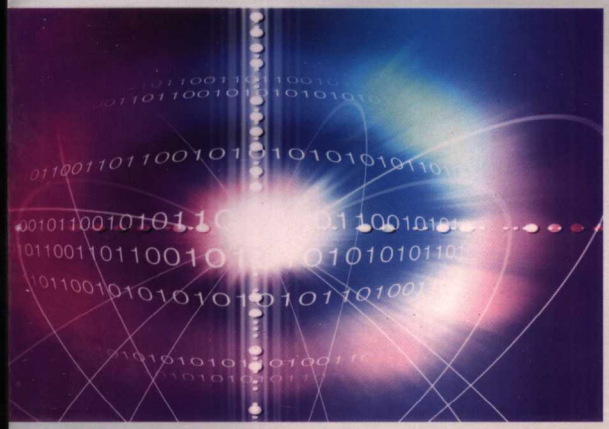
Broadview®
www.broadview.com.cn

信息化经典书丛



Information Technology Audit (Second Edition)

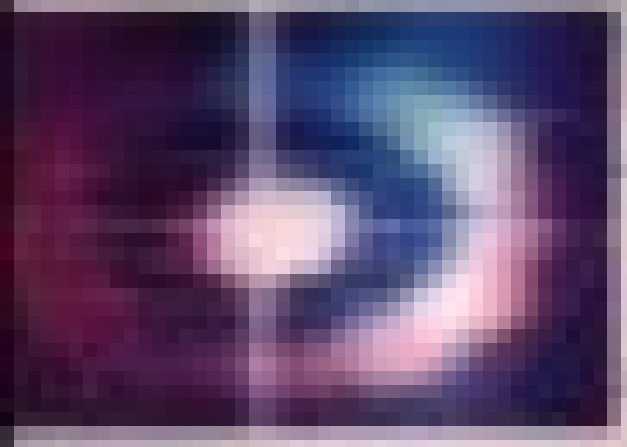
IT审计（第二版）

胡克瑾　等编著
高新民　审校

IT审计——全面控制信息系统的风险！

- → 中国IT审计领域首部著作
- → IT审计师培训与考试教材
- → 国际信息系统控制与审计协会CISA考试必备读物

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn



Information Technology Audit

IT审计

[第二版]

信息化经典书丛

IT 审计（第二版）

胡克瑾　等编著

高新民　审　校

電子工業出版社

Publishing House of Electronics Industry

北京· BEIJING

内 容 简 介

为了确保信息系统的安全、可靠和有效，需要开展由独立的具有资格的IT审计师对以计算机为核心的信息系统进行的IT审计。本书全面透彻地介绍了IT审计的基本概念、目标、理论方法及技术；深入浅出地介绍了IT审计准则的框架、基本要求及与此相关的知识。力求做到既有理论深度，又有较强的实务性。这是国内第一本有关IT审计的书籍，由国家经贸委信息中心资深专家审校，本书将指导IT审计人员系统准确地把握IT审计的思想，正确有效地运用IT审计的方法与技术。本书又在第二版中增加了大量案例并回答了读者关心的问题。本书可作为IT审计师的培训教材，也可作为信息系统主管的参考手册，还可作为信息管理专业或信息安全专业的本科生及研究生的教科书或参考书。

图书在版编目(CIP)数据

IT审计 / 胡克瑾等编著. —2版. —北京：电子工业出版社，2004.11
（信息化经典书丛）
ISBN 7-121-00371-6

Ⅰ.I... Ⅱ.胡... Ⅲ.信息系统—审计 Ⅳ.F239.6

中国版本图书馆CIP数据核字（2004）第093710号

责任编辑：郭 立 胡辛征
印 刷：北京智力达印刷有限公司
出版发行：电子工业出版社
北京市海淀区万寿路173信箱 邮编 100036
经 销：各地新华书店
开 本：787×980 1/16 印张：39 字数：537千字
印 次：2004年11月第1次印刷
印 数：4 000册 定价：62.00元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

