

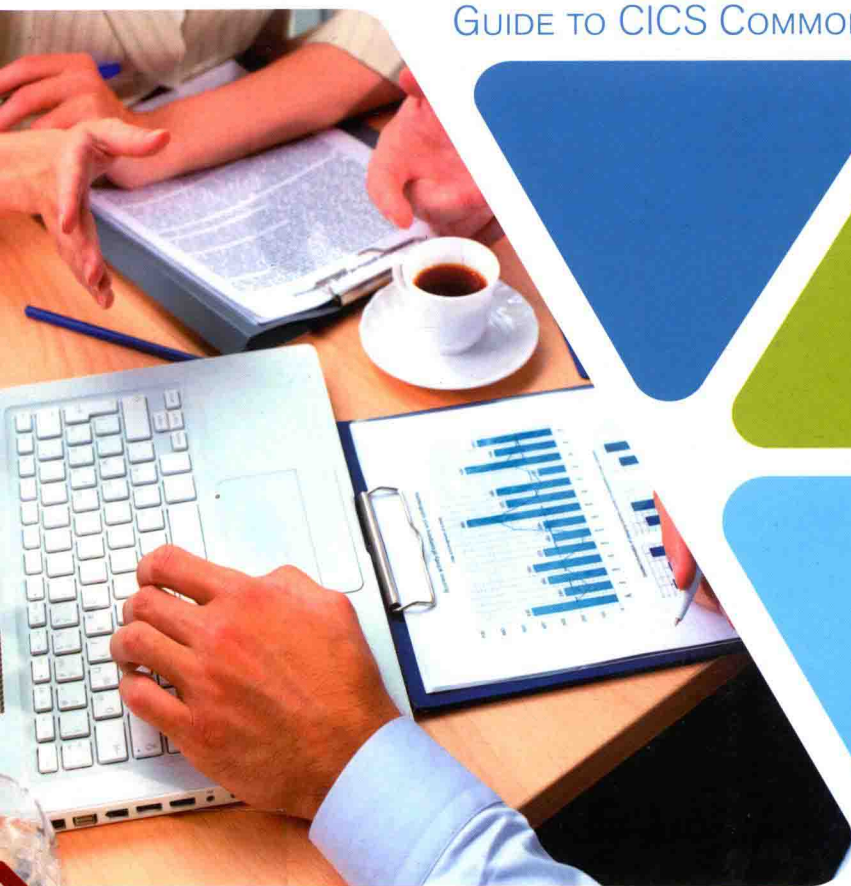
国际注册内部控制师（CICS）资格认证考试指定用书

内部控制管理技能

国际内部控制协会（ICI）编著

张玉 编译

GUIDE TO CICS COMMON BODY OF KNOWLEDGE



INTERNAL CONTROL INSTITUTE

国际注册内部控制师(CICS)资格认证考试指定用书

内部控制管理技能

国际内部控制协会(ICI) 编著

张 玉 编译

企业管理出版社

图书在版编目(CIP)数据

内部控制管理技能 / 国际内部控制协会(ICI)编著;张玉编译. -- 北京:企业管理出版社, 2017.9

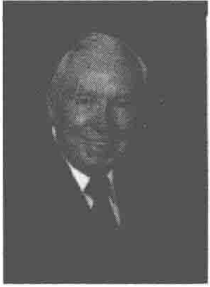
ISBN 978-7-5164-1585-6

I. ①内… II. ①国… ②张… III. ①企业内部管理-资格考试-教材 IV. ①F272.3

中国版本图书馆 CIP 数据核字(2017)第 213419 号

书 名:内部控制管理技能
作 者:国际内部控制协会(ICI)
译 者:张玉
责任编辑:张平 田天
书 号:ISBN 978-7-5164-1585-6
出版发行:企业管理出版社
地 址:北京市海淀区紫竹院南路 17 号 邮编:100048
网 址:<http://www.emph.cn>
电 话:编辑部(010)68701638 发行部(010)68701816
电子信箱:qyglcbs@emph.cn
印 刷:北京大运河印刷有限责任公司
经 销:新华书店
规 格:185 毫米×260 毫米 16 开本 24.5 印张 475 千字
版 次:2017 年 9 月第 1 版 2017 年 9 月第 1 次印刷
定 价:158.00 元

