

运营审计 手册

(第2版)

(英) 安德鲁·钱伯斯 (Andrew Chambers) 著
格雷厄姆·兰德 (Graham Rand) 著
刘宵伦 朱晓辉 译

The Operational Auditing
Handbook
Auditing Business and IT Processes
(2nd Edition)

运营审计 手册

(第2版)

(英) 安德鲁·钱伯斯 (Andrew Chambers) 著
格雷厄姆·兰德 (Graham Rand)
刘宵伦 朱晓辉 译

The Operational Auditing
Handbook
Auditing Business and IT Processes
(2nd Edition)

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

Andrew Chambers and Graham Rand: The Operational Auditing Handbook: Auditing Business and IT Processes, 2nd Edition

ISBN: 9780470744765

Copyright © 2010 John Wiley & Sons, Ltd

All rights reserved. Authorized translation from the English language edition published by John Wiley & Sons, Ltd. No part of this book may be reproduced in any form without the written permission of John Wiley & Sons, Ltd.

Simplified Chinese translation edition copyrights@ 2012 by Century Wave Culture Development Co-PHEI.

Copies of this book sold without a Wiley sticker on the 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。

版权贸易合同登记号 图字：01-2011-1878

图书在版编目（CIP）数据

运营审计手册：第2版 /（英）钱伯斯（Chambers,A.），（英）兰德（Rand,G.）著；刘宵伦，朱晓辉译。—北京：电子工业出版社，2012.10

书名原文：The Operational Auditing Handbook:Auditing Business and IT Processes（2nd Edition）

ISBN 978-7-121-17370-7

I. ①运… II. ①钱… ②兰… ③刘… ④朱… III. ①企业—内部审计—手册 IV. ①F239.45-62

中国版本图书馆 CIP 数据核字(2012)第 129691 号

责任编辑：李 静

印 刷：北京东光印刷厂

装 订：三河市鹏成印业有限公司

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：36.5 字数：770 千字

印 次：2012 年 10 月第 1 次印刷

定 价：98.00 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 zltts@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

长期以来，由于企业经营的复杂性所致，无论对于企业外部人士，还是对于企业内部人士而言，在有限的时间内尽可能全面地掌握企业的运营状况，进而对企业价值进行评判，都是一项颇为艰巨的挑战。对于股权投资者等企业外部人士来说，对目标企业开展的法律和财务尽职调查，一是容易浮于表面，二是难于抓住重点、要害问题，三是往往局限于对财务报表进行分析，容易被误导，以偏概全，舍本逐末；对于企业内部审计人员以及风险管理和内部控制自我评价人员而言，从哪些方面着手及如何识别和评价企业运营流程中的风险及控制薄弱环节，也一直缺乏系统性的介绍和指导。而本书的出现，就填补了这方面的空白。

本书致力于帮助使用者在最短的时间内系统地了解并掌握企业的运营全貌，进而形成对企业运营状态、风险所在及投资价值的整体判断。对于企业风险管理和内部控制人员、内部审计人员及价值投资人士来说，本书是不可或缺的工作指南。

本书内容围绕如何评判企业的核心竞争能力而展开，包括理解运营审计、关键职能审计及信息技术审计三个组成部分。

企业的核心竞争能力，集中表现为对机会的把握和追求，以及对风险的防范和控制，两者缺一不可。企业的经营就是抓住并追求那些能使企业成功的机会，同时削减或控制那些导致企业不利的风险，两者共同作用于企业运行的各个层面。

首先是作用在企业治理层面。一般而言，企业治理机制包括企业治理结构的建立、战略目标确定、业务模式选择及文化及价值观建设。虽然本书定位在对企业运营层面的审计，但在第1部分“理解运营审计”中，仍然详尽介绍了治理、风险管理与内部控制的流程，以及不同经营管理思想（如业务流程再造、全面质量管理、扁平化管理、准时制管理以及授权和外包等）对于控制与审计的影响。

在企业业务模式确立之后，企业就进入运营阶段（从企业经营的层级看，也就是运营层面）。从企业价值链的视角看，运营阶段包括资金流程、采购流程、生产流程、销售流程等直线流程及人力资源流程、资产管理流程、财务报告流程、集团控制流程、研发流程、安保流程及环境保护流程等辅助或管理流程。本书对这些流程的审计都做了非常详尽的介绍。在这个过程中，有两点是需要加以强调的：

