


咨询顾问说 内控



田伟著

中国财经出版传媒集团

 中国财政经济出版社

咨询顾问说内控

田 伟 著

中国财经出版传媒集团
中国财政经济出版社

图书在版编目 (CIP) 数据

咨询顾问说内控/田伟著. —北京: 中国财政经济出版社, 2016. 10
ISBN 978 - 7 - 5095 - 6942 - 9

I. ①咨… II. ①田… III. ①企业内部管理 - 研究 - 中国
IV. ①F279.23

中国版本图书馆 CIP 数据核字 (2016) 第 207837 号

责任编辑: 卢关平
封面设计: 孙丽铭

责任校对: 刘靖
版式设计: 董生平

中国财政经济出版社 出版

URL: <http://www.cfeph.cn>

E-mail: cfeph@cfeph.cn

(版权所有 翻印必究)

社址: 北京市海淀区阜成路甲 28 号, 邮政编码: 100142

营销中心电话: 88190406 北京财经书店电话: 64033436 84041336

北京财经印刷厂印刷 各地新华书店经销

787 × 960 毫米 16 开 14.75 印张 237 000 字

2016 年 11 月第 1 版 2016 年 11 月北京第 1 次印刷

定价: 30.00 元

ISBN 978 - 7 - 5095 - 6942 - 9 / F · 5564

(图书出现印装问题, 本社负责调换)

本社质量投诉电话: 010 - 88190744

打击盗版举报电话: 010 - 88190492, QQ: 634579818

序 言

天职国际以审计业务为基础，发展到现如今已然成为国内领先的综合咨询机构，能够实现这种跨越的关键就在于天职国际不断对新业务的开拓和对人才的包容性发展。今天这本《咨询顾问说内控》的推出，也是天职国际这种发展模式的一种成果体现。

天职国际从2006年开始成立了专门的管理咨询部门，成立之初便有幸承接了中石油、中国移动等这样的中央企业的内控服务项目，而随着2008年的企业内控基本规范，以及稍后相关配套指引的推出，中国的很多企业都开始开展内控体系建设。但这一过程却也并非一帆风顺，回头看看，没有什么企业的内部管理提升行为会有如此多的企业聘请咨询机构来协助完成的，其个中缘由则主要是因为虽然有了一些外部规范文件，但是对于大多数从未接触过内控的企业来讲，如何将一些指导性的规范文件落实到企业的业务实际中去，这其中还是存在着不少的困难。而咨询顾问在这一轮企业内控建设中就主动承担起了实现理论与实践衔接的桥梁作用，天职国际的咨询业务也因此获得了快速的发展。也正是在这种项目历练中，天职国际也在不断地进行总结和研究，以求能够更好地解决企业所面临的内控问题，也因此培养了一支熟知内控理论和企业实践的独立咨询团队，这也算是天职国际对人才包容性发展的直接体现。

《咨询顾问说内控》从一名管理咨询顾问的视角对当前的企业内控理论与实践进行了全方位的分析解读，可以算是天职

国际集体智慧的结晶。通读书稿会发现：这是一本从咨询顾问视角对内控进行360度解读的咨询操作教材，不仅视角独特，而且就所分析的内容来看不仅包括了通常所谈及的一些内控基本内容，而且还谈及了几组常见的内控相关关系这样企业经常会碰到的疑惑，而即便是内控的内容也并不是完全的照搬，而是体现了作者的独特视角及其观点。

这是一本最接地气的企业内控人员的工作指南，这本书的目标读者群体可以明显地体现出是企业内控相关岗位和内控咨询顾问这两个群体，几乎完整解答了天职国际在给客户提供服务过程中客户的所有重要疑问，企业内控相关岗位完全可以把本书作为内控工作操作指南。

这是一本源于内控咨询项目实践但又不是案例汇编的案例库，之所以如此说是因为书稿中并未完整地去分析某一个案例，甚至都没有刻意地去揭示读者哪些是案例，但是通读书稿后就会发现书中的所有内容却又都是来源于一个个活生生的案例的，很多的问题就是企业当前所正遇到的问题，而作者都从自己的案例中总结出了答案。

