企业内部控制精要

方法·模板·案例

娄权◎著

面向一线管理　丰富实战技巧　开拓内控视野

暨南大學出版社
JINAN UNIVERSITY PRESS

企业内部控制精要

方法·模板·案例

娄 权◎著

暨南大學出版社
JINAN UNIVERSITY PRESS
中国·广州

图书在版编目（CIP）数据

企业内部控制精要：方法·模板·案例 / 娄权著 . —广州：暨南大学出版社，2014.12
ISBN 978-7-5668-1128-8

Ⅰ . ①企… Ⅱ . ①娄… Ⅲ . ①企业内部管理 Ⅳ . ① F270

中国版本图书馆 CIP 数据核字（2014）第 192192 号

出版发行：暨南大学出版社

地　址：中国广州暨南大学
电　话：总编室（8620）85221601
　　营销部（8620）85225284　85228291　85228292（邮购）
传　真：（8620）85221583（办公室）　85223774（营销部）
邮　编：510630
网　址：http://www.jnupress.com　http://press.jnu.edu.cn

排　版：广州市天河区东棠尚诚图文快印服务部
印　刷：佛山市浩文彩色印刷有限公司

开　本：787mm×1092mm　1/16
印　张：16
字　数：335 千
版　次：2014 年 12 月第 1 版
印　次：2014 年 12 月第 1 次

定　价：39.80 元

前 言
PREFACE

2002年，美国发布了著名的《萨班斯·奥克斯利法案》，被视为近80年来最重要的法规之一，在世界范围内影响深远。2008—2013年间，我国陆续发布了《企业内部控制基本规范》、《企业内部控制配套指引》等内控法规，内部控制是当下及未来企业管理的重要热点。

一、缘起

在为企业提供内控咨询时，我最常被问到的问题是：① 企业建设内控，主要是做什么工作，有没有模板？② 怎样有效地开展内控工作？③ 在内控工作过程中，有哪些常见问题或困难？如何解决？

可见，内部控制在我国尚属新鲜事物，大家的认识还比较模糊，唯有从书籍或网络中去寻求答案。

然而，纵览坊间内部控制相关书籍，我们发现，大致可分为5类：① 学术类，如博士论文或教授专著，侧重于理论探索或实证研究；② 教材类，侧重于概念或知识点介绍；③ 法规解读类，侧重于内控规范及配套指引的阐释；④ 工具类，侧重于制度、流程图介绍；⑤ 案例类，侧重于案例分析。而系统介绍内控方法论、模板的书籍较为少见，虽然从网络上可以获取相关文献或资料，但不够系统。

