企业内部控制和风险管理

——《萨班斯—奥克斯利法案》释义

Qiye Neibu Kongzhi He Fengxian Guanli

友联时骏管理顾问 编著

复旦大学出版社

图书在版编目(CIP)数据

企业内部控制和风险管理——《萨班斯-奥克斯利法案》释义/友联时骏管理顾问编著. —上海:复旦大学出版社,2005.7
ISBN 7-309-04559-9

Ⅰ.企… Ⅱ.友… Ⅲ.企业管理:财务管理-美国
Ⅳ.F279.712

中国版本图书馆 CIP 数据核字(2005)第 052012 号

企业内部控制和风险管理——《萨班斯-奥克斯利法案》释义

友联时骏管理顾问 编著

出版发行 复旦大学出版社

上海市国权路 579 号 邮编 200433

86-21-65118853(发行部) 86-21-65109143(邮购)

fupnet@fudanpress.com http://www.fudanpress.com

责任编辑 苏荣刚

总 编 辑 高若海

出 品 人 贺圣遂

印 刷 上海江杨印刷厂

开 本 787×960 1/16

印 张 17

字 数 238 千

版 次 2005 年 7 月第一版第一次印刷

印 数 1—4 100

书 号 ISBN 7-309-04559-9/F·1002

定 价 28.00 元

前　言

中国经济经过二十多年的发展，取得了举世瞩目的业绩，随之而来也产生了庞大的赴海外募集资金直至谋求上市的企业群体。对于国际投资者而言，国内企业在资源和市场方面的巨大潜力使他们对投资中国寄予厚望，而国际上关于企业管制等理论及实践发展的最新趋势，也使得国际投资者对国内企业在公司治理、财务报告、合规性披露等方面提出了极高的要求。越来越多的事例证明，在何种程度上满足国际投资者对企业管制等方面的要求，不仅仅决定了该企业能否顺利融资或成功上市，而更是成为了直接影响企业所在的行业、上下游行业，乃至中国上市公司整体形象和信誉的关键问题。

面对新的形势，很多中国企业希望通过借鉴国际先进经验及国内知名企业的成功案例，不断改善自身的经营状况和提高内部管理水平，以期迅速提升企业的核心竞争力。而要实现这个目标，企业则需要整合财务管理、风险管理、商业模式、商业流程、信息技术、法律等各方面的资源，并在风险管理方面进行了深入细致、以实战为导向的研究工作。

在长期的咨询实践中，我们认识到，企业的风险管理并非事无巨细地针对所有风险，而是要细分其类型，分别提出应对策略。此外，这些结合企业发展的应对策略，还须针对国际投资者的期望及上市地的法律监管要求而展开。

企业为了使某项重大决策获取最高的成功率，必须做到未雨绸缪，在策划阶段就要充分考虑到诸如环境风险、运营风险、信息风险等各类风险，必须制定数套方案应对环境的变化，必须充分解读国家的相关法

律及上市地的法规，并完全遵从上述的法律及法规，遵从产业规章，承担相应的社会责任。另外，还必须建立一套完整可靠、有据可查的内部监控机制，有效控制信息在业务运行和财务报告中流转的完整性和准确性。

面对这些全新的环境和要求，国内众多企业开始逐渐关注各类风险，并开始聘请具备国际水平同时拥有丰富国内经验的咨询公司，来改进企业的风险管理能力。但是，我们深刻认识到众多的中国企业在建立起风险管理的政策和程序时，仍然将自己定位在了一个过于狭小的空间。根据我们的实践，下述各方面已经成为了企业日常运行中局限风险管理有效实施的因素。