这是一本体现咨询顾问项目实践过程中思考方式与结论的总结，本书不仅服务于企业内控相关岗位，而且对于目前正在从事内控咨询工作，或者有志于从事内控咨询工作的新人都有很好的帮助。透过本书，可以更为清晰地了解咨询顾问这一特殊的角色对内控的思考方式及其结论，对咨询顾问的工作有着很强的现实意义。

这是一本饱含咨询顾问社会责任担当和内控实践人情怀的抒情之作，本书不仅单独用了第八章来表达咨询顾问的这种情怀，而且全书中透露着一名咨询顾问对于企业内控建设、评价及其运行的深度思考。如果不是发自内心的这种服务意识和社会担当，是不可能总结出这样的一些观点和工作建议的。

相信本书的出版将有助于推动企业内控体系的建设和完善，

为企业内控相关岗位和内控咨询顾问的工作带来便利，并将推动中国内控理论的进一步发展。

天职国际会计师事务所（特殊普通合伙）

总 经 理

谭 宪 才

目 录

第一章	内控在中国的十年	(1)
	章节导读	(1)
	第一节 第一阶段：满足境外上市披露要求	(1)
	第二节 第二阶段：内控手册正当时	(8)
	第三节 第三阶段：向内控要效益	(11)
第二章	有关内控的几组关系	(19)
	章节导读	(19)
	第一节 内控与现有管理体系	(19)
	第二节 内控与制度	(26)
	第三节 内控与内控手册	(30)
	第四节 内控体系与管理层级	(39)
	第五节 内控与风险管理	(45)
第三章	内控责任体系	(49)
	章节导读	(49)
	第一节 内控职责经典表述	(49)
	第二节 有关内控职责体系的调查	(54)
	第三节 内控部的应有职责	(55)
	第四节 审计部的角色	(62)
	第五节 业务部门的内控责任	(69)

第六节 内控体系中的领导角色	(73)
----------------------	--------

第四章 内控建设一般思路

章节导读	(77)
第一节 总体思路——内控三要素	(78)
第二节 目标辨识	(80)
第三节 风险识别	(88)
第四节 控制活动设计	(100)
第五节 成果汇编	(106)
第六节 RAARCC 内控执行体系	(109)

第五章 控制活动要素

章节导读	(114)
第一节 控制措施的概念说明	(115)
第二节 控制措施的要素	(122)
第三节 控制措施的一般方法	(130)
第四节 控制措施与流程	(141)

第六章 其他四大内控要素

章节导读	(145)
第一节 内控五要素的尴尬	(145)
第二节 其他四大内控要素内容	(153)
第三节 探索内控五要素的融合	(168)

第七章 内控评价过程与要点

章节导读	(172)
第一节 内控评价的外部要求	(172)
第二节 内控测试的一般方法	(179)
第三节 内控缺陷评价	(187)

第四节	内控测试底稿与报告	(192)
第八章	合格内控咨询顾问	(197)
章节导读	(197)
第一节	咨询顾问的困难	(198)
第二节	知识与技能	(207)
第九章	内控发展的一般见解	(212)
章节导读	(212)
第一节	专业化内控更具有生命力	(212)
第二节	价值内控的含义	(217)
第三节	量化内控实施效果	(220)
第四节	内控 3.0 时代展望	(223)

第一章

内控在中国的十年

章节导读

虽然内控这一概念目前在企业已经变得耳熟能详了，但是只要稍微回头看看就会发现，如果不做学究派的追根溯源式研究，现代内控观念在中国真正的发展充其量也就十余年而已。

了解过去十年间内控在中国的基本形成与发展过程对理解内控大有裨益。笔者认为，作为舶来品的内控在中国过去的十年中主要经历了三个发展阶段：第一阶段是部分在境外上市的企业为了满足上市地的披露要求，首先开始接触内控并将内控这一框架正式引入中国；第二阶段是国家层面开始重视内控，并在上市公司大力推行内控体系，这一阶段最为显著的特征就是内控手册大行其道；第三阶段是更多的企业从提升自身管理水平的目的出发开始重视内控，这个时候的内控已经不完全是为了满足监管要求，而更希望通过内控提高内部管理的效率和效果，目前已经有少部分企业开始了这一阶段的内控。本章将按照这三个阶段的发展顺序介绍每一阶段的基本情况。

