

布林克现代内部审计

——通用知识体系(第7版)



**Brink's Modern Internal Auditing:
A Common Body of Knowledge, Seventh Edition**

【美】 罗伯特·R·穆勒 (Robert R. Moeller) 著

章之旺 等译



中国工信出版集团



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

華信
經管
大
引
進
精
品

布林克现代内部审计

——通用知识体系(第7版)



Brink's Modern Internal Auditing:
A Common Body of Knowledge, Seventh Edition

【美】 罗伯特·R·穆勒 (Robert R. Moeller) 著

章之旺 等译

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

《布林克现代内部审计：通用知识体系》第7版不但内容更加丰满、结构更加合理，而且具有很强的理论前瞻性，能够引领内部审计的未来发展。该版本引入了内部审计通用知识体系(CBOK)概念，内容既涵盖内部审计师需要熟练掌握的知识领域，也包括内部审计师仅需一般了解的知识领域，充分考虑了内部审计理论体系的完整性。

本书不仅适合作为高等教育中内部审计课程的专业教材，也可作为从事内部审计工作的人员的参考工具书。

Brink's Modern Internal Auditing: A Common Body of Knowledge, Seventh Edition

ISBN: 978-0-470-29303-4

Robert R. Moeller

Copyright © 2009 John Wiley & Sons, Ltd.

All rights reserved. This translation published under license.

Authorized translation from the English language edition published by John Wiley & Sons, Ltd.

Copies of this book sold without a Wiley sticker on the back cover are unauthorized and illegal.

本书简体中文字版专有翻译出版权由 John Wiley & Sons, Ltd. 授予电子工业出版社。未经许可，不得以任何方式复制或抄袭本书的任何部分。

本书封底贴有 John Wiley & Sons, Ltd. 防伪标签，无标签者不得销售。

版权贸易合同登记号 图字：01-2013-2464

图书在版编目(CIP)数据

布林克现代内部审计：通用知识体系：第7版/(美)穆勒(Moeller, R. R.)著；章之旺等译。

北京：电子工业出版社，2015.5

(华信经管引进精品)

书名原文：Brink's Modern Internal Auditing: A Common Body of Knowledge, Seventh Edition

ISBN 978-7-121-24994-5

I. ①布… II. ①穆… ②章… III. ①内部审计 IV. ①F239.45

中国版本图书馆 CIP 数据核字(2014)第 279054 号

策划编辑：石会敏 章海涛

责任编辑：石会敏

印 刷：三河市华成印务有限公司

装 订：三河市华成印务有限公司

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

开 本：787×1092 1/16 印张：31.25 字数：800 千字 插页：1

版 次：2015 年 5 月第 1 版(原著第 7 版)

印 次：2015 年 5 月第 1 次印刷

定 价：72.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010)88254888。

质量投诉请发邮件至 zlt@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：(010)88258888。

译者序

本世纪初，安然、世通等财务丑闻的爆发促使内部审计从幕后走向前台，内部审计受到前所未有的关注，成为公司治理的“四大基石”之一。但是，毋庸讳言，内部审计实务的发展与其理论储备并不相称。实务工作者往往囿于“纷繁芜杂”的内部审计现状，对现代内部审计的完整框架缺乏清晰的认识。但是早在《布林克现代内部审计》刚出版时，维克多·布林克(Victor Brink)就已经奠定了现代内部审计的基本架构。该书第7版在迄今为止出版的内部审计经典教材中版次最高。较之前6版，《布林克现代内部审计(第7版)》不但内容更加丰满、结构更加合理，而且更具有理论前瞻性，能够引领内部审计的未来发展。这是我们选择将其译成中文的原动力。

我们翻译本书，还基于以下两点考虑：

其一，我们认同本书的写作风格。纵观国内外内部审计教材，写作风格大抵分为以内部审计业务为主线或以内部审计流程为主线。前者存在的主要问题是内部审计业务涉及的领域十分宽泛且很难按其重要性排序。本书采纳的是后一种风格。

其二，本书内容新颖、涵盖面宽。该版本引入了内部审计通用知识体系(CBOK)概念，内容既涵盖内部审计师需要熟练掌握的知识领域，也包括内部审计师仅需一般了解的知识领域，充分考虑了内部审计理论体系的完整性。正如作者所言——“成为一名杰出的内部审计师所必需的知识领域尽在本书囊括之中”。

本书的翻译由南京审计学院章之旺教授承担主译，历时1年半完成。具体翻译分工如下：南京审计学院王芳副教授(博士生)负责第2章、南京审计学院硕士研究生王玮负责第33章、李冰阳负责第34章。其他部分皆由章之旺教授翻译。在翻译过程中，硕士研究生王路、林夏菁、梁朔、薛茜文、丁慧茹、王亚堃、单淑敏、潘虹、杨芳、苏晗、范钦参与了初译和文字整理工作。电子工业出版社高等分社财经事业部石会敏主任对翻译工作提供了悉心指导。在此一并表示衷心的感谢！

