◆王光远◆时　现／主编

【内部审计前沿报告书系】

Global Technology Audit Guide

全球信息系统审计指南

（上）

●时　现●李庭燎／等译

中国时代经济出版社
China Modern Economic Publishing House

◆王光远◆时　现／主编

【内部审计前沿报告书系】

Global Technology Audit Guide

全球信息系统审计指南

（上）

●时　现●李庭燎／等译

中国时代经济出版社
China Modern Economic Publishing House

图书在版编目(CIP)数据

全球信息系统审计指南(上册)/时现,李庭燎等译.
—北京:中国时代经济出版社,2010.1
(内部审计前沿报告书系)
ISBN 978-7-5119-0077-7
Ⅰ.①全… Ⅱ.①时…②李… Ⅲ.①信息系统-审计-指南 Ⅳ.①F239.6-62
中国版本图书馆 CIP 数据核字(2009)第 232974 号

书　　名:全球信息系统审计指南(上册)
出 版 人:宋灵恩
作　　者:时现,李庭燎等
出版发行:中国时代经济出版社
社　　址:北京市西城区车公庄大街乙 5 号鸿儒大厦 B 座
邮政编码:100044
发行热线:(010)68320825　68320484
传　　真:(010)68320634
邮购热线:(010)88361317
网　　址:www.cmepub.com.cn
电子邮箱:zgsdjj@hotmail.com
经　　销:各地新华书店
印　　刷:北京市鑫海达印刷有限公司
开　　本:787×1092　1/16
字　　数:330 千字
印　　张:20
版　　次:2010 年 1 月第 1 版
印　　次:2010 年 1 月第 1 次印刷
书　　号:ISBN 978-7-5119-0077-7
定　　价:78.00 元(上、下册)

译　序

本书中 IIA 所使用的“技术审计”，其实质就是信息系统审计。

20 世纪 60 年代 IBM 出版《Audit Encounters Electronic Data Processing》一书，首次提出计算机审计概念，随着计算机技术的不断普及和发展，其审计的内涵和外延也不断拓展，进入 21 世纪，信息系统审计框架逐渐形成。

原本，信息系统审计与组织内部的管理审计是沿着技术和管理两条路线并行发展的，但因计算机应用技术逐步发展到信息技术和网络技术，并从早期的辅助应用演进为与企业的经营活动相融合，于是，相对独立的信息技术就从纯技术层面走向与财务管理、会计核算、组织营运等活动相融合的技术经济综合体。计算机技术的应用与发展，改变了企业、机关等组织的作业环境和作业条件，使现代企业运营对于信息技术与网络依赖与日俱增。在遵从 SOX 法案的过程中，尤其是在规范企业管理方面，信息系统起着极为重要的作用，因此，信息系统审计与内部管理审计相融合成为历史的必然。2005 年，IT 治理协会第三次修订了“信息及相关技术控制目标（Control Objectives for Information and Related Technology）”框架（简称 COBIT4.0），它与 COSO 和 SOX 紧密结合，将 IT 治理和 IT 控制纳入组织治理和组织内部控制范畴，该框架的颁布，加速了信息系统审计与内部管理审计的结合。

现实中一直存在信息技术与内部审计不能完全相融合的矛盾，许多内部审计人员具有

财务会计、企业管理或相关的专业背景，但对信息技术却知之甚少，从而无法很好地胜任信息系统审计工作。为了解决这个问题，大部分组织把这信息系统审计业务外包给计算机专家。这虽可解决技术性问题，但另外两个问题又随之而来：一是计算机专家不熟悉组织的营运和管理，不熟悉财务会计，依然无法很好地完成信息系统控制审计任务；二是外部专家介入，会在一定程度上给企业增加安全风险。

如何让内部审计人员胜任信息系统审计工作？首席审计执行官从哪里可以获得一套全面的信息系统审计标准？IIA 苦苦地思索并为之做出了不懈的努力。

1977 年，IIA 发布了“系统的可审性与控制”（Systems Audit Ability and Control，简称 SAC），这是一部探索如何科学地开展信息系统审计的研究报告，是一部影响内部审计发展进程的原创性著作。2001 年，IIA 第三次修订《内部审计专业实务框架》，将信息系统控制与审计纳入内部审计范畴；2006 年，IIA 制定了“基于风险的信息系统控制评价指南”即 GAIT（Guide to the Assessment of IT General Controls Scope Based on Risk），它是一套原则和方法，帮助企业评价信息系统控制的成本收益以及效率效果，一方面帮助企业识别信息系统控制中的关键因素，避免财务数据错弊发生；另一方面指导管理层和审计人员识别信息系统的关键控制点，以满足企业遵守 404 条款的要求。GAIT—使信息技术与内部控制、风险管理的融合初现端倪。2009 年，IIA 颁布了第四次修订的《国际内部审计专业实务框架》，再度强调 IT 审计的重要性；最近，IIA 又推出了《IT 审计》月刊杂志，它为内部审计师提供了第一手 IT 审计信息资源，帮助内部审计师和 IT 专家们在世界范围内共享信息和交流经验。

