21世纪高等学校规划教材 | 信息管理与信息系统

信息系统审计理论与实务

吴桂英 主编
唐志豪 冯占国 等 编著

清华大学出版社

信息系统审计理论与实务

吴桂英 主编
唐志豪 冯占国 等 编著

清华大学出版社
北京

内 容 简 介

信息系统审计的诞生与发展是政府和企事业单位信息化发展到一定程度的必然结果，也是审计现代化转型的必由之路。本书借鉴当前国内外主流的信息系统审计准则指南，如美国审计总署的联邦信息系统控制审计手册、国际ISACA协会的信息系统审计实务手册和国际IIA协会的全球信息系统审计指南等，同时结合我国信息系统审计的相关规范及应用现状，全面系统地提出了信息系统审计的内容框架及知识体系，书中案例具有很好的实务操作指导作用。

本书可作为高等学校审计和信息管理等相关专业学生的教材，也可以作为从事审计实务工作者的参考用书。

图书在版编目(CIP)数据

信息系统审计理论与实务/吴桂英主编；唐志豪，冯占国等编著. --北京：清华大学出版社，2012.4
(21世纪高等学校规划教材·信息管理与信息系统)
ISBN 978-7-302-28093-4

Ⅰ. ①信… Ⅱ. ①吴… ②唐… ③冯… Ⅲ. ①信息系统－审计－高等学校－教材 Ⅳ. ①F239.6

中国版本图书馆CIP数据核字(2012)第029486号

责任编辑：郑寅堃　张为民
封面设计：傅瑞学
责任校对：时翠兰
责任印制：王静怡

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　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
课 件 下 载：http://www.tup.com.cn，010-62795954
印 刷 者：北京四季青印刷厂
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：10　　**字　　数**：244千字
版　　次：2012年4月第1版　　**印　　次**：2012年4月第1次印刷
印　　数：1～2500
定　　价：19.00元

产品编号：045126-01

出版说明

随着我国改革开放的进一步深化，高等教育也得到了快速发展，各地高校紧密结合地方经济建设发展需要，科学运用市场调节机制，加大了使用信息科学等现代科学技术提升、改造传统学科专业的投入力度，通过教育改革合理调整和配置了教育资源，优化了传统学科专业，积极为地方经济建设输送人才，为我国经济社会的快速、健康和可持续发展以及高等教育自身的改革发展做出了巨大贡献。但是，高等教育质量还需要进一步提高以适应经济社会发展的需要，不少高校的专业设置和结构不尽合理，教师队伍整体素质亟待提高，人才培养模式、教学内容和方法需要进一步转变，学生的实践能力和创新精神亟待加强。

教育部一直十分重视高等教育质量工作。2007 年 1 月，教育部下发了《关于实施高等学校本科教学质量与教学改革工程的意见》，计划实施“高等学校本科教学质量与教学改革工程（简称‘质量工程’）”，通过专业结构调整、课程教材建设、实践教学改革、教学团队建设等多项内容，进一步深化高等学校教学改革，提高人才培养的能力和水平，更好地满足经济社会发展对高素质人才的需要。在贯彻和落实教育部“质量工程”的过程中，各地高校发挥师资力量强、办学经验丰富、教学资源充裕等优势，对其特色专业及特色课程（群）加以规划、整理和总结，更新教学内容、改革课程体系，建设了一大批内容新、体系新、方法新、手段新的特色课程。在此基础上，经教育部相关教学指导委员会专家的指导和建议，清华大学出版社在多个领域精选各高校的特色课程，分别规划出版系列教材，以配合“质量工程”的实施，满足各高校教学质量和教学改革的需要。

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 21 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”。推出的特色精品教材包括：

(1) 21 世纪高等学校规划教材·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) 21 世纪高等学校规划教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 21 世纪高等学校规划教材·电子信息——高等学校电子信息相关专业的教材。

(4) 21 世纪高等学校规划教材·软件工程——高等学校软件工程相关专业的教材。

(5) 21 世纪高等学校规划教材·信息管理与信息系统。

(6) 21 世纪高等学校规划教材·财经管理与应用。

(7) 21 世纪高等学校规划教材·电子商务。

(8) 21 世纪高等学校规划教材·物联网。

清华大学出版社经过三十多年的努力，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

联系人：魏江江

E-mail：weijj@tup.tsinghua.edu.cn

序

信息是人类认识客观事物的基础，是改造物质世界的资源，是各种社会行为决策的依据。人类社会发展不但不可须臾离开信息，而且，发现水平、质量和速度在更大程度上取决于识别、获取和利用信息的能力。因为，信息已经成为最重要的战略资源。获取和利用信息的手段由于计算机、网络和通信技术的出现而发生革命性的变化，这种变化使信息价值得到空前提高，并使信息利用成为政治、经济和社会生活的最重要手段。