第一节 第一阶段：满足境外上市披露要求

所谓满足境外上市企业披露要求，可能首先需要弄清楚的一个问题就

是境外企业的披露要求究竟是什么。其实，中国有许多企业在境外上市的，美国、中国香港可能是听起来最多的地方，但除此之外，还有新加坡、英国等地也有中国企业上市。因此，通常所讲的境外上市企业披露要求实际上是一个泛称，并不能直接表示是哪一项具体要求，而要说清楚具体要求，则必须明确到具体的上市地。在所有不同的上市地中，美国是第一个对内控披露提出实质性要求的国家，同时从法理层级上看其要求也是最高的，起始时间也是最早的国家。因此，如果不做内控发展历程的专题研究，那么，清楚美国的要求对于理解基础性的内控发展脉络已经足够了。

一、SOX 法案及其要求

在美国上市的中国企业需要满足的直接法规要求就是 SOX 法案，该法案全称是《萨班斯—奥克斯利法案 2012》（Sarbanes-Oxley Act of 2012）。该法案在 2012 年 7 月 30 日由小布什总统公开签字颁布而成为美国的正式法律。SOX 法案所包括的内容非常广泛，被称为是继美国 1934 年《证券法》之后的最为重要的一部法律，或者说是《证券法》的重要补充，其内容包括创建美国上市公司会计监督委员会（Public Company Accounting Oversight Board, PCAOB）、审计师的独立性要求、公司的责任、财务信息披露以及公司舞弊的刑事责任、白领刑事责任、公司欺诈责任等众多章节和条款，对在美国上市的所有上市公司的信息披露质量与责任进行了系统性的规范要求。但是，通常与内控联系起来的核心条款则主要是 302 和 404 两大条款，这两大条款的内容分别是：

302 条：公司对财务报告的责任

➔ 在本法案生效后 30 天内，证券交易委员会应当要求所有上市公司按 1934 年《证券法》13（a）段和 15（d）段呈报定期报告，主要执行官（们）、首席财务官（们），或履行相似职务的人员，在依上述法案各段的要求呈报的每一份年度或季度报告时应证实：

➔ 签字的官员已经复核了该报告；

➔ 据该官员所知，报告中不存在对重要事项的任何不真实陈述，或遗漏了对必要的重要事项的陈述，从而保证该陈述不会误导读者；

➔ 据该官员所知，报告中包括的财务报表和其他财务信息，在所有重要方面公允地反映了上市公司在报告期内的财务状况和经营成果；

➔ 签署的官员：（A）负责建立和维护内部控制；（B）设计了这些内

部控制，以保证这些官员了解了与上市公司及其合并报告的下属机构有关的重要信息，尤其是那些在定期报告期内的信息；(C) 在报告发布前 90 天内评价了上市公司的内部控制系统的有效性；(D) 在报告中陈述了对上市公司内部控制系统的有效性的评价结论；

➔ 签署官员们向上市公司审计师和董事会的审计委员会（或履行相同职能的人员）披露了：(A) 内部控制的设计和运作中的所有重大缺陷，这些缺陷可能影响上市公司记录、处理、总结和报告财务数据的能力，并且已经为审计师指明了所有重要的内部控制弱点；(B) 涉及上市公司管理层或其他在内部控制系统中具有重大作用的人员的任何欺诈行为，无论该欺诈行为严重与否；

➔ 签署官员们已在报告中指明，在内部控制评估结束之后，内部控制系统或其他对内部控制具有重大影响的因素是否发生了重大变化，包括对重大缺陷或重要弱点进行的任何改正。

404 条：管理层对内部控制的评价

➔ 要求证券交易委员会制订规则，规定按照 1934 年《证券法》第 13 (a) 或 15 (d) 段的规定呈报的每一份年度报告，必须包括一份内部控制报告，它应当：(1) 写明公司管理层建立和维护一套充分的内部控制结构和程序的责任；(2) 包括一份上市公司最近财政年度末的，对财务报告的内部控制结构和程序的有效性的评价。

