



普通高等教育“十一五”国家级规划教材

中国高等学校信息管理与信息系统专业规划教材

信息系统 审计、控制与管理

陈耿 韩志耕 卢孙中 编著



根据教育部管理科学与工程类学科专业教学指导委员会主持鉴定的《中国高等院校信息系统学科课程体系》组织编写



与美国ACM和IEEE/CS Computing Curricula 2005同步



清华大学出版社

014013487

F239.6
30



普通高等教育“十一五”国家级规划教材

中国高等学校信息管理与信息系统专业规划教材
清华大学出版社
ISBN 978-7-302-32839-0

信息系统 审计、控制与管理

陈耿 韩志耕 卢孙中 编著



清华大学出版社
地址：北京清华大学学研大厦A座
邮编：100084
电话：010-62770175
网址：http://www.tup.com.cn, http://www.wqbook.com
ISBN 978-7-302-32839-0
定价：44.00元

清华大学出版社



北航 C1700125

F239.6
30

784810410

林峰出版集团“正”内容简介 陈耿等编著

本书围绕现代信息系统审计的三大基本职能(审计、控制、管理)进行编写,在审计职能方面,突出审计的目的与本质,按照真实性审计、安全性审计和绩效审计等三个基本审计类型展开;在控制职能中,以IT安全为核心介绍了IT内部控制的方方面面;在管理职能中,以IT风险为导向,围绕IT风险管理展开。本书结构新颖独特,既具有较好的系统性和理论性,又具有很强的实战性和可操作性。

全书每一篇均包含一个案例,可以围绕案例组织教学,适用于高校信息管理类、会计、审计、财务管理、企业管理、计算机应用等专业本科生和研究生作为教材或参考书;书中还提供了大量实用表格等,为信息系统审计师、内部审计师、注册会计师、管理咨询师、企业管理人员等专业人士提供工作指导,是一本实用的工具书。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

信息系统审计、控制与管理/陈耿等编著.--北京:清华大学出版社,2014

中国高等学校信息管理与信息系统专业规划教材

ISBN 978-7-302-33839-0

I. ①信… II. ①陈… III. ①信息系统—审计—高等学校—教材 IV. ①F239.6

中国版本图书馆CIP数据核字(2013)第215848号

责任编辑:闫红梅 赵晓宁

封面设计:常雪影

责任校对:时翠兰

责任印制:李红英

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦A座 邮 编:100084

社 总 机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

印 刷 者:清华大学印刷厂

装 订 者:三河市溧源装订厂

经 销:全国新华书店

开 本:185mm×260mm 印 张:28.25 字 数:671千字

版 次:2014年1月第1版 印 次:2014年1月第1次印刷

印 数:1~2000

定 价:44.50元

产品编号:041964-01

林峰出版集团
北京



序

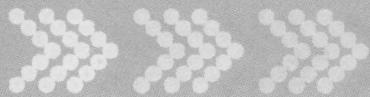
在信息技术刚刚兴起的时候,信息系统还没有作为一个专门的学科独立出来,它更多的只是计算机学科的一个附属。但是,随着信息技术的跳跃式发展和计算机系统在生产、生活、商务活动中的广泛应用,信息系统作为一个独立的整体逐渐独立出来,并得到了迅速发展。由于信息系统是基于计算机技术、系统科学、管理科学以及通信技术等多个学科的交叉学科,因此,信息系统是一门跨专业,面向技术和管理等多个层面,注重将工程化的方法和人的主观分析方法相结合的学科。