- 判断失误（Judgment）：风险管理的效力受经营决策中人为判断所导致过失的限制。
- 管理层凌驾（Override）：为达到违法目的而支配或不执行已制定的政策或程序（管理层“凌驾”不应与管理层“干涉”相混淆。管理层“干涉”对于处理不合规定的交易极为必要，且干涉行为会对外进行披露，并有文件记录；而凌驾行为的行为人则有意隐藏其活动）。
- 共谋（Collusion）：两个或两个以上员工的共谋活动会导致风险管理的失败。共谋犯罪或隐瞒活动有可能以风险管理程序不可辨别的方式更改财务数据或其他管理信息。
- 成本收益分析的主观化（Costs Versus Benefits）：资源是稀缺的，所以在决策时必须考虑相关的成本和收益。从成本分析来看，存在难以量化与特定的内部环境因素相关的成本或某一外部信息成本的问题。从收益分析来看，可能存在主观评价，如难以量化对某些风险采取措施后所带来的收益。
- 分类过细（Breakdowns）：设计良好的风险管理可以被细分。但是员工可能会误解过于细分的指示，做出错误的判断或由于疏

忽而导致错误。

这些因素不仅使得企业所实施的风险管理程序低效甚至无效，更会严重挫伤投资者的信心，使企业面临上市融资被长期搁置，企业产业整合缺乏资金无法实施的尴尬境地。正如前面所提及的，海外的资本市场和国际投资者对企业管制已经提出了一系列严格的标准，特别是在美国资本市场（NASDAQ，NYSE，AMEX）上市，更需要完成针对《萨班斯—奥克斯利法案》（Sarbanes-Oxley Act，简称“SOA”）的合规性工作。自2003年10月份起，美国证券交易委员会要求实施的SOA法案在各类企业的风险管理领域均开始占据首要地位。公开上市的公司或拟上市公司，都在重新审视其公司治理结构、报告和披露过程及内部控制流程。SOA的核心条款302款及404款涉及企业多方面的运行管理流程。

综合资本市场对企业管制新的要求，我们将通过本书中对美国资本市场萨班斯法案的详述，勾画出一幅公司治理和内部控制明快清晰的图案，不仅为已经或者计划在美国上市的企业作出指引，也为我国的上市监管部门和完善企业内部控制及提升公司治理的咨询公司提供更多的借鉴。

感谢陈嘉剑先生为本书附录《萨班斯—奥克斯利法案》所作的文字整理工作。

友联时骏

2005年6月

目　录

1

萨班斯—奥克斯利法案(SOA)简介

1.1 SOA 概要

1.1.1 《萨班斯—奥克斯利法案》的背景和提要

当今财经时代,人们普遍认识到注册会计师在维护市场经济秩序,协调和保护企业管理者、投资人及社会公众的合法权益方面发挥着重要作用。为了确保注册会计师能恰当行使其职能,需要对注册会计师行业进行管理。这种管理具体体现在两个方面:一是行业内部自律;二是通过立法机构的介入,以法律形式固定下来,对注册会计师职业进行监管。

作为西方资本市场的代表国家,美国强调以法律形式加强对注册会计师资格的要求和监管。事实上,美国第一个会计职业团体——美国公共会计师协会(The American Association of Public Accountants)最早期的活动之一,就是设法在纽约州获得法律认可。其活动结果是,纽约州于 1896 年通过一项提案——《对公共会计师职业的监管》,这是美国第一部关于会计职业监管的成文法。在纽约州立法后,其他各州也相继制定了类似的法律。其中,对注册会计师职业影响最大的,是《1933 年证券法》和《1934 年证券交易法》,这两部法律涉及注册会计师的民事责任

和刑事责任。注册会计师在执行审计业务时,要充分认识到可能的潜在责任,保持应有的职业谨慎,以降低职业风险。

立法机构的介入也对注册会计师职业有着重要影响。如果立法机构认为现有的证券法和会计法律没有从各方面恰当地控制注册会计师的活动,那么就可能会进一步关注并修改这些法律条款。美国安然公司会计造假丑闻发生后,美国国会草拟并通过了《萨班斯—奥克斯利法案》(Sarbanes Oxley Act 2002,以下简称 SOA),对注册会计师提供服务的独立性、公司内部控制和风险管理提出了更严格的要求。美国总统布什于 2002 年 7 月将此法案签署为法律。