值此背景，我决定系统地梳理过去几年内控咨询的经验与体会，系统地介绍内控实战方法、模板和案例，供实务工作者参阅和研讨。

二、用途

本书介绍内控建设、评价、审计、优化的全生命周期及注意要点，侧重于实战技能的开发和提升，但又不是唯工具论，提倡“理论框架+实战操作”，实现理论和实务的结合。

本书既可作为内控实务工作者的工具书，又可作为高等院校内部控制（或风险管理）课程的教材或课外读物，对MPAcc、MBA和内控研究者亦有参考价值。

三、特色

与坊间同类书籍相比，本书具有“全”、“细”、“新”、“活”四大特色。

（1）全：模板全面、资料丰富。本书几乎囊括了内部控制工作中所要用到的全套模板，并在书后附上“常用模板与资料索引”（见附录Ⅰ）。

（2）细：由表及里、注重细节。本书采用“动作研究法”将内控工作分解为6个阶段40项工作任务，并逐一解析具体工作任务的方法、模板及注意要点。

（3）新：内容新颖、与时俱进。本书既介绍COSO 2013年发布的17条内控核心原则，又介绍2014年发布的上市公司2013年度内控评价报告。

（4）活：图文并茂、形式灵活，可读性强。

四、结构

本书包括正文、案例资料、阅读材料、自测题目与附录等内容，正文共分为6章：

第1章“概述”，介绍舞弊三角理论、COSO内控框架等，为内控工作者构建必要的理论框架。

第2章“内部控制实战框架”，介绍内控工作应秉承的理念、应培养的意识，以及主要节点等。

第3章“内部控制建设”，介绍组织保障、启动及建设阶段的主要工作内容和注意要点。

第4章“内部控制评价”，介绍内控评价的工作流程与注意要点。

第5章“内部控制审计”，介绍如何选聘外部内控审计师及沟通技巧。

第6章“内部控制的持续优化”，介绍内控优化的主要方式，如流程再造、公司再造等。

本书还设计了11个附录，给出了各业务领域主要风险提示、常用网址、内控词典、常用模板与资料索引等，以便查阅。

五、致谢

感谢暨南大学出版社黄文科老师的支持和鼓励；感谢暨南大学出版社的编辑及工作人员，他们的辛勤劳动减少了本书的谬误；马晓菁同学不辞辛劳，帮我校阅全书，李秀青同学、张丰同学审阅部分章节，并协助推敲逻辑架构，他们分别从实务界、监管者的角度审视本书，并提出重要的修改意见，在此一并致谢。

当然，限于水平和时间，本书存有谬误在所难免，敬请诸君不吝赐教，假以时日，修订再版。

娄　权

2014年6月

目 录
CONTENTS

前 言 …… 1

第1章 概 述 …… 1

1.1 舞弊三角理论简介 …… 2

1.2 COSO 内控框架简介 …… 3

1.3 SOX 简介 …… 7

1.4 C-SOX 简介 …… 9

案例资料1 10 分钟，损失 30 亿元 …… 11

阅读材料1 大亨的黄昏 …… 12

自测题目1 …… 13

本章小结 …… 15

第2章 内部控制实战框架 …… 17

2.1 实战框架概要 …… 18

2.2 内部控制理念和意识 …… 19

2.3 内部控制工作流程及关键节点 …… 24

2.4 内部控制天龙八“不” …… 28

2.5 内部控制建设面临的挑战 …… 32

2.6 小企业内部控制的特殊考虑 …… 34

案例资料2 被炸毁的水电站 …… 36

阅读材料2 内部控制十大漏洞 …… 36

自测题目2 …… 40

本章小结 …… 42

第3章 内部控制建设 …… 43
3.1 组织保障阶段的工作内容及注意要点 …… 44
3.2 内控启动阶段的工作内容及注意要点 …… 54
3.3 内控建设阶段的工作内容及注意要点 …… 61
案例资料3 被举报的供销科长 …… 127
阅读材料3 内控建设常见问题 …… 127
自测题目3 …… 129
本章小结 …… 131

第4章 内部控制评价 …… 133
4.1 总体介绍 …… 134
4.2 编制工作方案 …… 136
4.3 组建评价工作组 …… 140
4.4 现场测试 …… 141
4.5 缺陷认定 …… 151
4.6 编制评价报告 …… 157
4.7 缺陷整改 …… 162
案例资料4 内控评价工作方案关乎成败 …… 166
阅读材料4 内控评审常见问题 …… 166
自测题目4 …… 168
本章小结 …… 170

第5章 内部控制审计 …… 171
5.1 选聘会计师事务所 …… 172
5.2 与内控审计师沟通的注意要点 …… 176
案例资料5 IT系统中的定时炸弹 …… 177
阅读材料5 财务会计基础工作常见问题 …… 177
自测题目5 …… 181
本章小结 …… 183

第 6 章 内部控制的持续优化 …… 185
6.1 总结提炼 …… 186
6.2 流程再造 …… 187
6.3 公司再造 …… 191
6.4 内控考核 …… 193
6.5 内控信息化 …… 194
6.6 迈向全面风险管理 …… 196
案例资料6 组织架构优化 成效显著 …… 198
阅读材料6 公司治理中的常见问题 …… 198
自测题目6 …… 203
本章小结 …… 206

