管理咨询与审计系列

（美）Jack J.Champlain 著

审计信息系统

（第2版）

AUDITING INFORMATION SYSTEMS

张金城 李海风 等 译

清华大学出版社

审计信息系统——信息系统审计师期待的工具、指南和程序

审计信息系统

（第2版）

AUDITING INFORMATION SYSTEMS

审计信息系统（第2版）清楚地阐述了如何审计各类信息系统环境下的控制的安全问题。书中的概念和技术使具备各方面知识背景和技能水平的审计师、信息安全专业人员、管理者和审计委员会成员，真正理解其所在机构的计算机系统的安全性问题。本书为审计专业人员提供了如何做好本职工作所需的工具，是每位审计师书库中的必备参考书。

★本系列中的每本书都将对审计实务界产生重大的影响！

审计信息系统（第2版）

咨询的核心概念：面向管理者和会计师

超越COSO：加强公司治理的内部控制

控制自我评估：以协调为基础的咨询指南

管理审计职能：公司审计部门程序指南

风险的简要规则：再看金融风险管理的艺术

ISBN 7-302-09720-8

9 787302 097204 >

定价：39.00元

管理咨询与审计系列

（美）Jack J.Champlain 著

审计信息系统

（第2版）

张金城 李海风 等 译

清华大学出版社
北 京

Jack J. Champlain
Auditing Information Systems, 2rd ed.
ISBN: 0-471-28117-4

图书在版编目(CIP)数据

审计信息系统/(美)坎普林(Champlain, J. J.)著;张金城,李海风等译. —北京: 清华大学出版社,2004.11
(管理咨询与审计系列)
书名原文: Auditing Information Systems
ISBN 7-302-09720-8

Ⅰ. 审… Ⅱ. ①坎… ②张… ③李… Ⅲ. 审计—管理信息系统 Ⅳ. F239.1

中国版本图书馆 CIP 数据核字(2004)第 105328 号

出 版 者: 清华大学出版社 **地 址**: 北京清华大学学研大厦
http://www.tup.com.cn **邮 编**: 100084
社 总 机: 010-62770175 **客户服务**: 010-62776969
责任编辑: 龙海峰
版式设计: 肖 米
印 装 者: 北京国马印刷厂
发 行 者: 新华书店总店北京发行所
开 本: 185×230 **印张**: 21.75 **插页**: 2 **字数**: 435 千字
版 次: 2004 年 11 月第 1 版 2004 年 11 月第1 次印刷
书 号: ISBN 7-302-09720-8/F·960
印 数: 1～3000
定 价: 39.00 元

丛书序 PREFACE

近年来，从美国的安然公司破产到世通公司的财务丑闻，从中国的银广夏、蓝田到中科创等违规案的公开舞弊都将注意力集中在财务报告的各个方面。作为美国公司的舞弊和给美国国会带来的相关压力的结果，《萨班斯—奥克利法案》于2002年夏天通过。美国证券交易委员会（SEC）和纽约证券交易所（NYSE）随后制定的规则和管制，对于上市公司的公司治理、内部控制将产生重大的影响。

法案的302节要求CEO和CFO就他们的内部控制系统进行报告，并在提交给SEC的财务报表上签字——以此作为保证，因此，这部法律将迫使高级执行官确保其内部控制系统的适当性；而法案的404节要求公司要：（1）陈述管理层建立和保持适当的内部控制结构和财务报告程序的责任；（2）在上市公司的财政年度末，对内部控制结构和财务报告程序的效果的评估。现在，NYSE第一次要求所有登记上市的公司都要有内部审计职能。

鉴于这部法案使公司治理、内部控制和内部控制系统的作用变得越发关键，董事会、高层管理者、外部审计师与内部审计师作为有效的公司治理的基石，会成为开展上述关键、必需职责的重要组成部分。

中国公司治理结构存在先天性的缺陷以及组织基础的稚弱问题，更加大了公司治理和内部控制的难度。公司治理问题、会计师违规问题以及有关部门的立法事件使审计行业的作用和重要性大幅提升。