出 版 说 明

“以信息化带动工业化”——国民经济信息化被提到了前所未有的高度、深度和广度。电子工业出版社作为信息产业部直属的大型IT专业出版社，积极投入到信息化建设的浪潮中来。为推动信息化建设与应用的不断深入，实现建立在自主的信息产业基础之上的信息化，培养大批适合我国信息化建设的高素质人才，我们邀请国内外信息化领域资深专家，撰写了这套针对我国信息化领域焦点问题及主流技术的丛书。

我们推出的这套《信息化经典书丛》的特点是：经典、前沿、主题分明和可操作性强。

经典——特邀信息化领域的资深顾问、一线实施专家，将多年经验和心得介绍给读者。

前沿——介绍信息化领域最前沿的思想与技术。

主题分明——确定三大主题：企业信息化、政府信息化及与信息化发展密切相关的核心问题。

可操作性强——内容注重由浅入深，注重可操作性和实用性。

本套丛书的“企业信息化”主题，包括对目前企业界最关心的ERP，CRM和SCM等核心问题的深入而全面的介绍，以及企业信息化实施细则。特邀在企业信息化领域从事多年研究及一线实施的国际著名公司（如SAP，Siebel，I2）及国内著名的用友和金蝶公司的资深专家及顾问，将他们多年宝贵的开发及实施经验介绍给读者。这些多年未公开的实施细节和经验，可帮助各企业及实施专家探讨一条适合自身的、成功的企业信息化之路。

本套丛书的“政府信息化”主题，包括目前公认为成功的电子政务工程的理论与实践，以及一些知名软件公司的电子政务解决方案。该主题将为政府部门的信息主管、立志从事电子政务开发与应用的高级技术人员规划和实施电子政务提供权威指南，是集专业性、权威性、可操作性于一体的经典之作，可使政府信息化的实施风险降到最低。

本套丛书的“与信息化发展密切相关的核心问题”这一主题，包括与目前政府和企业信息化建设密切相关的知识管理、IT 审计、信息工程建设监理等热门问题。作者都是国内最早、并一直致力于研究这类问题的专家。内容涉及面广，无论对理论还是实践都做了非常深入细致的探讨，可帮助信息化领域相关人员建立高效、可靠、安全且高度智能的信息化系统。

本套丛书旨在为国内信息化领域的政府部门及企业领导、信息化主管、项目经理及各类高级技术人才提供权威的指南，帮助他们走出一条适合我国国情的、成功的信息化道路，开发出适合我国政府、企业及社会信息化建设的软件。另外，本套丛书可作为通过各类信息化认证考试的参考书，也可作为与信息化相关的管理及计算机专业研究生、本科生的教材及参考书。

出版高品位、高品质的图书是电子工业出版社计算机图书事业部的努力目标。如果您是读者，希望您对我们的图书关注并多提宝贵意见。您的意见是我们创造精品的动力源泉。

如果您是多年从事信息化建设的资深专家，欢迎您能对我们的工作提出建议并参与到我们的图书出版工作中来。我们将为您提供一流的服务，将您的宝贵经验编撰成图书精品。

我们的联系方式如下。

地址：北京市复兴路 47 号天行建商务大厦 604 室

电话：010-51922832

传真：010-51922823

E-mail：jsj@phei.com.cn, editor@broadview.com.cn

电子工业出版社

博文视点资讯有限公司

2004 年 10 月

序　一

信息系统（1T）审计是指根据公认的标准和指导规范对信息系统及其业务应用的效能、效率、安全性进行监测、评估和控制的过程，以确保预定的业务目标得以实现。按照科学的、符合实际的决策原则，一项信息系统要经历规划阶段、实施阶段以及运行维护阶段的审计。

审计不仅是项目完成时验收的需要，而且在信息系统运行、维护过程中更为更要，因为任何一项信息系统不可能在规划和实施阶段就十全十美，又一成不变。这就要求定期或不定期地进行审计，发现问题，解决问题，以适应新的环境变化和业务需求。信息系统审计的目的是保证信息化过程每个环节经常处在可控之中。

