审计·IT审计

网络环境下信息系统审计的职能与类型

陈 耿

(南京审计学院 信息科学学院, 江苏 南京 211815)

[摘 要]最近十年,信息系统审计在企业管理中的职能与地位都产生了质的飞跃:企业的生存与发展越来越依赖信息系统,而电子商务对企业经营管理又造成一定的潜在风险,信息系统审计成为外部审计不可或缺的一环,同时它也成为内部控制的主要参与者。现代信息系统审计应当包括真实性审计、安全性审计和绩效审计三种基本类型,它们都有各自的具体目标。

[关键词]信息系统审计;IT审计;真实性审计;安全性审计;绩效审计;电子商务;电子数据处理;计算机审计

[中图分类号]F239.1 [文献标识码]A [文章编号]1672-8750(2012)01-0045-06

一、引言

信息系统审计最早可以追溯到20世纪60年代,当时称为电子数据处理(Electronic Data Processing,EDP)审计,主要针对财务软件中的数据进行审计。美国执业会计师协会于1968年出版了《电子数据处理系统与审计》,次年在洛杉矶成立了电子数据处理审计师协会(Electronic Data Processing Auditor Association, EDPAA),1994年,电子数据处理审计师协会更名为信息系统审计与控制协会(Information System Audit and Control Association,ISACA),电子数据处理审计也改为信息系统审计(Information System Audit,ISA),审计的内容从电子财务数据审核拓展到整个信息系统本身。当时企业的信息系统都是一个个的"信息孤岛",没有来自外部的威胁,因此信息系统审计在企业管理中职能和作用仍然是相当有限的。

石勇等分析了网络环境下政府信息系统审计,认为网络环境不仅对政府信息系统审计,而且对社会信息系统审计、企业内部信息系统审计都产生了巨大影响[1]。互联网导致现代意义上的信息系统审计的产生,信息系统审计的外延大大拓展,其内涵也越来越丰富,从而极大地提升了信息系统审计在企业管理中的作用,改变了其与财务审计之间的关系[2]。许多研究者常常分不清计算机审计与信息系统审计的区别,这不利于信息系统审计研究的开展。庄明来认为,无论是产生与发展,还是基本概念、审计目标、审计内容,抑或是适用准则与采用的审计技术,二者都有着很大的区别,它们在我国审计发展过程中都有自己特定的地位与作用[3]。本文从分析网络对信息系统审计的影响入手,阐述信息系统审计的内涵,以期真正将二者区分开。

[收稿日期]2011-07-07

[基金项目]国家自然科学基金(70971067);江苏省"六大人才高峰"项目(2007148);江苏省高校自然科学重大基础研究项目(08KJA520001)

[作者简介]陈耿(1965—),男,江苏无锡人,南京审计学院信息科学学院副院长,教授,博士,主要研究方向为信息系统审计。

二、信息系统审计的职能和地位

（一）企业的生存与发展越来越依赖信息系统

与“信息孤岛”时期的信息系统在企业经营管理活动中的作用完全不同，在互联网时代，企业的经营管理活动越来越依靠信息系统，信息系统的安全与可靠也越来越重要，企业信息系统的安全问题已经不仅仅关系到企业的生存与发展，而且更关系到国家经济的安全。

由财政部会同证监会、审计署、银监会、保监会联合发布的《企业内部控制基本规范》之《企业内部控制应用指引第 18 号——信息系统》中明确指出，现代企业的运营越来越依赖信息系统[4]。比如航空公司的网上订票系统、银行的资金实时结算系统等，如果没有信息系统的支撑，业务开展就将举步维艰、难以为继；还有一些新兴产业，其商业模式完全依赖于信息系统，如新浪、网易、百度等各种网络公司，阿里巴巴和卓越等各种电子商务公司，假如没有信息系统，这些企业将失去生存的空间。

据 Gartner Group 公司的调查，在经历大型灾难而导致信息系统停运的企业中，至少有 40% 的公司再也没有恢复运营，而剩下的企业中，也有三分之一在两年内破产。英国特许管理协会关于企业危机事件的调查显示，企业最普遍面对的危机事件中失去信息系统位居第一。由此可见，企业的业务已经越来越多地依赖于信息系统，信息系统审计的重要性也越来越突出。

