可下载教学资料

http://www.tup.tsinghua.edu.cn

高等学校教材

信息管理与信息系统

信息系统审计

陈耿 王万军 编著

王家新 主审

清华大学出版社

高等学校教材

信息管理与信息系统

信息系统审计

陈耿 王万军 编著

王家新 主审

清华大学出版社

北京

内 容 简 介

本书全面、系统地阐述了基于互联网环境下的现代信息系统审计知识体系，突破了传统的基于信息孤岛状态下的信息系统审计概念，对提高信息系统审计师等一系列新型职业人才的专业素质具有很强的针对性和可操作性。内容包括：信息系统导论、信息系统审计的实施、审计证据收集与评价、信息中心审计、操作系统审计、管理软件系统审计、网络与数据传输审计、数据库审计、电子商务审计、系统开发与维护审计、IT 内部控制以及信息系统绩效审计等。本书提供了大量近年发生的典型案例，供教学和自学参考。

本书结构合理，内容系统，观点新颖，针对性强，可以作为高校计算机应用、管理信息系统、管理工程、审计、会计、企业管理等专业高年级本科生和研究生的教材，也可作为信息系统审计师、企业中高级管理人员、政府机关和企业信息中心管理人员、内部审计师、注册会计师、系统分析师及 IT 咨询顾问等专业人士的参考书。

本书的电子课件可从清华大学出版社网站(http://www.tup.com.cn)下载。

图书在版编目(CIP)数据

信息系统审计/陈耿，王万军编著. —北京：清华大学出版社，2009.6
(高等学校教材·信息管理与信息系统)
ISBN 978-7-302-19719-5

Ⅰ. 信…　Ⅱ. ①陈…　②王…　Ⅲ. 信息系统－审计－高等学校－教材　Ⅳ. F239.6

中国版本图书馆 CIP 数据核字(2009)第 037200 号

责任编辑：索　梅
责任校对：时翠兰
责任印制：王秀菊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　　总　　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京市昌平环球印刷厂
装 订 者：三河市兴旺装订有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：15　**字　数**：375 千字
版　　次：2009 年 6 月第 1 版　　**印　　次**：2009 年 6 月第1 次印刷
印　　数：1～3000
定　　价：25.00 元

出版说明

改革开放以来，特别是党的十五大以来，我国教育事业取得了举世瞩目的辉煌成就，高等教育实现了历史性的跨越，已由精英教育阶段进入国际公认的大众化教育阶段。在质量不断提高的基础上，高等教育规模取得如此快速的发展，创造了世界教育发展史上的奇迹。当前，教育工作既面临着千载难逢的良好机遇，同时也面临着前所未有的严峻挑战。社会不断增长的高等教育需求同教育供给特别是优质教育供给不足的矛盾，是现阶段教育发展面临的基本矛盾。

教育部一直十分重视高等教育质量工作。2001 年 8 月，教育部下发了《关于加强高等学校本科教学工作，提高教学质量的若干意见》，提出了十二条加强本科教学工作提高教学质量的措施和意见。2003 年 6 月和 2004 年 2 月，教育部分别下发了《关于启动高等学校教学质量与教学改革工程精品课程建设工作的通知》和《教育部实施精品课程建设提高高校教学质量和人才培养质量》文件，指出“高等学校教学质量和教学改革工程”是教育部正在制定的《2003—2007 年教育振兴行动计划》的重要组成部分，精品课程建设是“质量工程”的重要内容之一。教育部计划用五年时间（2003—2007 年）建设 1500 门国家级精品课程，利用现代化的教育信息技术手段将精品课程的相关内容上网并免费开放，以实现优质教学资源共享，提高高等学校教学质量和人才培养质量。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”（以下简称“编委会”），旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上；精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性（新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量）、先进性（对原有的学科体系有实质性的改革和发展，顺应并符合新世纪教学发展的规律，代表并引领课程发展的趋势和方向）、示范性（教材所体现的课程体系具有较广泛的辐射性和示范性）和一定的前瞻

性。教材由个人申报或各校推荐(通过所在高校的“编委会”成员推荐),经“编委会”认真评审,最后由清华大学出版社审定出版。

目前,针对计算机类和电子信息类相关专业成立了两个“编委会”,即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。首批推出的特色精品教材包括:

(1) 高等学校教材·计算机应用——高等学校各类专业,特别是非计算机专业的计算机应用类教材。

(2) 高等学校教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 高等学校教材·电子信息——高等学校电子信息相关专业的教材。

(4) 高等学校教材·软件工程——高等学校软件工程相关专业的教材。

(5) 高等学校教材·信息管理与信息系统。

(6) 高等学校教材·财经管理与计算机应用。

清华大学出版社经过20多年的努力,在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌,为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格,这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

