萨班斯法案 404条款：后续进展*

陈汉文 吴益兵 李 荣 徐臻真

(厦门大学会计系 361005)

【摘要】2002年萨班斯 - 奥克斯利法案 404条款发布之后，美国证券交易委员会 (SEC) 通过制定规则，为 CEO 和 CFO 对主体财务呈报内部控制和披露控制的报告提供指南；公众公司会计监管委员会通过为注册会计师制定审计准则，直接影响注册会计师该类审计合约的计划与实施；COSO 委员会制定内部控制标准框架，作为管理当局和注册会计师进行内部控制评价的基础。本文主要对 SEC规则、第 2号审计准则和 COSO 委员会最新的内部控制框架 (即 ERM) 作一介绍，以期为我国监管机构在上市公司内部控制制度的强制性规定方面提供借鉴。

【关键词】萨班斯 —奥克斯利法案 SEC规则 审计准则 内部控制框架

2002年的萨班斯 - 奥克斯利法案 (Sarbanes - Oxley Act of 2002, 本文简称萨班斯法案) 对财务呈报程序产生了十分重大的影响。其中，404条款要求公众公司管理当局对企业内部控制的有效性进行披露报告，注册会计师必须对该份报告进行审计。在实践层面，美国证券交易委员会 (SEC) 通过制定规则来具体执行萨班斯 - 奥克斯利法案 404条款，这些规则为 CEO和 CFO对主体财务呈报内部控制 (entity's internal control over financial reporting) 和披露控制 (disclosure control) 的报告提供了指南；公众公司会计监管委员会 (PCAOB) 通过为注册会计师制定审计准则，直接影响注册会计师该类审计合约的计划与实施；COSO委员会制定内部控制标准框架，作为管理当局和注册会计师进行内部控制评价的基础。本文介绍上述几方面的最新进展。

一、萨班斯法案 404条款与 SEC规则

为了配合萨班斯法案 404条款有关内部控制规定的实施，SEC提出了“财务呈报内部控制”的操作性定义。SEC规则 13a - 15 (f) 规定：财务呈报内部控制是一个过程，由发行人的主要执行官员、主要财务官员或者行使类似职权的人员设计或监控，受发行人的董事会、管理当局和其他人员所影响，为财务呈报的可靠性和财务报表 (供外部使用的) 的编制符合公认会计原则提供合理的保证。具体包括以下控制政策和程序：(1) 保持详细合理的会计记录，准确公允地反映发行人资产的交易和处置情况；(2) 为下列事项提供合理的保证：发行人对发生的交易进行必要的纪录，从而使财务报表的编制满足公认会计原则的要求；发行人所有的收支活动均得到管理当局和董事的合理授权；(3) 为下列事项提供合理保证，即防止或及时发现发行人的资产未经授权地取得、使用和处置，因为发行人资产的取得、使用和处置会对财务报表产生重大影响。从 SEC财务呈报内部控制定义可以看出：其一，内部

* 本文是教育部人文社会科学重点研究基地重大招标项目 (02JAZJD630008) 的研究成果之一。

控制是一个广义的概念，涉及到企业管理的各个方面。SEC将主体对内部控制的考虑限定在财务报表编制的内部控制的范围内，因此使用了“财务呈报内部控制”这一术语。其二，SEC期望其所定义的内部控制与 COSO委员会报告里的财务呈报目标相一致。其三，规则特别提到了主体资产的利用与处理，意在资产保护。

1. 萨班斯法案 404条款要求首席执行官 (CEO) 和首席财务官 (CFO) 对主体财务呈报内部控制的有效性进行评价和报告。该份报告包括在公司按年度递交给 SEC的 10K表格 (Form 10K) 中，为此，SEC已经为其注册成员制订了规则，要求公司的 10K表格必须包括：(1) 管理当局对企业财务呈报内部控制的年度报告，具体为：①关于管理当局建立和维护适当企业财务呈报内部控制的责任报告；②管理当局用于评价企业财务呈报内部控制有效性的方法框架的报告；③管理当局对到最近财年末为止的企业财务呈报内部控制的有效性的评价，包括企业财务呈报内部控制是否有效的声明，其中，必须披露管理当局所确认定的企业财务呈报内部控制的任何重大弱项，如果存在一个或多个重大弱项，则管理当局不得认定其财务呈报内部控制是有效的；④一个声明，即会计事务所 (对公司包含在年报中的财务报表进行审计的机构) 已经对管理当局的财务呈报内部控制有效性评价意见签发鉴证报告。(2) 会计师事务所的鉴证报告，提供审计人员对管理当局财务呈报内部控制评价意见的鉴证报告。(3) 财务呈报内部控制的变动，对于任何重大地影响或可以合理预期将重大地影响企业财务呈报内部控制的任何变动都应予以披露，该项披露要求从 2003年 8月 14日起生效。上面所提及的其他规定，如管理当局对企业财务呈报内部控制有效性的报告及相关审计人员鉴证意见的生效日期，由公司的归档状态决定，即①对第一个财政年度在 2004年 6月 15日或以后结束的所谓“加速编报”(Accelerated filer) 公司，必须在该财政年度的年报中开始遵守内部控制报告和鉴证要求；②小规模公司、外国私人发行人和其他非加速编报公司，要求在 2005年 4月 15日或之后结束的财政年度年报中遵循新规则的所有规定。