信息技术是一种崭新而又独特的文化现象。由于各种计算机软硬件、网络设施和通信设备的产生，以及计算机技术和传统机器设备的融合，使信息技术对人类物质生产工具的变革产生了至关重要的影响。如同系统论和控制论一样，信息技术理论也具有哲学意义。由于在设计、开发和使用过程中的独特性，并且在人类社会生活的方方面面得到广泛应用，信息技术也使人类精神领域发生了奇妙的变化，产生了新的思维模式、众多的交叉学科和不同以往的价值判断标准。

信息化的社会需要信息化的思维模式和信息化的技术手段。同理，信息化的审计环境需要信息化的审计思维模式和信息化的审计技术手段。然而，正如整个人类社会从过去走向现在一样，审计从传统走向现代的过程也交织着沮丧与兴奋、痛苦与快乐、山重水复与柳暗花明。

用怎样的思维方式组织审计行为？用怎样的手段获取和使用审计信息？控制与降低审计风险？用怎样的标准评价审计质量？这些问题的出现有时令人沮丧，然而寻找解决问题的过程令人兴奋；在过程中出现挫折令人苦恼，但是，看到一线希望又乐在其中。应当承认，我们现在仍处在山重水复与柳暗花明的交替变化过程之中。

在信息化的审计环境中，获取数据难，分析数据难，深度利用数据难。诸难之中，识别与判断数据质量是难中之难。因为，产生数据的信息系统在所有信息化审计事项中最为复杂，对于时下的审计人员而言最为陌生。近年来，为了克服这些困难，我们组织了数次信息系统审计实验和研究，鼓励全国审计机关积极尝试信息系统审计，并连续征集信息系统审计案例。一分耕耘，一分收获。今天，我们终于看到，多年的努力已初见成效。越来越多的审计包含了信息系统审计内容，越来越多的审计人员领悟了信息系统审计要领，越来越多的文章总结着信息系统审计经验。

在众多的信息系统审计实践者中，浙江的同事们应该是佼佼者。他们能快速接受信息技术，提升信息技术素养，提高信息技术应用水平。难能可贵的是，他们还迅速地体会了信息技术作为一种文化现象的精髓，将信息技术视为资源和效率，将信息技术的开发利用视为审计可持续发展的必经途径和手段。他们自觉地改变自己的思维方式，毫不迟疑地将信息技术带入自身的审计行为，并对后者加以变革。良好的悟性和高度的自觉，使他们很快将信息系统审计纳入重点攻关范围，在实践中学习，在总结中提高，在借鉴中成熟。

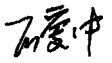
浙江同事的出色实践证明了前述的道理，即信息技术文化不仅影响着物质生产工具的

变革，而且丰富着人类的精神生活。当大家还在探索之时，他们就已经毫不犹豫地将当今实践与已有理论相结合，总结成书，奉献给全国审计人员。其速度令人惊愕，其贡献令人钦佩。此事意料之外，此书情理之中。

时下，我们正在研究制订信息系统审计指南，也还在全力推动信息系统审计工作的开展。这一过程可能还很漫长，途中可能还会遇到各种障碍，但是，我们相信，有了像浙江的同事们的这种时不我待的心理、畅游科海的情怀、实事求是的态度、坚忍不拔的毅力和脚踏实地的精神，就一定能够将这一过程缩短，越过断层，达到理想的彼岸。

我们认定，此书的出版一定会有助于信息系统审计的科学研究、审计学科的建设、审计人才的培养和信息系统审计队伍的形成。

细看造物初无物，春到江南花自开。感慨为序。



前言

信息技术(IT)在组织中多层次、横纵向嵌入,改变组织业务流程,使得组织内部控制与运营受到了巨大的冲击与挑战。信息系统成为组织日常运作,甚至赖以生存的基础,基于授权和岗位分工的内部控制发展成以信息技术为基础的IT内部控制,信息系统的安全、稳定和可靠性对于组织的正常运营具有重要意义。信息系统及相关控制若存在风险,会严重影响组织信息披露的可靠性和组织的日常运作,甚至危及组织的生存。

信息系统审计是一个获取和评价证据,对计算机信息系统及其相关资产的获取与运行过程的安全性、可靠性和效益性进行专业判断的过程,审计对象包括计算机硬件、软件、网络、数据和人。信息系统审计的诞生与发展是政府和企事业单位信息化发展到一定程度的必然结果,也是审计现代化转型的必由之路。作为一名审计、信息管理等相关专业学生,以及审计实务工作者来说,掌握信息系统审计理论与实务相关知识是非常必要的。