➔ 关于本段要求的对内部控制的评价，每一个为上市公司编制和发表审计报告的备案登记的注册会计师事务所，应当对管理层提供的评价，进行审核和报告。该审核应当依据监管委员会颁布或采用的审核业务标准。这种审核不应当作为一项割裂的业务。

上述法案生效后，要求市值超过 7500 万美元的美国公司自 2014 年 11 月 15 日及之后各财政年度均需要披露管理层报告，即通常说的内控自评报告；审计师也需要在同一时间开始披露鉴证报告。但是对于在美国上市非美国的公众公司则做出了特别安排，几经推迟，最后要求市值超过 7500 万美元的非美国上市公司自 2006 年 7 月 15 日及之后的各财政年度开始披露管理层报告和审计师鉴证报告，也就是对非美国公司提供了一个缓冲期。而对于中国公司而言，真正被要求披露内控评价报告的时间节点就是 2006 年 7 月 15 日。除了时间之外，无论是美国公司，还是非美国公司在披露的内容要求上则是完全一样的。

也正是在这一时间，部分在美国上市的中国公司，如在美国纽约证券

交易所上市的中国人寿、东方航空、中国石化、中国石油、中国联通、中国电信等企业，第一次被要求披露内控评价报告。为了满足这一披露要求，这部分企业，以及另外一部分美国公众公司在中国的分支结构开始系统性地建设内控体系的建设与评价工作，这也意味着内控开始以体系的形式被引入到中国。这也是为什么可以说内控到中国真正的发展只有十年的原因。

二、SOX 法案与 COSO 内控框架

大致了解 SOX 法案之后可能第二个需要重点了解的就是 COSO 委员会的内控框架了。现如今凡是提及内控的无不提到 COSO 内控框架，甚至对大多数人来讲，COSO 的内控框架比 SOX 法案更熟悉。那么为什么这一内控框架如此盛行呢，它又是如何与 SOX 法案牵扯到一起的呢？

首先说说 COSO 委员会，而要说 COSO 委员会，首先必须了解美国全国反虚假财务报告委员会，这个委员会由美国注册会计师协会、美国会计协会、财务经理人协会、内部审计师协会、管理会计师协会联合于 1985 年创建，旨在探讨财务报告中的舞弊产生的原因，并寻找解决之道。1987 年，该委员会成立了一个下属机构委员会，即我们常说的 COSO 委员会，按照中国的一般层级概念，COSO 委员会相当于美国全国反虚假财务报告委员会的一个专业委员会，这一专业委员会的专注领域就是内部控制。COSO 委员会在 1992 年发表了第一份正式的研究成果叫做《内部控制——整体框架》（Internal Control-Integrated Framework）的报告，在这一报告中第一次明确提出了内控的三大目标、五大要素等内容。这一报告中所提出的这些基本内容也就构成了所谓的 92 版 COSO 内控框架了。

那么 COSO 的这一框架是如何成为一个公认的标准了呢，这就要感谢我们前面提及的 SOX 法案了，正如前文所说，SOX 法案要求美国公众公司披露内控有关的报告。但是 SOX 法案中仅规定了应该披露的内容和程序，对于报告应该写成什么样子，这些内容以一种什么样的形式披露出来，SOX 法案并没有对这些细节问题进行规定。于是，2003 年 6 月 5 日，美国证券交易委员会（Securities and Exchange Commission, SEC）为了贯彻落实 SOX 法案中 302 和 404 条款的披露要求，编写了一套有关内控披露的最终规则，在这一最终规则中 SEC 明确认为 COSO 委员会提出的内部控制框架可以作为企业内部控制体系建立的标准，从而正式确立了 COSO 内控框架的官方地位。此外，美国上市公司会计监管委员会（PCAOB）在 2004 年 3 月 9 日，为了贯彻落实 SOX 法案的要求，也相应发布了