2005 年，由当时的 IIA 主席大卫·理查兹（David A. Richards，CIA，CPA）发起了名为《IT 控制指南》的项目计划，该指南后来成为 GTAG（Global Technology Audit Guide，全球技术审计指南）指南系列中的第一个，从此，以信息系统控制为起点，系列指南陆续产生。到 2009 年 3 月，GTAG 系列已经包括了 12 个成熟的指南，分别是：《信息技术控制》《变更和补丁管理控制：组织成功的关键》《连续审计：对保证、监控和风险评估的意义》《IT 审计管理》《管理和审计隐私风险》《IT 弱点的管理与审计》《信息技术外包》《应用控制审计》《身份和访问管理》《业务持续性管理》《制订 IT 审计计划》《IT 审计项目》。该系列指南已被《国际内部审计专业实务框架》列入推荐执行之列。

本书主要包括如下三部分内容：

第一部分：信息系统审计的内容。指南1～3主要涉及的是信息系统控制与审计的问题。这三个指南从信息系统控制概念入手，明确了IT控制的内容、类型及与组织控制、IT治理、IT管理之间的关系，建构了IT控制框架，规定了IT控制测试与评价的程序与方法。以此为基础，指南系列逐步确立了变更和补丁管理控制的基本思路和方法，并系统地设计了连续审计的路径框架；指南12以IT项目为对象，从IT项目概念介绍开始，逐渐深入地分析了影响IT项目成功的主要因素、IT项目管理与组织管理之间的关系，确定了内部审计在IT项目中的角色，并明确了IT项目审计的思路、方法及组织管理要求；指南5、6从IT审计延伸到隐私审计、IT薄弱点审计及相关的管理要求部分。其中指南5提出了隐私和隐私风险的概念框架，确立了内部审计在其中的角色、审计程序和审计方法；指南6提示审计人员注意识别与确认IT弱点，关注IT薄弱环节对组织效率和营运效果可能带来的负向影响，设计了延伸到薄弱点管理与审计的操作框架。

第二部分：IT审计程序、审计技术与审计方法。指南7～11从信息技术外包、审计应用控制到身份识别和访问管理、业务持续性计划与开发IT审计计划，逐渐深入系统地确定了IT审计的基本程序、特别技术和主要方法等工具性内容及应用要求。与其余的指南前后呼应，相得益彰。

第三部分：IT审计质量控制与管理。指南4从IT定义范围的界定开始，逐步研究了与IT控制审计有关的风险，并基于雪花理论、风险管理理论的分析，确立了内部审计人员在履行信息系统审计职责时应执行标准和管理框架，明确了IT审计资源管理的主要内容，提出了审计加速器的概念，架构了IT审计管理框架，为保障IT审计质量明确了管理的方向。

与一般的指南相比，本书有三个显著特征：1. 系统性。GTAG的每一个指南都从基本概念介绍开始，循序渐进地分析其所应用的基本理论，之后，设计作业流程、确认审计工具、设计审计路径。2. 依据的充分性和资源的丰富性。在每一个指南正文之后，都有大量的信息，提供指南设计时使用的政策、标准和文献的来源信息、研究机构、行业组织及相关的网站等，这样的信息，可以帮助使用者很好地追根溯源。3. 适用性和针对性。该系列指南将信息技术与组织活动紧密地融合起来，使原本分立的信息技术与内部审计相

互渗透，突出了内部审计人员使用的基本需要，能够达到帮助 CAE 更好地组织与参与信息系统审计的目的。

本书将 COBIT、COSO、SOX 有机地结合起来，使管理层和内部审计人员能够快速了解 IT 治理、IT 控制、IT 审计的实质性内容以及它们与企业的内部控制之间密不可分的重要联系。

本书的作者来自全球（主要是北美）各地，他们是从事内部审计和信息系统控制理论研究的专家、学者和实务工作者，如大学教授、董事会成员、首席执行官、财务主管、信息技术专业人员和安全管理人员等。