其一，要正确理解财务报告的作用。对于企业运营过程而言，财务报告绝非最重要的环节，更非企业经营的目的，而只是在企业经营权与所有权分离的背景下，企业经营的“副产品”。由于注册会计师审计过程中委托代理机制存在的固有缺陷，再加上中国恶劣的道德环境，使得财务报告中存在着极大的错报、漏报风险。因此，简单地、单纯地依赖财务报表分析进行运营审计，无疑是不全面甚至会得出误导性结论的。

其二，强调了企业预算编制的重要性。本书的一大突出贡献，就我本人的认识而言，就是明确界定了究竟什么是运营的效率、效果及效益（经济性）。这一问题已经困扰了企业界、审计界、风险管理和内控界良久。例如，在各类审计教科书中，一般都会介绍“3E审计”，但对于什么是“3E审计”，大都语焉不详。国内审计实务中颇具特色的绩效审计、经济责任审计，虽然也能够发挥一定作用、查出一些问题，但是由于其没有从理论上清晰、有效地界定何谓经营（以及资金使用）的经济性、效率性和效果性，在方法论层面存在着根本缺陷，因而并未发挥其全部积极作用。在风险管理和内控领域也面临着同样的问题，即使“运营的效率 and 效果”被写入了风险管理和内控的目标，但是人们仍普遍不了解怎么才算是提高（或者更确切的说法，“合理保证”）企业“运营的效率 and 效果”。本书澄清了人们长期以来的模糊认识，明确提出：所谓运营的效率、效果及效益（经济性），就是对预算和实际决算的投入和产出的不同口径比较，因此，运营的效率、效果及效益（经济性）必须建立在有效编制预算的基础上。为此，就必须纠正企业普遍存在的预算松弛现象，这对于企业管理的正规化，将起到巨大推动作用。

无论在企业的治理层面还是运营层面，信息系统都贯穿其中，构成企业经营过程中不可或缺的组成部分。企业内外部人士在对企业运营进行了解时，不应再“绕过”信息系统进行审计，而必须专门对企业的信息系统进行审计。因此，本书的第3部分专门介绍了信息技术审计的相关内容，包括对信息技术的战略规划、组织、政策框架、具体应用等40个具体专题的介绍。

由以上介绍，相信读者能够领略到本书的巨大价值。但是，由于本书成书于英伦三岛，在应用于中国具体环境时，还应该注意一些基本假设与中国现实环境的差别。例如，本书所谈的运营审计思想，隐含前提是建立在一定社会道德水准之上的，企业成员秉持相同的价值观，不存在串通舞弊的情况。因此，本书对道德审计及舞弊审查的内容关注略嫌不足。但即便如此，本书对于中国读者提高运营审计水平来说，仍然是一本难得的佳作。

本书经由李海风先生向我推荐。海风与我是北京大学MBA同班同学，在到北京大学学习前，我们也都从事审计工作。或许是由于对中国审计行业发展状况有同样的观察和评价，同属理想主义者，又都能耐得住寂寞，毕业后我们不约而同、异曲同工地从事了外版专业图书的引进和翻译工作，但由于相互之间疏于联络，直到《超越COSO》中文版“撞车”，我们才知道彼此在做着同样工作。之后我们陆续合作了《布林克现代内部审计学》、

《Wiley CIA 备考精要系列》等书。MBA 毕业十余年来，我们各自以及合作翻译、审校的国外一流专著、教材，已逾 50 本，并受到读者的普遍欢迎和好评。十余年心血，甘苦自知，乐在其中。谨以此书，作为我们翻译工作的纪念。

本书由朱晓辉初译，由刘霄仑审校，并由中国投资协会创业投资专业委员会戴晓春副秘书长审定。本书翻译过程中，周天虹女士对本书第 3 部分的翻译工作有贡献，在此表示感谢。

因译者水平所限，文中如有错漏之处，请读者不吝赐教。我的邮箱是：
liuxl@mail.nai.edu.cn.