结 语 …… 207

附 录 …… 209
附录 A 各业务领域主要风险提示 …… 209
附录 B 内控工作自查表 …… 215
附录 C 中化国际内控规范实施情况简介 …… 219
附录 D 案例分析参考答案与点评 …… 222
附录 E 自测题目参考答案 …… 225
附录 F 常用网址 …… 226
附录 G 内控词典 …… 227
附录 H 会计师事务所综合评价排名 …… 232
附录 I 常用模板与资料索引 …… 235
附录 J 图目录 …… 238
附录 K 表目录 …… 240

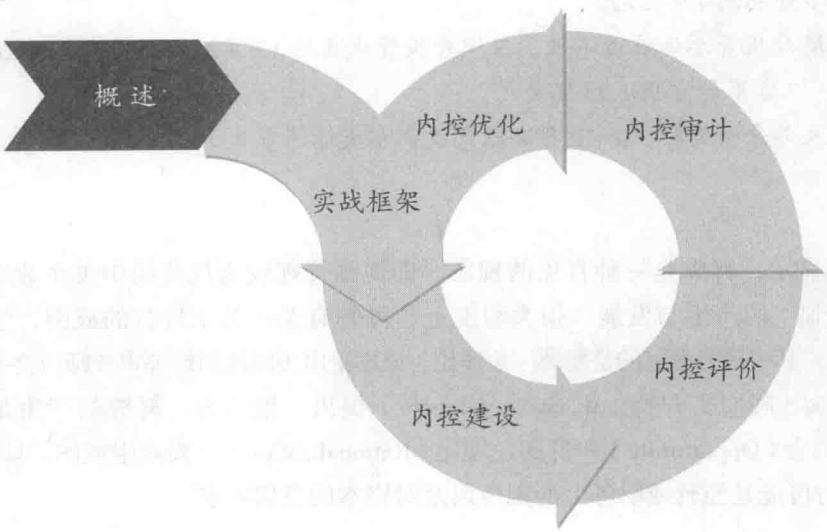
参考文献 …… 242

跋 …… 247

第1章
概　述

本章重点

1. 舞弊三角理论及其对内控设计的启示
2. COSO 内控框架主要内容及 17 条核心原则
3. 萨班斯·奥克斯利法案（SOX）重要条款
4. 我国内部控制规范及演进



公司失败都是由内部控制的失败引起的。
——Adrian Cadbury 爵士

“工欲善其事，必先利其器。”从事内控工作，要提前做好理论、方法和资料的储备。根据我多年内控咨询的经验，做好内控工作需要有一个比较系统的理论框架，这样不仅知道怎么做，还知道为什么这样做。我发现有的内控工作者没有一个系统的理论框架，不了解国内外权威的内控框架，甚至不看内控方面的文件，更谈不上看相关文献，说不出个一二三。这样头脑空空地搞内控，效果不会理想。

本章旨在帮助内控工作者构建一个必要的内控理论框架，包括：①舞弊三角理论；②COSO 框架；③萨班斯·奥克斯利法案（SOX）；④我国内控法规框架（C-SOX）。掌握这些框架对内控工作大有裨益。