早在1984年,邓小平同志就提出了要开发信息资源,服务四个现代化(工业现代化、农业现代化、国防现代化和科学技术现代化)建设。1990年,江泽民同志曾经指出,四个现代化恐怕无一不和电子信息化有着紧密的联系,要把信息化提到战略地位上来,要把信息化列为国民经济发展的一个重要方针。2004年,胡锦涛同志在APEC(亚洲太平洋经济合作组织)上的讲话明确指出:“信息通信技术改变了传统的生产方式和商业模式,为亚太地区带来了新的经济增长机遇。为把握住这一机遇,我们应抓住加强信息基础设施建设和人力资源开发这两个关键环节。”我国的经济目前正处在迅速发展阶段,信息化建设正在成为我国增强国力的一个重要举措,信息管理人才的培养至关重要。因此,信息系统学科面临着新的、更为广阔的发展空间。

近年来,我国高等学校管理科学与工程一级学科下的“信息管理与信息系统”专业领域的科研、教学和应用等方面都取得了长足的进步,培养了一大批优秀的技术和管理人才。但在整体水平上与国外发达国家相比还存在着不小的差距。由于各所高校在相关专业的历史、特点和背景上的差异以及社会对人才需求的多样化,使得我国信息管理与信息系统专业教育面临着前进中的机遇和挑战。如何适应人才需求变化进行教育改革和调整,如何在基本教学规范和纲要的基础上建立自己的教育特色,如何更清晰地定义教育对象和定位教育目标及体系,如何根据国际主流及自身特点更新知识和教材体系等都是我们在专业教育和学科建设中需要探讨和考虑的重要课题。

2004年,教育部高等学校管理科学与工程类专业教学指导委员会制订了学科的核心课程以及相关各专业主干课程的教学基本要求(简称《基本要求》)。其中,“管理信息系统”是学科的核心课程之一,“系统分析与设计”、“数据结构与数据库”、“信息资源管理”和“计算机网络”是信息管理与信息系统专业的主干课程。该《基本要求》反映了相关专业所应构建的最基本的核心课程和主干课程系统以及涉及的最基本的知识元素,旨在保证必要的教学规范,提升我国高等学校相关专业教育的基础水平。

2004年6月,IEEE/ACM公布了“计算教程CC2004”(Computing Curriculum 2004),其中包括由国际计算机学会(ACM)、信息系统学会(AIS)和信息技术专业协会(AITP)共同



提出的信息系统学科的教学参考计划和课程设置(IS 2002)。与过去的历届教程相比,IS 2002 比较充分地体现出“技术与管理并重”这一当前信息系统学科领域的主流特点。IS 2002 中的信息系统学科也涵盖了“信息管理”(IM)、“管理信息系统”(MIS)等相关专业,与我国的信息管理与信息系统专业相兼容。

为了进一步提高我国高等学校信息系统学科领域课程体系的规划性和前瞻性,反映国际信息系统学科的主流特点和知识元素,进一步体现我国相关专业教育的特点和发展要求,清华大学经济管理学院与中国人民大学信息学院共同组织,于2004 年秋成立了“中国高等院校信息系统学科课程体系2005”(CISC 2005)课题组,通过对国内外信息系统的发展现状与趋势进行分析,参照IS 2002 的模式,课题组研究探讨了我国信息系统教育的指导思想、课程体系、教学计划,确定了课程体系的基础内容与核心内容,制订出了一个符合我国国情的信息管理与信息系统学科的教育体系框架,我们希望CISC 2005 有助于我国信息管理与信息系统学科的建设,促进我国信息化人才的培养。

2006 年,根据CISC 2005 的指导思想编写的系列教材——《中国高等学校信息管理与信息系统专业规划教材》被列入教育部普通高等教育“十一五”国家级规划教材。同年,CISC 2005 通过了教育部高等学校管理科学与工程类专业教学指导委员会组织的专家鉴定。为了能够使这套教材尽快出版,课题组成员和清华大学出版社一道,对教材进行了详细规划,并组织了国内相关专家学者共同努力,力争从2007 年起陆续使这套教材和读者见面。希望这套教材的出版能够满足国内高等学校对信息管理与信息系统专业教学的要求,并在大家的努力下,在使用中逐渐完善和发展,从而不断提高我国信息管理与信息系统人才的培养质量。