刘霄仑

序

本手册第1版于1997年首次出版，在第2版出版之前，第1版一直在印刷发行，无疑表明了本手册经久不衰。本手册旨在从业务流程的角度，为运营审计提供最新指南，从而填补一项空白。本手册简洁、实用。

本手册第2版新增的内容包括有关治理流程、风险管理流程和内部控制流程的深入思考。我们大胆尝试，将本手册内容更新并扩展至信息技术审计。我们相信，我们对国际数据保护立法和国际信息立法自由的介绍全面、新颖地涵盖了当代这些重要话题。实际上，本手册的使用者会发现，本手册为他们提供了在信息技术领域开展有效审计服务所需要的最新工具包。为了遵守《萨班斯—奥克斯利法案》第404条，评估财务报告内部控制效果的方法也应运而生，并且得到了广泛应用，对此我们也予以了关注。读者会发现有关控制自我评价的更详细的内容，我们还专门安排了一章，探讨有关内部审计活动评估的问题。第2版还在相关内容上与美国内部审计师协会的最新准则及其他机构的公告保持了统一。

本手册旨在成为业务流程自我评估计划设计人员的工作伙伴；同样，它是代表他人开展审计工作的内部审计师和管理咨询师的专业顾问。本书的编写针对的是私营企业、公共机构及非营利性组织，旨在作为设计效益审计方法的基础。我们相信从事财务、会计系统审计及开展管理审计的外部审计师会发现本手册大有裨益，也值得收藏。

同时，我们考虑到美国内部审计师协会在这个学科领域的专业认证要求，希望本手册能成为标准教材。我们还特别考虑了学生的需要，在各章末对特定知识点做了适当的交叉参考注释，并附上了详细的参考文献。

本手册的时效性在一定程度上源于所涵盖的业务流程与其当代处理方法的结合；在一定程度上也源于我们加入了有关业务流程再造、准时制管理、缩减规模、扁平化管理、授权、环境、道德、控制自我评价及IT等问题和当代处理方法；在一定程度上还涉及我们常视为业务流程审查与评估人员的助手的风险评估技术。

本手册旨在唤醒人们对一系列广泛的运营及活动的基本问题、风险和目标的意识。换言之，它旨在激发人们对运营审计的经济背景的创新思维。在实践中，为任何一个组织的各运营领域定义一套普遍适用的万能方法都是极其困难的任务，因为不同实体的动机和背景各异。我们采用了一种以所要解决的关键问题的最佳实践为支持的业务导向观，希望借

此鼓励审计创新，而不是被过于规范性的计划和惯例所窒息。读者需结合自身经验与所在企业主导文化的相关方面，考虑它们对本手册内容的影响，创造出量身定制的运营审计方法。

我们尽力区分按照企业的组织方式开展审计工作的方法与确定和评估跨组织边界的自然业务流程的方法。后一种审计方法往往具有创造价值的最大潜力。

我们相信，因为本手册根植于“现实世界”，所以会对从事审计师、直线管理人员、管理顾问，以及希望获得运营审计师资格的人员大有裨益。

我们欢迎读者对未来版本提出宝贵意见和建议。

安德鲁·钱伯斯

电话和传真：+44 (0) 1790 763 350

互联网电话：+44 (0) 207 099 9355

互联网传真：+44 (0) 207 099 3954

电子邮箱：ProfADC@aol.com

网址：www.management-audit.com

格雷厄姆·兰德

grahamrand@btinternet.com

手机：+44 (0) 7729 374074

致谢

我们感谢一直以来激励我们写作本书的许多客户和朋友；感谢所有认真阅读了本书全部手稿并提出许多宝贵的改进意见的人。我们引用了大量资料：在我们所引用的任何资料中，我们都力求注明出处并征得适当许可。如果我们有任何疏漏之处，欢迎批评指正，一有机会，我们将立即更正。