本书充分借鉴当前主流的美国审计总署的联邦信息系统控制审计手册(FISCSM)、国际ISACA协会的信息系统审计实务手册(CISA Manual)和国际IIA协会的全球信息系统审计指南(GTAG)等,同时结合我国信息系统审计的相关规范及应用现状,全面系统地提出了信息系统审计的内容框架及知识体系,书中案例均在实践基础上提炼,具有很好的实务操作指导作用。

本书共分11章,第1章概述信息系统审计的基本概念、内容体系和审计程序等知识,提供关于信息系统审计的总体概念框架;第2章归纳总结当前国内外的信息系统审计准则与规范;第3章论述信息系统审计的常规方法和计算机辅助审计技术;第4章论述应用控制审计的基本知识、审计内容与程序及相关案例;第5~9章分别论述IT治理审计、信息系统开发采购审计、信息系统运营维护服务审计、信息系统安全审计和信息系统业务持续性审计共5个方面的一般控制审计基本知识、审计内容与程序及相关案例;第10章论述数据审计概念和关键技术,以及现场和非现场数据审计的不同工作流程;第11章论述了信息系统绩效审计概念、审计程序、绩效指标和评价方法等。

本书第1章由唐志豪、吴桂英编写,第2章由何世宏、陈铁锋编写,第3章由吴叶葵编写,第4、5、8章由唐志豪、冯占国、肖爱元编写,第6章由邱君杰编写,第7章由陈宪宇编写,第9章由齐峰编写,第10章由李笑璐和蒋萍编写,第11章由于秀艳编写。其中,唐志豪、冯占国拟定全书框架并负责统稿,吴桂英审定全书框架及内容。

在本书的编写过程中,得到了审计署曹洪泽、陈剑的大力支持,浙江财经学院信息学院王衍、姚建荣教授在百忙之中审阅了全稿并提出宝贵建议,在此表示深深的感谢。

本书得到了浙江财经学院"信息管理与信息系统"省级特色专业建设项目、浙江省公益性技术应用研究项目(2011C31024)和浙江省自然科学基金项目(Y6110396)的支持。

由于信息技术和审计日新月异的发展,信息系统审计理论与实践尚在探索之中,书中难免存在不足之处,恳请同行和读者批评指正。

作　者

目 录

第1章 信息系统审计概论

信息系统的普遍深入应用提升了组织效率和效益，也使得组织对信息系统日益依赖。因此，检查、监督与评价信息系统的安全性、可靠性和效率性显得更加必要，信息系统审计日趋重要与紧迫。本章主要阐述信息系统审计发展史、基本概念、内容框架和信息系统审计的程序，以及信息系统审计师的知识结构等，为学习后续章节打下基础。

1.1 信息系统审计产生与发展

1954 年，通用电气公司利用计算机进行工资计算是基于计算机的企业信息系统应用的开端。今天以集成共享为特征，对企业所有人、财、物资源进行统一管理的 ERP 系统成为企业应用信息系统的典型代表。这样的信息化环境下，企业财务软件数据源自整个信息系统其他功能模块(生产、进销存、人力资源等)的实时业务数据，在进行财务审计时，纸质会计凭证的电子化使得审计人员不得不关注电子数据的取得、分析、计算等数据处理业务，不得不考虑信息系统的安全性、可靠性和效率，以保证被审计信息的真实和可靠。

另外，伴随公共行政、公共管理与公共服务领域的信息化应用深入，电子政务系统成为政府、公共事业部门日常工作不可缺少的手段。电子政务项目投资及运作的有效性与安全性，也日益变得重要。电子政务系统审计能有效降低电子政务信息系统建设以及运营维护阶段的风险，是保证政府投资有效性和安全性的重要手段。

综合来看，信息系统审计的产生是信息化应用与审计发展的必然：一方面，企业信息化及电子政务的深入运用，使信息系统成为组织运作甚至赖以生存的基础，其安全、稳定和可靠性需要得以保障；另一方面，目前 IT 控制成为很多被审计单位内部控制的有机组成部分，国家审计、社会审计和内部审计的所处环境、审计对象都发生了变化，审计内容和重点都需要随之变化。

美国斯坦福研究院的调查报告显示 20 世纪 60 年代以后，特别是会计电算化之后，信息系统审计开始诞生。

萌芽期的信息系统审计通常称之为电子数据处理(EDP)审计或计算机审计，是作为传统审计业务的扩展发展起来的，主要是由会计事务所对金融企业进行外部审计，严格说来，萌芽期的信息系统审计与现在信息系统审计内涵还是有些不同的。