本期引进的6本书顺应了国内外审计业近些年的重大发展，总体上能够代表国外审计理论研究的最新成果，同时反映出国外审计实务的发展状况，尤其是内部审计行业。6本书的选题务实，密切关注业界的核心主题，如内部控制、控制自我评估、风险管理、会计师咨询、信息系统审计、审计部门管理，可以说，每个主题都会对中国的审计实务界产生重大的影响。另外，上述内容的读者群绝不仅限于会计审计业，公司的高层管理者、董事会成员以及相关专业人士也会从中受益。

《超越COSO：加强公司治理的内部控制》一书对COSO报告如何运用于各种强制的控制提供了清晰的指导，并且其重要性还表现在其严格的框架体系，使公司的执行官和领导者将内部控制职能转化为有价值的战略工具，这在平衡公司各种力量以及提高业绩方面更为突出。该书清晰解释了COSO报告的复杂内容，对遵守COSO报告要求的既定技术作出了描述，为内部控制对业务流程的监督提供了详尽的理由，为如何更为有效率地开

展内部控制提供了专家性建议，并列出了大量可用的内部控制文献。该书对内部审计师、外部审计师、咨询师、财务总监、审计委员会成员以及公司管理者而言是一本极具价值的工作参考书。

《控制自我评估：以协调为基础的咨询指南》一书是国外第一本全面介绍控制自我评估技术运行机理的著作。该书概括了改进业务流程的最佳方法，一改以往传统咨询一对一的面谈方法，作者以协调为基础的咨询理念使咨询工作上升到"共享知识，达成一致"的境界，使员工能面对面地讨论公司不断作出的政策和进行的实务，削减了部门间的沟通幅度，使所有的观点意见都有公平表述的机会，最终能收集到对有关共识问题的解决方案。该书强调"如何做"，为从事咨询工作的人士评估和管理业务风险提供了实战技术，并对于理解控制自我评估简易化的流程提供了全面的指导，是一本非常有用的工具书，适用于咨询业、会计业。

《咨询的核心概念:面向管理者和会计师》一书是应对会计行业面临各种咨询压力和机会而最新推出的著作。该书详细介绍了会计咨询师的基本技能、推销、开发和管理咨询项目、咨询流程、会计师咨询的特殊问题等内容，对于广大从事会计审计咨询服务的人士特别有用。

《管理审计职能：公司审计部门程序指南》一书是依据最新公布的内部审计专业实务标准推出的力著，它为成功地开展内部审计制定了有效的程序，并用大量篇幅描述了内部控制、风险评估、控制策略和恶意活动、质量保证等主题。通过运用书中提到的权威指南，内部审计师在提高公司的整体业绩方面将发挥不可或缺的作用。此外，书中还涉及以下几方面重大内容：讨论了世界级审计部门的实务经验、平衡记分卡以及其他持续的改进技术；对内部审计工作的管理到报告的各项工作进行了详细的描述；概述了信息系统审计标准；介绍了质量保证和营销审计以及管理高层和董事会成员应该学习的内部控制系统的模型、工具和技术等有关内容。该书为会计、审计专业人员提供了有价值的指导和参考，是每个审计部门应备的参考手册。

《审计信息系统》(第2版)一书清晰解释了如何审计各类信息系统环境下的控制和安全问题。随着网上工作和企业资源规划（ERP）系统对企业资源的集中使用，信息系统完整性问题益发突出。本书赋予审计师、信息安全专业人员、管理者和审计委员会等不同层面有效地衡量信息系统控制的充分性和有效性的方法，并且书中有关的概念和技术使他们能真正的理解其所在机构的计算机系统的安全性问题。另外，本书为审计适用于所有计算机环境的信息系统提供了一个简易、务实的指南，并致力于当前信息经理们最为关注的特别问题，书中所附的80个案例翔实描述了运用于现实环境下的相应概念，其相关的主题有：信息系统审计方法（物理安全、逻辑安全、环境安全）；安全资格认证（如SAS70、CPA系统安全、网上信任认证）；电子商务和因特网安全；信息私密的法律和规章；信息系统项目管理控制以及新技术和未来的风险等内容。该书是每位审计师书