信息系统审计的必要性是基于这样一种认识：信息化是有风险的。信息系统规模越大，功能越复杂，风险也就越大。这是从实践中总结出来的。20 世纪 80 年代美国企业信息系统的失败率达 50%以上；90 年代美国电子政务的信息系统完全成功率仅 28%。这充分说明，信息系统的建设较之传统工业工程项目失败的风险更加突出。

国际上信息系统审计的概念起始于 20 世纪 60 年代，那时称之为计算机审计（Computer Audit）。主要对计算机的性能和效益进行监测和评估。20 世纪 90 年代以来，随着信息网络的广泛应用，信息系统日趋复杂，尤其是对关键业务应用的可靠性、可用性要求十分苛刻，人们对信息系统审计制度的作用更加重视。目前，国际上一些知名的咨询公司在承担信息系统审计委托时，均采用国际上通行的标准、规范，聘用经过认证的注册 IT 审计师进行。

按国际上通行的规范，信息系统审计有 6 个方面的主要内容。

1．评估信息系统计划、管理及组织架构的战略、政策、标准及相应的实践过程；

2．评估技术基础设施及运行实践的效能和效率；

3．评估信息资源在逻辑访问、运行环境以及 IT 基础设施等方面的安全性；

4．评估系统灾难恢复及保证业务连续性的能力；

5．评估业务应用系统开发、实施与维护的方法和过程；

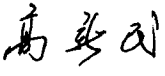
6．评估业务流程的风险管理水平。

由此可见，信息系统审计是全面的：不仅对技术基础设施，也涉及业务应用系统；不仅是IT系统本身，也包括其组织结构保证，而且特别突出系统的安全性和灾难恢复能力。为了实施审计，专业人员必须具备相当广泛的知识基础。

为了确保审计工作的公正性和客观性，必须具备两个前提：其一是有一批专业化的第三方审计机构以及经过资格认证的注册IT审计师队伍；其二，必须有一套公认的审计标准、过程规范及职业操守，并有相应的非赢利行业协会负责制定及监督执行。

当前，我国信息化事业已发展到一个新的阶段。各级政府正在推进“电子政务”，并认真落实“以信息化带动工业化”的战略。广大企业也开始着手整合与升级各自的信息化应用系统。可以预计，全国将有更多、更大的信息系统上马。但是，据我们了解，在信息化推进过程中，至今不同程度上存在着一些问题，主要表现在规划制定不够深思熟虑；项目管理不够严格；系统运行效益不够明显。导致相当一部分信息化项目失败，浪费了大量资源。究其根源是相当普遍地对信息化风险认识不足，规避风险的措施不力。中央领导同志在国家信息化领导小组会议中特别强调：信息化一定要讲求效益，不能搞花架子。我们认为，建立并逐步完善我国信息系统审计制度是落实上级会议精神的一项重要措施。

为了在我国培育一支高素质的信息系统审计师专业队伍，也为了普及有关信息系统审计的知识，电子工业出版社组织专家出版本书是有现实意义的。这是国内第一本有关IT审计的书籍，本书将指导IT审计人员系统准确地把握IT审计的思想，正确有效地运用IT审计的方法与技术。本书可作为IT审计师的培训教材，也可作为信息系统主管的参考手册，希望读者从此书能获取更多的有益知识。也希望本书的出版为我国更快、更好地进入信息化社会起到促进与保障作用。



序　二

我国信息化的实践经验证明，对信息系统进行严格规范的审计与控制是至关重要的。

全国信息系统与网络的发展正改变着经济、社会和文化的结构与运行方式，改变着人们的思维方式，其广度与深度都是以往任何一次产业革命所无法比拟的。正因为如此，我们才十分关注信息资源的合理、经济和正确的使用问题与信息系统和网络安全的风险问题。