安德鲁·钱伯斯
格雷厄姆·兰德

目录

第 1 部分 理解运营审计

第 1 章 运营审计方法	2
运营审计的定义	2
运营审计的审计范围	3
运营审计的审计方法	12
技术活动内部审计的智力支持	16
劳动生产率与绩效计量系统	18
效益审计	21
标杆管理	22
第 2 章 业务流程	25
引言	25
业务流程的审计范围	26
业务流程的自我评估	27
混合审计范围	28
业务流程存在缺陷的原因	28
确定组织的业务流程	29
在内部控制设计与审查中采用循环法或流程法	32
《标准审计计划指南》中介绍的业务流程	32
完善业务流程的标志	33
高校的学校管理循环	34
第 3 章 制定运营审查计划，服务管理与审计	37
引言	37
《标准审计计划指南》的实际应用	37
《标准审计计划指南》的格式	43
运营审计中的风险	47

第4章 治理流程	67
引言.....	67
内部控制流程是风险管理流程的有机组成部分.....	67
风险管理流程是治理流程的有机组成部分.....	68
治理流程、风险管理流程与内部控制流程的目标.....	69
COSO的目标观.....	70
应该制定一套统一的目标吗.....	71
内部治理流程.....	71
公司治理的董事会及外部因素.....	72
董事会的确认真空.....	72
内部治理流程的风险与控制问题.....	73
董事会的风险与控制问题.....	76
外部治理流程的风险与控制问题.....	78
第5章 风险管理流程	82
引言.....	82
风险管理目标.....	82
有效风险管理的基本要素.....	84
内部审计在风险管理中的职责范围.....	85
风险管理工具.....	86
风险矩阵.....	86
风险表.....	91
风险管理挑战.....	92
风险管理流程的控制问题.....	94
第6章 内部控制流程	98
引言.....	98
范例1：COSO内部控制框架.....	99
范例2：Turnbull内部控制框架.....	108
范例3：CoCo内部控制框架.....	109
范例4：系统论/控制论内部控制模型.....	110
范例5：分立加监管式控制.....	114
范例6：分类控制.....	116
内部控制目标.....	118
确定内部控制是否有效.....	119
控制的成本效果因素.....	120
内部控制流程问题.....	121

第 7 章 审查控制环境	124
引言	124
控制环境审查的控制目标	124
控制环境审查的风险和控制问题	124
欺诈	126
第 8 章 审查财务报告的内部控制——萨班斯—奥克斯利模式	128
引言	128
成本与效益	130
2007 SOX-Lite	131
“显著不足”和“重大缺陷”的修订定义	131
在评估时采用经认可的内部控制框架	132
《萨班斯—奥克斯利法案》第 302 条和第 404 条合规流程的风险与控制问题	143
第 9 章 经营/管理方法及其对控制与审计的影响	149
引言	149
业务流程再造	149
全面质量管理	152
扁平化管理	156
授权	158
外包	160
准时制管理	163
第 10 章 控制自我评价	167
引言	167
控制自我评价：问卷调查法与专题讨论会法	168
选择专题讨论会的参加者	168
控制自我评价的应用领域	168
管理者与内部审计在控制自我评价中的职责	169
避免直线管理者失望	170
高管的鼓励	171
协调控制自我评价的专题讨论会，组织控制自我评价的培训	172
匿名投票系统	172
比较控制自我评价与内部审计	173
控制自我评价是内部审计的再保证	174
混合法：内部审计与控制自我评价专题讨论会相结合	174
专题讨论会的形式	174

XII ⇨ 运营审计手册（第2版）

在控制自我评价中运用 CoCo 内部控制框架.....	175
阅读资料.....	177
控制自我评价的控制目标和模板.....	177
第 11 章 评价内部控制活动.....	180
引言.....	180
持续监控.....	180
定期内部审查.....	181
外部审查.....	181
质量确认审查中发现的常见缺陷.....	183
内部审计成熟度模型.....	184
有效计量内部审计对公司盈利能力的贡献.....	184
内部审计活动的控制目标.....	194

第 2 部分 关键职能审计

第 12 章 对财务与会计职能的审计.....	198
引言.....	198
财务与会计环境的系统/职能要素.....	198
控制目标与风险和控制问题.....	199
司库（或现金出纳）.....	200
工资.....	201
应付账款.....	203
应收账款.....	205
总账/管理账户.....	207
固定资产（和资本性支出）.....	209
预算编制与监控.....	211
银行账户与银行业务安排.....	212
销售税金（增值税）核算.....	214
税收.....	216
存货.....	218
产品/项目核算.....	220
备用金及费用.....	221
财务信息与报告.....	223
投资.....	224