（二）保护网络环境下企业的信息资产和信息系统安全

20 世纪末，互联网技术迅速普及，电子商务彻底改变了企业信息系统的“孤岛”状况，企业在享受电子商务的便捷、高效、低成本的同时，负面影响也不断显现，比如一个病毒可以使远隔千里的企业遭殃[5]。这时候，我们才发现企业的经营风险不仅仅来自传统市场风险、金融风险、技术风险、自然灾害等，互联网也成为企业经营风险的重要来源之一。

《2009 年中国计算机病毒疫情调查技术分析报告》显示，2009 年计算机病毒感染率为 70.51%，较 2008 年有所下降，但仍然维持在比较高的水平，其中多次感染病毒的比率为 42.71%[6]。这种情况与我国计算机病毒主要以木马病毒为主有关。潜伏性、隐蔽性是木马病毒的特征，病毒制造者和传播者在巨大利益的驱使下，或利用木马病毒技术进行网络盗窃、网络诈骗，或通过互联网贩卖病毒和木马。这些形式的网络犯罪活动明显增多，严重威胁企业信息系统安全，制约了企业业务的健康发展。

密码和账号被盗、受到远程控制、系统（网络）无法使用、浏览器配置被修改是计算机病毒造成的主要破坏后果。其中，“密码、账号被盗”选项是自 2006 年以后病毒破坏性调查新增加的项目，以更准确地反映病毒破坏性的变化情况。调查结果显示，用户密码、账号被盗的比例呈上升趋势，2009 年密码被盗占调查总数的 27.14%，比 2008 年增长了 8.44%，位居当年计算机病毒造成的主要危害的首位。如图 1 和图 2 所示[6]。

由此可见，网络世界潜伏着各种危险因素，威胁着企业信息系统的安全，随时可能导致系统中断、个人信息泄密或者数据被破坏等后果，危及企业生存，损害消费者利益，进而对整个国家的经济安全和信息安全造成严重影响。因此，保护企业的信息资产和信息系统安全已经成为信息系

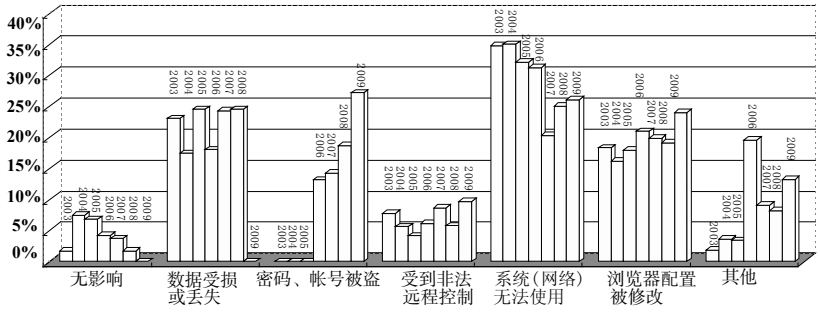

图 1　2009 年计算机病毒造成破坏的后果

统审计师最主要的职能之一。

（三）信息系统审计成为外部审计不可或缺的一环

自2001年以来，美国的安然、世界通信、默克制药和法国的威旺迪等国际大公司相继曝出假账丑闻，而且愈演愈烈。这些丑闻严重打击了投资者的信心，欧美股市不断创历史新低。