库中的必备参考书。

《风险的简要规则：再看金融风险管理的艺术》一书主要针对与风险理念、治理构架、风险确认、风险量化、风险监督/报告、风险管理等有关问题的开发与实施，并提供了实务细节和建议。该书对20世纪70年代以来的以数学模型和数学技术来管理风险的量化方法提出了不同的见解，并认为以风险接受为主导的机构应寻求定性与定量相结合的方法来管理其风险暴露，在量化方案中要加入判断、经验、市场知识和管理规定等定性因素，确保更为有效的风险管理框架。该书内容精简，通俗易懂，不失为了解金融机构风险管理的一本好书。

作为在公司治理、内部控制、风险管理、内部审计领域从事研究与实践的专业机构，德信思成将长期致力于上述各方面的研究和应用工作，并切切实实地为中国市场的各类机构提供多方面的服务，包括培训、咨询、顾问和提供完整的解决方案。我们也希望能与该领域的专家、学者和公司进行交流和合作，共同开拓公司治理、内部控制、风险管理、内部审计在中国的应用与发展。欢迎有幸读到本书的人员通过网站(www.dxsc.com 和 www.tup.com.cn）来了解相关的信息。

上述图书的选定得到了国内诸多专家的支持，我们对下列专家表示深深的谢意（排序以姓氏汉语拼音字母为序）：

陈汉文　厦门大学管理学院教授、博士生导师
陈　晓　清华大学经济管理学院会计系主任、副教授
陈小悦　国家会计学院院长、清华大学会计研究所所长、教授、博士生导师
陈信元　上海财经大学会计学院院长、教授、博士生导师
耿建新　中国人民大学会计学院院长、教授、博士生导师
胡玉明　暨南大学管理学院教授、博士生导师
罗　飞　中南财经政法大学会计学院院长、教授、博士生导师
李茂龙　中国注册会计师协会业务监管部主任、高级会计师
李若山　复旦大学管理学院教授、博士生导师
陆正飞　北京大学光华管理学院会计与财务管理系主任、教授、博士生导师
刘永泽　东北财经大学会计学院院长、教授、博士生导师
曲晓辉　厦门大学会计发展研究中心主任、教授、博士生导师
王立彦　北京大学光华管理学院教授、博士生导师
王智玉　国家审计署计算机技术中心主任、高级审计师
夏冬林　清华大学经济管理学院教授、博士生导师
尹　平　南京审计学院审计系主任、教授
杨雄胜　南京大学商学院会计系主任、教授、博士生导师
于增彪　清华大学会计研究所教授、博士生导师

杨志国　中国注册会计师协会标准部主任

易仁萍　南京审计学院院长、高级审计师

张金城　南京审计学院管理系主任、教授

张为国　中国证监会首席会计师、教授、博士生导师

本系列图书的翻译工作是集体劳动和智慧的结晶，是高效团队的有效运作，在此对每一位译者表示衷心的感谢。清华大学出版社的龙海峰编辑为图书的编辑、加工、润色付出了辛勤的劳动，在此一并致谢！

尽管我们尽了最大努力，但翻译中的不当之处在所难免，敬请广大读者雅正。

李海风

2004 年 2 月于北京紫竹院

序 言 PREFACE

审计师通常负有向管理者提供咨询的责任，以帮助确保机构内部存在充分、适当的内部控制，并将机构内的主要风险减缓到一个合理的水平。审计师运用职业判断来确认和量化风险，其职业判断是基于自身的知识水平、教育背景、职业经验以及历史事件。当重大事件发生时，审计行业就需要重新定位其风险评估的方法以适应新的环境。

1998年10月，在本书第1版出版之际，各类机构所面对的最大风险似乎是机构的内部人员滥用问题、黑客侵袭、病毒以及2000年问题。新闻报纸每天都充斥着新黑客和新病毒的故事，并在有些时候神化了这些黑客和病毒的创造者。巨大的人力和财力资源投入到了解决2000年问题的工程中。回想几年前，美国和许多其他的西方国家确实被dot-com公司的成功冲昏了头脑，并因而变得无知、自满，且以自我为中心。许多企业只关心利润，许多个人只关心自己及其反政府的论调。这是一个充满“自我”的世界，一种惟我独尊的气氛笼罩着这个世界。

在过去的4年里，接连发生的几件大事从根本上重塑了全球的社会和经营环境，这些事件已对我们这些审计人员所处的内部控制环境，无论是公共部门还是私人机构的，都产生了直接的影响。尽管以前我认为这是不可能的，但是最近发生的一些事件过于重大，以致重新定义了多数人看待风险的方式，我将特别讨论三个事件。