总体而言,SOA 的目的在于促进企业责任感,加强信息的公众披露,提高财务报告和审计的质量及透明度,并对违反证券法律和其他法规的行为加大惩罚力度。SOA 增加了对企业报告的要求和责任,明确禁止了某些上市公司行为,显著地扩大了审计委员会的责任和权威。该法案同时创造出一个全新的会计行业监督机构——公众公司会计监察委员会(Public Companies Accounting Oversight Board,简称 PCAOB)。这个由五个成员组成的机构将监督公共会计事务所及它们的有关行为,如工作底稿的保留、第二合伙人审核、审计报告的通过以及内部控制系统的测试和报告等。

此外,该法规还规定:

- 加大了对企业欺诈行为的惩罚,加强了对企业检举人的保护。
- 要求包括财务报告在内的所有向美国证券交易委员会(The U. S. Securities and Exchanges Commission,简称 SEC)定期备案材料,必须经首席执行官和首席财务官签名确认。
- 要求年度报告中必须出具一份内部控制报告,与首席执行官和首席财务官对年度和季度报告的签名确认书一起备案。

由于这些新规定的出台,首席执行官和首席财务官将受到比以往任何时候更为严格的监督。即使是最具有职业操守、最小心谨慎的首席经

理人,都需要采取额外的措施以记录恰当的合规(compliance)努力,确保所有的相关各方都能获得充分和独立的法律支持和建议,并推行鼓励职业操守行为的企业文化。

很明显,SOA 强调禁止外部审计师向同一客户提供审计服务的同时又提供非审计服务,例如记账,财务信息系统设计、评估或者评价服务,内部审计外包服务,任何管理职能或人力资源服务以及投资咨询、代理或法律服务。

SOA 中其他一些值得注意的要求还有:

- 领导和审核外部审计的合伙人五年一轮换。
- 破坏、改变或伪造与联邦政府调查、破产过程和企业审计有关的记录的行为,将受到更加严厉的惩罚。

总而言之,SOA 通过以下措施改变了公司治理的根本意义:强化证券交易委员会(SEC)的监管职能;使审计委员会而非管理层成为公共会计师的首要雇主;严格限制外部审计师的行为以增强其独立性;通过真正的惩罚来强化管理层报告制度和信息披露。

1.1.2 《萨班斯—奥克斯利法案》概要

101 条款:公众公司会计监察委员会的建立及其成员

公众公司会计监察委员会(PCAOB)将设五个懂财务的成员,任期五年。其中两个是或者曾经是注册公共会计师(CPA),其余三个必须不是 CPA。主席可以由 CPA 中的一员组成,前提是他或她已有五年没有从事 CPA 业务。

委员会的成员全职服务。禁止成员在服务期内,除"固定的连续收入"如退休金之外,"分享任何利润,或者从任何公共会计事务所收取报酬"。委员会成员由证券交易委员会(SEC)"咨询联邦储备委员会主席和财政部长意见后"任命。成员可以由委员会用"正当理由"罢免。

103 条款:审计、质量控制及独立的标准和准则

公众公司会计监察委员会(PCAOB)将:

(1) 对公共会计事务所进行登记;

(2) 按规章建立或采纳"审计、质量控制、操守、独立性,及其他与准备审计报告相关的标准";

(3) 对会计师事务所进行检查;

(4) 进行调查和纪律检查活动,并执行适当的惩罚;

(5) 执行其他必要或者适当职责或功能;

(6) 强制执业行为与本法案、会计监察委员会规则、职业标准,以及与审计报告准备和发布相关的证券法律、会计师义务和责任保持一致;

(7) 制定预算,管理委员会的运作和委员会的员工。

审计标准。委员会必须"在长期合作的基础上"与为设定标准而召集的指定专业会计师群体和任何咨询群体合作。委员会虽然能够"以它认为合适的程度"采纳这些团体提出的标准建议,但有补充、修改、废除以及拒绝这些团体提出的标准、建议的权力。委员会必须每年向 SEC 报告其设定标准的活动。