本书由南京审计学院和中国内部审计协会内部审计发展研究中心的各位学者翻译成稿，时现教授、李庭燎博士直接参与翻译工作，并负责全书的校译和总撰；张文秀博士、沈静秋女士对部分内容进行了校对；参加翻译的主要人员有张丽娟、刘丹丹、徐印、肖雨潇、时代、左海枝、彭红喜、徐菁菁、吴飞红、郑颖、郭凤仙、张汝晶、闫小莉、李蓉蓉、马欢欢、原丽丽、许开瑞等。

从 2005 年第一个指南发布，至 2009 年 3 月第 12 个指南面世，我们跟踪进行翻译和校对，经过 4 年多的努力，终于在今天奉献给大家，期望我们的努力能够帮助内部审计人员理解信息系统审计、掌握程序和方法，提高信息系统审计的效率和效果。

受水平和能力所限，翻译文尚有许多缺陷，敬请读者批评指正。

时　现

2009 年 9 月

目　录

1

信息技术控制

国际内部审计师协会（IIA）

成立于1941年的国际内部审计师协会是一个国际性的职业组织，总部设在佛罗里达州艾尔塔蒙特泉（Altamonte Springs），拥有来自一百多个国家超过十万名的会员和代表，该协会是专业领域认证、教育、研究和技术指南的公认权威、主要培训者和领导者。

该协会通过提供专门的培训和有针对性的资源来帮助读者了解最新的科技进展。来自IIA和德勤会计师事务所的信息技术审计课程，帮助读者跟上不断变化的信息技术系统并适应诸如《萨班斯—奥克斯利法案》的要求。协会专门为首席审计执行官、审计监督者所写的全球技术审计指南（GTAG），及时提出有关信息技术管理、控制或安全方面的问题。协会的“IT Audit”是读者免费指南的在线资源，在这里读者可以获得关于信息技术发展趋势及审计工具方面的信息。IIA的IT会议于2006年2月在美国佛罗里达州奥兰多市举行。

如需详细资料和加入IIA，请访问www. theiia. org

电子格式、印刷品、影印、复印件等其他形式。

IIA提供这份指南的目的在于宣传和教育。指南的作用主要在于提供信息，但并非正式的法律或会计建议。IIA发布的指南，并不提供以上建议，也不为法律或者会计结果提供保证。如有法律或者会计问题纠纷，应寻求专业人士协助。

1.1 主席的信

在担任IIA主席之前，我曾经担任过首席审计执行官（CAE），在履行首席审计执行官职责时，深切地感受到为首席执行官编写信息技术管理和控制指南十分必要。因此，当我荣任IIA主席后，首先启动了编写IT控制指南这个项目计划。该指南主要适用于管理人员，但同时也有助于技术人员能够更好地从管理和治理的角度看待问题。

本文以便于CAE理解的方式解释IT控制和审计实务，以使CAE理解并与其沟通对IT控制的迫切需求，为了使读者能够通过整体框架来评估IT控制以及根据需要解决具体问题，本指南还提供了对IT控制进行评估的关键要素，并特别关注在组织的关键部门中能够推进IT资源治理的人员的角色和责任。读者可能已经熟悉了本指南的某些方面，但其他部分的内容将对如何运用关键的审计策略提供新的视角。

我们希望这些可以用来帮助指导用户，使他们了解IT控制是什么以及为什么组织管理和内部审计都必须对IT控制的基本方法予以适当的关注，从而实现良好的治理。

虽然IT为业务增长和发展提供了机会，但它也带来了新的威胁和风险，如干扰（disruption）、欺骗（deception）、偷窃（theft）和欺诈（fraud）。外界的攻击威胁着我们的组织，然而，我们所信赖的内部人员可能会是一个更大的威胁。所幸的是，在本指南中用户可以发现，技术也可以提供保护以免受这些威胁。管理人员应该知道该问的问题以及它的答案意味着什么。例如：

- 我们为什么要理解IT控制？答案是：保证。管理人员在保证信息可靠性方面起关键作用。保证，主要来自一系列相互依存的经营控制，再加上一些证据，这些证据可以证明控制是连续和充分的。管理和治理必须衡量由控制和审计提供的证据，并得出是否提供合理保证的结论。本指南将帮助您理解这些证据。
- 什么将受到保护？答案是：需要保护的对象首先从信任开始。信任有助于组织正常