国际内部控制协会（ICI）中国总部推荐培训教材

Internal Control and Operational Risk Management

内部控制与操作风险管理

——操作实务指南

Guide to the Operational Practice

邱胜利 ◎ 编著

中国金融出版社

国际内部控制协会（ICI）中国总部推荐培训教材

Internal Control and Operational Risk Management

内部控制与操作风险管理

——操作实务指南

Guide to the Operational Practice

邱胜利 ◎ 编著

中国金融出版社

责任编辑：李　融　邓瑞锁
责任校对：张志文
责任印制：丁淮宾

图书在版编目（CIP）数据

内部控制与操作风险管理——操作实务指南（Neibu Kongzhi yu Caozuo Fengxian Guanli——Caozuo Shiwu Zhinan）/邱胜利编著．—北京：中国金融出版社，2009.11
ISBN 978-7-5049-5313-1

Ⅰ．内…　Ⅱ．邱…　Ⅲ．企业管理：风险管理—指南　Ⅳ．F275.1-62

中国版本图书馆 CIP 数据核字（2009）第 196408 号

出版
发行　中国金融出版社
社址　北京市丰台区益泽路 2 号
市场开发部　(010)63272190，66070804（传真）
网上书店　http：//www.chinafph.com
　　(010)63286832，63365686（传真）
读者服务部　(010)66070833，82672183
邮编　100071
经销　新华书店
印刷　保利达印刷有限公司
装订　平阳装订厂
尺寸　169 毫米×239 毫米
印张　28.75
字数　473 千
版次　2009 年 11 月第 1 版
印次　2009 年 11 月第 1 次印刷
定价　58.00 元
ISBN 978-7-5049-5313-1/F.4873

前　言

进入21世纪，美国先后爆发了安然（Enron）、世通（WorldCom）、安达信（Arthur Andersen）等公司因欺诈、会计造假而导致公司破产倒闭的丑闻，使投资大众遭受了巨大的经济损失。为了加强公司治理，重建投资者的信心，2002年7月，美国国会颁布了著名的《2002年上市公司会计改革和投资者保护法案》，亦称《萨班斯—奥克斯利法案》（Sarbanes－Oxley Act，SOX，以下简称《萨班斯法案》），提出了建立以美国反欺诈财务报告委员会发起组织委员会（Commission of Sponsoring Organizations，COSO）发布的《COSO内部控制整合框架》为参照基准的内部控制框架体系，旨在强化公司和审计委员会责任，加强独立审计师的独立性，强化财务披露要求，控制企业风险，提高财务报告的可靠性，增强投资大众的信心。由于《萨班斯法案》80%的内容或措施都与内部控制有关，故也被称做内部控制法案。

《萨班斯法案》是1933年以来美国证券立法中影响最为深远的法案。它导致美国现行证券法、公司法和会计法进行多处重大修改，新增加了许多相当严厉的法律规定。例如，延长证券欺诈诉讼的时效期限；加重了公司主要管理者的法律责任；加强了对公司高级管理层收入的监管；对公司内部的审计委员会作出法律规范；强化了对公司外部审计的监管；加强了信息披露制度和其他有关公司监管规定等。

《萨班斯法案》在强化立法管制的同时，美国司法监管机构也加大了对“白领犯罪”的处罚力度。例如，2005年7月，前世通总裁伯

纳德·埃伯斯被判刑25年，没收个人资产4000万美元，用以补偿世通投资者的损失。2006年10月23日，经历5年调查和审讯后，美国地方法院判处安然公司前首席财务官杰弗里·斯基林有期徒刑24年零4个月，被没收4500万美元的财产（安然公司前总裁肯尼斯·莱当时已去世）。安然公司的破产还导致了为其做假账的安达信会计师事务所的破产，花旗银行、摩根大通、美国银行等也因财务欺诈，向安然破产的受害者分别支付了20亿美元、22亿美元和6900万美元的赔偿金。

2008年，肇始于美国华尔街由次贷引起的金融危机横扫全球，金融危机的影响正通过国际贸易蔓延到实体经济，直接导致金融机构数以十万甚至百万计人员的失业，间接引起房地产的贬值和实体经济部门裁员的逐步扩大。据报道，这次金融海啸已经使全球的财富损失了15万亿美元，但依然没有结束，随着金融海啸肆虐范围的迅速扩大，谁也不知道哪些地方和哪些机构将成为下一块倒下的骨牌。