陈国青



前言



自改革开放以来,我国经济之所以能够保持住平稳快速发展,创造出众多的经济奇迹,迅速跃居世界第二大经济体,审计起到了保驾护航的作用。坚持深入贯彻落实科学发展观,牢固树立科学审计理念,紧紧围绕保持经济平稳较快发展这条主线,切实履行审计监督职责,充分发挥审计在保障国家经济社会健康运行方面的“免疫系统”功能,这是审计人的“审计梦”。

随着我国信息化建设的不断深入,“以信息化带动工业化,以工业化促进信息化”的发展模式早已深入人心,日益显现出其强大的生命力。然而,伴随着信息化技术在国家经济生活中的广泛运用,以往公认的安全状态已经发生了显著的转变,信息及系统安全已经成为影响国家经济安全的重要因素。频频发生的安全事件正影响着企业的发展,严重损害着企业的信用。如何在企业数据海量增长、非法访问日益增多、隐私泄露频繁发生、企业应用趋于分布、信息系统广泛互联、内部风险与外部威胁并存的复杂信息环境中,保障企业信息行为的有效性、安全性和真实性,是摆在信息系统使用者、管理者和审计人员面前的重要任务。

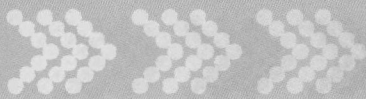
本书没有采取传统的一般控制与应用控制的组织模式,而是按照现代信息系统审计的三大基本职能(即审计、控制、管理)进行编排。所有环节均依据信息系统的本质有序展开,如审计职能按照真实性、安全性和绩效等基本类型展开;内部控制职能以信息系统安全为中心展开;管理职能则以信息技术风险为导向展开。本书结构新颖独特,既具有较好的系统性、理论性,又具有很强的可操作性。

全书由陈耿教授统稿,具体分工如下:第1章(陈耿),第2章(陈耿、卢孙中、李庭燎),第3章(陈耿、韩志耕、刘林源、景波),第4章(卢孙中、唐明伟、陈耿),第5章(韩志耕、陈耿),第6章(韩志耕),第7章(韩志耕、陈耿、卢孙中),第8章(韩志耕、陈耿),第9章(陈耿、张晋津),第10章(陈耿、张晓东、卢孙中),第11章(韩志耕),第12章(陈耿、和秀星、卢孙中),第13章(龚媛媛、刘林源),第14章(陈耿),第15章(杨琴、陈耿、韩志耕),第16章(杨琴、韩志耕),第17章(陈耿、韩志耕、杨琴),第18章(陈耿、李庭燎、韩志耕),第19章(韩志耕),第20章(韩志耕,陈耿)。

本书得到了国家自然科学基金(70971067, 71271117)、江苏省自然科学基金(BK2010331)、江苏省高校自然科学基金(12KJB520005)、江苏省网络与信息安全重点实验室项目(BM2003201)的资助。

审计署昆明特派办也给予我们大力支持,提供了大量信息系统审计案例,特别是周应良副特派员、夏军峰处长、朱立辉处长、赵辉处长等多次参与了讨论,提出了许多宝贵意见,在此表示衷心感谢。

南京审计学院副院长、著名审计专家王会金教授在百忙之中也审阅了书稿,提出了许多宝贵意见。在写作过程中科研处也给予了关心和帮助,科研处处长何平教授、副处长刘爱龙



教授提出了修改意见,向他们表示衷心感谢。同时也感谢清华大学出版社的广大员工,本书是在他们的不断帮助和鼓励下完成的。

本书可用于信息管理与信息系统专业、企业管理专业、会计专业、审计专业和计算机应用专业本科生和研究生的教材,每篇一个案例,可以围绕案例组织教学。书中还提供了大量信息丰富且实用的表格等,可以给企业管理人员、内部审计师、注册会计师、信息系统审计师、管理咨询人员等专业人士提供帮助和指导,是一本非常实用的参考书。