第二号审计准则，即内部控制审计准则（AS2），在这一准则中也明确审计师在对公众公司进行内部控制审计时也可以采用 COSO 内控框架作为审计的标准，并在 2007 年的第五号（AS5）中再一次确认了这一标准，由此从理论基础、政府监管机构到行业规范，均认可了 COSO 的内控框架，这也就进一步稳固了 COSO 内控框架在内控领域的地位，也使得 SOX 法案与 COSO 内控框架产生了天然的联系。

简单归纳一下就是，一个非营利组织，即 COSO 委员会，基于自身的行业研究发布了内控框架，这一框架本身仅代表 COSO 委员会的研究成果。但是在其发布 10 年之后，随着 SOX 法案的出台，要求上市公司开始披露内控信息，而为了贯彻这一法案的要求，SEC 和 PCAOB 从政府角度和行业角度都推崇采用 COSO 的这一框架作为内控建设、审计与披露的一般框架，从而正式将 SOX 法案与 COSO 内控框架结合到了一起。就好比在中国，财政部等部委发布了《企业内部控制基本规范》，而中国证监会则发布了内控评价报告的披露格式、中注协则发布了内控审计指南等。多方力量一起最终确立了 COSO 内控框架的历史地位。

需要补充一点的是，COSO 委员会继 1992 年发布《内部控制——整体框架》（以下简称 92 版内控框架），又在 2004 年发布了《全面风险管理——整合框架》，并在 2016 年发布了升级版。2013 年 COSO 委员会对 92 版内控框架进行了修订之后发布了 2013 版《内部控制——整体框架》。但这丝毫不能动摇 92 版内控框架的历史地位，而且就目前大多数企业来讲仍然采用的是 92 版内控框架。

根据新规定，所有在美上市的上市公司均需要从 2014 年底开始执行 2013 版内控框架，原版框架也将随之废止，但这与不在美国上市的企业来讲是一点关系都没有的。按照 COSO 主席 Robert Hirth 先生的说明，新框架涉及 7 项较大改变，分别是：明确列示了用以支持内部控制五大要素的原则、明确了目标设定在内部控制中的作用、反映了科技发展对企业内控的影响、更深入地讨论了有关治理的理念、扩大了报告目标类别、加强了对舞弊预期的考虑、更加关注非财务目标。但并未改变内控的基本框架。其列示了支持内部控制五大要求的原则，具体而言总共分为 17 条具体原则，这些原则分别是：

➡ 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；

➔ 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，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；

➔ 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；

➔ 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；

➔ 组织选择、设计和执行持续和单独的评价，以确认内控各关键要素存在且在持续发挥功；

➔ 组织对内部控制进行评价，并及时的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，具体视缺陷具体情况而定。

这些原则就可以作为企业开展内控建设的直接依据，也可以作为企业开展内控评价和外部审计师审计时的参考依据。换句话说，内控评价也好，内控审计也罢，如果都能完全满足上述 17 条原则的核心精神，那么就可以有足够的信心相信公司的内控是有效的。

三、COSO 内控框架来到中国

虽然说内控必然会讲 COSO 内控框架，但是对于在国内上市的公司以

及对于绝大多数还没有上市的中国企业来讲，COSO 内控框架依然可能是离我们比较遥远的概念，充其量只能算作是一种理论渊源。大部分接触到的内控，准确地说是中国版的内控，已经不叫 COSO 内控框架了，而叫做内控基本规范了，即《企业内部控制基本规范》，这是 COSO 内控框架中国化后的内控框架版本。