章之旺

2015年2月

作者简介

罗伯特·R·穆勒(Robert R. Moeller)从事内部审计行业30余年。他既是几家公司内部审计部门的创立者,也曾为“财富50强”企业提供过内部审计咨询服务,并担任审计主管。

穆勒拥有芝加哥大学的MBA学位(财务方向),本科阶段获得工程学士学位。他还获得了CPA、CISA、PMP、CISSP等众多的职业资格。他曾担任致同国际(Grant Thornton)会计师事务所信息系统审计国内主管。在此期间,他制定了适用于整个企业的审计程序,主管信息系统审计工作,并负责芝加哥分所信息系统咨询业务。

1989年,穆勒受聘于西尔斯·罗巴克公司,这家公司当时由好事达(Allstate)保险公司、添惠(Dean Witter)公司、Discover信用卡以及西尔斯零售部等机构组成。穆勒为该公司创建了信息系统审计职能,并担任内部审计主管,拓展了大量的内部审计新业务。他一直积极投身于IIA和AICPA的工作,曾担任IIA芝加哥分会总裁、IIA国际先进技术委员会委员和AICPA计算机审计专业委员会主席。

1996年,穆勒成立自己的公司——合规与控制系统协会(Compliance and Control Systems Associates, Inc.),多次举办全美内部控制与公司治理研讨会。早在萨班斯法案出台之前,他就预见性地探讨了相关问题。他帮助EMC公司推出一项新的咨询业务,并担任电信领域的咨询专家和项目经理。同时他还承担着该公司全球范围的移动电话业务财务系统项目管理工作。近期穆勒一直在忙于制造业、保险业等行业的萨班斯法案404条款合规性指导工作。他始终保持着与整个内部审计职业界的密切联系。

穆勒和他的妻子洛伊斯生活在芝加哥。他们喜欢夏天在密歇根湖上泛舟,冬天去科罗拉多和犹他州滑雪。他们爱好旅游、烹饪、种植蔬菜,并经常去芝加哥市区的各类剧场享受戏曲与音乐。

前 言

本书作为内部审计专业指南，旨在告诉读者如何成功地实施内部审计业务，以及企业如何建立有效的内部审计功能。本书的历史可追溯至第二次世界大战结束之初维克多·布林克撰写的第1版《现代内部审计》。当时的内部审计人员地位低下，只能算是会计文员或是为外部审计师提供文书支持服务的助理人员。但是布林克却深刻地洞察到内部审计作为一个新兴职业，应该为管理层提供更为广泛的服务。在本书的第1版中，布林克就已经奠定了现代内部审计的基本架构。

当今的内部审计工作必须面对不断变化的环境。内部审计师应提高对许多领域的了解和掌握程度，但很难将这些领域按重要性排序。本书的内容既涵盖内部审计师需要熟练掌握的知识领域，也包括内部审计师仅需一般了解的知识领域，二者共同构成内部审计通用知识体系（Common Body of Knowledge, CBOK）。

内部审计实践的重要性已得到当今全球范围内企业的认同。高管层、政府监管者及其他专业人士需要了解内部审计师的作用和能力。正如内部审计师需要通过CBOK更好地界定其职业，外部人员也需要了解内部审计师的职责，以及他们是如何从各个层面服务于管理者的。

本书介绍内部审计CBOK——对所有内部审计师都很重要的知识领域。无论内部审计师的经验水平、所处行业或工作地点是否存在差异，CBOK都是共通的。本书对CBOK主题的选择是基于作者在内部审计领域积累的多年经验、广泛的审计活动和阅读基础之上的。

下面列出每一章涉及的部分CBOK要素。

第一篇：现代内部审计基础。本篇的两章内容属导论性质，强调内部审计的重要性在企业、政府和其他活动中日益凸显，以及为什么需要CBOK。

第1章，内部审计基础。介绍内部审计的源起。虽然这些信息不属于关键CBOK，但了解内部审计的背景知识与历史，对当下的内部审计人员无疑非常重要。

第2章，内部审计通用知识体系。解释CBOK概念，并说明CBOK对所有内部审计人员的重要性。

第二篇：内部控制的重要性。内部控制评价是内部审计的重要活动。本篇的4章内容介绍萨班斯法案下的内部控制评价以及其他内部控制框架。

第3章，内部控制框架：COSO标准。COSO内部控制框架已成为评估内部控制的全球标准。所有的内部审计师都需要理解COSO内部控制框架模型，并能将其用于内部控制评估。

第4章，萨班斯法案及其他规定。萨班斯法案于2002年在美国获得通过。该法案几乎在全球范围内彻底改变了我们评估内部会计控制的方式。本章探讨萨班斯法案的现状，包括新发布的第5号审计准则。萨班斯法案的相关条款对内部审计师至关重要。

第5章，其他内部控制框架——CobiT。当今世界信息技术的应用甚广，内部审计师亟需一个度量和评估IT内部控制的指导框架。信息及核心技术工具的内部控制目标是关键所在。所有内部审计师至少应当对全球认可的CobiT内部控制框架做一般了解。