1.1 舞弊三角理论简介

2014年6月20日，审计署发布中石油等11家中央企业2012年财务收支审计结果公告[①]，公告显示：

中石油下属9家单位部分工程建设和物资采购未按规定招标，涉及合同金额260.35亿元，其中工程建设238.51亿元。

中冶集团所属的二十二冶及其下属12家单位采取虚开劳务费发票或直接以劳务分包预结算单入账等方式套取资金8,666.84万元，主要用于发放职工工资性津贴及奖金。

大唐集团下属5家单位存在将应计入递延收益的财政补贴资金一次性计入营业外收入等问题，导致多计利润1.9亿元。

兵装集团境外投资总体效益不佳，在境外投资成立的17家海外公司中，至2012年末有5家已停业、7家累计亏损1.38亿美元。

华润集团及部分所属单位2012年公款列支高尔夫球消费支出211万元。

……

上述数据显示，舞弊是一种常见的现象，即使在管理较为规范的中央企业中，亦不例外。内部控制[②]的产生与发展，很大程度上与舞弊有关。关于舞弊的成因，学者们提出了一些理论，其中最为著名的是舞弊三角理论。该理论由美国注册舞弊审核师协会（ACFE）的创始人史蒂文·阿伯雷齐特（W. Steve Albrecht）提出。他认为，舞弊的产生是由压力（Pressure）、机会（Opportunity）和自我合理化（Rationalization）三要素组成的，具体如下：

（1）压力可能是经营或财务上的困境以及对资本的急切需求。

① 资料来源：《南方都市报》，2014年6月21日A04版。
② 内部控制，是由企业董事会、监事会、经理层和全体员工实施的、旨在实现控制目标的过程。

（2）机会可能是宽松或松懈的控制以及信息不对称。

（3）自我合理化则可能是出于“我只是向公司借而不是偷”、“我们只是为了暂时度过困难时期”、“我的出发点是为了一个很好的愿望”等。

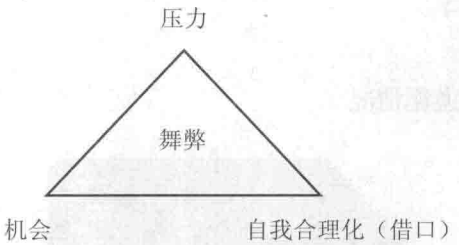


图 1-1 舞弊三角理论

舞弊三角理论对内控设计具有重要启示：

（1）一些企业的高管报酬与短期财务指标（如销售收入、利润）挂钩，当销售收入或利润严重下滑，高管层基于考核的压力，会产生强烈的舞弊动机，进而操纵利润[①]。这就要求考核制度设计应考虑长期的指标，如经济增加值（EVA）、经风险调整后的收益（RAROC），或考虑非财务指标，运用平衡计分卡（BSC）考核，促使企业追寻长期的企业价值，而不是短期的财务利益。

（2）在设计内控制度时，应分析现有的业务流程可能存在的舞弊机会，控制点的设计应从降低舞弊的机会入手，减少“跑冒滴漏”现象的发生，在兼顾效率的情况下，从严控制，不留控制盲区和盲点。

（3）在内控建设中，应形成诚信、健康的内控文化氛围，提升管理层和员工的道德素质，将外在的内控要求内化为自我追求，从“要我做”转向“我要做”，内控要求、风险意识无缝嵌入业务流程。

1.2 COSO 内控框架简介

1.2.1 内控框架：COSO（1992）

COSO[②]内控框架是世界上最著名、最权威、应用最广泛的内控框架。《萨班斯·奥克斯利法案》第 404 条款的最终细则明确表明 COSO 框架可以作为评估企业内部控制的标准。企业常常引进 COSO 内部控制框架，据此整合现有内部控制体系。

① 过去 100 年，舞弊形态从员工舞弊转向管理层舞弊，舞弊方式从榨取现金转向粉饰报表。内部控制的焦点从关注现金及银行存款管理、支付程序转向关注公司层面内部控制。参见丘仲文（p.34）。

② 全称是 The Committee of Sponsoring Organizations of the National Commission of Fraudulent Financial Reporting，是由美国注册会计师协会（AICPA）、内部审计协会（IIA）、财务经理协会（FEI）、美国会计学会（AAA）、管理会计学会（IMA）等多个专业团体组成。

1992年，COSO发布《内部控制—整合框架》[①]，在COSO（1992）框架中，内部控制被定义为一种程序，由一个实体的董事会、管理层和其他员工来实现，并且是为了提供实现下列目标的合理保证而设计的：