就在在美国上市的中国企业即将被要求披露内控评价报告的 2006 年，经国务院批准，由财政部牵头发起，证监会、国资委共同参与于 2006 年 7 月 15 日在北京正式成立“企业内部控制标准委员会”，这算是中国官方在总体层面开始探索内控框架的起点。在借鉴 COSO 框架的基础上，两年之后的 2008 年 5 月 22 日财政部、证监会、审计署、银监会、保监会联合发布《企业内部控制基本规范》，并在发文通知中要求自 2009 年 7 月 1 日起在上市公司范围内施行，鼓励非上市的大中型企业执行。执行该规范的上市公司，应当对公司内部控制的有效性进行自我评价，披露年度自我评价报告，并可聘请具有证券、期货业务资格的会计师事务所对内部控制的有效性进行审计。至此，中国版内控框架算是正式落地，COSO 内控框架也算是正式来到了中国，实现了这一舶来品的第一次正式靠岸，由此《企业内部控制基本规范》也经常性地被称之为中国版的 SOX 法案，可见内控这一概念舶来品之意味的浓烈。

为方便理解，这里还是需要对《企业内部控制基本规范》的内容进行一点简单介绍。基本规范共七章五十条，按照 COSO 内控基本框架中的五大内控要素依次划分为内部环境、风险评估、控制活动、信息与沟通、内部监督五大核心章节，外加第一章总则和第七章附则构成。这一规范虽然在很大程度上借鉴了 COSO 框架，但也还算有些小修小补，在一定程度上多少体现了一点中国特色，如基本规范第三条给出了内部控制的正式版定义为：“本规范所称内部控制，是由企业董事会、证监会、经理层和全体员工实施的、旨在实现控制目标的过程。内部控制的目标是合理保证企业经营管理合法合规、资产安全、财务报告及相关信息真实完整，提高经营效率和效果，促进企业实现发展战略。”相比较于 COSO 中的定义，这一定义中就增加了“资产安全、促进企业实现发展战略”这两个目标。黄京菁博士就对基本规范进行了总结，认为该规范：“开创性地建立了以企业为主体、以政府监管为促进、以中介机构审计为重要组成部分的内部控制实施机制。”但是对于不做专题研究的人来讲这都不重要了，重要的是我们了解到了《企业内部控制基本规

范》的发布时间、总体要求。由于基本规范的中条款仍然是比较宽泛的，对实际的企业内控建设工作的指导意义依然还是有限的，所以对于大部分人而言，重要的不是去一条条记住基本规范的内容，而更重要的是要认真理解基本规范中各条款规定所要表达的实质性含义，要切实理解这些含义也只能把这些条款放到具体的企业内控建设中去才可能理解到位。因此，本书就不在此赘述具体的条款了，本书之后的具体内容实际上需要完成的工作就是通过最为通俗的语言，跳出基本规范的条条来告诉读者一个最为贴近企业实际需求的内控。

第二节 第二阶段：内控手册正当时

随着 2008 年财政部等五部委《企业内部控制基本规范》的发布，内控正式来到了中国并取得了一个官方身份。按照基本规范执行的时间点要求，尤其是上市公司开始了大规模的内控体系建设工作。如果一定要给这一阶段划定一个时间段的话，笔者认为应该是 2009 年到 2013 年的五年，之所以如此划分，是因为 2009 年 7 月 1 日，是《企业内部控制基本规范》的发布通知中明确的上市公司正式开始实施的时间点，而 2013 年，是财政部和中国证券监督管理委员会联合发布的《关于 2012 年主板上市公司分类分批实施企业内部控制规范体系的通知》（财办会〔2012〕30 号）中明确的主板上市公司实施基本规范的最后时间。这一时期最大的特征就是内控手册大行其道。因此，本节我们将重点说说内控手册。

一、也说内控手册

要说清楚内控手册，首先需要说清楚内控手册是什么，是否必需、它包含哪些内容等基础性问题。

内控手册是什么？笔者查了不少资料也没找到内控手册的定义，但是最终还是在百度上找到了一个不知名的定义，贴出来共赏：“内控手册是从内部控制的角度按通行的内控框架记录企业关键内部控制活动的一种体系文件。”而之所以贴出来是个人认为这个定义应该还算是比较贴近现实的，权且当作内控手册的定义吧。但实际上纠结于定义并无多大意义，真正重要的是我们需要知道内控手册的具体内容说得通俗一点，无非就是将