2. 萨班斯法案 302条款要求对主体“披露控制与程序”的有效性作出季度报告。为此，在 SEC规则中，引入了一个新的概念，即“披露控制和程序”。SEC规则 13a - 15 (e) 将披露控制和程序定义为：被设计出来的控制和程序，应确保根据法案要求填写和提交的报告中发行人应该披露的信息，按照委员会规则所规定的期间和格式，进行记录、处理、汇总和报告。“披露控制和程序”包含证券交易法报告中所有重大的财务和非财务信息控制，包括重要合同签订、战略关系变化、管理当局薪酬或法律事件等，其所包含的信息超过主体财务呈报内部控制的范围。SEC的 S - K规章 307条款，要求管理当局披露公司主要执行官、主要财务官或者履行类似职权的人员在对到报告期间的披露控制和程序进行评价的基础上，就企业披露控制和程序的有效性作出评价。除了对披露控制的报告外，公司的季度报告也必须披露主体财务呈报内部控制的重大变动。值得注意的是，在这些季度性文件中，没有要求管理当局一定要对财务呈报内部控制进行评估和报告 (只是要求按年度进行其评价)，也没有要求公司独立审计人员一定要对管理当局的披露控制评价作出鉴证。

3. SEC建议所有公众公司建立信息披露委员会，以监督披露的生产和核查过程。包括核查 10Q、10K和其他 SEC文件，盈利发放和其他适当披露的公众信息；确定需要披露的重大性事件和交易；确定在披露控制和程序的设计和执行中的重大缺陷和不足；评价 CEO和 CFO对可能影响披露的重大信息的关注度。信息披露委员会的存在和有效运行，将会在评价主体内部控制有效性的工作范围和工作性质方面产生

重要影响：其一，信息披露委员会职能的有效运行，是强化主体控制环境的一个要素；其二，披露委员会的工作可以形成文档，以利于工作小组缩减其工作范围。

4. SEC要求公司的主要执行官和主要财务官签署两个书面证明，包括在公司的 10Q和 10K表格中。这两个书面证明是萨班斯法案 302和 906条款所要求的。（1）302条款，具体细化到 SEC规则 13a - 14（a）/ 15d - 14（a）中，要求在呈交 SEC季度和年度报告时提出证明：包括已经核查了 [某个确定注册公司的] 的特定报告；报告中没有存在任何重大的错报和漏报而导致对本期报告产生了误导性的信息；呈报的财务报表和其他报告公允地反映了注册公司在所报告期间和时点上的财务状况、经营业绩和现金流动状况；对建立和维护公司的披露控制和程序（如证券交易法 13a - 15（e）/ 15d - 15（e）规定）和企业财务呈报内部控制报告（如证券交易法 13a - 15（f）/ 15d - 15（f））承担责任；已经向公司的审计师和公司董事会的审计委员会进行披露（或者行驶相同职权的人），等等。（2）906条款，包括对具体联邦犯罪法典的证明，如证明报告是完全符合 1934证券交易法的 12（a）或 15（d）中的条款要求，报告中的信息在所有重大方面公允地反映了企业的财务状况和经营成果。