Make Internal Control Great Again



For too many people, including business executives, control is a negative term. That's wrong. Internal control should not be viewed as an expense, but rather a contributor to profit. Let's look at an easy to understand non-business example. When you are held up by a traffic light you think your travel time is being increased. Not true. Have you ever gone to a busy intersection without a traffic light and watched how very slowly traffic moves through an uncontrolled intersection? Integrating multiple traffic lights into a system, which is a system of internal controls, speeds up traffic even faster than a single traffic light. Internal control not only improves productivity, but minimizes the cost of errors and fines due to noncompliance to regulations. The Internal Control professionals need to continually market the value of internal control to their organizations. This can occur in many ways. Perhaps the most effective is to estimate the value of controls when they are installed versus the cost to build and operate internal controls. Other effective marketing approaches include explaining that internal controls are a part of a process (Dr. Deming's plan-do-check-act process model) , and publicize the potential costs of a lack of effective internal controls.

William E. Perry

Chairman Emeritus, Internal Control Institute

Founder of Internal Control Institute

Former President, Quality Assurance Institute

January 30, 2017

主席致辞

让内部控制再次伟大

对于许多人来说，包括企业高管，控制是一个消极的术语。这是不对的。内部控制不应被视为费用（成本），而是利润的贡献者。让我们来看一个容易理解的非商业例子。当你开车遇到红灯停止行驶时，你会认为这是在增加你的旅行时间吗？显然不会。你有没有去过一个没有交通信号灯管制的人车拥挤的十字路口，在那里你会看到车辆要通过不受控制的交叉路口，开车的速度有多慢。将交通信号灯集成到一个系统，即交通管理的内部控制系统中，可以比单一交通信号灯更快地提高车辆行驶的速度。内部控制不仅能提高生产率，而且可以最大限度地降低由于不遵守法规而产生的错误和罚款的成本。内部控制专业人员需要不断向他们的组织推广内部控制的价值。这可以采取许多方式，也许最有效的方法是，基于建立和运行内部控制的成本，来评估设置控制措施的价值。其他有效的方法包括，解释内部控制是业务流程的组成部分（戴明博士的计划、执行、检查、整改模型，即 PDCA 循环），并公布缺乏有效内部控制的潜在成本。

威廉·E. 佩里

国际内部控制协会荣誉主席

国际内部控制协会创始会长

美国质量保证协会创始人及原会长

2017 年 1 月 30 日

前 言

管理实践证明，企业一切经营管理活动，都是从建立和完善内部控制开始的。内部控制是企业运营和各项管理工作的基础，企业内部运行机制改革和管理模式的调整，都应统驭在完善的内部控制体系之下，并在合规合法的基础上运行，以规避变革中出现的各类风险，提升公司治理水平与核心竞争力。