早在 1969 年，美国洛杉矶成立了电子数据处理审计师协会(EDPAA)，1975 年日本情报处理开发协会也设立了 IT 审计委员会，开始了一系列的研究。1984 年，美国 EDP 审计

人员协会发布了《EDP 控制目标》，提出了一系列的总控制标准。1985 年，日本通产省公开发表了《IT 审计标准》，并开始培养从事 IT 审计的队伍。20 世纪 90 年代以后，信息系统审计的需求成倍增长，大多数发达国家已普遍实行了信息系统审计。1994 年，原来 EDPAA 协会更名为信息系统审计与控制协会（ISACA），制定和颁布信息系统审计准则、实务指南等专业标准来规范和指导信息系统审计师的工作。它还设立了信息系统审计与控制基金会，从事相关领域的研究工作，ISACA 每年还举办国际注册信息系统审计师（CISA）资格考试，通过考试的人员可以申请 CISA 资格，符合 ISACA 规定的工作经验及其他相关要求的申请人会被授予 CISA 资格。

信息系统审计的发展历程如图 1-1 所示。

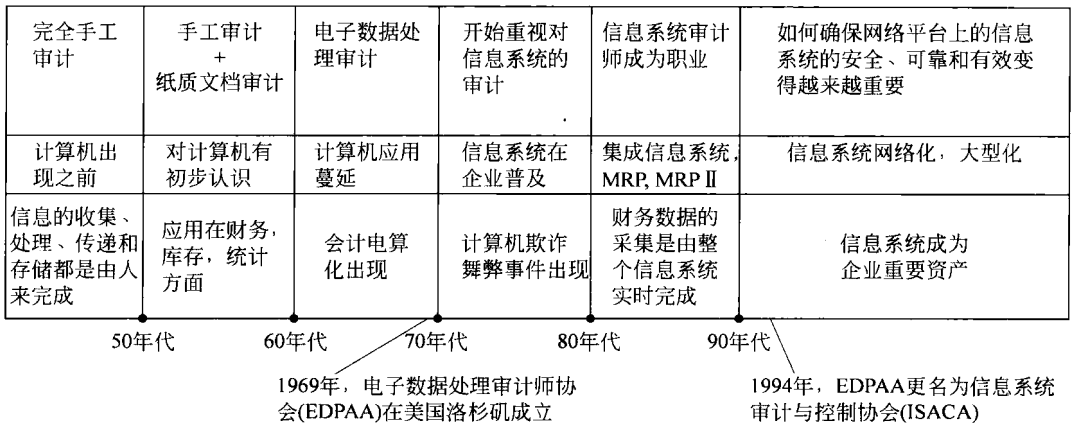


图 1-1　20 世纪信息系统审计的产生与发展

我国审计署于 1996 年 12 月颁布的《审计机关计算机辅助审计办法》是我国最早的关于计算机辅助审计的准则文件。中国注册会计师协会于 1999 年 2 月颁布的《独立审计具体准则第 20 号——计算机信息系统环境下的审计》。中国内审协会制定的《内部审计具体准则第 28 号——信息系统审计》于 2009 年 1 月颁布生效。审计署 2010 年颁布了《关于检查信息系统相关审计事项的指导意见》，提出了需要重点关注的 9 大类信息系统相关审计事项共 26 个事项，并对信息系统审计的对象、内容和方法进行了明确。

可以预见，随着我国信息化水平的提高，信息系统的有效控制与审计将逐渐成为热点。

1.2 信息系统审计概念与目标

1.2.1 信息系统审计概念

日本通产情报协会 1996 年的定义信息系统审计如下："为了信息系统的安全、可靠与有效，由独立于审计对象的 IS 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 IS 审计对象的最高领导，提出问题与建议的一连串的活动。"

美国学者 Ron. A. Weber 在《信息系统控制与审计》一书中对信息系统审计的定义是：信息系统审计是一个获取证据，对信息系统是否能保证资产的安全、数据的完整，以及是否

有效使用了组织资源并可靠地实现了组织目标做出评价和判断的过程。

综合上述定义，可知信息系统审计概念有如下内涵：

(1) 信息系统审计主体是独立的第三方审计师；

(2) 信息系统审计对象是计算机为核心的信息系统；

(3) 信息系统审计目标是促使信息系统安全、可靠和有效；

(4) 信息系统审计是一个过程，需要审计师的专业评价与判断；

(5) 信息系统审计需要遵循相关标准与规范；

(6) 信息系统审计需要对信息系统的规划、开发、使用维护等系列活动及产物进行检查和评估。

因此，本书认为信息系统审计是一个获取证据，依据相关标准和规范开展证据评价，并对计算机信息系统及其相关资产的获取与运行过程的安全性、可靠性和效益性进行专业判断的过程。

