利用互联网推广电子商务，已成为全球性商业发展的重要趋势之一。专业人员如何体察此种趋势，培养相关的能力，以掌握饥会，发挥专业服务功能，是值得重视的课题，从内部稽核及外部审计的角度，探讨网络技术对于单位交易处理流程及内部控制制度的冲击与影响具有深远意义（作者单位：南昌大学计划财务处）

相关链接

完善社会信用制度构建和谐文明社会
会计信息化环境下的会计风险及其防范
国际海运中无船承运人提单风险防范研究
刍议会计信息、成本效益不对称引起的信息失真
FIDIC合同条件在中国法律体系下的应用研究

地址：北京市朝阳区关东店甲1号106室 邮编：100020 电话/传真：（010）65015547/ 65015546

制作单位：集团经济研究网络中心