现代内部控制包含着管理控制的精髓和理念，并渗透到企业经营活动的各个方面。加强内部控制的重要意义如下：

第一，以国家宏观和长远发展趋势为主的外部控制必须与企业微观的和日常发生的内部控制相结合，才能发挥其应有的作用；

第二，内部控制源于会计控制与审计，但经过演变，现已超越会计控制与审计的范畴，渗透到企业经营管理全过程，并要求企业全员全面地参与内部控制管理活动；

第三，企业内部控制以降低风险为导向，以业务流程为载体，以成本效益平衡为前提，其本质是将内部控制的要求融入各项管理体系中，形成防范风险和控制舞弊的长效制衡机制；

第四，在当今以信息化管理为主要手段的情况下，企业采用的多种控制措施及其不同的控制方式，应以信息化系统为管理平台，才能达到节约成本、提高效率，实现发展战略的目标。

内部控制贯穿于整个企业管理，与其他管理体系相辅相成、密不可分，是企业管理的重要组成部分。企业内部控制体系建设作为一项可持续发展的系统工程需要有完善的法规体系作保障。国际较为完善的与内部控制相关的法规体系大致包括四个层面的内容：一是基本法律；二是政府法规与部门规章；三是行业协会的标准与指南；四是可参考借鉴的最佳实务。从美国内部控制法规体系的框架看，在基本法律层面，1977年，美国出台的《海外反腐败法案》和2002年的《萨班斯-奥克斯利法案》等法律对企业实施内部控制具有强制性约束力；在政府法规与部门规章层面，美国证券交易委员会（SEC）2003年发布的财务报告内部控制的规则，美国上市公司会计监管委员会（PCAOB）发布的第2号与第5号审计准则，以及实务提示促进了内部控制相关内容的规范化；行业协会等社团组织，例如，美国反虚假财务报告委员会所属发起组织委员会（Commission of Sponsoring Organizations, COSO）发布的内部控制框架性指导文件，美国内部控制协会（ICI）发布的内部控制量化评分指南和业务系统

控制等指南，旨在增强实施内部控制法规的可操作性；而一些标杆企业，例如，美国的通用电气公司（GE）、西南航空公司（Southwest Airlines）、沃尔玛公司（WAL - MART）的内部控制实务经验为企业实施内部控制提供了可参考借鉴的行之有效的鲜活案例。

企业建立和实施内部控制是一项专业性很强的工作，要求相关人员具备丰富的专业知识和充足的职业经验。由于内控专业人才储备不足，或相关工作人员缺乏相应的知识和经验，从而影响企业开展内部控制建设的进度和质量。开展 ICI 国际注册内部控制师资格认证项目的培训，有利于培养和造就我国内部控制专业人才，有利于吸收和借鉴国际经验，形成符合我国企业特点的内部控制指标体系，促进我国企业内部控制体系建设与国际内部控制最佳实务的趋同发展。

国际注册内部控制师从事的主要工作包括：内部控制战略的开发、设计、执行和自我评价，以确保董事会和高级管理层制定的发展战略和经营计划得到贯彻执行。为此，要开展风险评估，对重大风险和可能产生舞弊的环节进行有效控制，对业务执行过程中发现的问题和控制缺陷及时整改，并向管理层报告。这样做，可以避免事后监督难以及时发现问题和控制缺陷，整改的时效性也相应滞后的缺点。可以说，内部控制管理已经渗透到企业经营管理全过程。通过全面梳理各项管理制度和管理体系，从管理体制、制衡机制，以及落实各级权力责任等方面，将内部控制的要求融入各项管理体系中，并利用信息技术固化业务流程，形成内部控制的长效机制，使内部控制真正为经营管理服务。

中国内部控制网将采用“图书 + 面授 + 网课”的方式，通过名师讲解本书与内部控制相关管理技能的重点内容，使学员融会贯通，学以致用；通过精准配置模拟考题，使得学员在学习掌握先进的国际内部控制知识与技能体系的同时，顺利通过资格认证考试。此外，在学员取得证书后，通过内控俱乐部的沙龙活动、在线专题培训和名企考察等活动，帮助持证者完成后续教育学习，不断更新知识和技能，同时增进相互之间的交流和友谊。

中经安信息科技（北京）有限公司

2017 年 8 月

译者的话

国际内部控制协会（ICI）创始会长和荣誉主席威廉·E. 佩里先生（William E. Perry）指出：“全球从事内部控制相关工作的大多数人都没有受过现代内部控制定义的适当教育或训练。值得注意的是，大多数的审计师，无论是独立审计师还是内部审计师，接受过的只是财务定义内部控制方面的培训”。正因如此，国际内部控制协会组织内控领域的专家、学者和咨询顾问编写了国际注册内部控制师资格认证考试指定用书《内部控制管理技能》。书中所述的这些技能有助于组织的管理者和内部控制专业人士应对内部控制领域所面临的挑战，增强为内控体系建设服务的本领。