于润泽湖畔

目录

第一篇 总论

第1章 信息系统审计概述

1.1 信息系统审计的历史

1.1.1 早期的信息系统审计

1.1.2 现代信息系统审计的形成

1.2 信息系统审计的概念

1.2.1 信息系统审计定义

1.2.2 信息系统审计辨析

1.2.3 信息系统审计分类

1.2.4 信息系统审计目标

1.2.5 信息系统审计职能

1.2.6 信息系统审计过程

1.2.7 信息系统审计方法

1.2.8 信息系统审计依据

1.3 信息系统审计的规范

1.3.1 与信息系统审计相关的组织

1.3.2 ISACA的准则体系

1.3.3 审计师的职业准则

1.3.4 与IT服务管理相关的规范

1.3.5 与信息安全技术相关的标准

1.3.6 与计算机犯罪相关的法律

第2章 信息系统审计实施

2.1 管控审计风险

2.1.1 什么是审计风险

2.1.2 审计风险的特征

2.1.3 审计风险的模型

2.1.4 评估固有风险和控制风险

2.1.5 确定重要性水平

2.1.6 控制检查风险

2.2 制订审计计划

2.2.1 审计计划的作用

2.2.2 审计计划的规范

2.2.3 审计计划的内容

2.2.4 审计计划中风险评估的运用

2.3 收集审计证据

2.3.1 审计证据的属性

2.3.2 审计证据的种类

2.3.3 数字证据的特点

2.3.4 数字证据的形式

2.3.5 收集证据的充分性

2.3.6 收集证据的适当性

2.3.7 收集证据的可信性

2.4 编制工作底稿

2.4.1 工作底稿的作用

2.4.2 工作底稿的分类

2.4.3 编制工作底稿的注意事项

2.4.4 工作底稿的复核

2.4.5 工作底稿的管理

2.5 编写审计报告

2.5.1 审计报告的作用

2.5.2 审计报告的规范

2.5.3 审计报告的格式

2.5.4 编写审计报告的注意事项

第3章 信息系统审计方法

3.1 证据收集方法

3.1.1 证据收集方法概述

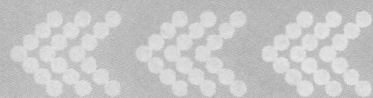
3.1.2 收集证据的方法

3.2 数字取证方法

3.2.1 数字取证的概念



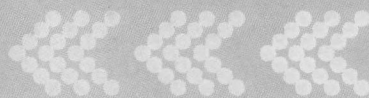
3.2.2 数字取证的作用	50	4.2 管理信息系统	75
3.2.3 数字取证的方法	51	4.2.1 管理信息的定义	75
3.2.4 数字取证的工具	52	4.2.2 管理信息的特征	75
3.2.5 数字取证的规范	53	4.2.3 管理信息的发展	76
3.3 数据库查询方法	54	4.2.4 管理信息的概念结构	77
3.3.1 数据库查询工具	54	4.2.5 管理信息的层次结构	77
3.3.2 对单个表的查询	55	4.2.6 管理信息的系统结构	78
3.3.3 对单个表的统计	56	4.2.7 管理信息的硬件结构	80
3.3.4 生成审计中间表	57	4.3 系统流程审核	81
3.3.5 对多个表的查询	58	4.3.1 系统流程的审计目标	81
3.3.6 应用实例	58	4.3.2 数据流图的概念	81
3.4 软件测试方法	59	4.3.3 分析业务流程	83
3.4.1 概述	59	4.3.4 画出数据流图	84
3.4.2 黑盒测试	60	4.3.5 分析数据的逻辑关系	85
3.4.3 白盒测试	61	4.3.6 发现审计线索	86
3.4.4 基于故障的测试	63		
3.4.5 基于模型的测试	64	第5章 财务数据的真实性	87
案例1 安然公司破产——信息系统 审计的转折点	66	5.1 财务信息系统	87
		5.1.1 财务信息系统的发展过程	87
		5.1.2 财务系统的功能	88
		5.1.3 销售与应收子系统	88
		5.1.4 采购与应付子系统	90
		5.1.5 工资管理子系统	91
		5.1.6 固定资产子系统	92
		5.1.7 财务信息系统对审计的影响	93
		5.1.8 财务信息系统审计内容	93
		5.2 账务处理的真实性	93
		5.2.1 总账子系统的真实性问题	93
		5.2.2 总账子系统的主要功能	94
		5.2.3 总账子系统的处理流程	95
第二篇 真实性审计			
第4章 真实性审计概述	69		
4.1 真实性审计概念	69		
4.1.1 真实性审计的含义	69		
4.1.2 真实性审计的内容	69		
4.1.3 真实性审计的分类	70		
4.1.4 业务流程审核	71		
4.1.5 财务处理审核	72		
4.1.6 交易活动审核	72		
4.1.7 真实性审计的方法	72		