第6章，COSO企业风险管理框架。风险管理是一个重要的内部审计知识领域。内部审计

师应当掌握 COSO 的 ERM 模型，并将其用于内部审计计划与评估活动。本章介绍风险管理框架，并说明其对于内部审计师的重要性。

第三篇：计划与实施内部审计。本篇共 5 章，介绍现代内部审计的一些重要概念和基本要素。

第 7 章，实施有效的内部审计。本章简介如何计划、实施和完成一项有效的内部审计，阐述了内部审计师实施审计业务所需的基本步骤。

第 8 章，内部审计专业实务准则。所有内部审计师都需要掌握 IIA 发布的这些准则。本章对内部审计专业实务准则中的重要部分进行概述，并提供查找进一步信息的途径。

第 9 章，测试、评估与评价审计证据。内部审计的主要活动就是检查原始记录或由加工信息形成的审计证据，判断其是否满足既定的审计标准。这是内部审计的基本技能要求。

第 10 章，编制审计方案与确定审计范围。企业的许多领域都在内部审计可承担业务的潜在范围之内，但是内部审计师需要筛选、确定实际的审计范围。本章针对如何确定审计范围、如何编制审计方案提供具体指导。

第 11 章，控制自我评估与标杆法。IIA 在这一方面制定了很多标准，以指导评估工作。本章介绍这些评估流程。

第四篇：组织与管理内部审计活动。本篇的 6 章内容介绍内部审计启动、实施与完成的业务流程。

第 12 章，内部审计章程与内部审计职能的建立。在内部审计职能的建立与管理方面有着大量的最佳实务。本章的主题是新企业内部审计职能的初设，包括内部审计章程的制定。

第 13 章，内部审计关键胜任能力。内部审计师除了要掌握萨班斯法案的关键要求、IT 一般控制等技术性较强的技能之外，还必须具备访谈、写作等其他关键胜任能力。本章集中探讨各级内部审计人员所需的必要技能。

第 14 章，了解项目管理。不论是制定下一年度审计进度安排，还是对特定的审计业务进行规划，各级内部审计人员都需要掌握项目管理技术。本章探讨内部审计项目管理。

第 15 章，计划与实施内部审计。与其他章节讨论技术性更强的内部审计技能不同，本章归纳总结实施内部审计业务的基本步骤。

第 16 章，通过流程建模和工作底稿记录审计结果。内部审计师需要运用富有效率、经济可行的审计程序评价和记录各类业务流程。在此，我们提供许多可供选择的程序。本章介绍如何从内部审计的视角理解这些流程，并通过审计工作底稿予以记录。

第 17 章，内部审计结果报告。报告内部审计工作结果并提出整改建议是内部审计的主要工作。本章为如何形成有效的内部审计报告提供方法论指导。

第五篇：信息技术对内部审计的影响。内部审计师必须懂得如何评估 IT 控制以及将 IT 运用到内部审计实施过程中。本篇共 5 章，拟概述这些重要的内部审计 CBOK 领域。

第 18 章，IT 一般控制与 ITIL 最佳实践。本章阐述 IT 一般控制的审计流程。此外，本章还介绍国际认可的、旨在推进业务运营与 IT 职能之间协作关系的最佳实践——ITIL，并说明 ITIL 对内部审计师的重要性。

第 19 章，IT 应用控制的审查与评价。除了 IT 运营的一般控制之外，内部审计师还要懂得如何审计特定应用的内部控制，这些特定应用涵盖的范围很广，从办公桌面程序到企业大型应用软件，不一而足。本章主要介绍 IT 审计最佳实践。

第20章，网络安全与隐私控制。IT安全与隐私问题需要专门化的技能，这往往超出了许多内部审计师的能力范围。本章旨在介绍一些基本的网络安全与隐私控制概念，以及内部审计师在这一领域的最低知识要求。

第21章，计算机辅助审计工具与技术(CAATT)。内部审计师在评估自动化应用软件与流程时应通过计算机实施审计。本章介绍一些计算机辅助审计工具与技术(CAATT)以及信息系统审计工具。

第22章，业务连续性计划与IT灾难恢复。内部审计很早就要求对重要电子文档进行备份，目的是在IT服务中断时能够恢复数据。本章探讨业务连续性计划，重点介绍专门用于恢复IT与业务运营的工具和程序。

第六篇：内部审计与企业治理。本篇的4章内容突破了内部审计范畴，探讨内部审计与审计委员会的关系，以及道德程序与舞弊调查等领域的重要性。

第23章，与审计委员会沟通。萨班斯法案规定，内部审计向审计委员会报告工作。这种报告关系虽然在很大程度上属于审计管理的范畴，但所有内部审计师应清楚地认识到其在这种报告关系下所起的作用与应承担的职责。