（1）运作的效果和效率。

（2）财务报告可靠性。

（3）适用法律规章的遵循情况。

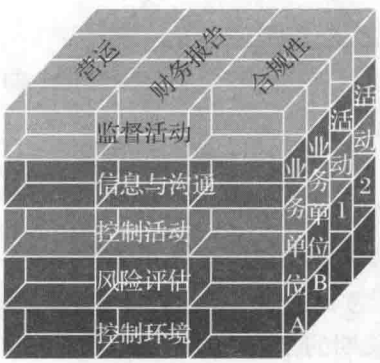


图1-2 COSO内部控制框架

COSO定义了为实现上述目标所需要存在和综合的五个内部控制要素[②]：控制环境、风险评估、控制活动、信息与沟通、监督活动。其中，控制环境是内部控制的基础，五大要素必须同时发挥作用，才能让内部控制有效地运作。

表1-1 COSO五要素主要内容及常见问题举例

COSO五要素	主要内容	常见问题举例
控制环境	控制环境是内部控制的基础 • 员工的诚信和价值观 • 员工的胜任能力 • 董事会和审计委员会 • 管理层的经营理念和经营风格 • 组织机构 • 管理层授权和职责分工 • 人力资源政策和措施	• 缺乏诚信文化、内控文化 • 员工对企业文化缺乏认同 • 高管层蔑视制度、凌驾于制度之上 • 高管层指使、授意员工舞弊 • 员工流动率过大 • 独立董事不懂事 • 组织机构不合理、职责不清 • 非正式的管理程序（潜规则） • 缺乏细化、合理的业绩考核指标

① 2004年，COSO发布全面风险管理框架（ERM），我们将在第6章中介绍。

② COSO—ERM（2004）在此基础上增加企业战略目标和三个要素：控制目标设定、风险事件识别、风险应对。

（续上表）

COSO 五要素	主要内容	常见问题举例
风险评估	评估风险是为了有效控制风险 • 管理层对风险的识别 • 目标实现过程中相关内外部风险分析 • 估计风险的重大程度、可能性 • 随着经济、产业、制度和操作环境的不断变化，需要建立相应机制以发现和处理这些变化所带来的特殊风险	• 对风险缺乏整体性认识和系统性归类 • 没有风险管理的制度 • 没有风险分析、排序 • 缺乏对风险评估方式、方法的了解 • 识别的风险过于理论化，不具有实操性
控制活动	对确认的风险采取必要措施，以保证公司目标得以实现 • 遍布公司各处，涉及公司各个层面以及各项职能 • 按照不同作用，控制活动可分为预防性控制和发现性控制两类 • 控制活动的形式也可以分为责任分离（如业务授权、业务执行、业务记录、检查的职能分离）、实物控制（如定期盘点，对计算机及数据资料的权限控制）、授权等	• 说一套、做一套，制度放空炮 • 缺乏完整细化的“标准运作流程” • 不健全的职责分离 • 关键岗位未定期轮换 • 过度的集权 / 分权体系 • 子公司管理失控 • 控制过程未留痕迹 • 缺乏应急机制、预警机制 • 缺乏有效的成本管理及预算方法
信息与沟通	企业定期获取及交流内外部的信息，帮助员工履行自己的职责 • 信息的识别和获取 • 信息加工和报告 • 内部沟通和外部沟通	• 信息沟通不畅 • 部门之间配合不流畅 • 大部分采用手工控制 • 缺乏反舞弊机制 • 信息系统无序开发，造成资源浪费 • 信息分析、挖掘力度不够
监督活动	监督活动是评估内控系统在一定时期内运行质量的过程，目的是保证内部控制持续有效 • 其范围和频率取决于风险的重大性或现有监控程序实施的有效性 • 监控的方式包括：持续性监控，如复核；独立的评估，如内部审计	• 没有内部审计部门 • 内部审计部门人手不足 • 过于集中在财务领域的内部审计职能 • 监控上缺乏独立性