次贷危机也警示我们：首先，金融创新不能消除风险，只能管理或者转嫁风险，政府监管部门应该加强对次贷这类衍生产品的前瞻性监管；其次，开拓国内市场，创新产品，其限度必须是市场可以承受的，为此，需要严把基础资产的质量关，做好风险控制；最后，现代的风险管理正朝着平衡风险与回报的方向发展。探讨在健全企业风险控制的同时，如何应用信息技术（IT）对企业实施风险防范将是一个永恒的主题。

2006年，为全面落实科学发展观，进一步加强和完善国有资产监管工作，深化国有企业改革，健全内部控制制度，加强风险管理，促进企业持续、稳定、健康发展，国务院国有资产监督管理委员会颁布了《中央企业全面风险管理指引》（见附录二）。上海证券交易所、深圳证券交易所先后发布了《上市公司内部控制指引》，旨在推动和规范我国上市公司建立健全内部控制制度，提高风险管理水平，保护投资者的合法权益。2007年，银监会也先后颁布了《商业银行内部控制

评价试行办法》、《商业银行操作风险管理指引》（见附录三）、《商业银行信息科技风险管理指引》。

2008年6月3日，我国财政部、证监会、审计署、银监会和保监会五部委联合印发了《企业内部控制基本规范》（财会〔2008〕7号）（见附录一）。这一被称为中国版《萨班斯法案》的《企业内部控制基本规范》是我国第一部加强和完善企业内部控制系统，提高企业经营管理水平和风险防范能力，促进企业可持续发展，维护社会主义市场经济秩序和社会公众利益的重要法规文件。根据《企业内部控制基本规范》的执行要求，自2009年7月1日（目前延至2010年1月1日）起在上市公司范围内施行，鼓励非上市的大中型企业执行。上市公司要对本公司的内部控制有效性进行自我评估，披露年度自我评价报告，并可聘用具有证券、期货业务资格的会计师事务所对内部控制的有效性进行审计。

胡锦涛同志在党的十七大报告中指出："科学发展观，是立足社会主义初级阶段基本国情，总结我国发展实践，借鉴国外发展经验，适应新的发展要求提出来的。"《企业内部控制基本规范》正是有机地融合和借鉴了国际主要经济体加强内部控制的做法和发展经验，在吸收《萨班斯法案》和《COSO内部控制整合框架》要素标准的基础上，提出了我国上市公司和大中型企业内部控制的目标和具体执行要求，强调企业内部控制的目标是合理保证企业经营管理的合法合规、资产安全、财务报告及相关信息的真实完整、提高经营效率和效果、促进企业实现发展战略。《企业内部控制基本规范》的执行实施，促使我国的上市公司和大中型企业，建立健全本企业的内部控制制度，运用信息技术加强内部控制，建立和提升与经营管理相适应的信息系统，促进内部控制流程管理与信息系统的有机结合，实现对业务和事项的自动控制，减少或消除人为操纵因素。因此，企业执行《企业内部控制基本规范》，需要做好以下准备工作：

（1）组织内部控制系统知识的培训学习；
（2）建立与经营管理相适应的信息系统；
（3）组建内部控制自我评估测试团队；
（4）实施内部控制自我评估；
（5）改进内部控制缺陷；
（6）披露年度自我评价报告；
（7）接受外部审计。

20世纪90年代以来，许多国家都发生了严重的金融危机。金融风险使具有200多年历史的巴林银行倒闭就是一个典型的例子。1995年，由于巴林银行驻新加坡业务员里森违规操作，缺乏内部控制，经营期货失败，亏损10亿英镑而迫使巴林银行倒闭。1997年爆发的东南亚金融危机，国际金融界受到了震惊，各国都把防范和化解金融风险放在了首要位置，纷纷探讨如何应用IT技术对银行经营业务实施非现场监管，防范金融风险在金融界是一个永恒的主题。2001年1月，巴塞尔委员会公布了《巴塞尔新资本协议》，其核心内容是提高资本的风险敏感度，更加强调对信用风险、市场风险和操作风险的监测与内部控制，全面推行风险管理理念。