第24章，道德规范与举报计划。萨班斯法案和企业治理实践的发展要求企业应建立道德规范与举报计划。本章提出内部审计能够改进道德领域运作的举措。

第25章，舞弊检测与预防。舞弊识别与检测是内部审计的重要技能。本章专门讨论这些有助于准确定位舞弊风险的基本内部审计技术。

第26章，HIPAA、GLBA及其他合规性要求。在美国，很多法规对企业提出了合规性要求，如健康保险转移和责任法案(HIPAA)、格雷姆-里奇-比利雷法案(GLBA)等。本章拟阐述这些法规中与企业治理和内部审计相关的重要规定。

第七篇：职业内部审计师。本篇的3章介绍几种内部审计职业资格，并讨论内部审计师在企业中的顾问角色。

第27章，职业认证资格——CIA、CISA及其他。诸如CIA一类的职业资格证书对内部审计师很重要。本章介绍几种重要的内部审计职业资格及其认证要求。

第28章，作为企业顾问的内部审计师。直到最近，IIA准则还禁止内部审计师在曾经接受审计的同一领域承接咨询业务。修订后的IIA准则允许内部审计师担任其所在企业的顾问。本章探讨内部审计作为企业顾问这一新角色所发挥的作用和承担的责任。

第29章，持续审计与XBRL。本章探讨这两个重要的审计模式。持续审计通过自动化过程实施实时监控，建立审计预警机制。XBRL则是一种能够实现财务报表信息自动链接至其他内部与外部资源的编码技术。当今的内部审计师应当了解这两门技术。

第八篇：内部审计职业趋同——CBOK的要求。本篇内容包括质量审计的重要性和ISO对内部审计的影响。此外，我们还逐章进行总结，前述章节汇总起来即构成内部审计通用知识体系。

第30章，ISO27001、ISO9000和其他国际标准。随着企业运作的全球化，ISO质量标准体系的重要性日益凸显。本章阐述ISO流程，并针对其中与内部审计非常相关的部分做出评价。

第31章，质量审计与ASQ标准。以流程和产品为导向的美国质量协会(ASQ)设置了内部审计部，其审计程序类似，但不等同于IIA的内部审计准则。我们预期将来IIA和ASQ在专业上走向趋同。本章讨论ASQ内部审计程序及其与IIA的相似之处。

第 32 章，六西格玛与精益制造技术。全球范围内的企业利用六西格玛等技术提高运营效率。本章介绍一些对内部审计师有用的技术，探讨其如何应用于内部审计活动。

第 33 章，国际内部审计与会计准则。IIA 最初成立时仅是以美国为基础的组织，现在已发展成为真正全球性的职业组织。然而从全球范围来看，内部审计的实务和准则还是存在一定的差异。本章探讨内部审计和其他相关全球性标准存在的重大差异。此外，本章还讨论美国采纳国际财务报告准则对内部审计的潜在影响。

第 34 章，适用于现代内部审计师的通用知识体系。最后一章对哪些是内部审计师必须熟练掌握、哪些是内部审计师只需一般了解的知识领域进行归纳总结，形成内部审计 CBOK 建议。

本书是第 7 版，我们更加侧重于介绍对当今内部审计人员来说比较重要的知识领域。尽管书中有些主题可能会随着时间的推移而改变，但总体而言，成为一名杰出的内部审计师所必需的知识应当尽在本书。

目 录

第一篇 现代内部审计基础

第 1 章 内部审计基础	2	职业的经验	7
1.1 内部审计历史与背景	3	2.2 国际内部审计师协会 CBOK	
1.2 本书架构	5	研究基金会	8
第 2 章 内部审计通用知识体系	7	2.3 内部审计师需要懂什么	12
2.1 何谓 CBOK——来自其他		2.4 现代内部审计 CBOK 展望	12

第二篇 内部控制的重要性

第 3 章 内部控制框架：COSO 标准	14	4.1.2 第 II 章：审计师的独立性	37
3.1 有效内部控制的重要性	14	4.1.3 第 III 章：公司的责任	39
3.2 内部控制标准：相关背景	15	4.1.4 第 IV 章：强化财务信息	
3.2.1 1977 年《反海外贿赂法》对内部		披露	42
控制的定义	16	4.1.5 第 V 章：分析师利益冲突	46
3.2.2 《反海外贿赂法》之后的		4.1.6 第 VI 章至第 X 章：舞弊责任和	
情况	17	白领犯罪	46
3.3 Treadway 委员会成立的背景	17	4.1.7 第 XI 章：公司舞弊责任	47
3.3.1 早期 AICPA 准则：审计准则		4.2 根据第 5 号审计准则实施	
公告(SAS)第 55 号	18	404 条款评价	48
3.3.2 Treadway 委员会报告	19	4.2.1 404 条款：当今内部控制的	
3.4 COSO 内部控制框架	20	评价	48
3.4.1 控制环境	21	4.2.2 实施 404 条款合规性审计	49
3.4.2 风险评估	25	4.3 第 5 号审计准则与内部审计	54
3.4.3 控制活动	26	4.4 萨班斯法案的影响	55
3.4.4 信息与沟通	27	第 5 章 其他内部控制框架——CobiT	56
3.4.5 监督	29	5.1 CobiT 简介	56
3.5 COSO 内部控制框架的其他		5.2 CobiT 框架	57
维度	32	5.2.1 CobiT 要素：IT 资源	59
3.6 内部审计 CBOK 需求	32	5.2.2 CobiT 要素	59
第 4 章 萨班斯法案及其他规定	33	5.3 CobiT 在内部控制评估中的	
4.1 萨班斯法案的关键要素	33	应用	60
4.1.1 第 I 章：公众公司会计监督		5.3.1 规划与组织	62
委员会	34	5.3.2 取得与应用	63