我国信息网络化的实践证明，要建设一个有效、安全和可靠的信息系统，必须对信息系统开发和运行进行严格的审计和控制。

美国等发达国家早就开展了由独立的具有资格的第三方进行的IT审计，对信息系统从计划开始，到设计、编程、测试、运行、维护直至淘汰的整个生命周期都实施 IT 审计。信息系统审计与控制协会ISACA（Information System Audit and Control Association）已在世界上100多个国家设立了160多个分会，制定和颁布IT审计准则、实务指南等，来规范与指导IT审计师的工作。该协会还举办一年一度的注册IT审计师的考试CISA（Certified Information System Auditor），由通过该资格考试的人员（即IT审计师）按照IT审计准则、实务指南等来进行 IT 审计。IT 审计作为信息社会的安全对策，能有效地管理与IT相关的风险，从而确保信息系统的安全性、可靠性和有效性。

为了推进我国信息化事业，保护信息化建设成果，IT审计是必不可少的。信息系统的安全与经济安全、社会安全、国家安全紧密相连，是我国信息化进程中具有重大战略意义的问题。本书是国内第一本有关IT审计的书籍，介绍国外先进的IT审计与控制的思想与方法，对促进我国更好地进入信息化社会，保障信息安全是很有意义的。希望本书的出版能推进我国的IT审计工作，有助于培养IT审计师队伍，从而为我国信息化建设做出一份贡献。

何德全

再 版 前 言

《IT 审计》第一版面市后，引起 IT 界的强烈反响。如何控制信息化过程各个环节的风险，如何管理好信息与信息资源？如何保护好信息与信息平台，如何确保赖以生存的信息系统的安全、可靠与有效？如何发挥信息技术的最大正面效应，如何让全社会都充分享受到信息化变革带来的利益？本书对这些问题的解答越来越受到国内政府部门、企业与社会各界的重视。本书以其较高的理论深度与较强的务实性，指导系统审计师有效地实施系统审计以及参加 CISA 考试等特色而深受读者的欢迎。图书出版后，作者收到数百封读者来信。

为了更好地满足读者的需求，并不断地与国际上最新的、权威的信息系统审计标准接轨，作者决定再版。第二版新增了以下内容：

1. 第 8 章新增了信息系统审计与控制基金会 ISACF 与 IT 治理研究所共同研究与开发的一套信息及其相关技术的控制目标 COBIT。

2. 每章后面都新增案例，有国内与国际的案例，并给出了启示。

3. 更新第 8 章国际信息系统审计与控制协会颁布的 IT 审计标准。

4. 在附录中新增摘录读者来信和解答读者关心的问题。

由于本书的选题较新，涉及内容较多，时间紧迫，而且作者的经验与水平有限，难免存在不足之处，希望广大读者批评指正。同时希望本书的再版能满足读者的需求，吸引各界同仁共同研究与探讨信息系统审计在我国的发展与实践。

本书的再版得到了电子工业出版社的大力支持，在此表示诚挚的感谢！

胡克瑾

2004 年 8 月于同济大学

前　言

随着社会信息化程度的不断提高，我们正逐步向信息化社会迈进。信息将是维持社会的重要基础性资源，信息系统广泛深入地渗透到社会的各个领域，成为政治、经济、军事、文化乃至社会一切领域的基础，其结果导致了整个社会对信息系统的极大依赖性。一方面，信息系统变革着经济、生活、文化等诸多方面的结构和运行模式，改变着人们的思维方式，人类社会正享受着信息化给予的方便与效益；而另一方面，由于信息系统的负面效应及控制不当，导致信息化过程、信息系统及其业务应用产生风险，即当信息系统发生故障、停止运行或发生错误而丧失其有效功能时，该领域的业务活动就失去了支撑和保障，甚至还要影响到社会生活等其他许多方面。

那么，如何控制信息化过程各个环节的风险，管理好信息与信息资源？如何保护好信息与信息系统平台，确保赖以生存的信息系统的安全、可靠与有效？如何发挥信息系统的最大正面效应，让全社会都充分享受到信息化变革带来的利益？

这些问题越来越受到国际国内政府部门、企业与社会各界人士的广泛关注，特别是美国等发达国家很早就开展了由独立的具有资格的第三方进行的IT审计，建立了完善的IT审计制度。事实表明，IT审计能有效地控制信息与信息系统的风险，是信息化的基础，是更好地进入信息化社会的可靠保证。