2001年的“9·11”事件

恐怖主义突然间成为所有风险中的头号风险，它甚至比战争更令人心神不宁。战争尚可在某种程度上预测敌方是谁以及在哪里交战，而恐怖分子通常是来去无踪影的，并能在任何地方、任何时间进行攻击，即便是美国的中心地带也不能侥幸逃脱。没有哪个机构可以忽略遭受恐怖分子袭击的可能性。

在本书的第1版中，1995年俄克拉何马州联邦大楼的爆炸事件以及1993年纽约世贸中心的爆炸事件是美国遭到的最严重的恐怖主义活动。美国政府怒火冲天，因为联邦大楼的爆炸案凶手居然是两个美国人。但是，上述罪恶行为与2001年的“9·11”事件相比，就显得苍白无力了，在这起事件中有上千人丧命，没有人能忘记那种惊惶和微弱的求助的感觉，尤其是当我们看到那曾几何时如双胞胎般的两座世贸中心的大楼，因本·拉登策划的飞机撞击而倒塌变形的那一刻，看起来坚不可摧的五角大楼也遭到了攻击，这超出了任何人的想象极限。

这起恐怖行为不仅造成了极大的物质上和情感上的创伤，它同时打击了世界经济系统的心脏。航空业突然间就处于永久性停飞的危险中，商业航空制造业随后就被迫减产减员。世贸中心内部的许多企业被重创，政府的各项资源不得不随即从社会服务方面转向国防。股市在 dot-com 的失败造成的震荡中进一步低迷，任何振兴经济的想法都遭到了扼杀。投资者们损失了上十亿美元，我们每一个人也都直接或间接地受到了影响。

甚至那些看起来精心准备的灾难恢复与业务重整计划也不再是那么完美无缺了。许多计划都基于这样的假设：人员和数据存储设备能在热站（hot sites）启动，交通便利，出行自由，手机能发挥作用。"9·11"攻击向我们表明，上述便利设施无一可用。为此，针对"9·11"事件发布的灾难恢复和业务重整计划应为每个假设做备份程序。

Dot-com 公司的失败

1999 年末，那些忽视格林斯潘(Alam Greenspen)著名的"非理性繁荣"描述的不切实际的 dot-com 股市开始摇摇欲坠。到 2001 年底，即便是昔日最牛气的 dot-com 公司也开始面临生存危机，许多蓝筹股甚至损失了一半以上的市值。事实证明，格林斯潘先生是正确的。多数 dot-com 公司的业务模式没有任何赢利基础，仅是形成了收入与无形的市场投资。许多 dot-com 的经营者没有经营及管理技能，空有一些技术，却从风险资本公司以及那些不具技术技能的华尔街投资者手中取得了上十亿的投资。这样的业务模式注定要在长期经营中失败。尽管许多人最初在 dot-com 股市中赚了数百万美元，但只有少数在 1999 年以前投资股票和期权的幸运儿可以收回本金，多数人丧失了一生的储蓄。许多主营退休金计划、共同基金、401（k）基金的机构投资者损失了投资者的上亿美元，许多个人再也不能挽回其损失。

"安然"的倒闭

2001 年末安然公司的倒闭事件恐怕是最糟糕的事情了，该事件指出审计师需要重新审视自己，重新评价自己及自身的道德行为。在众多有关高层管理者的不道德做法如何使一家看上去宏大的机构在短时间内迅速失败的故事中，安然事件是最近期间最值得关注的例子。对于安然和其他能源贸易公司操纵能源价格，致使个体消费者为能源账单多支付 2~3 倍价钱的情况，国内谴责之声不断。这种情况影响到美国的每一个公民，无论是直接增加能源价格，还是间接减少股票持有者或投资在 401（k）计划、共同基金和退休金计划的价值。有些州和地方政府投资了持有安然股票的共同基金也受到了损失，从而投资收益减少，而日益增加的政府需要以让他们减少公共服务、增加赋税，以此弥补损失。