委员会必须要求注册公众会计事务所"准备并保存不少于 7 年的审计工作文件和其他与审计报告有关的信息,以提供足够的细节支持其在这些报告中做出的结论"。

委员会必须要求联席合伙人审核和认可审计报告,注册会计事务所必须施行质量控制的标准。

委员会必须采用一个审计标准来进行内部控制的审核。这个标准要求审计者评估内部控制的结构和程序是否包括了准确公正地反映交易的记录,是否合理地保证了记录交易的方式能确保财务报表的编制与通用会计原则 (GAAP)一致,并能反映内部控制中的实际缺陷。

106 条款:外国公共会计事务所

《萨班斯—奥克斯利法案》规定,审计美国公司的外国会计事务所需要在委员会进行登记。这包括那些只进行了部分审计工作——如承

担一家美国公司海外分部的审计工作——但其审计结果为该公司主要审计公司所采用的外国会计事务所。

107 条款(d)：对委员会的监督

证券交易委员会(SEC)拥有对公众公司会计监察委员会(PCAOB)的监管权。SEC 可以通过规章和命令赋予 PCAOB 额外的责任。SEC 可以要求 PCAOB 保留某些记录，并有权力检查 PCAOB，如同对全美证券经纪商公会（NASDAQ)这样的自我监管组织(Self Regulatory Organization，SRO)一样。

在制定规则的过程中，PCAOB 将被看做如同一个“注册证券机构”，即一个自我监管组织。委员必须将提议的规则及对提议规则的改变在 SEC 备案。SEC 可以同意、拒绝或者补充这些规则。

109 条款(d)：资金来源；公众公司会计监察委员会的年度会计支持费用

审计上市公司的公共会计师事务所必须在公众公司会计监察委员会(PCAOB)登记。PCAOB 对每个进行登记的公共会计师事务所征收“注册费”和“年费”，收费金额以能“足够”负担处理和审核申请以及年度报告的成本为准。

PCAOB 还将按规章建立一个合理的“年度会计支持费用”，以维持该委员会的运转。这项费用只摊派到证券发行人。

201 条款：审计师职责范围之外的服务；禁止的服务

一个注册的公共会计师事务所在对同一客户执行审计工作的同时，如果提供任何非审计内容的服务，那将是“非法的”，这些服务包括：①为审计客户提供与会计记录或者财务报表相关的记账和其他服务；②财务信息系统的设计和运用；③评估或估价服务、出具公证意见或实物捐赠报告书；④精算服务；⑤内部审计外包服务；⑥管理功能或人力资源服务；⑦经纪或代理，投资顾问，或者投资银行服务；⑧法律服务和其他与审计无关的专业服务；⑨委员会按照规章不允许的任何其他服务。

委员会可以针对具体的个案情况，在经过证券交易委员会（SEC）审核之后，对任何个人、证券发行公司、公共会计师事务所或者具体的交易活动免除上述禁令。

如果审计委员会事先以下述方式批准，那么提供审计之外的其他服务不列为非法。SOA 规定，只有在经证券发行公司的审计委员会事先批准的情况下，才允许某个会计师事务所从事上面没有罗列的非审计服务，包括税务服务。审计委员会将在定期报告中向投资者披露事先批准的非审计服务。保险公司的监管审计被列为审计服务内容，因此不需要事先审批。

如果所有非审计服务的累计收入占证券发行人支付给审计公司的总报酬的比例不超过 5%（根据证券发行人在非审计服务发生的那个财政年度里所支付的金额来计算），证券发行人在要求服务之时尚没有将其认定为非审计服务，且及时通知了审计委员会，并在审计结束之前获得批准，那么审计公司在为证券发行人提供非审计服务时可以免除事先审批的要求。