本书是 ICI 国际注册内部控制师资格认证考试指定用书。本书共分两部分：第一部分包括两章内容，主要介绍国际注册内部控制师（CICS）资格认证项目意义与特点，国际注册内部控制师的申报条件和考试指南及相关要求；第二部分包括八章内容，分别介绍国际注册内部控制师必须掌握的八大技能。这八大技能涵盖了内部控制体系设计、执行、评价和改进全过程所需的理论知识和相关技术方法，注重理论与实际相结合，有利于学员学以致用。本书的逻辑结构如下：

技能一：介绍内部控制的基本原理、COSO 与 AICPA 的内部控制定义、PDCA 循环的概念。内部控制体系建设的灵魂是建立决策、执行和监督相互制约的制衡机制，为此，本章介绍了控制的层级制度和应建立的问责机制。

技能二：介绍建立内部控制环境的重要意义、管理层的职责和相关要求，有效控制环境的十大属性，建立授权、沟通、不相容职责分离、员工绩效考核、资产保护、监控等制衡机制及控制措施，以及如何构建计算机安全控制环境。

技能三：介绍风险管理的领域和概念。以风险为导向创建内部控制体系是一种成本较低和见效快的方法，故这一章阐述了 COSO 内部控制框架、风险因果关系分析、风险管理流程及其组成部分、内控系统三个层级的风险与控制，以及从五大业务循环入手解决风险管理的落地问题。

技能四：涉及业务层面内部控制评估，要求制定测评目标和编写评估方案，选择适用的评价标准，开展内控五要素测评的内容、评估需完成的核对清单和可采用的评估方法。

技能五：阐述在企业内外重大风险识别与排序之后，如何在业务系统中根据不同

层级的控制目标设置关键控制点。本章介绍了识别控制缺陷的风险暴露矩阵，业务系统交易处理六个环节的控制与评估，以及如何计算控制措施的成本效益。

技能六：主要介绍与风险评估相关的概念、风险分析流程、内外风险评分指标、五级风险的识别与排序以及量化风险的步骤等技术方法。

技能七：针对企业遵守《萨班斯－奥克斯利法案》的要求，介绍该法案的意向目标、七个层面合规性内控测评的重点和核对清单，如何汇总合规性评估结果，以便更好地向董事会和高级管理层报告。

技能八：阐述公司治理实务，本章介绍了三种被广泛接受的公司治理模型，ICI 公司治理模型，COSO 对董事会和高级管理层的控制目标，公司诚信道德价值观的治理要求，使用最佳实务实施治理的方法和改进公司治理流程。控制环境和业务层面实施的有效的控制举措，最终都将提炼和上升为公司治理机制或程序，旨在强化董事会对管理层执行的风险管理和控制过程进行监督，以保护股东和利益相关者的利益。

本书介绍了 2013 年 5 月 COSO 颁布新《内部控制——整合框架》的内容，包括内控新框架整体变化和拓展的领域，重点介绍 COSO 内控新框架五要素和 17 原则及其关注点，以及对企业建立有效内部控制体系的影响。此外，还介绍了近几年来美国加强内部控制相关的法律，例如《多德－弗兰克法案》《沃尔克规则》等。

译者在忠实原文的基础上，尽可能将书中较为晦涩难懂的词句翻译得通俗易懂，并符合中国人的阅读习惯。

在此，对协助完成本书翻译工作的人员邱健庭、孙彤、骆培涛、徐莉莉、张勉、孙月红、金琳、索源明、靳晔、高京，以及提出宝贵审稿意见的姜维壮教授、邱胜利主任表示衷心的感谢。