1.2.2 信息系统审计目标

从信息系统审计的概念可以知道其有三个目标：安全性、可靠性和有效性。

系统安全性是指信息系统资源是否受到妥善保护，不因自然和人为的因素而遭到破坏、更改或者泄露系统中的信息。其中信息系统资源包括硬件、软件、网络、数据和人。

系统可靠性包括三个方面的含义：硬件、软件和数据。硬件系统的可靠性是指在一个指定的时间周期内，在给定的控制条件下，硬件系统执行所需功能的成功概率。软件系统的可靠性是指在运行环境中，在规定的运行时间内或规定的运行次数下，程序和所有数据元素运行不同测试用例的无差错概率。数据的可靠性是指数据的真实、准确和及时，它取决于系统对数据的处理过程是否准确无误，以及确保数据可靠的控制措施是否有效。

有效性是个含义丰富的目标：一方面是指信息系统是否能够实现既定的业务目标(效益性)，信息系统的处理过程是否符合国家法律和有关规章制度的要求(合规性)；另一方面是指系统的效率性——系统利用各种资源输出用户所需要信息的及时程度和运行速度。

1.3 信息系统审计内容体系

信息系统是一个以人为主导，利用硬件、软件、网络通信设备以及其他办公设备，进行信息收集、传输、加工、存储、更新和维护，以企业战略竞优、提高效益和效率为目的，支持企业高层决策、中层控制、基层运作的集成化的人机系统。

信息系统审计是以信息系统为审计对象的一类审计业务，因此，信息系统的所有组成部分都是信息系统审计的实体对象，包括操作系统、主机、网络、数据库、应用软件、数据、人和管理制度，如图 1-2 所示。

遵循目前信息系统审计的国际惯例，整合国际审计与控制协会(ISACA)的 COBIT 报告、美国审计总署(GAO)的 FISCAM 报告和美国内审协会 IIA 的 GAIT 审计指南，本书构建信息系统审计的两大内容域——一般控制与应用控制，并整理出各内容领域内的典型审计事项。

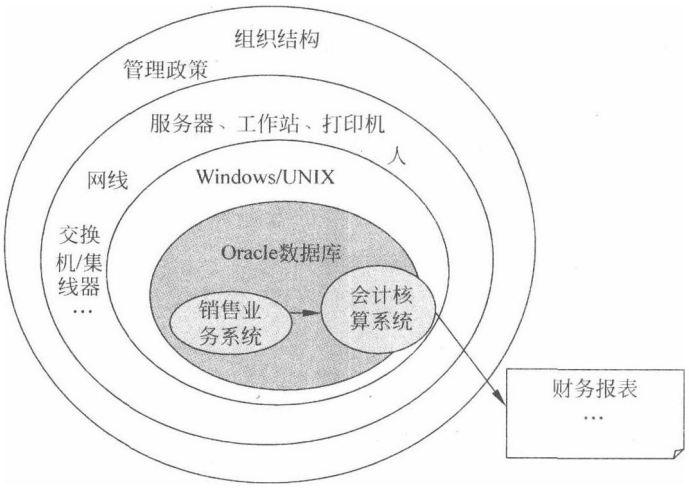


图 1-2 信息系统的逻辑组成结构

一般控制是指与网络、操作系统、数据库、应用系统及其相关人员有关的信息技术政策和措施。一般控制用于保障信息系统持续稳定的运行，其控制措施适用于被审计单位的所有应用系统，是一种环境上的保证。

应用控制指在业务流程层面为了合理保证应用系统准确、完整、及时完成业务数据的生成、记录、处理、报告等功能而设计、执行的信息技术控制。应用控制与具体应用系统紧密相关，用于保障数据处理完整和准确。

一般控制与应用控制之间存在如下相互影响关系：

(1) 应用控制的有效性取决于一般控制的有效性。

(2) 一般控制是应用控制的基础，当一般控制薄弱时，应用控制无法提供合理保障。

本书的信息系统审计内容框架如表 1-1 所示。

表 1-1 信息系统审计的内容体系

信息系统审计内容域	审计事项子类
一般控制审计	IT 治理
	信息系统开发采购
	信息系统运营维护服务
	信息系统安全
	业务持续性与灾难恢复
应用控制审计	参数控制
	应用程序的访问控制与职责分离
	输入控制
	处理控制
	输出控制
	接口控制
系统数据审计	现场数据审计
	非现场数据审计