5.3.3	交付与支持	64	6.3.4	风险评估	86
5.3.4	监控与评估	66	6.3.5	风险应对	87
5.4	CobiT 在萨班斯法案 404 条款 评价中的应用	69	6.3.6	控制活动	88
5.5	CobiT 认证框架指南	70	6.3.7	信息与沟通	89
5.6	CobiT 的未来展望	71	6.3.8	监控	90
第 6 章	COSO 企业风险管理框架	72	6.4	ERM 的其他维度——企业风险 目标	91
6.1	风险管理基础	72	6.4.1	运营风险管理目标	91
6.1.1	风险识别	73	6.4.2	报告风险管理目标	91
6.1.2	关键风险评估	75	6.4.3	合规性风险管理目标	92
6.1.3	定量风险分析	77	6.5	企业层面的风险	93
6.2	ERM 简介	79	6.5.1	涵盖整个组织的风险	93
6.3	ERM 的关键要素	81	6.5.2	业务单元风险	93
6.3.1	内部环境	81	6.6	风险的整合分析	94
6.3.2	目标设定	83	6.7	审计风险与 ERM 流程	94
6.3.3	事件识别	84	6.8	风险管理与 ERM 未来展望	95

第三篇 计划与实施内部审计

第 7 章	实施有效的内部审计	98	7.5.6	向管理层报告初步审计 发现	115
7.1	内部审计组织与计划	98	7.6	完成现场审计工作	116
7.2	内部审计准备活动	99	7.7	实施单项业务内部审计	117
7.2.1	确定审计目标	101	第 8 章	内部审计专业实务准则	118
7.2.2	审计进度安排与时间预算	101	8.1	内部审计专业实务准则	118
7.2.3	初步调查	102	8.1.1	IIA 准则制定的背景	119
7.3	开始审计	103	8.1.2	IIA 现行准则: 有哪些 变化	120
7.3.1	内部审计现场调查	105	8.1.3	2009 版内部审计新准则	120
7.3.2	内部审计现场调查的记录	106	8.2	IIA 准则的内容	121
7.3.3	内部审计现场调查的结果	106	8.2.1	内部审计属性准则	121
7.4	制定和准备审计方案	107	8.2.2	内部审计工作准则	123
7.4.1	审计方案格式及其制定	108	8.3	IIA 和 ISACA 的职业道德 规范	126
7.4.2	审计证据的类型	110	第 9 章	测试、评估与评价审计证据	129
7.5	实施内部审计	111	9.1	收集适当的审计证据	129
7.5.1	内部审计现场工作程序	112	9.2	审计评估与评价技术	130
7.5.2	审计现场工作技术支持	113	9.3	内部审计判断抽样	131
7.5.3	审计管理人员对现场工作的 监控	113	9.4	统计抽样简介	132
7.5.4	潜在的审计发现	114			
7.5.5	审计方案与进度调整	115			

9.4.1	统计抽样概念	133			
9.4.2	制订统计抽样计划	136			
9.4.3	审计抽样类型	138			
9.5	货币单位抽样	146			
9.5.1	货币单位抽样示例	146			
9.5.2	实施货币单位抽样测试	148			
9.5.3	评价货币单位抽样结果	148			
9.5.4	货币单位抽样的优势和 局限性	149			
9.6	变量抽样与分层变量抽样	149			
9.7	其他审计抽样技术	151			
9.7.1	多阶段抽样	151			
9.7.2	重复抽样	151			
9.7.3	贝叶斯抽样	152			
9.8	如何有效运用审计抽样技术	152			
第 10 章	编制审计方案与确定审计 范围	155			
10.1	内部审计范围与目标的确定	155			
10.2	内部审计能力与目标的评估	158			
10.3	审计时间与资源约束	159			
10.4	向审计委员会和管理层“兜售” 审计范围	160			
10.5	编制审计方案	161			
10.5.1	审计方案格式及其制定	161			
10.5.2	审计证据的类型	163			
10.6	审计范围与审计方案的调整	164			
第 11 章	控制自我评估与标杆法	165			
11.1	CSA 的重要性	165			
11.2	CSA 模型	166			
11.3	实施 CSA 流程	166			
11.3.1	实施协调性 CSA 评价	168			
11.3.2	实施问卷调查式 CSA 评估	169			
11.3.3	实施管理层分析式 CSA 评估	169			
11.4	评价 CSA 结果	170			
11.5	标杆法与内部审计	171			
11.5.1	应用标杆法改进流程	171			
11.5.2	标杆法和 IIA 的 GAIN 构想	173			
11.6	更好地理解内部审计活动	176			

