加强信息系统审计风险控制的若干思考

金治中

伴随着信息技术的快速发展，信息系统审计概念也在不断地被深化。作为审计的一个重要分支，信息系统审计的风险理应与传统审计风险一样受到重视。

一、信息系统审计风险的定义

信息系统审计风险目前还没有明确的定义，对其初步的定义一般是借鉴审计风险的概念。对于审计风险的解释，目前国内外主要有以下几种说法：

新修订的《国际审计准则第200号——财务报表审计的目标和一般原则》(ISA200)认为，审计风险是当财务报表存在重大错报时，审计人员发表了不恰当审计意见的可能性。美国注册会计师协会(AICPA)将审计风险定义为：审计风险是指审计人员针对含有实质性错误陈述(或重大错误陈述)的财务报表发布不恰当审计意见的风险，审计风险由固有风险、控制风险与检查风险组成。加拿大特许会计师协会(CICA)指出，审计风险就是审计程序没有发现重大错误的风险。我国注册会计师《独立审计具体准则第9号——内部控制与审计风险》指出：审计风险是会计报表存在重大错报或漏报，而注册会计师审计后发表不适当审计意见的可能性。

虽然这些定义是从不同角度对审计风险进行解读，但仔细分析会发现这些定义中有某种共同之处：审计风险是财务报表没有公允地揭示企业实际状况，但审计人员经过审计后得出了相反的观点，致使审计意见失当的风险。这里的要义表现在，首先，审计风险的根本来源是审计人员不恰当的审计行为；其次，导致审计风险的最基本的原因是审计人员发表的不恰当的审计意见；最后，审计主体的损失是一种还没有出现的潜在威胁，还不是一种现实发生的结果。据此，可以结合信息系统审计的目标推导出信息系统审计风险的相关定义，即信息系统审计风险是在IT环境下，信息系统的有效性、可靠性、安全性存在严重的漏洞，而信息系统审计人员实施相关审计后，由于发表了不恰当的审计意见，致使审计主体在特定的经济环境下遭受损失的可能性。

二、信息系统审计风险未被重视的原因分析

一是从审计结果的最终受众来看。财务审计报告的使用者常与利益相关者相联系，包括投资者、债权人、政府、银行等。各种利益群体都会从各自的角度出发理解和密切关注自己的利益。根据“深口袋理论”，大多数审计案件起诉的原因是由于企业经营失败，受到损失的投资者只希望从审计人员那里获得更多的赔偿，而不管审计人员在审计中是否遵循了公认的审计准则，这种广泛的直接或间接的利益关注容易引起更多的风险。而信息系统审计报告常与用户相联系，这从日本通产省对IT审计的定义可以看出：IT审计是指为了信息系统的安全、可靠与有效，由独立于审计对象的IT审计师，以第三方的客观立场对以计算机为核心的信息系统进行综合的检查与评价，向IT审计对象的最高领导提出问题与建议的一连串的活动。这项定义比较明确地提出了审计报告的使用对象——最高领导者，即信息系统审计报告的使用者仅局限在用户的高层，而无论是总经理还是董事会，都不会涉及太多的利益群体，所以引发的风险相对较小。

二是从信息系统审计所处的位置来分析。先有信息系统建设，再有信息系统运行。由于信息系统初始建设成本巨大，一旦建设失败，将会给企业造成巨大的损失，因此，为保障信息系统的顺利建设，我国建立了信息系统工程监理制度。然而，由于过分重视系统建设环节，以致忽视了对系统运行环节应有的关注，也导致了对信息系统审计师工作进行规范的相关制度和管理办法几近缺失的局面。这种对信息系

统重建设、轻管理的状况说明对信息系统审计风险的认识还存在很大的不足。

三是从信息系统审计和财务审计的关系来看。在审计实践中，目前大多数还是采用与财务审计相结合的组织方式对信息系统进行审计，其重点关注的是信息系统及相应模块处理得是否正确、合法，功能是否完备，内部控制是否健全有效以及是否为实现被审计单位的目标服务。此时，信息系统审计是财务审计中的一个环节，信息系统审计的所有风险已归属于财务审计风险之中，从而容易导致在审计中只看到财务审计风险，而忽视信息系统审计风险的存在。