5.2.4	总账子系统的数据来源	95
5.2.5	系统的初始化	97
5.2.6	科目与账簿设置	97
5.2.7	自动转账凭证的设置	99
5.2.8	总账子系统的审计	100
5.3	财务报表的真实性	100
5.3.1	报表子系统的真实性问题	100
5.3.2	报表系统的主要功能	100
5.3.3	报表系统的处理流程	101
5.3.4	财务报表自动生成原理	102
5.3.5	报表子系统的审计	108
第6章	交易活动的真实性	109
6.1	电子商务	109
6.1.1	电子商务的概念	109
6.1.2	电子商务的功能	110
6.1.3	电子商务体系结构	111
6.1.4	电子商务工作流程	112
6.1.5	电子商务对审计的影响	113
6.1.6	电子商务审计	113
6.2	电子交易方的真实性	114
6.2.1	身份冒充问题	114
6.2.2	身份认证概述	114
6.2.3	单向认证	115
6.2.4	双向认证	117
6.2.5	可信中继认证	118
6.2.6	Kerberos 系统	121
6.3	电子交易行为的真实性	124
6.3.1	交易欺诈问题	124
6.3.2	不可抵赖证据的构造	124
6.3.3	不可否认协议概述	125
6.3.4	不可否认协议安全性质	125
6.3.5	Zhou-Gollmann 协议	127
6.3.6	安全电子支付协议	130
案例2	超市上演“无间道”——舞弊导致电子数据不真实	131
第三篇 安全性审计		
第7章	安全性审计概述	137
7.1	安全性审计概念	137
7.1.1	安全性审计的含义	137
7.1.2	安全性审计的内容	137
7.1.3	调查了解系统情况	138
7.1.4	检查验证安全状况	138
7.1.5	安全性审计的方法	139
7.2	系统安全标准	143
7.2.1	可信计算机系统评价准则	143
7.2.2	信息技术安全评价通用准则	145
7.2.3	信息系统安全等级划分标准	148
7.3	物理安全标准	149
7.3.1	数据中心安全标准	149
7.3.2	存储设备安全标准	151
第8章	数据安全	156
8.1	数据的安全问题	156
8.1.1	数据的安全性	156
8.1.2	数据的保密性	156
8.1.3	数据的完整性	157
8.1.4	数据的可用性	157
8.1.5	数据安全审计	158