内部控制的作用

作为上述事件的结果，全球各个机构不得不重估风险，重新思考其内部控制。由于

安然的倒闭，现今，高层管理者、董事会成员、外部审计师，甚至是内部审计师的道德行为都要比以往更为重要。高层的态度在每位审计师的内部控制清单中应列在最前面。如果安然执行了恰当的内部控制，公司就不会不计代价鼓励增长，也不会因如此造假高估价值而解体。

Dot-com 公司的失败已经使风险投资家和其他投资者对于新成立和现有公司的管理技能和业务模式进行了仔细的审核，公司自身也必须仔细地审核其内部控制，包括公司治理方面的控制，以确保能保持可行的业务。审计师必须在这一评估的过程中起关键作用。

尽管美国政府内部相对较好的内部控制可能延缓了“9·11”袭击的部分或全部损失，不过，很可能还有很多因素，不能完全阻止以后类似的悲惨事情的发生。诸如政府机构间更为及时和准确地沟通与协调等更好的内部控制，可能会让恐怖分子的步伐慢下来，并使其业务网络和财务网络陷入困境。经全面开发并测试过的灾难恢复与业务重整计划也可能会拯救某些机构，帮助其减轻那些能予以管理的其他冲击，从而经受住这次袭击。

审计师的作用

刚刚谈及的三大事件——“9·11”事件，dot-com 公司的失败以及安然倒闭，均指出每一个人都有必要关注 21 世纪的这些新风险带来的灾难性的影响，审计师的作用就在于确保管理层和各领域的领导者不再由于忽视因消除重要、必备的控制而引发潜在风险。我们再也不能用老眼光来看待风险，而要从历史中吸取教训，否则就会重蹈覆辙。潜在的风险类型仅受到我们的想象力，以及我们想象的全球范围内的邪恶的人和机构的限制。在我们的执业生涯中，当每次听到某位经理或执行官对重大的风险的控制不予重视时，我们都应保持信念，并不断提醒自己不能自满或屈服于无知、自负，否则，我们就是以机构的未来、我们的家庭以及我们的生活方式在冒险，使他们处于危险之中。

所有的机构都必须开展全面的风险评估，执行适当的控制，以帮助管理所有重大的风险。这样做的需要随处可见，但其紧迫性已明显增加。西方世界正处于随时会发生的袭击之中，这不仅仅是恐怖分子造成的，更常见的是由一些窃贼和其他罪犯造成的，他们不择手段获取金钱，以牺牲老百姓的良好生活秩序为代价，制造混乱。

由于计算系统在所有机构中都起着关键作用，所以，对这些系统和存储于其中的信息的保护就成为一个战略性的要求。对所有设备的物理安全控制（包含对那些家用计算系统和信息的控制）都应审慎地应用。同样，对计算系统和存储于其中的信息的逻辑安全控制也应确实存在。

在所有这些不幸事件中，还是有一些好消息的。用以评估计算和信息系统的物理和逻辑安全控制是否适当的审计方法基本上与过去的一致。本书提到的方法实际可应用

于任何的信息系统环境中，同 20 年前一样，它至今仍起作用，它在未来依然有用。

随着 20 世纪 80 年代以来计算系统类型层出不穷的增加，关键的计算系统程序以指数级在各机构增长，而多数都发生在终端用户环境中。 计算机处理速度的惊人增长以前所未有的速度，推进了各项业务的生产力。 如果一个计算系统得不到适当的保护，则同样巨大的处理能力也可以在真实世界范围内以指数级夸大控制隐患的重要性。 其结果是，公司要依赖越来越多的非技术性审计师，来确认风险，评价关键计算系统的控制适当性。 此外，在当今这个热衷于诉讼的社会中，审计经理、审计委员会成员、高层管理者、执行官以及董事会成员还必须了解对机构的关键计算系统的控制的适当评估是如何完成的。 否则，一旦机构遭受重大损失或因关键计算系统的控制不适当而失败时，他们就冒有个人承担责任的风险。

鉴于许多审计人员对他们借以有效率且有效果开展计算系统审计的技术和资源不熟悉，这成为一个主要的挑战。 这种情况在许多扁平化报告结构的公司里更为突出，这种结构缩减了审计部门，并因成本控制工作而使预算减少。 许多机构并没有专职的信息系统审计师，也不安排联系外部专家或咨询师的财务资源，用以评价关键计算系统和相关程序控制的适当性。 不过，由于机构不具备必要的用以评价关键计算系统控制和安全的资源和技能，他们正因其控制环境中存在的不利差距而面临重大的风险。

