SOX

【现代内部审计经典系列】

How to Comply With Sarbanes-Oxley Section 404
Assessing the Effectiveness of Internal Control

中国内部审计协会 中国智慧工程研究会 隆重推荐

如何遵循SOX404条款
——评估内部控制的效果

（第二版）

【美】迈克尔·拉莫斯／著
◆李海风／主译 张玉／审校

中国时代经济出版社
China Modern Economic Publishing House

《现代内部审计经典系列》

How to Comply With Sarbanes-Oxley Section 404
Assessing the Effectiveness of Internal Control

如何遵循SOX404条款
——评估内部控制的效果

（第二版）

SOX

【现代内部审计经典系列】

How to Comply With Sarbanes-Oxley Section 404
Assessing the Effectiveness of Internal Control

中国内部审计协会 中国智慧工程研究会 隆重推荐

如何遵循SOX404条款
——评估内部控制的效果

（第二版）

【美】迈克尔 · 拉莫斯／著
◆李海风／主译 张玉／审校

中国时代经济出版社
China Modern Economic Publishing House

著作权合同登记　图字：01-2006-6939 号

图书在版编目（CIP）数据

如何遵循 SOX404 条款：评估内部控制的效果（第二版）/（美）拉莫斯著；李海风主译，张玉审校. —北京：中国时代经济出版社，2007.8

ISBN 978-7-80221-341-8

Ⅰ.如...　Ⅱ.①拉...②李…③张…　Ⅲ.企业管理—经济评价—研究　Ⅳ.F270

中国版本图书馆 CIP 数据核字（2007）第 081319 号

如何遵循 SOX 404 条款——评估内部控制的效果（第二版）

〔美〕迈克尔·拉莫斯　著

李海风　主译

张　玉　审校

出 版 者	中国时代经济出版社
地　　址	北京市东城区东四十条 24 号 青蓝大厦东办公区 11 层
邮政编码	100007
电　　话	（010）68320825（发行部） （010）88361317（邮购）
传　　真	（010）68320634
发　　行	各地新华书店
印　　刷	北京鑫海达印刷厂
开　　本	787×1092　1/16
版　　次	2007 年 8 月第 1 版
印　　次	2007 年 8 月第 1 次印刷
印　　张	21
字　　数	370 千字
印　　数	1~5000 册
定　　价	42.00 元
书　　号	ISBN 978-7-80221-341-8

译者序

2002年,美国发布《公众公司会计改革和投资者保护法》(简称《萨班斯-奥克斯利法案》或SOX),对美国以至全球各地的会计、公司治理以及整个证券市场,都产生了相当大的影响,极大地改变了企业的经营环境和法律环境。该法案第404条款提出的内部控制评审要求,目的是通过加强内部控制来改进公司治理状况,并最终加强公司的受托责任。①

实践表明,404条款引发了许多财务报告流程方面的重大变革,变革之一就是要求管理层按季度和年度提交一份单位对财务报告的内部控制特定效果的报告。该内部控制报告必须清楚地说明管理层有建立和保持适当的财务报告的内部控制的责任,以及管理层须在年末就单位内部控制的效果作出评估。对于许多公司来说,遵循404条款无疑是一个挑战,许多公司的董事、提供声明的高级管理人员、高级经理以及审计人员在共同执行该条款的过程中会在诸多方面存有疑问,而公司董事会及高层人员也可能需要独立顾问来帮助他们解决此类问题。

本书对有关公司根据第404条款实施以风险为导向的、自上而下的评估方法提供了实际的指导,它可以协助单位的404条款项目发起人、主管人员和团队成员在组织内的工作。为了遵循SOX的内部控制报告要求,美国证券交易委员会(SEC)界定了财务报告的内部控制,指出财务报告的内部控制是一个由(股票)发行人的主要经理人员和主要财务官员、或从事类似职能的人员设计或受其监督的流程,该流程受发行人的董事会、管理层和其他人员的影响,为财务报告的可靠性和依照一般公认会计原则编制对外的财务报表提供合理的保证。

鉴于在遵循SOX第404条款的过程中,选择适当的控制标准是对一个单位内部控制效果进行评估的前提条件,因此,本文着重提到特雷德威委员会的发起组织委员会(COSO)于1992年发布的《内部控制-整体框架》,这也是众多在美国上市公司最常用的评估内部控制效果的标准。实际上,美国上市公司会计监管委员会