限于译者水平，本书如有误漏之处，恳请读者指正。

张玉

2017 年 7 月于北京

目 录

第一部分 国际注册内部控制师资格认证介绍

第 1 章	国际注册内部控制师资格认证概述	3
1.1	资格认证项目的背景与介绍	3
1.1.1	内部控制立法的背景	3
1.1.2	国际内部控制协会	4
1.1.3	组织实施内部控制的重要性	5
1.1.4	资格认证须知	6
1.2	成为国际注册内部控制师的好处	7
1.2.1	对内部控制职业发展提供的价值	7
1.2.2	对专业人士提供的价值	8
1.2.3	对用人单位提供的价值	8
1.2.4	对同事提供的价值	9
第 2 章	国际注册内部控制师资格考试指南	10
2.1	国际注册内部控制师资格考试申报条件与程序	10
2.1.1	申报条件	10
2.1.2	申报程序	11
2.2	国际注册内部控制师资格考试要求	12
2.2.1	总体要求	12
2.2.2	考试须知	13
2.3	对国际注册内部控制师的期待	14
2.3.1	精通专业技术的职责	14
2.3.2	养成终生学习的习惯	14
2.3.3	遵守职业道德规范	14
2.3.4	接受继续教育	15
2.4	如何准备国际注册内部控制师（CICS）资格考试	16
2.4.1	注重增强职业胜任能力	16

2.4.2 掌握内部控制管理技能..... 17

第二部分 国际注册内部控制师内部控制管理技能

第3章 技能一：掌握内部控制原理 21

3.1 内部控制的定义 21

3.1.1 美国注册会计师协会的内部控制定义..... 21

3.1.2 COSO 内部控制定义 22

3.1.3 控制系统的含义..... 23

3.1.4 内部控制的局限性..... 24

3.2 计划—执行—检查—整改（PDCA）循环 25

3.2.1 PDCA 循环的概念 25

3.2.2 两个 PDCA 循环 26

3.3 业务工作流程 27

3.4 控制的基本词汇 29

3.5 控制的三个层级 30

3.6 内部会计控制 32

3.7 内部控制的层级制度 33

3.8 控制的问责机制 34

3.8.1 内部控制的责任..... 34

3.8.2 COSO 定义的内部控制角色与职责 36

3.8.3 区分不同的控制责任..... 39

3.8.4 恢复内部控制方面失去的信任..... 40

3.8.5 改进内部控制评估..... 43

第4章 技能二：加强控制环境建设 44

4.1 控制环境的职责与概念 44

4.1.1 执行管理层建立控制环境的责任..... 44

4.1.2 控制的层级制度..... 44

4.1.3 控制环境（公司治理）如何行使职责 46

4.1.4 控制环境与公司风险..... 47

4.1.5 有效控制环境的十大属性..... 48

4.1.6 行为准则政策..... 49

4.1.7	企业的价值观	52
4.1.8	首席执行官的表率作用	53
4.1.9	组织结构（职责分离）	53
4.1.10	员工的胜任能力	54
4.1.11	特别授权与责任权限的沟通	55
4.1.12	一般授权（预算和财务报告）与问责机制	55
4.1.13	内部审计	57
4.1.14	资产保护	57
4.1.15	定义工作流程	58
4.2	建立控制环境	59
4.2.1	管理层设定“高层基调”	59
4.2.2	控制环境要素——组织结构	60
4.2.3	控制环境要素——计划	61
4.2.4	控制环境要素——指导	62
4.3	监督控制的责任	62
4.4	控制环境的属性	63
4.4.1	控制环境中的授权	63
4.4.2	控制环境中的沟通	64
4.4.3	控制环境中的职责分离	64
4.4.4	胜任能力与可信度	66
4.4.5	记录保留程序	66
4.4.6	建立物理访问控制	66
4.4.7	制衡机制	67
4.4.8	监测合规性	67
4.5	计算机安全控制环境	68
4.5.1	计算机安全风险	68
4.5.2	定义关键的成功因素	69
4.6	组织的计算机安全政策	73
4.7	计算机安全的角色和职责	74
4.7.1	首席安全官	75
4.7.2	计算机安全规划委员会	76
4.7.3	安全员	77
4.7.4	安全保证人	77