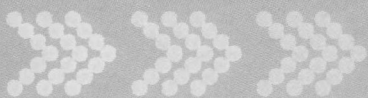
8.2 数据的加密技术	159	9.2.2 身份验证	179
8.2.1 数据加密与安全的关系	159	9.2.3 访问控制	180
8.2.2 对称加密算法	159	9.2.4 加密文件系统	181
8.2.3 非对称加密算法	160	9.2.5 入侵检测	181
8.2.4 散列加密算法	162	9.2.6 事件审核	182
8.3 数据的访问控制	163	9.2.7 Windows 日志管理	183
8.3.1 访问控制与安全的关系	163	9.3 UNIX 安全机制	184
8.3.2 自主访问控制	164	9.3.1 UNIX 安全机制概述	184
8.3.3 强制访问控制	166	9.3.2 账户的安全控制	184
8.3.4 基于角色的访问控制	167	9.3.3 文件系统的安全控制	185
8.4 数据的完整性约束	167	9.3.4 日志文件管理	186
8.4.1 完整性与安全的关系	167	9.3.5 密码强度审查	187
8.4.2 数据完整性	168	9.3.6 入侵检测	188
8.4.3 完整性约束条件	168	9.3.7 系统日志分析	188
8.4.4 完整性约束机制	170		
8.4.5 完整性约束的语句	171		
8.4.6 完整性约束的实现	171		
第9章 操作系统安全	173		
9.1 操作系统的安全问题	173	第10章 数据库系统安全	190
9.1.1 操作系统的概念	173	10.1 数据库系统的安全问题	190
9.1.2 操作系统的种类	174	10.1.1 数据库系统的概念	190
9.1.3 操作系统的结构	174	10.1.2 数据库系统的组成	190
9.1.4 操作系统面临的威胁	174	10.1.3 数据库系统的结构	191
9.1.5 操作系统的安全策略	175	10.1.4 数据库管理系统	192
9.1.6 操作系统安全等级的划分	175	10.1.5 数据库系统面临的威胁	194
9.1.7 操作系统的安全机制	176	10.1.6 数据库系统的安全需求	194
9.1.8 操作系统安全性的测评	178	10.1.7 数据库系统安全等级划分	195
9.2 Windows 安全机制	178	10.2 数据库系统安全机制	195
9.2.1 Windows 安全机制概述	178	10.2.1 数据备份策略	195
		10.2.2 数据库备份技术	196
		10.2.3 数据库恢复技术	198
		10.2.4 数据库审计功能	198
		10.2.5 数据库访问安全	199



10.3 Oracle 审计机制	201
10.3.1 Oracle 审计功能	201
10.3.2 标准审计	202
10.3.3 细粒度的审计	204
10.3.4 审计相关的数据字典视图	206
10.4 SQL Server 审计机制	206
10.4.1 SQL Server 审计功能	206
10.4.2 服务器审计	207
10.4.3 数据库级的审计	208
10.4.4 审计级的审计	209
10.4.5 审计相关的数据字典视图	210
第 11 章 网络安全	212
11.1 网络的安全问题	212
11.1.1 计算机网络	212
11.1.2 网络的体系结构	213
11.1.3 网络协议的组成	215
11.1.4 网络面临的威胁	215
11.1.5 网络的安全问题	215
11.2 网络入侵的防范	216
11.2.1 网络入侵问题	216
11.2.2 网络入侵技术	217
11.2.3 网络入侵防范	220
11.3 网络攻击的防御	222
11.3.1 服务失效攻击与防御	222
11.3.2 欺骗攻击与防御	224
11.3.3 缓冲区溢出攻击与防御	229
11.3.4 SQL 注入攻击与防御	231
11.3.5 组合型攻击与防御	232
案例 3 联通盗窃案——信息资产安全的重要性	232