① 参见李海风、刘霄仑翻译的《布林克现代内部审计学》校译者序,中国时代经济出版社,2006年。

(PCOAB)将 COSO 框架报告作为审计准则第 2 号的基础,该准则要求对 COSO 所定义的内部控制五要素进行评价。

COSO 框架将内部控制定义为一个流程,它的效果是该流程在一个或多个时点上的状态或条件。内部控制是受单位的董事会、管理层以及其他人员影响的流程,其目的是为运营(operation)[①]的效率和效果、财务报告的可靠性、遵守适用的法律和规章等目标的实现提供合理的保证。内部控制渗透于整个组织的一系列活动中,它存在于计划、组织、执行和监督等基本的管理过程,是附加于这些管理过程的必不可少的部分。[②] COSO 框架还认识到控制存在于组织内部的两个不同层面:单位层面和活动层面。为了恰当评价活动层面的控制,需定义单位的业务流程活动。COSO 框架建立在用于理解业务活动和价值链分析的某个模式之上。

内部控制五要素是控制环境、风险评估、控制活动、信息和沟通以及监控,这些要素来自管理层管理企业的方式,并整合在管理过程中。具体表现为:

- *控制环境*体现并影响着组织文化,设定了组织基调,影响着组织成员的控制意识。它是内部控制其他要素的基础,为内部控制提供了规范和架构。
- *风险评估*是要识别和分析组织目标实现所面临的相关风险,并为确定如何管理这些风险形成依据。风险评估的前提是要制定在不同层面相互联系并在内部保持一致的目标。
- *控制活动*是有助于确保管理层的指令得到贯彻执行的各种政策和程序,有助于确保针对单位目标实现的风险采取必要的措施。控制活动贯穿于整个组织的所有层面和所有职能中,并包括批准、授权、验证、核对、业绩评价、资产的安全保障以及职务分离等一系列的活动。
- *信息和沟通*,永久性信息必须以一定形式和期限来识别、获取和沟通,这样可便于人们履行其职责。有效沟通的意义较为宽泛,可能发生在组织的方方面面。所有人员必须收到来自最高管理层的明确信息,确保控制职责得到严格执行。他们必须理解各自在内部控制系统中的角色,以及个人活动对他人的影响。他们必须拥有向上沟通重要信息的方式,还要和顾客、供应商、管制机构以及股东等外部当事方有效地沟通。
- *监控*。内部控制系统有必要进行监控,即在多年间对内部控制系统的运行

---

① 国内财务界同仁倾向于将该词译为"经营",管理界一般译为"运营",译者认同后者,详情见波特 1985 年的《竞争优势》一书对价值链的分析,COSO《内部控制 - 整体框架》第二卷对一般商业模式的讨论。

② 参见李海风、李媛媛翻译的《内部审计活动在治理、风险和控制中的作用》第 268 页,电子工业出版社,2007 年。

质量进行评估。它可以通过持续性监控活动、单独评价或是结合上述两种情况来实现。持续性监控发生于整个运营过程中，包括日常管理和监督活动，以及员工在履行其工作任务时的其他活动；单独评价的范围和次数主要取决于风险评估以及持续性监控程序的效果。

这些要素互相联系，构成一个有机整体，对变化的环境做出动态反应。内部控制系统和单位的运营活动密不可分，它的存在有重要的商业原因。当控制建立在单位的基础架构中并成为单位的实质性部分时，内部控制是最为有效的。“嵌入式”控制支持质量改进和授权行动、避免不必要的成本，并能快速响应外部环境的不断变化。①

正如 COSO 报告的执行纲要所述，内部控制在公司实现盈利目标、完成使命以及最小化意外情况的过程中发挥作用，并使管理层迅速应对不断变化的经济和竞争环境，转移顾客需求以及优先考虑有关事项，调整结构适应未来增长。内部控制能够提升效率，降低资产损失风险，并有助于确保财务报表的可靠性以及遵循有关法律法规。