E-mail: dingl@tup.tsinghua.edu.cn

前言

信息化与工业化(以下简称“两化”)是人类文明进程中两个重要的发展阶段。信息化高潮开始于20世纪中叶的西方发达国家,建立在高度的工业化基础之上,是工业化和科技进步到一定程度的结果。信息化是信息资源、信息技术及其产业在国民经济和社会中的作用不断加强的过程,发达国家经济增长中的60%～80%是由信息技术贡献的,信息已经成为经济发展的重要战略资源。2000年,中共中央第十五届五中全会正式提出了“以信息化带动工业化,发挥后发优势,实现社会生产力的跨越式发展”,到中国共产党第十六次全国代表大会又提出“信息化带动工业化,工业化促进信息化”的发展战略。目前,信息化和工业化正处于相互促进、相互影响、相互融合的过程中。

就企业而言,信息化对企业的经营发展带来了革命性变化。一些企业已经成长为“信息系统依赖型”企业和“信息资产密集型”企业。电子数据、计算机、网络和软件等,已经成为企业除资金、人力资源以外的第三种资产,成为企业核心竞争力的重要来源之一。

水能载舟,也能覆舟。任何事物的发展都具有两面性,信息化对企业发展也是一把“双刃剑”。企业对信息技术的依赖度越高,信息系统给企业乃至整个经济造成伤害的严重性也越高。安然公司利用信息系统创造“发展神话”,但最终酿成整个社会的信用危机;法国兴业银行的“内鬼”利用信息系统几乎导致百年企业的破产。这些无不说明了企业与信息技术之间的关系也越来越复杂。企业的内部人员利用信息技术的种种舞弊行为动摇了以财务会计为基础的信用体系,需要信息系统审计师对企业信息系统提供鉴证服务,保护企业投资者、债权人、经营者等的合法利益,维护信息时代的市场经济秩序,保护资本市场的有序发展。这是社会需求对信息系统审计起到拉动作用的结果。

另一方面,信息技术的飞速发展也推动着信息系统审计的理论、技术、方法的发展变化。特别是自从20世纪90年代以来,信息化又以网络化为主要标志,对企业的影响越来越深入,作用越来越明显,形式越来越多样,速度也越来越快。美国著名未来学家阿尔温·托夫勒认为:“计算机网络的建立和普及将彻底改变人类生存及生活的模式,控制与掌握网络的人就是未来命运的主宰。谁掌握了信息,控制了网络,谁就拥有整个世界”。企业一方面要利用和依赖网络,一方面又不得不面对无处不在的网络威胁,特别是银行、证券、电信、国防、贸易、保险等企业,它们对信息系统的安全性、可靠性、保密性等要求极为苛刻,信息系统审计师必须承担起为企业的安全与稳定保驾护航的企业

管理职能。

在“拉”和“推”两方面的共同作用下，以“两化”的融合为标志，信息系统审计进入了一个新的快速发展期。在知识经济时代，市场经济是信用经济的本质属性没有改变，但是，“两化”的融合使得政府的管理和企业的经营与信息技术之间存在非常复杂的相互关系，这种复杂性导致管理者、投资人、债权人等如果想了解企业真实的经营状况，就必须关注信息系统的安全性、真实性、合法性和可靠性问题，因此，信息系统审计师已经成为越来越重要的新兴热门职业人才，属于既懂经济管理又懂信息技术的复合型高层次专业人才，是经济安全、健康、可持续发展的“守夜人”。

本书首次全面系统地阐述了基于互联网环境下的现代信息系统审计知识体系，突破了传统的基于信息孤岛状态下的信息系统审计概念，为“两化”融合下的经济安全问题提供了新思路和新方法。

本书的写作得到了中国博士后基金（编号为 20070411019）、江苏“六大人才高峰”项目（编号为 2007148）、江苏省高校自然科学重大基础研究项目（编号为 08KJA520001）、江苏省高校自然科学基金（编号为 06KJB120051）等项目的支持。书中内容系统，观点新颖，针对性强，所选案例也为近年发生的典型案例。

本书可以作为高校计算机应用、管理信息系统、管理工程、审计、会计、企业管理等专业高年级本科生和研究生的教材，也可作为信息系统审计师、企业中高级管理人员、政府机关和企业信息中心管理人员、内部审计师、注册会计师、系统分析师、IT 咨询顾问等专业人士的参考用书。

中国审计学会副会长、南京审计学院院长王家新教授在百忙之中审阅了全稿，并提出了许多宝贵的意见和建议，在此向他表示衷心的感谢。

由于作者水平有限，书中不足之处恳请同行和读者批评指正。

作　者

2009 年 2 月

目 录

第1章 导 论

信息系统审计(information system audit,ISA)可以追溯到20世纪中叶,但是信息系统审计的快速发展则始于世纪之交。企业的内部人员利用信息技术的种种舞弊行为动摇了以财务会计为基础的信用体系,需要信息系统审计师对企业信息系统提供鉴证服务,保护企业投资者、债权人、经营者等的合法利益,保护信息时代的信用体系。