第四篇 绩效审计

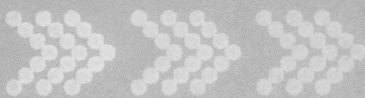
第 12 章 IT 绩效审计概述	237
12.1 绩效审计概念	237
12.1.1 绩效审计的出现	237
12.1.2 绩效审计的定义	237
12.1.3 绩效审计的目标	238
12.1.4 绩效审计的对象	238
12.1.5 绩效审计的分类	239
12.1.6 绩效审计的方法	240
12.1.7 绩效审计的评价标准	240
12.1.8 绩效审计的特点	241
12.2 IT 绩效审计概念	242
12.2.1 IT 绩效审计的必要性	242
12.2.2 IT 绩效审计的含义	243
12.2.3 IT 绩效审计的特点	244
12.2.4 IT 绩效审计的评价标准	244
12.2.5 IT 绩效审计的视角	245
12.2.6 IT 绩效审计的阶段	246
12.2.7 IT 绩效审计的方法	246
12.3 信息化评价指标	247
12.3.1 评价指标的提出	247
12.3.2 评价指标的内容	247
12.3.3 评价指标适用性	251
12.3.4 评价标准的层次	252
第 13 章 IT 项目经济评价	254
13.1 资金等值计算	254
13.1.1 资金的时间价值	254
13.1.2 若干基本概念	254
13.1.3 资金等值计算	256



13.2 软件成本估算	262
13.2.1 软件估算方法	262
13.2.2 软件规模估算	262
13.2.3 软件工作量估算	265
13.2.4 软件成本估算	266
13.3 项目效益评价	269
13.3.1 效益评价方法	269
13.3.2 项目现金流分析	269
13.3.3 财务静态分析法	273
13.3.4 财务动态分析法	275
第14章 IT项目应用评价	282
14.1 IT应用评价的复杂性	282
14.1.1 企业信息化的作用	282
14.1.2 ERP投资陷阱	283
14.1.3 IT生产率悖论	284
14.1.4 IT应用评价的作用	285
14.2 IT评价理论的发展	285
14.2.1 IT评价的内涵	285
14.2.2 IT评价的发展历程	286
14.2.3 IT评价的种类	288
14.3 平衡计分卡技术	289
14.3.1 平衡计分卡的提出	289
14.3.2 平衡计分卡的作用	290
14.3.3 平衡计分卡的内容	290
14.3.4 平衡计分卡的使用	293
14.4 IT平衡计分卡构建	293
14.4.1 IT平衡计分卡	293
14.4.2 财务评价	294
14.4.3 用户体验评价	295
14.4.4 内部流程评价	295
14.4.5 创新能力评价	296
14.4.6 指标权重计算	297
案例4 许继公司ERP实施失败—— 绩效审计的作用	297
第五篇 内部控制	
第15章 IT内部控制概述	301
15.1 IT内部控制的概念	301
15.1.1 内部控制观念	301
15.1.2 财务丑闻	302
15.1.3 IT内控重要性	304
15.1.4 IT内控的定义	305
15.1.5 IT内控的准则	306
15.2 IT内部控制的构成	312
15.2.1 IT内控的目标	312
15.2.2 IT内控的要素	312
15.2.3 IT内控的特征	313
15.2.4 IT内控的分类	314
15.3 IT内部控制的设计	314
15.3.1 控制设计原则	314
15.3.2 IT内控的作用	316
15.3.3 控制措施设计	316
15.3.4 控制涉及对象	317
15.3.5 控制的实施	318
第16章 IT内部控制应用	320
16.1 一般控制	320
16.1.1 概述	320
16.1.2 组织控制	321
16.1.3 人员控制	324
16.1.4 日常控制	328