第四篇 组织与管理内部审计活动

第 12 章	内部审计章程与内部审计职能的 建立	178			
12.1	建立内部审计职能	178			
12.2	内部审计章程	179			
12.3	内部审计人员	180			
12.3.1	CAE 的职责	180			
12.3.2	内部审计管理层职责	181			
12.3.3	内部审计人员职责	182			
12.3.4	信息系统审计专家	183			
12.3.5	其他内部审计专家	184			
12.4	内部审计部门的组织模式	184			
12.4.1	集权式与分权式内部审计 组织结构	185			
12.4.2	组织内部审计职能	186			
12.5	内部审计政策与程序	189			
12.6	内部审计的职业发展	190			
第 13 章	内部审计关键胜任能力	191			
13.1	内部审计关键胜任能力的 重要性	191			
13.2	内部审计访谈技巧	192			
13.3	分析技术	193			
13.4	测试与分析技术	193			
13.5	内部审计存档技术	194			
13.6	审计建议与整改措施	196			
13.7	内部审计沟通技巧	197			
13.8	内部审计谈判技巧	197			
13.9	对学习的承诺	198			
13.10	内部审计核心胜任能力的 重要性	199			

第 14 章 了解项目管理	200	16.3 内部审计工作底稿	218
14.1 项目管理流程	200	16.3.1 工作底稿标准	219
14.1.1 项目管理知识体系	201	16.3.2 工作底稿格式	220
14.1.2 制订项目管理计划	203	16.3.3 工作底稿文档管理	221
14.2 PMBOK 方案与项目组合 管理	205	16.3.4 工作底稿编制技术	224
14.3 组织流程成熟度模型	207	16.3.5 工作底稿复核流程	225
14.4 运用项目管理提高内部审计计划的 有效性	208	16.4 内部审计文档管理	226
14.5 项目管理最佳实践与内部 审计	208	16.5 内部审计档案管理的 重要性	227
第 15 章 计划与实施内部审计	209	第 17 章 内部审计结果报告	228
15.1 了解内部审计环境	209	17.1 内部审计报告的目的与 类型	228
15.2 记录与了解内部控制环境	210	17.2 内部审计报告	229
15.3 实施适当的内部审计程序	212	17.2.1 审计报告的模式	230
15.4 结束现场审计工作	212	17.2.2 审计发现的基本要素	232
15.5 实施内部审计	213	17.2.3 审计报告平衡表述指南	235
第 16 章 通过流程建模和工作底稿记录 审计结果	214	17.2.4 可供选择的审计报告 格式	236
16.1 内部审计存档要求	214	17.3 内部审计报告循环	237
16.2 适用于内部审计师的流程 建模	215	17.3.1 起草审计报告	239
16.2.1 了解流程建模层次结构	216	17.3.2 审计报告:跟踪和总结	241
16.2.2 描述和记录关键流程	216	17.3.3 审计报告和工作底稿 留存	242
16.2.3 流程建模与内部审计师	217	17.4 有效内部审计的沟通机会	242
		17.5 审计报告和理解内部审计	244

第五篇 信息技术对内部审计的影响

第 18 章 IT 一般控制与 ITIL 最佳 实践	246	18.3 大型机和遗留系统的组件 和控件	255
18.1 IT 一般控制的重要性	246	18.3.1 大型 IT 系统的特征	255
18.2 客户端-服务器与小型系统的 IT 一般控制	247	18.3.2 经典的大型机或遗留计算机 系统	257
18.2.1 小型业务系统的一般 控制	248	18.3.3 操作系统软件	257
18.2.2 小型系统的 IT 运营内部 控制	251	18.4 遗留系统一般控制审计	258
18.2.3 小型 IT 系统的 IT 一般控制 审计	252	18.5 ITIL 服务支持与交付系统 最佳实践	262
		18.5.1 ITIL 服务支持事件管理	264
		18.5.2 服务支持问题管理	265