本章介绍了信息系统审计发展演化的过程,分析了现代信息系统审计的内涵,提出了信息系统审计的3种基本类型,即信息系统的真实性审计、信息系统的安全性审计和信息系统的绩效审计。其中,真实性审计是对传统审计的补充,防止假账真审;安全性审计是对企业的信息资产的安全性的审核,防止来自信息系统造成的经营风险;信息绩效审计则是对信息系统投入产出比的审核。在此基础上进一步提出了现代信息系统审计的目的体系,即真实性、安全性、完整性、可用性、保密性、可靠性、合法性、效果、效益、效率等。

在信息社会中,企业已越来越重视信息安全管理问题。特别是美国出台了一系列政策法规规定了企业的电子数据如何保留和储存的问题,为妥善保存企业在信息系统中的宝贵的数据资源提供了法律依据,同时也成为审计线索和证据的重要来源。

虽然企业的发展高度依赖信息技术,但市场经济是信用经济的本质属性没有改变。信息系统审计师是知识经济时代造就的新型经济管理高级人才,本章最后提出了信息系统审计师人才队伍建设和培养的问题。

1.1 信息系统审计的发展演化

1.1.1 早期的信息系统审计

第一台计算机诞生于20世纪40年代中期,主要用于科学计算。随着技术的进步,计算机也进入信息处理领域。到了20世纪60年代初,计算机已经应用在企业管理方面,其中应用最早、最有效的是企业财务数据处理和会计核算等。为了进一步开拓计算机的商业应用价值,当时主要的计算机制造商IBM公司出版了《电子数据处理审计》(Audit Encounters Electronic Data Processing)和《内部电子处理和审计轨迹》(In-line Electronic Processing and Audit Trail)等,给出了在电子数据环境下的内部审计规则和组织方法,提出了许多新的概念、术语和审计技术等,成为信息系统审计方面最早的文献。与此同时,由于工作上的

需要，会计师和审计师也自然成为最早关注信息系统审计的一群人，美国执业会计师协会也于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)。可见，这时信息系统审计的含义还比较窄，主要是针对财务数据的审计。

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)，以适应信息系统审计发展的需要，总部设在美国的芝加哥。目前在世界上100多个国家设有160多个分会，现有会员2万多人。该协会是影响最大的信息系统审计方面的国际化组织，也是职业资格考试——注册信息系统审计师(Certified Information System Auditor，CISA)考试的发起者和组织者。CISA资格得到许多国家的认可。在这一阶段，虽然信息系统审计发展得很快，但仍属于传统信息系统审计范畴。

1.1.2 现代信息系统审计

信息系统审计必然伴随着计算机技术的发展而发展。

现代意义上的信息系统审计产生于世纪之交，信息系统审计的外延得到极大的拓展，其内涵也越来越丰富。一方面是计算机技术的进步，特别是互联网的广泛应用，企业健康、稳定的发展面临着来自互联网的威胁，关注网络空间的经营风险，加强企业内部控制，已经成为现代信息系统审计的非常重要的内容之一，网络空间也是企业风险的重要来源之一；另一方面是企业内部对信息系统的依赖度越来越高，利用信息技术进行舞弊的风险也在增加，信息技术在企业发展中的“乘数效应”是双向的，既可以加速企业的发展，又可能加速企业的死亡。美国的安然事件，以及2008年发生的法国兴业银行事件等，给新世纪的信息系统审计提出了挑战，因此，应预防企业利用信息技术进行舞弊是现代信息系统审计的重中之重。

1. 信息系统审计的外延不断扩大

20世纪末，互联网的迅速普及改变了自计算机出现以来的“信息孤岛”格局，互联网彻底颠覆了几千年来人类社会信息传播的方式，人们在享受便捷、高效的同时，负面的影响也不断显现。一个病毒可以使远隔千里的大量企业遭殃，并从此一蹶不振。此时人们才发现，企业的经营风险源不仅仅是经典教科书上所说的市场风险、政治风险、技术风险、自然灾害等，互联网也成为企业经营风险的一个重要来源，而且越来越重要。

根据美国计算机安全事件响应组协调中心(Computer Emergency Response Team/Coordination Center，CERT/CC)[①]的统计，1988年—2003年报告的安全事件总计319 992件，其中1998年为6件，2003年增至137 529件。统计数字表明，互联网的安全事件增长趋势远远超过了互联网规模的增长速度，而这些安全事件许多是与网络的不可信任性有关，比如大量的敏感信息泄漏、地址欺骗、身份假冒、拒绝服务攻击、垃圾邮件泛滥、网络欺诈等事

① CERT/CC是一个由联邦政府提供资金的机构，成立于1998年，位于匹兹堡的卡内基-梅隆大学内。它的主要职能是对软件中的安全漏洞提供咨询，对病毒和蠕虫的爆发提供警报，向计算机用户提供保证计算机系统安全的技巧以及在处理计算机安全事故的行动中进行协调。