企业自身的稳健、持续发展也是社会进步和经济繁荣的基本保障，加强企业的全面风险管理离不开操作风险管理这一古老而现代的话题。例如银行系统，过去人们总认为银行最大的风险是信用风险和市场风险，国内将不良资产和呆坏账统统归为信用风险。但是，对照《巴塞尔新资本协议》中关于操作风险的定义，发现很多原来认为是信用风险的风险事项其实是操作风险。巴塞尔委员会早在2002年对操作风险进行了全球性的调查，发现每年因操作风险损失高达77.95亿欧元。我国对银行业操作风险的认知也是从国家审计署的“审计风暴”和银监会公布的金融机构处理涉案人员的人数、发生经济案件和违规经营案件的数量，以及2005年银监会《关于加大防范操作风险工作力度的

通知》开始的。该通知明确提出："迅速改进科技信息系统，提高通过技术手段防范操作风险的能力，支持各类管理信息的适时、准确生成，为业务操作复核和稽核部门的稽查提供坚实基础。"银监会在2007年5月印发的《商业银行操作风险管理指引》中指出："商业银行应当按照本指引要求，建立与本行的业务性质、规模和复杂程度相适应的操作风险管理体系，有效地识别、评估、监测和控制/缓释操作风险"；"为有效地识别、评估、监测、控制和报告操作风险，商业银行应当建立并逐步完善操作风险管理信息系统。管理信息系统至少应当记录和存储与操作风险损失相关的数据和操作风险事件信息，支持操作风险和控制措施的自我评估，监测关键风险指标，并可提供操作风险报告的有关内容。"这样，银监会在新时期如何建立银行的监测监控系统、建立操作风险管理体系、建立和完善《操作风险管理信息系统》提供了严谨的法规保障。

国务院办公厅《关于利用计算机信息系统开展审计工作有关问题的通知》要求："为了适应我国国民经济信息化的发展，并将高新技术运用于审计工作之中，更有效地对财政收支、财务收支进行审计监督。审计机关应积极稳妥地探索网络远程审计。"企业如何运用信息化技术手段，开展经营风险监测监控和风险预警体系建设；如何应用IT技术进行操作风险管理、网上审计、风险预警、信息系统审计和计算机审计，提高非现场审计监督水平，防范操作风险的问题已提到了议事日程，势在必行。

非现场审计监督起源于英国，美国从20世纪70年代开始探索并取得快速发展，我国从1989年开始研究和推广应用。目前，它已成为风靡全球的一种金融审慎的监督方式。总部设在美国的信息系统审计与控制协会（Information System Audit and Control Association，ISACA）是国际上唯一的信息系统审计组织，在100多个国家设有分会，该协会通过制定信息系统审计准则来规范IT审计师的工作。随着信息技术

的发展，非现场监督已从传统的手工报送报表发展成为网上审计、非现场报表监测监控、风险实时预警模式，促使非现场监督工作效率和成本效益发生革命性飞跃，实现企业风险预警性。

银行系统已广泛采用IT技术实现柜面业务、信贷、国际结算、资金交易、结算清算、会计核算、核心业务系统网络化管理。随着票证扫描影像技术、网络技术和信息压缩存储技术的发展应用，银行系统业务实现了网络化管理，数据处理加快，信息量巨大，逐步实现了数据大集中，完善了数据中心建设，提出了“绿色数据中心”理念，强化了风险管理，促进了企业稳健、安全运营，提高了经济效益。同时，企业的信息化建设，也拉近了监管部门与被监督企业的业务信息的距离，每年一度的现场手工审计手段已无法适应现代企业信息化发展的需要。因此，开展网上审计（非现场审计）、操作风险监控、风险预警模式是未来企业风险防范的重要手段和有效方法。