1.2.2 内控核心原则：COSO（2013）

COSO在2013年5月发布了最新内控框架，其中一个重大变化就是基于原有的COSO五要素提出了17条内控核心原则[①]，增强了五要素的可操作性。

表1-2 COSO（2013）内控核心原则

COSO五要素	内控核心原则
控制环境	• 组织明确承诺将遵从职业操守及道德规范 • 董事会相对于管理层保持独立性并对管理层建立/执行内控情况进行监督 • 在董事会的监督下，管理层建立相应的组织结构、汇报路径、恰当的授权/职责体系，以实现组织目标 • 组织致力于吸引、发展和保留具有职业胜任能力且与组织整体目标匹配的人才 • 组织明确个人的内控职责，以实现组织目标
风险评估	• 组织制定清晰的目标，进而能够有效识别和评价威胁目标实现的风险 • 组织在整个实体层面识别可能威胁组织目标实现的风险，以便判断如何对这些风险进行管理 • 组织在评价威胁组织目标实现的风险时，应考虑潜在的舞弊 • 组织对可能对内控体系产生重大影响的变化事项进行识别与评价
控制活动	• 组织选择并且设置控制活动，以将威胁组织目标实现的风险降低到可接受的水平 • 组织针对技术选择并且设置一般控制活动，以支持组织目标实现 • 组织通过制定政策（以明确控制期望）和具体流程（以将控制期望转换为具体行为）来贯彻控制活动
信息与沟通	• 组织获取或者产生符合使用者需求的、高质量的信息，以支持内控体系发挥功能 • 组织在内部沟通相关信息（包括控制目标、控制职责），以支持内控体系发挥功能 • 组织与外部相关各方沟通可能对内控功能发挥产生影响的事项
监督活动	• 组织选择、设计和执行持续和/或单独的评价，以确认内控各关键要素存在且在持续发挥功能 • 组织对内部控制进行评价，并及时将发现的内控缺陷报给负责执行纠正性措施的主体，这些主体包括高级管理层、董事会，视缺陷具体情况而定

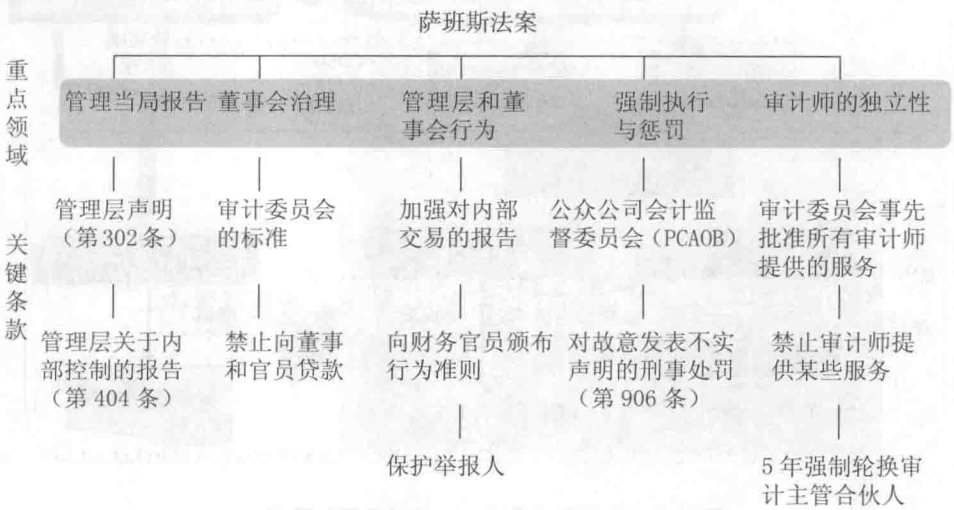
① 参考冯萌．最新2013年COSO框架“17条核心内控原则”：分析与应用．阅洲研究系列，2013（8）。