18.6	服务交付最佳实践	269	19.7	IT 应用控制审计的重要性	299
18.6.1	服务交付服务水平管理	269	第 20 章	网络安全与隐私控制	300
18.6.2	服务交付财务管理	271	20.1	网络安全基础	300
18.6.3	服务交付能力管理	272	20.1.1	数据安全	301
18.6.4	服务交付可用性管理	273	20.1.2	IT 密码的重要性	302
18.6.5	服务交付连续性管理	274	20.1.3	病毒和恶意程序代码	303
18.7	IT 基础架构管理审计	274	20.1.4	网络钓鱼和其他身份威胁	304
18.8	内部审计 CBOK 对 IT 一般控制的要求	275	20.1.5	IT 系统防火墙	305
第 19 章	IT 应用控制的审查与评价	276	20.1.6	其他计算机安全问题	306
19.1	IT 应用控制的构成	277	20.2	IT 系统的隐私问题	306
19.1.1	应用程序输入要素	277	20.2.1	数据采集隐私问题	306
19.1.2	应用程序	279	20.2.2	在线隐私和电子商务问题	307
19.1.3	应用程序输出要素	283	20.2.3	无线电频率识别	307
19.2	选择应用程序进行审计	283	20.2.4	美国联邦隐私保护法的缺位	307
19.3	实施 IT 应用控制的基本步骤	284	20.3	IT 安全与隐私审计	308
19.3.1	执行应用程序穿行测试	286	20.4	内部审计部门的安全与隐私	309
19.3.2	制定应用控制目标	287	20.4.1	审计师电脑安全与控制	310
19.4	完成 IT 应用控制审计	288	20.4.2	工作底稿安全	310
19.4.1	阐明并测试内部控制审计目标	289	20.4.3	审计报告与隐私	312
19.4.2	完成应用程序控制审查	291	20.4.4	内部审计安全与隐私标准和培训	312
19.5	IT 应用控制审计示例——客户端—服务器预算系统	292	20.5	支付卡行业数据信息安全标准 (PCI - DSS) 基本原理	312
19.5.1	审查资本预算系统记录	292	20.6	内部审计在隐私控制与网络安全方面发挥的作用	313
19.5.2	识别资本预算应用程序关键控制	293	第 21 章	计算机辅助审计工具与技术 (CAATT)	314
19.5.3	执行应用程序合规性测试	293	21.1	CAATT 概论	314
19.6	正在开发的应用程序审计	294	21.2	CAATT 的必要性	316
19.6.1	启用前审计的目标和障碍	294	21.3	CAATT 软件工具	318
19.6.2	启用前审计目标	295	21.3.1	通用审计软件	319
19.6.3	启用前审计存在的问题	295	21.3.2	报告生成器语言	320
19.6.4	启用前审计程序	296	21.3.3	台式机和笔记本电脑 CAATT 工具	321

21.3.4	测试数据法	322	22.2.3	台式机和笔记本电脑应用程序的连续性计划	336
21.3.5	专用审计测试与分析软件	324	22.3	IT业务连续性计划的制订	337
21.3.6	嵌入式审计程序	325	22.3.1	风险、业务影响分析以及潜在紧急事件的影响	338
21.4	选择适当的CAATT流程	327	22.3.2	为可能发生的紧急事件做准备	339
21.5	CAATT应用步骤	328	22.3.3	灾难恢复：紧急事件的处理	341
21.6	应用CAATT获取审计证据	329	22.3.4	业务连续性计划培训	342
第22章	业务连续性计划与IT灾难恢复	330	22.4	业务连续性计划与服务协议	342
22.1	IT灾难与业务连续性计划现状	331	22.5	业务连续性计划新技术——数据镜像技术	343
22.2	业务连续性计划流程审计	332	22.6	业务连续性计划审计	344
22.2.1	内部审计师集中式数据中心BCP审查	332	22.7	业务连续性计划未来展望	344
22.2.2	客户端-服务器连续性计划内部审计程序	335			

第六篇 内部审计与企业治理

第23章	与审计委员会沟通	346	24.1.2	理解道德风险环境	361
23.1	审计委员会的作用	346	24.1.3	总结道德规范调查结果：是否存在问题	363
23.2	审计委员会组织与章程	347	24.2	企业行为准则	363
23.3	审计委员会财务专家与内部审计	351	24.2.1	行为准则的内容	364
23.4	审计委员会对内部审计的责任	352	24.2.2	与利益相关者沟通，确保遵守行为准则	365
23.4.1	CAE的任命	352	24.2.3	违反准则与纠正措施	366
23.4.2	批准内部审计章程	353	24.2.4	保持行为准则及时更新	367
23.4.3	内部审计计划和预算审批	354	24.3	举报与热线职能	367
23.4.4	审计委员会对重要的审计结果进行复核并采取措施	355	24.3.1	联邦举报规则	368
23.5	审计委员会与外部审计师	356	24.3.2	萨班斯法案举报规则与内部审计	369
23.6	举报计划与行为准则	356	24.3.3	设置企业求助或热线职能	370
23.7	审计委员会的其他职能	357	24.4	企业道德规范审计	371
第24章	道德规范与举报计划	358	24.5	改进公司治理实践	372
24.1	企业道德规范、合规性与治理	358	第25章	舞弊检测与预防	373
24.1.1	拟定使命声明	359	25.1	舞弊概论	373
			25.2	红旗标志——内部审计师的舞弊检测符号	374

25.3	公共会计师在舞弊检测中的作用	377	框架(PKI)和HIPAA安全规则	387
25.4	IIA 舞弊检测与调查准则	379	26.1.3 HIPAA 安全管理程序	388
25.5	内部审计舞弊调查	380	26.1.4 技术安全服务与机制	389
25.6	信息技术舞弊检测流程	381	26.1.5 HIPAA 和电子商务前瞻	389
25.7	舞弊检测与内部审计师	383	26.2 《格雷姆-里奇-比利雷法案》内部审计规则	390
第26章	HIPAA、GLBA 及其他合规性要求	384	26.2.1 GLBA 财务隐私规则	390
26.1	HIPAA: 健康保险及其他	385	26.2.2 GLBA 安全维护规则	391
26.1.1	HIPAA 病历记录隐私规则	385	26.2.3 GLBA 借口防备规定	392
26.1.2	密码系统、公共密码基础		26.3 其他个人隐私和安全立法要求	393