三、加强信息系统审计风险控制的措施

关于风险控制，巴鲁克•费什霍夫(B. Fischhoff)提出，首先是预防那些可能引起不利后果的事件发生，其次是在事件发生后要积极预防其后果，最后是当事件及其结果都发生时应尽量减轻损失。具体到信息系统审计风险，笔者借鉴这三种策略，特别是第一种风险控制策略，提出了加强信息系统审计风险控制的若干措施。

(一) 选派恰当的审计人员

选派恰当的、具有执业能力的审计人员是防范风险的重要措施之一。信息系统审计人员的执业能力、业务素质在很大程度上决定着审计项目的质量，这使得选派适当的信息系统审计人员具有重要的意义。笔者认为，在选派适当的审计人员时应重点关注以下几个方面：首先是审计人员的独立性。信息系统审计人员的独立性是保障信息系统审计质量、控制信息系统审计风险的基础。其次，选派的信息系统审计人员应该具有完成审计工作任务的技术能力，并保持职业所要求的谨慎性，这一点能够直接影响信息系统审计业务的质量。最后，信息系统审计小组的各个成员需要具备良好的合作精神与协调能力，以便保证信息系统审计业务按要求及时完成。

(二) 强化信息系统审计风险控制意识

信息系统审计所要求的技术比较复杂，因此审计人员可能会有意避开技术问题，仍然热衷于传统的财务手段，加之公众最关心的仍是财务数据，这也导致了各种利益主体难以对信息系统审计风险形成一致的认识。另外，当前我国在信息系统审计中重大失败的案例比较鲜见，容易让人忽视信息系统审计风险的存在。并且，由于信息系统审计并不是一项强制性的审计，且在我国开展的时间也还不长，许多企业和审计主体对信息系统审计的重要性还没有充分的认识，对信息系统审计风险的认识就更加不足了。随着IT技术的快速发展，信息系统审计的风险将会逐步加大，因此，必须加大对信息系统审计及其风险的宣传力度，让更多的经营管理者特别是企业高级管理层，从企业战略发展的角度来重新认识信息系统审计的重要意义，进而推动相关工作的顺利开展。

(三) 加快建立信息系统审计准则体系

当前国际上通用的信息系统审计准则是国际信息系统审计协会(ISACA)发布的信息系统审计准则，包括审计准则、审计指南和审计程序三个层次的内容。国际会计师联合会(IFAC)也制定了《国际审计准则第401号——在计算机信息系统环境下审计》等规范。此外，国际内部审计师协会(IIA)发布了全球信息技术审计指南，美国、英国等发达国家也分别制定了自己的相关准则。我国现有的独立审计准则不能满足信息系统审计的需要，还不能对信息系统审计人员的执业行为进行规范，因而加大力度制定适合我国国情的信息系统审计标准、指南、程序显得尤为迫切。我们应以国外现有的信息系统审计理论和方法为基础，积极借鉴其较为先进的信息系统实践经验，努力探索适合我国国情的的信息系统审计原则和方法，制定符合我国国情的信息系统审计准则体系，从而为规范我国信息系统审计业务、降低信息系统审计风险提供保障。

(四) 建立信息系统审计组织机构

建立专门的信息系统审计组织机构，主要目的在于能够有效地管理信息系统审计师行业。ISACA、IFAC、IIA这些组织虽属于非盈利性的民间组织，但由于其非常契合主要发起国的政权组织结构和文化，所以运作很有效率。相比之下，我国是政府主导型的国家，在重大事务方面需要由政府组建的官方机构进行处理，才能形成足够的权威，解决问题才比较有效率。因此，笔者认为我国应在国家审计署领导下成立专门的信息系统审计研究中心，负责对信息系统审计标准、操作指南、职业规范体系进行研究。为了减少信息系统审计执业风险，我国还应尽快建立专门的信息系统审计组织机构。这不仅在宏观上会对我国信息系统审计工作起到重要的监督和指导作用，在微观上也将有利于信息系统审计风险的控制。■

(作者单位：厦门大学管理学院会计系)

责任编辑 李 卓

参考文献

1.朱小平，叶友.2003."审计风险"概念体系的比较与分析.审计与经济研究，5

2.戴佳君，张奇峰.2009.审计风险研究综述，上海立信会计学院学报，6

3.胡晓明.2007.风险导向信息系统审计及其发展思路.经济管理，2