目前，国际上因美国次贷引发了全球性的金融危机，《萨班斯法案》开始实施。我国《企业内部控制基本规范》的实施，国内企业将会加速应用IT技术，建设信息系统，强化内部控制、流程管理、风险管控，可持续地发展，稳健生产经营，提高经济效益，迎来企业信息化建设的高峰期。作者愿将20多年来所经历的信息化建设、操作风险管理的肤浅经验，与企业和广大读者分享，希望起到抛砖引玉的作用，主要包括以下方面：实施信息化规划，流程梳理，数据清理，规范数据代码标准；应用IT技术建立内部控制评价体系、操作风险管理体系；开展网上审计、非现场审计、风险预警；进行信息系统审计、计算机审计。

本书由两大部分内容组成，共分十四章。

第一部分内容是企业内部控制，操作风险管理操作实务。主要讲述：构建银行系统操作风险管理体系，《巴塞尔新资本协议》内部控制13项原则，《萨班斯法案》内部控制五要素；五部委颁发的《企业

内部控制基本规范》的控制要点，企业流程管理以及流程管理工具NIMBUS－Control系统的应用方法，企业操作风险管理信息系统的建立。重点描述：

（1）企业内部控制五要素。内部环境、风险评估、控制活动、信息与沟通、内部监督。举例说明如何建立企业内部控制过程指标评价体系，风险评估，内部控制测评，操作风险管理分析。

（2）建立基于流程管理的授权控制体系。流程梳理，流程再造，风险点设置，运用NIMBUS－Control系统，建立基于流程管理的授权控制体系的方法步骤。

（3）建立操作风险管理体系。操作风险监测监控，风险识别，风险预警，数据仓库，操作风险管理信息系统。

第二部分内容是信息系统审计。主要是修改、补充和完善《网上审计》中有关系统总体架构设计的内容。主要讲述：网上审计与风险预警系统总体设计，信息系统审计，信息系统的控制评估，计算机舞弊审计，信息系统审计的技术方法和步骤。重点描述：

（1）建立网上审计与风险预警系统的方法步骤。网上审计财务系统，建立风险预警指标体系，风险度级别设置，规范数据代码标准。运用美国赛仕SAS/IntrNet网络软件工具建立数据处理系统、数据仓库、非现场审计与风险预警监管模式的总体结构设计。

（2）信息系统审计、信息系统的控制评估、计算机审计（IT审计）、计算机舞弊审计的方法技巧。比较详细地介绍了计算机信息系统风险控制，信息系统审计实例（从信息系统开发计划、需求设计、系统设计、程序设计、系统测试、系统运行、系统维护等周期性流程）。揭示计算机舞弊犯罪的特点，开展计算机舞弊审计的方法和原则，以及计算机审计的技术方法等实务性内容。

附录内容是我国财政部、证监会、审计署、银监会、保监会等五部委颁发的《企业内部控制基本规范》；国资委发布的《中央企业全

面风险管理指引》；银监会发布的《商业银行操作风险管理指引》等法规。

本书技术概念新颖、内容丰富、实用性强，适用于金融机构、大中型企业（公司）、董事、监事、审计监督、风险管理；财务会计、审计评估、审计咨询、项目管理；企业建立内部控制过程指标评价体系、内部控制测评；基于流程管理的操作风险控制、授权管理；信息系统开发；操作风险管理，风险预警；信息系统审计、舞弊审计、计算机审计的培训教材和参考用书，也可作为以上专业在校学生的参考教材。

本书在编写过程中，得到中央财经大学终身教授姜维壮导师的教诲，同时，对中国金融出版社编辑部主任戴硕、责任编辑李融，国资委干部教育培训中心处长季学恒，中经安（北京）信息科技有限公司总经理张玉，国资委研究中心企业部研究所所长刘海全、所长助理何明，NIMBUS 中国总部总经理杜豪、执行总监朱东海，政府文化战略研究中心副主任张孟，珠海金长源软件公司高级经理罗钰雯、蒙碧军，中国航空信息网络股份有限公司邱健庭，中国民生银行徐莉莉，中国赛仕公司高级经理刘海亮、王莉华，北京卡斯特信息系统技术有限公司高级经理刘虹露等的大力支持和热情帮助表示衷心的感谢。

由于本书编写时间紧，难免出现差错，敬请读者批评指正。

邱胜利

2009 年 6 月于北京

目　录

第一部分　内部控制与操作风险管理

第二部分　信息系统审计

第一部分

内部控制与操作风险管理