16.2 应用控制	332	18.1.2 IT 风险评估	368
16.2.1 概述	332	18.1.3 IT 风险识别	369
16.2.2 输入控制	332	18.1.4 IT 风险计算	370
16.2.3 处理控制	336	18.1.5 IT 风险处理	374
16.2.4 输出控制	340	18.1.6 IT 风险控制	375
第 17 章 软件资产控制	342	18.2 IT 治理	375
17.1 概述	342	18.2.1 IT 治理的定义	375
17.1.1 信息资产的含义	342	18.2.2 IT 治理的内容	376
17.1.2 软件生命周期与过程控制	343	18.2.3 IT 战略制定	376
17.1.3 软件开发方法	345	18.2.4 IT 治理的目标	377
17.1.4 软件开发方式与控制评价	347	18.2.5 IT 治理委员会	378
17.2 软件全过程控制	348	18.2.6 首席信息官	378
17.2.1 总体规划阶段	348	18.2.7 内部 IT 审计	380
17.2.2 需求分析阶段	349	18.3 IT 管理	381
17.2.3 系统设计阶段	349	18.3.1 IT 管理的定义	381
17.2.4 系统实施阶段	349	18.3.2 IT 管理的目标	382
17.2.5 系统运行与维护阶段	352	18.3.3 IT 管理的资源	382
17.2.6 软件资产控制措施	354	18.3.4 IT 管理的内容	382
17.2.7 软件资产变更控制措施	356	第 19 章 安全应急管理	387
17.3 软件质量控制	357	19.1 概述	387
17.3.1 软件质量标准	357	19.1.1 应急响应目标	387
17.3.2 软件质量控制方法	359	19.1.2 组织及其标准	387
17.3.3 软件质量控制措施	359	19.1.3 应急响应体系	390
案例 5 法国兴业银行事件—— 传统内控的终结	363	19.2 应急准备	392
		19.2.1 任务概述	392
		19.2.2 应急响应计划准备	392
		19.2.3 应急响应计划编制	393
		19.2.4 应急响应计划测试	394
		19.2.5 其他准备事项	395
		19.3 启动响应	395
第六篇 风险管理			
第 18 章 IT 风险管理概述	367		
18.1 IT 风险	367		
18.1.1 IT 风险管理	367		



19.3.1	任务概述	395	20.1.5	业务连续性计划的更新	413
19.3.2	信息安全事件分类	395	20.2 安全防范体系建设	414	
19.3.3	信息安全事件确定	399	20.2.1	网络安全防范原则	414
19.3.4	信息安全事件分级	401	20.2.2	网络安全体系结构	415
19.4 应急处置	404		20.2.3	IPSec 安全体系建设	415
19.4.1	任务概述	404	20.2.4	防火墙系统建设	418
19.4.2	遏制、根除与恢复流程	405	20.3 灾难恢复体系建设	421	
19.4.3	处理示例	405	20.3.1	灾难恢复计划	421
19.5 跟踪改进	408		20.3.2	灾难恢复能力划分	421
19.5.1	任务概述	408	20.3.3	容灾能力评价	425
19.5.2	证据获取	408	20.3.4	灾备中心的模型	426
19.5.3	证据分析	409	20.3.5	灾备中心的解决方案	428
19.5.4	行为追踪	409	20.3.6	灾备中心的选址原则	429
			20.3.7	制定灾备方案的要素	430
			20.3.8	建立有效的灾备体系	430
第 20 章 业务连续性管理	410		案例 6 9·11 事件——IT 风险对企业的	431	
20.1 业务连续性计划	410		影响	431	
20.1.1	业务连续性的重要性	410			
20.1.2	影响业务连续性的因素	411	参考文献	433	
20.1.3	业务连续性计划的制定	411			
20.1.4	业务影响分析	412			

第一篇 总 论

现代企业的运营越来越依赖信息系统,如航空公司的网上订票系统、银行的资金实时结算系统、携程旅行网的客户服务系统等。没有信息系统的支撑,这些公司的业务开展就举步维艰、难以为继,企业经营就很可能陷入瘫痪状态。当前,一些新兴产业和新兴企业,其商业模式则完全依赖于信息系统,如各种网络公司(如新浪)、各种电子商务公司(如阿里巴巴)。没有信息系统,这些企业将彻底失去生存的空间。因此,信息系统和数据的“资产”性价值越来越受到重视,成为企业继资金、人力资源之后又一个重要资产;保障这一类资产的合法、安全、真实是信息系统审计的主要职责。