二、萨班斯法案 404条款与 PCAOB审计准则

为了配合审计人员对管理当局财务呈报内部控制有效性评价的审计工作，2004年 PCAOB发布了第 2号审计准则（AS2），用以指导审计的计划与实施。

1. AS2提出财务呈报内部控制审计的目标是，对管理当局就企业财务呈报内部控制有效性的评价发表意见。这个目标分解为两个步骤：管理当局必须对主体的内部控制进行评估并得出结论；审计人员将对管理当局就内部控制有效性的评价是否公允作出评价并发表独立意见。因而，对内部控制进行了双重评价，先是由管理当局，然后是审计人员。在一些情况下，审计人员可能对已经由企业执行过的测试进行再测试，不过，这并不减除管理当局对于内部控制存档、测试和报告的责任。AS2指出，管理当局在财务呈报内部控制审计过程中的责任有：对企业财务呈报内部控制有效性承担责任；运用恰当的控制标准评估企业财务呈报内部控制的有效性；有足够的证据（包括文件）来支持其评估结论；就到最近财年末为止企业财务呈报内部控制的有效性作出书面的评估报告。如果管理当局未完成上面列举的责任，那么，审计人员应以书面的形式与管理当局和审计委员会进行沟通，明确其对财务呈报内部控制的审计无法满意地完成，以至无法发表意见。

2. AS2要求审计人员评估管理当局应用于评价主体内部控制的程序方法的可靠性；复核和使用一些管理当局、内部审计人员和其他人的评价过程中取得的测试结果；或自己进行测试，以形成独立意见。（1）对管理当局评价程序的评估。准则要求审计人员必须理解和评价管理当局对财务呈报内部控制有效性的评价过程。在取得理解之后，审计人员要确定管理当局是否执行了以下步骤：第一，决定需要测试的控制，包括所有与财务报表重大会计账户和披露有关的认定的控制。一般来说，这些控制指有关发生、授权、记录、处置和报告财务报表重要账户和披露以及报表中的相关认定的控制；对遵循公认会计原则的会计政策选择与运用的控制；反舞弊的程序和控制；其他控制及其所依赖的信息技术总控制；对重要的偶发性和非系统性交易如涉及判断和估计的账目的控制；企业层面的控制，包括控制环境和年末财务报表编制过程的控制，如记入总分类帐的业务金额汇总的程序控制、记录调整和非调整事项的控制活动（如报表合并、重分类等）。第二，评价控制失败将导致的错报的可能性和其他

有效控制能够达到相同控制目标的程度。第三，确保对多区域和多分部公司的评价涵盖了下属公司和部门。第四，评价控制设计的有效性。第五，评价控制执行的有效性，比如内部审计的控制测试，管理当局指导下的其他人进行的控制测试，利用服务机构的控制报告，控制应用证据的审查，进行自我评估测试以及部分的管理当局持续监督活动。仅仅完成这项评估是不够的。为评估企业财务呈报内部控制的有效性，管理当局必须对与所有重大会计科目和披露有关的认定的控制进行评估。第六，确定财务呈报内部控制缺陷的重大性和可能性。第七，与审计人员和其他人员沟通。第八，评价结果是否合理，是否支持管理当局的评估结果。

3. AS2指出如果导致财务报表重大错报的错误或舞弊在控制得到遵守的情况下会被制止或被发现，那么财务呈报内部控制的设计就是有效的。审计人员判定企业控制能否满足控制的标准是：确定企业每个部门的控制目标；确定满足每个目标的控制；如果控制有效执行，确定内部控制是否能防止或发现导致财务报表重大错报的错误或舞弊。

4. AS2指出审计人员评价运行的有效性通过判定控制是否如其设计般执行，执行控制的人员是否具备必要的权力和素质以有效地执行控制程序来进行。对运行有效性的控制测试，包括对相关人员的询问、相关证据的检查、公司经营活动的观察以及控制应用的重复执行。对于测试控制的时间安排，AS2作出了详细规定，比如准则指出，对于重要的非常规性交易、带有高度主观判断的账户或程序以及期末调整记录的控制，审计人员应该在接近或正在那个时点上实行控制测试，而不是针对一段时期。对于控制测试的范围，AS2要求审计人员每年都要收集足够的证据，证明企业对财务呈报内部控制包括对所有内部控制环节的控制是否有效执行。这就意味着，审计人员每年必须收集控制有效性的证据，这些控制涉及所有财务报表重大账户和披露有关的认定。另外，AS2还对其他人员的工作的应用、财务呈报内部控制有效性的意见发表、财务呈报内部控制审计与财务报表审计的关系等内容作出了规范。

三、萨班斯法案 404条款与 COSO委员会《企业风险管理综合框架》

内部控制标准体系是公司内部管理当局与外部注册会计师完成财务呈报内部控制有效性评价的基础。在美国，COSO委员会于 1992年制定的内部控制综合框架 （IC - IF）是至今管理当局和注册会计师在财务呈报内部控制有效性评价方面的依据之一。萨班斯法案 404条款颁布之后的一个新变化是，COSO委员会于 2004年 9月 29日正式发布了《企业风险管理综合框架》（ERM - IF），并提出将以 ERM取代 IC - IF。何时取代，未见时间表，但趋势既定。