4.7.5	安全质量保证	77
4.7.6	计算机安全计划的持续行动	78
4.7.7	激发员工的安全热情	78
4.8	下达安全任务	79
4.8.1	下达安全任务的方法	79
4.8.2	安全的个人所有权	80
4.8.3	个人对安全任务效果的反馈	81
4.8.4	计算机安全活动的奖励制度	81
第5章	技能三：做好风险管理	83
5.1	风险管理领域	83
5.1.1	风险的概念和词汇	83
5.1.2	什么是风险	84
5.1.3	风险词汇	85
5.1.4	风险与控制	85
5.1.5	计算由于风险造成的损失	86
5.1.6	商业环境中的风险	87
5.1.7	风险与控制的三个层级	88
5.1.8	COSO 内部控制框架要求的风险评估	90
5.2	COSO 对业务系统的控制活动	91
5.3	系统设计师如何解决业务应用系统中的风险	92
5.4	风险的原因和结果	93
5.4.1	技术使用不当	94
5.4.2	级联错误	95
5.4.3	不合逻辑的处理	96
5.4.4	无法将用户需求转化成技术需求	97
5.4.5	无法控制技术	98
5.4.6	重复错误	99
5.4.7	数据输入错误	100
5.4.8	数据的不正确使用和解释	101
5.4.9	数据集中	102
5.4.10	无法快速反应	103
5.4.11	无法证实处理情况	104

5.4.12	职责集中	105
5.5	与业务系统有关的一般风险暴露	106
5.5.1	不同类型的风险分类	107
5.5.2	职能领域的风险分类	107
5.5.3	交易处理的风险分类	108
5.6	风险管理过程	109
5.6.1	风险管理的6个组成部分	109
5.6.2	采用风险与控制模型	109
5.6.3	建立内部控制	111
5.6.4	控制设计方法	111
5.7	控制环境的目标	112
5.7.1	能干又诚信的员工	113
5.7.2	不相容职责分离	113
5.7.3	适当的授权程序	113
5.7.4	适当的会计程序	114
5.7.5	适当的资产保护程序	114
5.7.6	适当的文档记录程序	114
5.7.7	遵守法规的适当程序	114
5.7.8	有效果、经济和高效率的运营	114
5.7.9	实现既定目标	114
5.7.10	持续经营(盈利能力)	115
5.7.11	独立检查业绩	115
5.8	系统控制和交易处理控制的目标	115
5.9	定义业务系统循环	117
5.10	控制措施如何最大限度地降低风险	119
5.11	制定风险管理计划	120
第6章	技能四：开展应用控制评估	123
6.1	应用评估方案的概念	123
6.1.1	评估方案的重要性	123
6.1.2	特定评估涉及的PDCA循环	124
6.1.3	评估方案的改进周期	124
6.1.4	评估方案框架的必要性	124

6.2	审计标准	125
6.2.1	国际内部审计师协会（IIA）专业标准	126
6.2.2	美国银行管理协会的标准	126
6.3	COSO 企业风险管理框架	126
6.4	COSO 内部控制框架	128
6.4.1	COSO 内部控制新框架的主要变化简介	130
6.4.2	COSO 内部控制 17 项原则及其关注点	132
6.5	《萨班斯－奥克斯利法案》及相关法律法规	144
6.6	将适用的法规、标准和框架纳入应用评估方案	145
6.7	应用控制评估方案框架	145
6.7.1	评估企业风险管理计划	146
6.7.2	评估控制环境	147
6.7.3	评估和测试应用控制	147
6.7.4	评估与信息沟通相关的活动	148
6.7.5	评估与监控相关的活动	148
6.7.6	评估业务循环内相关活动的接合	148
6.8	ICI 应用控制评估的组成部分	149
6.8.1	企业风险管理的组成部分与评估计划核对清单	150
6.8.2	评估本组织控制环境的可依赖性	153
6.8.3	评估控制活动的组成部分	155
6.8.4	评估信息与沟通的组成部分	159
6.8.5	评估监控的组成部分	162
6.8.6	评估相关业务活动接合的适当性	164
6.9	五大业务循环概述	166
第 7 章	技能五：实施业务系统控制评估	169
7.1	业务系统控制词汇	169
7.2	系统控制目标	171
7.3	交易处理控制目标	171
7.4	单独应用与应用循环	173
7.5	标准与合规性与强制实施	176
7.6	系统控制和交易处理控制的类型	177
7.6.1	流程、可交付产品和控制连续区域	179