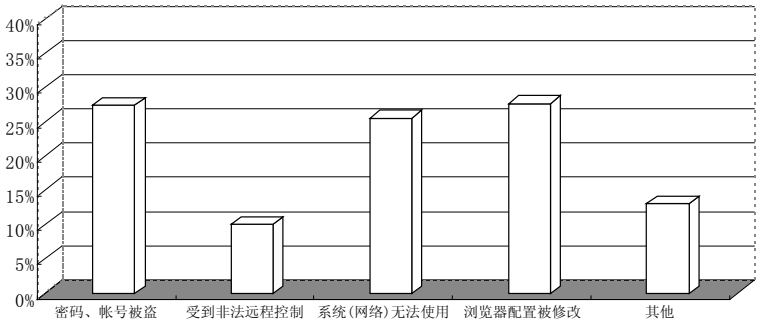

图2　2009年计算机病毒造成的主要危害

从1990年到2000年，安然公司的销售收入从59亿美元上升到1008亿美元，净利润从2.02亿美元上升到9.79亿美元。1999年，安然公司创建了基于互联网的全球商品交易平台“安然在线”，提供从电和天然气现货到复杂衍生品的1500多种商品。在不到一年时间内，“安然在线”发展成为年交易规模近2000亿美元的全球最大的电子商务交易平台。安然公司从一家名不见经传的普通天然气经销商，逐步发展成为世界上最大的天然气采购商和出售商、世界最大的电力交易商、世界领先的能源批发商，在全球拥有3000多家子公司和世界最大的电子商务交易平台，被评为最具创新精神的公司，然而，安然公司利用复杂的关联企业网，通过电子商务交易平台进行虚假的关联交易，形成虚假利润，误导公众，抬高股价，最终导致了泡沫破灭，公司破产、股民巨亏，而公司的高管却通过抛售股票获得巨额收益。电子交易的特点是虚拟化、无纸化、匿名、支付手段电子化，信息流、物资流和资金流是完全分离的，操作过程隐蔽性强，复杂度高，增加了审计取证的难度，交易的真实性无法按照传统方法审核，安达信公司没有针对电子交易这一新生事物采取相应对策，造成对电子数据真实性审计的缺失，导致对财务报告真实性的审计失去了意义，这又进一步助长了安然公司的舞弊行为，以致泡沫越来越大。

安然事件不仅造成了公司破产，更导致了公众对审计产生信任危机。为了挽回公众对资本市场的信心，美国国会和政府通过了萨班斯法案（SOX法案），规范企业电子数据的保存、审计和责任等问题，赋予了信息系统审计前所未有的功能定位。正如国际会计联合会会长梅尔所指出的：“会计师将不得不对实际上通过计算机报告的财务信息承担责任。”目前，一些大的会计师事务所都成立了独立的风险管理部门，专门从事信息系统审计工作。

（四）信息系统审计师成为内部控制的主要参与者

2008年，法国第二大银行兴业银行的交易员杰罗姆·凯维埃尔（Jerome Kerviel）进行的未经授权的交易导致该行损失49亿欧元，这几乎等于该银行一年的总收入。这是历史上单个交易员造成的最大一笔损失。凯维埃尔闯过了银行信息系统设置的五道关卡，动用的资金超过500亿欧元，这一数字超过了兴业银行当时的市值，远远超过了他的权限。他还利用信息系统隐瞒他所进行的违规交易，规避内部审计，因而在2007年末之前这些行为一直没有被发现。

在风险较高的金融衍生品市场中，兴业银行凭借严格的风险控制管理能力长时间位居头把交椅，即使在2007年夏天的金融市场动荡期，行业杂志仍然给予它最高评级。可是，兴业银行的一整套严格成熟的风险控制机制并没有与银行的信息系统很好地衔接，从而让凯维埃尔钻了空子。

兴业银行事件提醒了人们，当企业的许多内部控制机制已经程序化、数字化、虚拟化以后，内部控制与信息系统已经成为相互融合的一个整体，这是内部控制面临的新问题。我国的《企业内部控制应用指引第18号——信息系统》做了这样的阐述：“信息系统，是指企业利用计算机和通信技术，对内部控制进行集成、转化和提升所形成的信息化管理平台。”[4] 该定义非常准确地描述了信息系统与内部控制的关系。内部控制建设问题更多地变成了信息系统建设问题，对内部控制的审计更多地变

成了对信息系统的审计，因此，信息系统审计师应该参与企业内部控制的修订，向决策层提供咨询，从信息系统入手加强业务风险控制体系的建设和管理，以帮助企业协调信息系统控制与业务风险控制。

三、信息系统审计的三种基本类型

根据前面的分析，我们发现网络环境下的信息系统所面临的问题与“信息孤岛”时期不可同日而语，其外延不断拓展，内涵也越来越丰富，信息系统审计成为现代企业不可或缺的管理职能。信息系统审计的内容以信息系统为中心，企业的持续能力和容灾能力是企业信息系统安全性的综合体现；企业的信息基础设施是企业信息系统安全的物质基础；网络架构、通讯设备与技术等是信息系统安全的结构基础；操作系统是信息系统安全的软件基础；数据库系统的安全可靠直接影响信息系统中数据的安全与真实；财务软件影响财务审计的真实性，电子商务软件影响交易的真实性，其他的应用软件影响企业业务数据的真实性。图3反映了信息系统审计的内容及其相互之间的关系。信息系统审计内容丰富，相互之间关系复杂，因此，信息系统审计的类型和目标也一定是丰富多样的。审计目标将在下一节分析，这里笔者提出了现代信息系统审计应当包括真实性审计、安全性审计和绩效审计等三种不同的基本类型[7]。