美国等先进国家开展IT审计始于20世纪60年代，对以计算机为核心的信息系统从计划开始，到设计、编程、测试、运行、维护直至淘汰的全生命周期实施IT审计。国际上惟一的信息系统控制与审计协会ISACA（1nformation System Audit and Control Association）总部设在美国，目前已经在世界上100多个国家设立了160多个分会，现有会员两万多人。该协会通过制定和颁布信息系统审计准则和实务指南等来规范和指导IT审计师工作。ISACA还在许多国家举办一年一度的注册IT审计师CISA（Certifide Information System Auditor）考试，

考试合格并获得执业资格者可在全世界范围内开展 IT 审计工作。

近年来，Internet、电子商务与电子政务等的兴起，更是为 IT 审计业务的发展带来了无限机会，如防火墙审计、安全审计、信息技术论证以及 ERP 等相关的新型业务正不断涌现。目前 IT 审计师已经成为全世界范围最抢手的高级人才，这些人才必须具备全面扎实的计算机软硬件知识与审计实务能力，对网络、信息系统及其业务应用有独特的敏感性。

本书力求把国外先进的 IT 审计与控制思想引入国内，并结合国内实际情况，力求理论与实践相结合。中国加入 WTO 后，如何保证我国在加入世贸组织之后经济社会与科技方面的稳步发展，IT 审计是必不可少的。信息系统的安全与经济安全、社会安全、国家安全紧密相连，是我国信息化进程中具有重大战略意义的问题，因此 IT 审计已势在必行，应尽早纳入我国信息化发展的规划之中。因此本书的出版对促进我国更好地进入信息社会，保障信息安全将具有十分重要的意义。目前围内还没有这方面的书籍，希望本书的出版能推进我国的 IT 审计，培养 IT 审计师队伍，促使信息系统更加安全、可靠与有效。这将会产生极大的社会与经济效益。

本书全面翔实地介绍 IT 审计的基本概念、目标、理论方法与技术；IT 审计准则的框架及基本要求，全面、系统、深入浅出地介绍了 IT 审计及与此相关的知识，指导 IT 审计人员系统准确地把握 IT 审计的思想，正确有效地运用 IT 审计的方法与技术。本书力求做到既有理论深度，又有较强的实务性。

本书分 5 大部分，共 8 章。

第一部分　IT 审计概念

　　第 1 章　概论

第二部分　IT 审计实施过程

　　第 2 章　信息系统开发过程的审计

　　第 3 章　信息系统运行维护过程的审计

　　第 4 章　信息系统生命周期共同业务的审计

第三部分　IT 审计技术

第 5 章　IT 审计方法、技术与工具

第 6 章　IT 审计中的评价技术

第四部分　IT 审计实践

第 7 章　信息系统安全与风险管理

第五部分　IT 审计标准

第 8 章　IT 审计标准与相关 IT 标准

全书由胡克瑾主编，其中第 1，7，8 章由胡克瑾编写，第 2，3 章由梅洁、刑蕙、谢莉等编写，第 4 章由韩慧群、郝晓玲、张峰等编写，第 5、6 章由赵永超编写。第 8 章内容参照了中国国家信息安全测评认证中心下达同济大学完成的《信息系统监查标准体系》项目的研究成果。全书最后由信息化资深专家、原国家信息中心主任高新民审校。在本书编写过程中得到了中国工程院何德全院士指导，在此表示衷心的感谢！

本书是国内第一本有关 IT 审计的书籍，概念清晰、阐述严谨、选材广泛而精炼、具有较强的可读性。本书可作为 IT 审计师的培训教材，也可作为信息系统主管的参考手册，指导他们如何应用 IT 审计有效地管理与 IT 相关的风险，从而确保系统的安全、可靠与有效。本书还可作为信息管理专业或信息安全专业的本科生及研究生的教科书或参考书。

限于时间与水平，不妥之处在所难免，敬请批评指正。

编　者

2002 年 7 月于上海

目 录