本书意在弥补这些差距，它向读者展示了一套简单、实用的方法，使读者理解如何在真实的计算系统类型下评估控制的适当性，不管这些计算系统是用于支持成百上千个应用程序的大型主机，还是运行在支持开发商应用程序的中型机，以及由机构内部的技术人员支持的广域网或局域网，传送或接收关键信息的独立的台式机，或是开发商的用以为其他机构处理数据的计算系统（这类开发商有时也被称为服务机构、服务处，或第三方处理者）。 本书无意成为一本包罗万象的审计信息系统的技术型百科全书，因为这方面的书已出版了很多本。 相反，我是想提供一种简单易行的审计信息系统的方法。然后，将这种方法辅之以现实世界的情形和例子，以阐明如何运用上述技术。 最后，本书还补充了关于控制自我评估、加密和密码学、计算机辩术、信息系统审计的人性化方面、信息系统项目管理等内容，以及我们迈进新千年所面临的其他的信息系统审计挑战。

本书所讲到的技术意在引起非技术类审计师、审计经理、审计委员会成员、负责关键计算系统的高层管理者、执行官和董事会成员的兴趣。 我希望上述成员在读完本书后，会对其所在机构遇到的审计或评价计算系统的审计过程备感轻松，同时我也希望本书能够成为审计专业学生、审计新人以及那些渴望成为信息系统（IS）审计专家的人员的一本参考书。 即便是对于有经验的信息系统审计师，本书也会提供一种独特的视角，至少其中的一些案例场景很有趣，有教育价值，且有些启发性。

本书假定读者对于审计程序的不同组成部分至少有一个基本的了解，这些组成部分

包括计划、风险评估、业务备忘录、系统描述或叙述、流程图和纲要图、审计方案（如要实施的一系列审计步骤）、测试、对工作底稿和其他测试材料的管理复核、与客户或被审计方管理层的结束会议、编制审计报告、管理层对报告中的建议的回应、事后审计调查，以及能确保恰当解决问题的建议追踪。

本书分为三部分。第一部分的章节主要探讨计算系统的基础，以及如何识别机构中的计算机系统领域。第二部分主要根据我自己开发的、针对与任何计算系统有关的主要风险的通用信息系统审计方案。如果恰当执行了该方案的步骤，读者就对关键控制部署在关键的计算系统上有合理的认同。读者还应能够得到充分的信息，以确定这些控制是否适当地保护计算机的硬件、软件和数据免遭未授权登录和意外或有意地破坏、变更。减轻这些风险将有助于机构实现其战略性的业务目标。

审计方案的步骤一般由4个部分组成：（1）环境控制测试；（2）物理安全控制测试；（3）逻辑安全控制测试；（4）信息系统操作控制测试。每一部分的概念都会在第4章到第9章详述，审计方案中将指出每一部分包含的章节。

本书的这样一种结构可以使读者不必查找全书就可找出探讨特定审计领域的相关章节，审计方案的有些步骤可能适用也可能不适用于某一特定的计算系统，但这些步骤集合起来却能针对实际中所有计算系统的风险和控制。第3章阐述了通用的信息系统审计方案，第4章至第9章与以下概念有关：信息系统安全政策、标准和指南；服务机构应用程序；服务机构和开发商评估；物理安全；逻辑安全以及信息系统操作。

第4章到第9章的第一部分都以为何要开展这个特定步骤的理论讨论开篇。在这些章节的第二部分，都以一个或多个案例场景来例证该章节的主要概念。这些场景都是以我多年的审计体验中遇到的实际发现、情况和事件为依据的。同时，我还描写并参考了各种其他的信息系统控制隐患给公司造成的损失或暴露机构的重大风险的事件。