1. COSO委员会提出，企业风险管理是企业的董事会、管理层和其他员工共同参与的一个过程，应用于企业的战略制定和企业的各个部门和各项经营活动，用于确认可能影响企业的潜在事项并在其风险偏好范围内管理风险，对企业目标的实现提供合理的保证。根据管理者经营的方式划分，企业风险管理包括八个相互关联的组成要素：内部环境、目标设定、事件识别、评估风险、应对风险、控制活动、信息与沟通和监督。内部环境是企业风险管理的基础，为企业风险管理所有其他组成部分运行提供了平台和结构。企业的目标制定是企业风险管理的起点，是其他步骤的驱动力量。整个过程是环环相扣的。在目标制定的前提下，企业需对影响目标的风险进行事件识别，进而对识别的事项进行风险评估，风险评估驱动风险反应，影响控制活动，信息与沟通和监督贯穿于企业风险管理的整个过程，并对前面的各个组成要素进行修正。这样，企业风险管理不只是一个直线过程，即一个组成部分只会对下一个部分产生影响，而且是一个

多元化的相互作用的过程，即几乎任何组成部分都能够并将会影响另一个部分。企业风险管理的八个组成部分体现的是一个动态的过程，是一个有机的整体。

2. 内部控制综合框架到企业风险管理综合框架，不是局部的修补和简单改良，而是在理念上的本质突破。体现在从“控制环境”到“内部环境”，这一修改使得企业关注的范围不再局限于控制方面，而是从更宽阔的视野更综合更直接地考虑各种因素对风险的影响；目标制定中增加“战略目标”，使企业在追求短期利益的同时，从战略的高度关注企业的长远目标和可持续发展；将“风险评估”扩展为“事件识别”“风险评估”和“风险反应”，不是对原“风险评估”进行简单的细化，而是代表着企业风险意识日益增强和积极主动管理风险。企业风险管理强调应对所有事件既包括正面事件与负面事件进行综合识别，并且应该将其以适当的组合方式加以看待，而后通过对固有风险和剩余风险的综合评估做出适当的风险应对措施。这样一方面可以减少经营偏差的发生及相关成本和损失，另一方面有利于企业抓住机会（正面事件），及时调整策略，以达到经营和获利目标，避免资源浪费。

四、启示

美国上市公司监管机构推出的一系列针对内部控制的制度安排，对我国市场监管颇具借鉴意义。2004年年底发生的中航油（新加坡）事件说明了借鉴的紧迫性，尽管中航油（新加坡）内部存在风险控制方面的内部控制制度，照理应该是能够满足企业风险管理需要的，但由于管理层对内部控制的破坏，内部控制制度形同虚设，进而导致悲剧发生。这个案例告诉我们，必须评估企业内部控制的设计与执行两个方面的有效性，确保内部控制规范真正落到实处，从而维护正常的市场秩序，保护投资人、债权人、经营者的长远利益。从这个意义上看，借鉴萨班斯法案、SEC规则、PCAOB的审计准则和COSO的企业风险管理，我国监管机构在上市公司内部控制制度的强制性规定方面，应该有所作为。

主要参考文献

Public Company Accounting Oversight Board, 2004, Auditing Standard No. 2 - An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements

Michael Ramos, 2004, How to Comply with Sarbanes - Oxley Section 404, John Wiley & Sons, Inc.

The Committee of Sponsoring Organization of the Treadway Commission, 2004, Enterprise Risk Management - Integrated Framework, Executive Summary Framework.

The Committee of Sponsoring Organization of the Treadway Commission, 2004, Enterprise Risk Management - Integrated Framework, Application Techniques

严晖，2004，风险导向内部审计研究，厦门大学博士学位论文打印稿

朱荣恩，贺欣，2003，内部控制框架的新发展——企业风险管理框架，《审计研究》，6

陈汉文，王华，郑鑫成，2003，《安达信：事件与反思》，暨南大学出版社

刘宗柳，陈汉文，2000，《企业内部控制：理论、实务与案例》，中国财政经济出版社

吴水澎，陈汉文，邵贤弟，2000，论改进我国企业内部控制，《会计研究》，9

吴水澎，陈汉文，邵贤弟，2000，企业内部控制理论的发展与启示，《会计研究》，5