（一）真实性审计

真实性审计的主要目标是审核企业信息系统和电子数据的真实性、完整性、合法性，为财务审计提供依据。

图3　信息系统审计的内容及相互关系

安然公司虚构交易量是通过电子商务平台实现的，可是这些电子数据是否真实地反映了实际情况，财务审计的方法和手段已经无能为力了。因此，信息系统审计的作用就是审核企业计算机系统所提供的数据，只有保证计算机系统中的数据是真实、完整、合法的，基于这些数据之上的财务审计才能是真实而有效的，也才能防止“假账真审”现象的出现，为财务审计保驾护航。因此，真实性审计属于财务审计的必要组成部分，二者相互印证，共同承担审计职能。

（二）安全性审计

安全性审计的主要目标是审查企业信息系统和电子数据的安全性、可靠性、可用性、保密性，既要预防来自互联网对信息系统的威胁，也要预防来自企业内部对信息系统的危害。现代企业的风险不仅来自市场、财务，也来自互联网和信息系统自身。来自互联网的病毒、木马、黑客等可以中断企业的正常业务，甚至导致企业破产。与此同时，来自企业信息系统自身的漏洞也可能给企业造成伤害，甚至造成毁灭性打击，例如凯维埃尔利用信息系统的缺陷等越权进入系统，进行违规操作导致百年银行几乎破产。可见，信息资产已经成为企业最重要的资产之一，审计师仅为投资者、债权人、经营者提供财务风险鉴证是不够的，他们还需要为企业的信息系统和信息系统安全提供审计服务。

安全性审计是真实性审计的基础与前提，很难想象一个在安全方面存在严重问题和缺陷的信息系统，它提供的数据会真实可靠。安全性审计也是一种专门审计事项，它向投资人、债权人、经营者提供信息资产安全方面的审计和咨询服务。

（三）绩效审计

信息系统的绩效审计是对企业在信息系统方面的投入产出比的审核。信息系统为企业创造的经济效益不是直接的，难以简单地用货币进行核算，因而如何衡量信息系统的贡献是十分复杂而困难的事情，而且，信息化应用项目实施也非常复杂，耗费的时间长、投入大，但是成功率又比较低，因此常常被称为“投资黑洞”。但是虽然面临种种困难，企业仍然必须不断地推广应用信息技术，以提升自身的核心竞争力，正因如此，企业在投资信息系统、管理信息系统的开发和应用、评价信息系统的使用效

果等方面需要加强风险控制、监督和评价工作，这些都是信息系统绩效审计面临的挑战。正确、合理地评价企业信息系统投资的绩效，给企业的投资者、债权人、经营者、管理者等提供决策参考，这是信息系统绩效审计的主要作用。

信息系统绩效审计属于绩效审计的范畴，只是信息系统绩效审计的对象是信息系统本身，其中对信息系统使用效果的评价是关键，也是难点。

四、信息系统审计的目标

由图 3 可知，信息系统审计的目标也应当是多元的。笔者认为信息系统审计的目标应该包括真实性、完整性、合法性、安全性、可用性、可靠性、保密性、效果、效率和效益等。三种基本的信息系统审计类型既相互区别，又具有一定的关联，它们都有着各自不同的审计目标。图 4 反映了信息系统审计的基本类型与审计目标之间的对应关系。

图 4　信息系统审计的基本类型与审计目标的对应关系

		真实性	完整性	合法性	安全性	可用性	可靠性	保密性	效果	效率	效益
信息系统审计	真实性审计	√	√	√							
	安全性审计				√	√	√	√			
	绩效审计								√	√	√

真实性是指信息系统中的数据要如实地反映企业的实际生产经营活动，可以通过一系列技术手段来确保数据的真实性，如数字签名、时间戳、不可否认协议、不可修改存储装置等。对真实性的破坏，可能来自企业高层的舞弊行为，例如通过财务软件故意做假账或通过电子商务系统虚构交易等达到虚增或虚减利润的目的；还可能来自企业的中层或基层员工的舞弊行为，例如通过非法访问或修改信息等手段，达到非法牟利目的；还可能来自企业外部，如黑客入侵、病毒破坏等，达到商业秘密外泄、删改企业信息等目的。

完整性是指信息系统中的数据不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。在信息系统中，数据与元数据是存放在不同地方的，数据的逻辑地址与物理地址也不一样，因此设备故障、误码、人为攻击、计算机病毒等都会破坏数据完整性。在信息系统中，数据完整性是数据真实性的基础。