第七篇 职业内部审计师

第27章	职业认证资格——CIA、CISA 及其他	396	第28章	作为企业顾问的内部审计师	416
27.1	注册内部审计师的职责与要求	396	28.1	内部审计师担任企业顾问相关准则	416
27.1.1	CIA 考试	397	28.2	内部审计开展内部咨询活动所需要的能力	418
27.1.2	CIA 资格的保持	406	28.3	最佳咨询实务	420
27.2	IIA 其他认证资格	406	28.3.1	第一步: 接受咨询任务	420
27.2.1	注册内部控制自我评估师(CCSA)考试要求	407	28.3.2	咨询约定书	421
27.2.2	注册政府审计师(CGAP)考试要求	408	28.3.3	咨询流程: 对“理应是……”与“是……”目标的界定	422
27.2.3	注册金融服务审计师(CFSA)考试要求	409	28.3.4	咨询建议的实施	422
27.2.4	CIA 专业认证考试的重要性	410	28.3.5	记录与完成咨询业务	423
27.3	注册信息系统审计师的要求	411	28.4	内部审计服务拓展	423
27.4	注册信息安全经理资格	412	第29章	持续审计与XBRL	424
27.5	注册舞弊审计师	413	29.1	实施持续审计	425
27.6	信息系统安全职业认证资格	414	29.1.1	什么是持续审计监控流程	425
27.7	美国质量协会内部审计资格	414	29.1.2	应用CAA的资源	427
27.8	其他内部审计资格认证	415	29.2	持续审计的优点	429
			29.3	XBRL——基于网络的可扩展商务报告语言	429
			29.3.1	XBRL 定义	430
			29.3.2	XBRL 的实施	431

29.4	数据仓库、数据挖掘与联机 分析处理·····	432	29.4.3	在线分析处理·····	435
29.4.1	存储工具的重要性·····	432	29.5	新技术、持续结清与内部 审计·····	436
29.4.2	数据仓库和数据挖掘·····	433			

第八篇 内部审计职业趋同——CBOOK 的要求

第 30 章	ISO27001、ISO9000 和其他 国际标准·····	438	第 32 章	六西格玛与精益制造技术·····	466
30.1	ISO 标准在当今世界的 重要性·····	438	32.1	六西格玛——背景与概念·····	466
30.2	ISO 标准概览·····	440	32.2	六西格玛应用·····	467
30.2.1	ISO9001 质量管理体系与 萨班斯法案·····	440	32.2.1	六西格玛的领导职责·····	468
30.2.2	IT 安全标准：ISO17799 和 ISO27001·····	444	32.2.2	启动六西格玛项目·····	470
30.2.3	IT 安全技术要求： ISO27001·····	445	32.3	精益六西格玛·····	471
30.2.4	服务质量管理： ISO20000·····	446	32.4	六西格玛流程审计·····	473
30.3	ISO19011 质量管理体系 审计·····	447	32.5	六西格玛在内部审计中的 应用·····	474
30.4	ISO 标准与内部审计师·····	448	第 33 章	国际内部审计与会计准则·····	475
第 31 章	质量审计与 ASQ 标准·····	449	33.1	国际会计与审计准则演进·····	475
31.1	质量审计师的职责·····	449	33.2	财务报告准则趋同·····	476
31.2	质量审计师的作用·····	450	33.3	国际财务报告准则·····	478
31.3	实施 ASQ 质量审计·····	452	33.4	国际内部审计准则·····	478
31.4	质量审计师与 IIA 内部 审计师·····	454	33.5	内部审计准则未来发展·····	479
31.5	内部审计部门的质量认证·····	454	第 34 章	适用于现代内部审计师的通用 知识体系·····	480
31.5.1	内部审计质量认证的 价值·····	455	34.1	第一篇：现代内部审计基础·····	480
31.5.2	内部审计质量认证的 要素·····	456	34.2	第二篇：内部控制的重要性·····	481
31.5.3	谁来实施 QA·····	457	34.3	第三篇：计划与实施 内部审计·····	481
31.6	内部审计质量认证的实施·····	458	34.4	第四篇：组织和管理内部 审计活动·····	482
31.6.1	质量认证方法·····	459	34.5	第五篇：信息技术对内部审计 的影响·····	482
31.6.2	内部审计部门质量认证 示例·····	460	34.6	第六篇：内部审计与企业 治理·····	483
31.6.3	报告内部审计质量认证 结果·····	464	34.7	第七篇：职业内部审计师·····	483
31.7	质量认证审计未来展望·····	465	34.8	第八篇：内部审计职业趋同—— CBOOK 的要求·····	483
			34.9	适用于内部审计师的通用 知识体系·····	484