当前，中国的内部控制标准体系正在建设中。2006 年，财政部会同证监会、国资委、审计署、银监会、保监会等相关部门成立了企业内部控制标准委员会，着手建设中国企业内部控制标准体系，并且取得了重要的阶段性成果，同时就制定和完善我国企业内部控制标准体系，是新形势下会计管理工作贯彻落实科学发展观、走长期可持续发展道路的必然要求，是促进经济健康运行、规范资本市场秩序、完善现代企业制度的现实需要，是完善我国会计法规制度、推动中国会计走向国际市场的正确选择等达成共识。当然，在建设中国特色的内部控制标准体系过程中，我们需要借鉴国外同行的研究成果，内部控制的建立是企业发展到一定程度的必然管理要求，它受公司治理、价值创造、风险和机会、监管、企业文化、技术发展以及受托责任等各方面的影响。② 身处国际化舞台的中国，如何从 COSO 框架中吸收合理内核，在内部控制、风险管理等标准、框架的制定上同国际主流框架保持一致，是很重要的事情，这样会有利于沟通，有利于企业管理层次的提升，执行能力的到位，以及良好业绩的实现。

呈现在您面前的《如何遵循 SOX404 条款——评估内部控制的效果》（第 2 版）一书，是著名管理咨询顾问以及内控专家迈克尔·雷墨斯（Michael Ramos）的最新力著，他在内控方面的另一本著作是《萨班斯－奥克斯利法案》404 条款工具箱：面

① 见 COSO《内部控制－整体框架》，1992 年。

② 参见付涛等翻译的《超越 COSO：加强公司治理的内部控制》一书，清华大学出版社，2004 年。

向管理者和审计人员的实务指南。作为内部控制领域的实践者和管理咨询顾问，他为各类企业组织的顾客成功建立了有效的内部控制系统，帮助各类机构更好地遵循SOX所要求的内控评审制度。本书内容涵盖了内部控制评审领域的最新变化，相信本书在中国境内的出版，无论从理论上还是实务上，都会使中国的管理界、财务审计行业以及咨询行业大受裨益。

本书的翻译工作是团体合作的结果，全书由李海风主持翻译，初译译者包括：李海风译序言、目录和词汇表，马婧译第1、3、4、5章，杨莉译第2章，张玉译第6－8章，勾越对全书图表进行了整理，李海风审译并统改了各章，林小驰协助审改了第1章和第5章，张玉对译稿进行了审校，孙强、孟秀转对初译稿进行了审阅，并提出了宝贵意见。最后，我要对家人的理解和支持表达感激之情，在过去的近3年时间里，我和团队成员在努力完成现代内部审计、内部控制、风险管理、IT治理等领域的最新理论及实务用书的翻译及写作工作，这些工作占去了我们3年中的大部分时间，而其中一些时间本应该是留给我们的家人和孩子的。

对现代内部审计、内部控制、风险管理以及IT治理有兴趣的同仁，敬请留意以下经典著作：《布林克现代内部审计学》、《SOX与内部审计新规则》、《内部审计活动在治理、风险和控制中的作用》、《实施内部审计业务》、《内部审计手册精要》、《超越COSO：加强公司治理的内部控制》、《管理审计职能》、《控制自我评估：以协调为基础的咨询指南》、《控制自我评估：面向风险管理和其他实务应用》、《审计信息系统》、《舞弊防范和内部控制执行路径图：创建合规性文化》、《COSO企业风险管理：全新理解ERM整体框架》、《管理者合规性指南：最佳实务和案例研究》、《信息化绩效评价》、《信息系统审计：安全、风险管理与控制》、《信息安全管理：全球最佳实务与实施指南》、《基于ITIL的IT服务管理导论》、《IT领导力》等。

限于译者水平，本书如有漏误之处，恳请读者指正。

李海风

2007年6月

于中国智慧工程研究会

第1版序

在我还是十几岁的孩子时，头一次听到了“旅程本身就是收获”这句话，人生不禁有了意义。所谓结果，不过是旅程的副产品而已。在我写作本书时，桌子上就放着一杯咖啡，它令我想起咖啡的品质是和咖啡豆的选用、烘烤、碾磨以及用热水混合的过程有着直接关系的。可以衡量的目标是重要的事情，可是我设法不去过分注重于结果，因为太多的事情不是我能控制的。作为本书的作者，我无法保证这本书可以售出多少。我所能做到的就是在（写作）过程中付之以相当的诚信，有机会将书写得更好。至于书的销量，我确实不想多说，我知道一本畅销书的必要条件首先是一本好书。

我们生活的社会越来越强调结果，这正好验证了“为了正当目的可以不择手段”这句格言。过程可以无关紧要，结果才是要紧的。我对质量流程的观点，在当今的社会中仿佛多少有些滑稽。