1.3 SOX 简介

美国于 2002 年发布了著名的《萨班斯·奥克斯利法案》（Sarbanes-Oxley Act，简称 SOX，萨班斯法案）。该法案出台的背景是安然公司、世通公司等系列财务舞弊案严重打击了投资者对美国股市的信心，旨在恢复公众对财务报告的信任。该法案对内部控制进行了总体表述，随后的美国证监会（SEC）以及公众公司会计监督委员会（PCAOB）发布的文件和准则为该法案提供了进一步的实施细则。

SOX 是继《1933 年证券法》和《1934 年证券交易法》以来，美国政府制定的涉及范围最广、处罚措施最严厉、最具影响力的公司法律。SOX 法案要求组织机构使用文档化的财务政策和流程来改善可审计性，并更快地拿出财务报告。该法案要求企业针对产生财务交易的所有流程，必须详加记录到可追查交易源头的地步。

SOX 的重点领域包括五个方面：管理当局报告、董事会治理、管理层和董事会行为、强制执行与惩罚、审计师的独立性（见图 1-3）。其中，以该法案第 302 条“企业对财务报告的责任”、第 404 条“管理层对内部控制的评审”和第 906 条“公司对财务报告的责任”最为关键，影响最为深远。



（第 302 条和第 404 条强调通过内部控制加强公司治理，第 906 条强调刑事处罚）

图 1-3 萨班斯法案的重点领域及关键条款

第 302 条“企业对财务报告的责任”，要求首席财务官或首席执行官签署书面声明，声明以下事项：

（1）签字人已审阅向证监会呈交的报告。

（2）该报告不存在对重要事件的不实描述或遗漏。

（3）确认财务报告和其他财务信息的披露在所有重要方面均公允地反映公司状况。

（4）承担责任，建立、维护和评估内部控制，确保信息披露正确。

（5）已经向外部审计师和审计委员会披露内部控制存在的显著缺陷之处、重大漏洞和重要岗位舞弊。

（6）披露评估日后内部控制的重大变动和改善措施。

第404条“管理层对内部控制的评审”要求：

（1）管理层为公司建立和维持足够的与财务报告相关的内部控制的责任陈述。

（2）管理层为评估公司与财务报告相关的内部控制的有效性而采用的评估架构陈述。

（3）管理层就公司最近财政年度与财务报告相关的内部控制的有效性作出评价。

（4）陈述外部审计师已发出对《管理层就公司最近财政年度与财务报告相关的内部控制的有效性作出的评价》的审计意见。

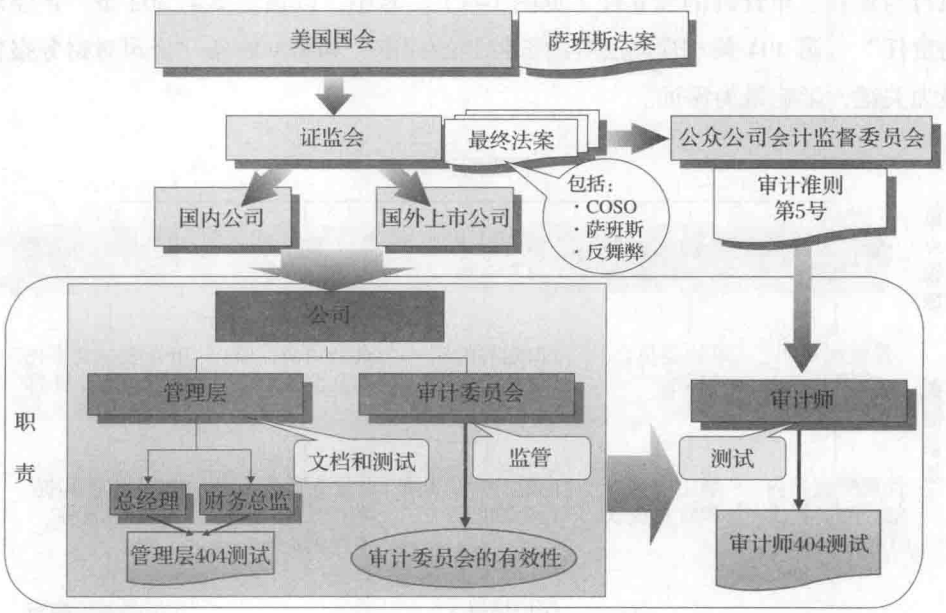


图 1–4　萨班斯法案第404条涉及团体及责任[①]