事先审批权力可以授予一个或一个以上审计委员会的成员，但是任何获授权成员的决定必须报告给审计委员会全体成员。

203 条款：审计合伙人轮换

审计项目的主要审计合伙人、协调合伙人，或对该项目负责审核的合伙人必须每五年轮换一次。

206 条款：利益冲突

公司现任首席执行官、财务总监、首席财务官、会计主管或者同等职位的人在审计前一年里必须不曾在审计该公司的会计师事务所工作过。

302 条款：财务报告的公司责任

证券发行人的首席执行官和首席财务官要在审计报告后附上一份声明，保证“定期报告中的财务报表和信息披露是适当的，在所有重大方

面公正地报告了公司的运营和财务状况”。任何违反这个条款的行为都被视作明知故犯,必须承担责任。

303 条款:对审计活动的不当影响

任何证券发行公司的官员或董事欺骗性地影响、胁迫、操纵或者误导审计师,导致财务报表出现误导信息的任何行为,均属非法。

304 条款:对公司管理层特定奖金和收益的罚没

如果证券发行人因为财务报表“重大不合规”而被要求重新提供财务报表,其首席执行官和首席财务官应该在不合规材料发布或备案之后的 12 个月内“将所获得的任何奖金,或其他与业绩挂钩或与股票表现有关的报酬”,以及在此期间“通过出售发行人证券实现的利润”,返还给证券发行人。

305 条款:对公司管理层和董事的限制和惩罚

证券交易委员会(SEC)对违反证券法的行为而采取的任何行动,如果给投资者带来损失,联邦法院有权“给予投资者适当或必要的公正补偿”。

如果 SEC 发现任何个人违反了 1934 年交易法案(The Exchange Act)第 10(b)条款,并证明其行为令其不适于担当证券发行公司的管理或董事职位,SEC 可以颁布命令,有条件或无条件、永久或暂时地禁止其担任上市公司的管理或董事职位。

306 条款:养老金管制期间禁止内部交易

在管制期内禁止公司高层管理人员和董事,以及其他内部人士购买和销售股票。任何因违反此项规定而从销售中获得的利润“必须归属于证券发行人,该发行人有权取得这些利润”。如果发行人没有控告或者积极起诉,“发行人的任何证券拥有者”可以提起诉讼并要求获得该利润。

401 条款(a):定期报告的披露;必须披露的信息

任何根据通用会计准则(GAAP)编制的财务报告都必须“反映所有

由注册的会计师事务所发现的重大更正性调整……”。

“各年度、季度财务报表……应该披露所有账外重大交易”，以及与目前或将来可能对上市公司财务状况产生重大影响的“未合并企业”的“其他关系”。

SEC将制定规定，要求预估的财务信息必须“不包含不真实的陈述”，或省略重大事实，保证预估财务信息不产生误导效果。

402条款(a)：禁止对公司管理人员的个人贷款

通常情况下，证券发行人给任何董事或管理人员提供私人信用均属非法。对消费信用公司来说，如果是在常规业务中进行，并与针对大众的条件无异，它们可以向其董事或者管理人员提供家庭改善或消费信用贷款，或对他们发放信用卡。

403条款：对管理层和主要股东交易活动的披露

董事、高层管理人员以及持有10%股份的股东，必须在交易执行后的一个工作日内报告他们的该项交易。

404条款：管理层对内部控制的评估

SOA要求发行人在每份年度报告里包含一份“内部控制报告”，该报告要求：

(1) 描述管理层关于为财务报告建立并维护一套适当的内部控制结构及程序的职责；

(2) 对截至发行人财政年度末该内部控制结构及程序的有效性进行评估。

公众公司会计监察委员会(PCAOB)在与《萨班斯—奥克斯利法案》同时颁布的一份报告中这样解释其法律意图：“(公众公司会计监察)委员会无意将审计公司对内部控制报告的评估看作一项单独业务，或者以此为基础增加收费。”

409条款：实时披露

证券发行人必须在迅速和及时的基础上对其财务状况或者运营的