下面来谈谈《萨班斯－奥克斯利法案》（SOX）。

《萨班斯－奥克斯利法案》和流程有关系。在过去70多年的时间里，对投资公众的保护主要着重于报告结果。向公众提供公允、透明的财务结果，让他们了解这些结果的必要信息，这就是公众得出全面而精明的决定所需的全部东西。《萨班斯－奥克斯利法案》改变了这一切，它指出只有结果报告是不够的，除了财务结果之外，单位现在还要分析并评价报告这些结果所采用的流程和控制的质量。

关于评价某个单位的流程和控制这个新规定，在观点上是一个重要的转变。遵守这个规定的实际意义是令人惊奇的，我们还需要若干年才能全面理解这个规定。评价某个流程和分析某个结果大大不同。流程分析是不明确的、主观的、非线性的，我们用于开展这类评价的工具和技术相对较为有限。不同学科的专业人士要全面实施《萨班斯－奥克斯利法案》的规定，这些来自信息技术、风险管理、证券法律、组织发展和业务流程分析领域的专业人士，在内部控制的评价方面起到了宝贵的促进作用。在写作本书的时候，我受益于上述各个学科的知识。

我是一名注册会计师，一名受训的审计人员，多年前曾积极地参与过审计业

务。审计人员对于内部控制效果的评价和报告，会提出一些很有价值的观点。毕竟，内部控制评价和报告只注重于财务报告，这是审计人员的专长领域。单位管理层的报告要经过独立审计师的审计，因此管理层采用的评价流程要同外部审计师的期望和要求相吻合。这个新规则中的很多概念、测试技术以及报告要求，都汲取自审计文献。在写作本书时，我希望运用审计方面的学识来描述针对复杂的、需要精心构建的内部控制评价的流程。

2003 年 4 月，在我开始本书写作之时，美国证券交易委员会（SEC）有关内部控制报告的最终规则还没有发布，时至今日，在我完成本书终稿时，上市公司会计监管委员会（PCAOB）有关独立审计师对内部控制进行审计的责任的关键准则还是以前的东西，很多参与财务报告流程的人员在试着履行职责时，都面临着重要的不确定性。

从某种意义上讲，本书还不是最终的产品，只要你愿意，可以将它当作第 1 版。在往后的日子里，有关内部控制评价和报告的知识会迅速膨胀。随着我在这个主题方面的经验和知识的完善，我认为有必要去写作第 2 版书。

很显然，第 1 版书不会是有关内部控制评价和控制这个主题的确定性产品。在本书写作过程中，面临着太多的不确定性，对于这个主题的经验也有所欠缺，我写作本书的目的很简单，只是尽可能去收集有关这个主题的信息，对信息进行归类，然后运用我的专业知识和技能，将它们按合乎逻辑的、易于接触的方式组织起来。

很多人都对如何执行《萨班斯 - 奥克斯利法案》第 404 条款的规定提出问题。我希望我所做的工作能尽可能全面地思考这些问题，并将我的发现和大家分享。

迈克尔·雷墨斯

2003 年 9 月

第2版序

自本书第1版完稿后，有些事情发生了戏剧性的变化。在准备本书第2版时，提前报送文档的上市公司已完成最初的合规性工作，许多公司正在进行第二年度的《萨班斯－奥克斯利法案》第404条款的遵循工作。现在，可以得到很多不同格式的指南，来帮助管理层、公司的咨询师、公司的外部审计师评价内部控制效果。

在这一版中，我不仅将自己的经验写进去，还吸收了来自朋友和客户那里的经验。我还阅读并思考了大量的有关内部控制的资料。很多想法、经验和出现的一些最佳实务，都在本书中有所体现。我希望这些内容可以增加深度，而且及时。

很多人都在写遵循404条款的成本问题，这使那些相信“所要求的”工作量超出极限的公司大大地后退。在听到了很多争论故事，并且亲身参与了几次激烈讨论之后，我相信很多上市公司发表的言论是有价值的。我观察到以下两个最大的问题：