合法性是指购买、使用、开发、维护信息系统的过程以及信息系统里的数据在生产、加工、修改、转移、删除等处理过程中，必须符合相关法律、法规、准则、行规以及企业内部的规定。

安全性是指信息系统在遭受各种人为因素破坏的情况下仍然能正常运行的概率。威胁信息系统安全性的因素可能来自信息系统和企业的外部，如黑客入侵、病毒攻击、线路侦听、木马、非法用户访问等；也可能来自企业和信息系统的内部，如授权用户的越权访问、修改、删除等操作。

可靠性是指信息系统在遭受非人为因素破坏或误操作情况下仍然能正常运行的概率。威胁信息系统可靠性的因素包括自然灾害对硬件和环境的破坏，误操作对软件和硬件的破坏，以及设备故障、软件故障等。与安全性不同，可靠性所指的破坏因素是非人为的，安全性所指的破坏因素是人为的。

保密性是指防止信息系统中的数据泄漏给非授权用户的特性。常用的保密技术包括防侦收、信息加密、物理隔离等。与安全性不同，保密性是防止信息系统中信息的外泄，安全性是防止外界对信息系统的入侵。

可用性也是信息系统安全性的一个重要指标，它是指信息可被授权实体访问并按需求使用的特性，即信息系统在提供服务时允许被使用的属性，或者是信息系统在部分受损或需要降级使用时，仍能为用户提供有效服务的属性。信息系统最基本的功能是提供服务，而用户的需求是信息系统的可

用性。可用性还体现在身份识别与确认、远程控制、数据跟踪等方面。由于数据的访问与数据存储介质、显示介质、软件版本等有关,无法访问的数据也无真实安全可言,因此可用性还体现在数据访问方面。

效果是指信息系统在企业生产管理应用中产生的效果,即信息系统的应用使企业在生产、管理、产品、服务、财务、人力管理等方面得到改善和提升,如减少了产生时间,提高了资金周转速度,降低了库存,增加了服务质量,扩大了产品种类等。

效率是指信息系统在应用后对提高企业劳动生产率所作的贡献,如人均生产率的提升。

效益是指信息系统的投入产出比,通过同行业类别等方法,核算信息系统的投入与产出的比率,得到信息系统的效益值。

由此可见,"三效"是绩效审计的目标。效益是可以用货币核算的,而效果和效率需要采用其他方法进行评价。对于安全性审计而言,安全与保密是从人为角度看,可靠性是从技术层面看,可用性是信息系统的特有性质。而真实性审计的目标是真实、合法和完整,完整性也是信息系统的特性。

五、结语

信息技术的发展、安然舞弊事件的发生以及萨班斯法出台等一系列因素促成了现代信息系统审计的产生,分析这些变化对信息系统审计的影响之后,我们提出了三种基本的信息系统审计类型,从这三种类型入手分析审计目标,而不是反过来,这种研究视角可以帮助我们更好地认识与把握信息系统审计的发展规律。

参考文献:

[1]石勇,崔超,赵晓光. 网络环境下政府信息系统审计研究[J]. 财会通讯,2010(8):117-118.

[2]陈耿. 信息系统审计专业建设与人才培养研究[J]. 中国科教创新导刊,2010(35):194-196.

[3]庄明来. 计算机审计与信息系统审计之比较[J]. 会计之友,2010(2):82-85.

[4]财政部,证监会,审计署,等. 企业内部控制基本规范[S]. 2008.

[5]徐瑾. 基于信息化环境下数据式审计的特征与实施路径[J]. 审计与经济研究,2009(1):50-55.

[6]国家计算机病毒应急处理中心. 2009 年中国计算机病毒疫情调查技术分析报告[R]. 2009.

[7]陈耿,王万军. 信息系统审计[M]. 北京:清华大学出版社,2010.

[责任编辑:黄　燕]

The Function and the Kinds of Information System Audit in Internet

CHEN Geng

Abstract: With the profound development of information system audit in the past 10 years, its function and position in enterprise management have changed dramatically. The existence and the development of the enterprises become more and more dependent on information system, in the meanwhile, e-business may lead to potential risk to the enterprise. Information system audit has become an indispensable part of the audit, and also a participant of internal control. Modern information system audit includes authenticity audit, security audit and performance audit, each with its own objective.

Key Words: IS audit; IT audit; authenticity audit; security audit; performance audit