第三部分包含的6章讨论了迈入新千年后，与我们密切相关的与时俱进的审计技术和问题。第10章对控制自我评估做了详尽讨论，这是一种带给全球审计行业震动的主导性审计技术；第11章讨论加密和密码学，它们是全球范围内保障信息电子交换安全的关键；第12章讨论了计算机取证；第13章讨论了各类信息系统审计挑战，包括计算机辅助审计技术，计算机病毒，软件盗版，电子商务，网络安全以及信息隐私权；第14章讨论了信息系统审计的某些人性化方面，这是一个为许多审计文献经常忽略的地方。毕竟，审计师也是人，也要经历每一个工作人员所面对的许多同样的欲望、需要以及顾虑。

由于我深信，要求所有的审计师在与审计相关的职业协会中积极活动相当重要，所以第14章的其中一节致力于这个主题。这一节的信息应该能激励读者在一家或多家协会积极活动，以增长知识和专业技能，扩大职业交际网，增强职业历程。

第15章讨论了与信息系统项目管理相关的风险和控制。

附录提供了其他参考信息，附录 A 提供了一系列可选择的职业协会和其他与信息系统审计和计算机安全有关的机构，并提供了每家机构的名称、电话号码、网址和使命陈述。附录 B 是对信息技术安全评价通用标准的概述。附录 C 简要讨论了 ISO 的 7 层开放系统互联（OSI）模型，并附有一份与信息系统审计和计算机安全相关的参考书目清单。

尽管术语信息技术（IT）这个词已流行多年，但我依然认为信息系统（IS）这个短语更加精确一些，因为我们审计的不仅仅是技术。技术不应被视为一种真空存在的东西，相反，它必须被放入其所赖以生存的整个系统的环境中去检验，包括所有与人的接触。因而，我会在全书中继续使用“信息系统”这一短语。

为了不使本书形成以技术主导全文的风格，便于我与读者间的互动，本书以第一人称和第二人称写作。

致谢

我将致谢以下各人，感谢他们在本书的完成过程中提供的帮助。

我一生的伴侣，Shannon，由于她的耐心、爱和理解，我们一同经历了许多凌晨 3 点的写作过程；

我的两个儿子，Jonas 和 Joshua，感谢他们给我的爱，使我成为一个更好的父亲。

Sheck Cho，感谢他的衷心教导。

Steve Kirschbaum，感谢他对于本书的网络及因特网安全的指导。

我也要感谢以下部分计算机倡导者，有些人的书在他们去世多年后才出版。感谢他们创造了变革人类生活方式的技术，并创造了一个巨大的产业，使得我们这些信息系统审计专业人员可以享受一种美好的、有意思的且富有挑战性的生活。

Robert “Bob” Bemer，ASCII 码的创始人，他使该代码成为全球性的技术标准。20 世纪 50 年代，他还是开发 COBOL 编程语言的关键人员。

Tim Bernets-Lee，英国物理学家，1989 年他在 CERN 发明万维网（CERN 是瑞士日内瓦的一个粒子物理实验室）。

Fred Cohen 博士，1983 年，当他还是南加州大学的学生时，就写出了第一个计算机病毒程序来阐述这一概念。和多数计算机病毒程序的写作者不同的是，他的使命是帮助人类，而不是搞破坏。Cohen 博士还设计了一些确保音频网络、视频网络及数据网络安全的协议，并创建了第一个基于因特网的信息战争模拟室。

Seymore Cray，他在 1957 年与他人合伙创立了控制数据公司，随后制造出第一台使用晶体管而非电子管的计算机，使得机器变得更加可靠且部件更小，从而提高了台式机的性能。

Frences “Betty” Snyder Holberton，20 世纪 40 年代，他为军方设计出首台 ENIAC 数字计算机，随后又帮助创建了 COBOL 和 FORTRAN 语言。

Claude Shannon，被称为“数字化革命之父”，他在 1948 年列出一系列的数学公式，并通过这些公式减少了二进制数据——比特的传送过程，并计算出通过电话线或其他电信方式可传送的最大的比特量。

Ray Tomlinson，1971 年，在他将以前写出的两个程序（Sndmsg/Readmail 和 CYPNET）合并为一个单一的程序后，信息得以通过网络在两台计算机间传送，他选择符号“@”来区分用户名和主机名。

Unisys 公司，该公司在 1951 年 6 月 14 日引进了第一台 UNIVAC 计算机。

还有许多其他计算机倡导者，仍需要我去发现和认定。

目 录 CONTENTS

第1篇 核心概念

第2篇 标准信息系统审计方法