- *以系统地、自下而上的方法来评价内部控制。*有些公司及其审计师最初认定，对内部控制的评估要求对公司运用的各项控制进行文本记录和测试。这种方法是有误导的，会极大地增加合规成本。本书最初描述的综合性的结构化方法，严格遵循了PCAOB在其指南中阐明的以风险为导向的自上而下的方法，该指南在2005年初提交的内部控制报告的最初文档中得以遵循。这种方法明确，管理层及其审计师在确定哪些控制要进行评价时，应该运用他们的判断，并且这些判断应该根据对公司、公司目标以及为实现这些目标所面临风险的理解来做出。总而言之，这就是本书第1版最初描述的方法。在第2版中，在深入单个活动层面控制的细节前，我强调了风险评价的重要性，以及对单位层面的控制效果进行评价的重要性。
- *孤立地考虑内部控制缺陷。*在评价内部控制效果时，要将内部控制作为一个整体来考虑。以我的经验看，在控制缺陷的评价方面存在着诸多的误解，这些控制缺陷最终会产生大量的实质性薄弱环节的报告。当然，上市公司

的内部控制中存在着为数相当的实质性薄弱环节，绝大多数在过去是不用报告的。此外，至少在报告的第1年，存在着将事实上的各种控制缺陷归入实质性薄弱环节的趋势。促进这种趋势的很大一批人，评价控制缺陷的常规做法就是孤立地看待控制缺陷，不去适当地考虑补偿性控制的影响。在这一版中，我设法将评价控制缺陷的指南更多地包括进来。

在过去两年间，关于如何记录、测试和评价内部控制，我们已收获颇丰，还有很多东西有待于学习。我认为这个领域的审计和公司治理仍将持续演进，当然演进的速度是不一样的。我期望继续学习、思考并写作对于我们的财务报告系统而言是重要的那些问题。

迈克尔·雷墨斯

2005年9月

目　　录

第1章 业务方法

本章概述

回顾了美国证券交易委员会(SEC)关于以下方面的规则要求:

- 管理层评估单位财务报告的内部控制的效果
- 独立审计人员审计管理层有关内部控制的报告
- 管理层要按季报告单位的披露控制和程序的效果

概述了同内部控制相关的审计准则。

描述了评价单位的内部控制的结构化方法。

就外部顾问构建的用于帮助管理层评价内部控制的效果,以及独立审计人员审计管理层有关内部控制的报告业务提供建议。

管理层要评估单位的内部控制

2002 年发布的《萨班斯-奥克斯利法案》(SOX)引发了许多财务报告流程方面的重大变革。变革之一就是要求管理层按季度和年度,提交一份单位对财务报告的内部控制特定效果的报告。本章综述了这些报告要求,第 8 章提供了更详细的指南和示例。

内部控制的定义

为了遵循《萨班斯-奥克斯利法案》的内部控制报告要求，美国证券交易委员会（SEC）的规则提供了对财务报告的内部控制的工作定义。该规则 13a-15（f）按如下内容来界定对财务报告的内部控制一词：

> 对财务报告的内部控制是一个由（股票）发行人的主要经理人员和主要财务官员、或从事类似职能的人员设计或受其监督的流程，该流程受发行人的董事会、管理层和其他人员的影响，为财务报告的可靠性和依照一般公认会计原则编制对外财务报表提供合理的保证。它包括以下政策和程序：
> 1. 保持能在合理的细节水平上准确、公允地反映发行人的交易和资产处置的记录；
> 2. 对依照一般公认会计原则编制财务报表所需的交易记录提供合理的保证，对根据发行人的管理层和董事会授权发生的收入和费用提供合理的保证；
> 3. 就预防或及时检查可能实质性影响发行人的财务报表的未经授权的收购、使用或处置资产提供合理的保证。

在考虑 SEC 的定义时，应该注意以下几点：

- 内部控制是一个广义的概念，延伸到了一个企业各个领域的管理工作。SEC 的定义将单位对内部控制的考虑事项，收缩到了财务报表的编制方面。因此，我们使用“对财务报告的内部控制”一词。
- SEC 希望这个定义同特雷德威委员会的发起组织委员会（COSO）提供的与财务报告目标有关的内部控制定义保持一致（有关 COSO 报告的详细讨论，见第 2 章）。
- SEC 的规则明确提到了单位资产的使用或处置——也就是资产的安全保障。

本书中使用的内部控制一词，是指 SEC 规则中定义的“对财务报告的内部控制”，除非另有说明。

年度报告

《萨班斯-奥克斯利法案》的 404 条款要求首席执行官（CEO）和首席财务官