7.6.2	了解内部控制的“系统”	180
7.7	定义系统控制的目标	182
7.8	控制活动的交易处理部分	195
7.8.1	交易起始	196
7.8.2	信息技术交易录入	201
7.8.3	数据通信控制	206
7.8.4	计算机处理	209
7.8.5	数据存储与检索	211
7.8.6	输出处理控制	214
7.8.7	编写交易处理的控制目标	218
7.9	确定业务系统关键控制点的位置	218
7.9.1	识别潜在控制缺陷的风险暴露点矩阵	219
7.9.2	风险暴露点矩阵的流程	219
7.10	选择单个交易处理控制	225
7.10.1	交易处理阶段	226
7.10.2	控制强度	227
7.10.3	控制类型	228
7.10.4	通用控制的类别	228
7.10.5	成本效益考虑	229
7.10.6	敏感性考虑	231
7.10.7	重要性考虑	231
7.11	控制选择流程	232
7.12	应用控制文档矩阵	235
7.13	计算控制措施的成本效益	240
7.13.1	成本效益考虑事项	241
7.13.2	确定用于成本效益计算的控制措施	242
7.13.3	控制确认方法	243
7.13.4	成本效益计算方式	243
7.13.5	效益计算表	247
7.13.6	成本效益决定	248
第8章	技能六：执行风险评估	250
8.1	管理层的作用	250

8.2	意外损失与故意造成的损失	250
8.3	风险分析流程	252
8.4	识别风险、漏洞与威胁	254
8.4.1	调查以识别风险	254
8.4.2	风险分析小组用于识别风险的方法	256
8.4.3	人员风险（职责分离冲突矩阵）	262
8.5	测量风险大小程度	264
8.5.1	测量风险大小和发生概率的方法	264
8.5.2	风险评分（使用外部应用特性）	265
8.5.3	风险评分（使用内部应用特性）	273
8.5.4	量化风险的步骤	276
第9章	技能七：测评与报告内部控制合规性	286
9.1	《萨班斯－奥克斯利法案》对组织控制环境的影响	286
9.1.1	法案条文阐述的法案意图	287
9.1.2	《萨班斯－奥克斯利法案》的意向目标	288
9.2	内部审计在评估《萨班斯－奥克斯利法案》控制环境和意向目标方面的作用	289
9.3	《萨班斯－奥克斯利法案》的意向目标——改进公众对公司会计与报告做法的信任	290
9.4	评估控制环境的有效性	291
9.4.1	评估关注事项	291
9.4.2	评估指南	292
9.4.3	遵守《萨班斯－奥克斯利法案》评估核对清单	292
9.4.4	评估遵守“促使企业高管对其行为更加负责”的意向目标	293
9.4.5	评估遵守“加强内部控制系统和披露内控缺陷”的意向目标	297
9.4.6	评估遵守“鼓励与支持举报人”的意向目标	302
9.4.7	评估遵守“确保保留所需证据”的意向目标	305
9.4.8	评估遵守“增强董事会及其审计委员会监督职责”的意向目标	308
9.4.9	评估遵守“增强独立审计师独立性”的意向目标	312
9.5	汇总《萨班斯－奥克斯利法案》合规性评估结果	315