第 13 章 对子公司、远程经营单元与合资公司的审计	226
引言.....	226
事实发现.....	227
高层级审查计划.....	228
合资公司.....	228
第 14 章 对合同与采购职能的审计	233
引言.....	233
控制目标与风险和控制问题.....	233
合同签订.....	236
合同管理环境.....	238
评估承包商的生存能力和竞争能力.....	241
备案经批准的承包商名单.....	242
投标程序.....	244
合同签订与投标文件.....	246
合同选择与发包.....	247
绩效监控.....	249
评估工程进度并进行中期结算.....	250
承包商的决算账户.....	251
审查项目产出与绩效.....	253
第 15 章 对运营与资源管理的审计	256
引言.....	256
生产环境的系统/职能要素.....	256
控制目标与风险和控制问题.....	257
规划与生产控制.....	257
生产设施、厂房及设备.....	259
人员.....	261
材料与能源.....	263
质量控制.....	265
安全.....	267
环境问题.....	269
法律法规的遵循.....	271
维修.....	272
第 16 章 对市场与销售职能的审计	275
引言.....	275

XIV ◀ 运营审计手册（第2版）

市场与销售职能的系统/职能要素	275
总体评论	276
控制目标与风险和控制问题	276
产品开发	277
市场调研	279
宣传与广告	280
定价与折扣政策	282
销售管理	284
销售绩效与监控	287
分销商	288
母子公司关系	291
代理商	293
订单处理	295
保修安排	298
维修与服务	300
备件与物料用品	302
第 17 章 对分销职能的审计	304
引言	304
分销职能的系统/职能要素	304
控制目标、风险与控制问题	305
分销、运输和物流	305
分销商	307
存货控制	310
仓储	313
第 18 章 对人力资源职能的审计	316
引言	316
人力资源职能的系统/职能要素	316
控制目标与风险和控制问题	317
人力资源部门	317
人力资源部门的控制目标	317
招聘	320
人才与继任规划	322
员工培训与发展	324
福利	326
绩效工资、养老金计划（及其他福利）	328

医疗保险	334
员工考核与奖惩事宜	335
健康与安全	337
劳工关系	340
公司机动车辆	341
第 19 章 对研发职能的审计	345
引言	345
研发职能的系统/职能要素	345
产品开发	346
项目评估与监控	349
厂房及设备	351
开发项目管理	352
法律法规问题	354
第 20 章 对安保职能的审计	357
引言	357
控制目标、风险与控制问题	358
安保	358
健康与安全	360
保险	362
第 21 章 对环境责任的审计	365
引言	365
环境审计	366
环境问题的出现	367
欧洲生态管理与审计计划	367
将环境问题与公司战略和追求利益联系起来	369
环境评估与审计系统因素	370
内部审计的职责	371
环境问题审查计划范例	372
第 3 部分 信息技术审计	
第 22 章 信息技术	378
引言	378
信息技术及相关活动的公认标准	379

	信息技术与管理的系统/职能要素	384
	控制目标与风险和控制问题	386
第 23 章	信息技术战略规划	387
第 24 章	信息技术组织	390
第 25 章	信息技术政策框架	393
第 26 章	信息资产登记簿	398
第 27 章	生产能力管理	405
第 28 章	信息管理	407
第 29 章	档案管理	415
第 30 章	知识管理	430
第 31 章	信息技术网站和基础设施（包括物理安全）	439
第 32 章	信息处理活动	443
第 33 章	备份与存储介质管理	446
第 34 章	移动存储介质	449
第 35 章	操作系统软件（包括补丁管理）	452
第 36 章	系统访问控制（逻辑安全）	457
第 37 章	个人电脑（包括笔记本和掌上电脑）	460
第 38 章	远程工作	464
第 39 章	电子邮件	468
第 40 章	互联网使用	475
第 41 章	软件维护（包括变革管理）	481
第 42 章	网络	484
第 43 章	数据库	487
第 44 章	数据保护	489
第 45 章	信息自由	498
第 46 章	数据传输与共享（标准与协议）	505
第 47 章	法律责任	512