第906条“公司对财务报告的责任”指出，将对上市公司高管及白领犯罪予以重罚，高达500万美元的罚款及可能被处以10年或20年监禁的重刑。

① 资料来源：PWC。

1.4 C-SOX 简介

我国内控法规建设始于 2001 年 6 月，财政部发布《内部会计控制——基本规范（试行）》和《内部会计控制规范——货币资金（试行）》，明确了单位建立和完善内部会计控制体系的基本框架和要求，以及货币资金内部控制的要求；2002 年年底至 2004 年，财政部陆续发布了《内部会计控制规范——采购与付款（试行）》、《内部会计控制规范——销售与收款（试行）》、《内部会计控制规范——工程项目（试行）》，以及有关担保、成本费用、实物资产、对外投资等方面的征求意见稿。可以看出，那时的内控规范侧重于内部会计控制。2006 年 7 月，财政部成立企业内部控制标准委员会，为建立健全内控体系提供政策指导和咨询服务。2007 年，财政部发布《企业内部控制规范——基本规范》和 17 项具体规范（征求意见稿），上海和深圳证券交易所也先后发布《上市公司内部控制指引》。

2008 年，财政部等五部委发布《企业内部控制基本规范》，这时的内控规范已经不再局限于会计控制，而是拓展到了企业管理的全过程。《企业内部控制基本规范》的发布具有划时代的重要意义，被业界称为中国版的 SOX（简称 C-SOX）。

2010 年 4 月，财政部等五部委发布《企业内部控制应用指引》、《企业内部控制评价指引》、《企业内部控制审计指引》三个配套指引。境内外同时上市的公司于 2011 年执行，2012 年实施范围扩大到国有控股主板上市公司。

《企业内部控制应用指引》是企业建设内控的参照，《企业内部控制评价指引》是企业评价内部控制有效性的参照，《企业内部控制审计指引》是注册会计师实施内控审计的执业标准。

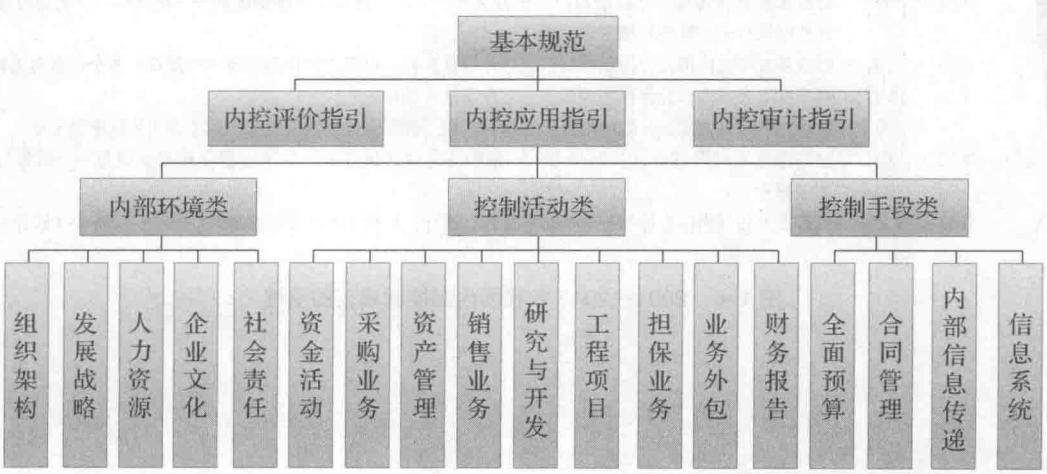


图 1-5 我国内部控制规范框架