内控体系建设100问
基于合规，超越合规
2013年COSO新框架介绍

《企业内部控制基本规范》合规实务指南

（第2版）

梁晟耀　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

《企业内部控制基本规范》合规实务指南

（第2版）

梁晟耀　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

图书在版编目（CIP）数据

《企业内部控制基本规范》合规实务指南 / 梁晟耀编著. —2 版. —北京：电子工业出版社，2013.7

ISBN 978-7-121-20600-9

Ⅰ. ①企… Ⅱ. ①梁… Ⅲ. ①企业管理－内部审计－规范－基本知识－中国 Ⅳ. ①F239.45-65

中国版本图书馆 CIP 数据核字(2013)第 120162 号

责任编辑：杨洪军
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：720×1000　1/16　印张：21.75　字数：279 千字
印　　次：2013 年 7 月第 1 次印刷
定　　价：56.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前言

一个注定不平静、不平凡的年代……

全球经济形势、政治环境、宏观政策、货币投放、市场、出口、投资、消费……无疑都是重要的话题。其中，某些因素在特定时点可能发挥决定性的作用。

早在农耕时代，气候变化对收成恐怕有着更重要的影响。那么，当时一个勤勉的耕作者，是否应以观测天气作为最重要的工作呢？

作为企业，对于经营环境变化的预知能力，未必就高于一个古代农夫对天气的预测。回到田间、聚焦沃野，才是更务实的选择。

任正非说，我们对未来的无知是无法解决的问题，我们只能用规则的确定来对付结果的不确定，矢志不渝地推动组织朝向长期价值贡献的方向去改革。一个企业的竞争力，不是预报天气的“先知先觉”，而是应对天气的实力。

2002 年 7 月，美国通过萨班斯法案（SOX），2006 年 6 月，国资委印发《中央企业全面风险管理指引》，2008 年 6 月，财政部等五部委颁布中国版萨班斯——《企业内部控制基本规范》，2012 年 5 月，国资委发布《关

于加快构建中央企业内部控制体系有关事项的通知》，11 月，财政部发布《行政事业单位内部控制规范（试行）》，无论是公司治理还是政府治理，无一例外都做出同样的选择——内部控制——这就是我们的方向。

韩寒在其《独唱团》创刊号上说："无论现实如何，我们总是要怀有理想的。写作者最快乐的事情就是让作品不像现实那样到处遗憾，阅读者最快乐的事情就是用眼睛摸一摸自己的理想。"本人深以为然。

正是抱着致力于推动内部控制在中国发展的理想，2006 年本人创建了国内唯一专注于内部控制与风险管理的网站 Cosox（www.cosox.cn）。借助这个平台，结识了许多业内同行。通过与他们的交流与学习，汲取了很多营养，结合本人多年来的实务操作经验，加深了对中国企业内部控制的理解和认识。

七年来，Cosox 不停为你加油：让无力者有力，让悲观者前行，让往前走的继续走，让幸福的人儿更幸福！在大家的共同努力下，Cosox 目前已成长为业内内容最丰富、专业人士最集中、交流最活跃的学习分享平台。这也是写作本书的一个动力。

光阴荏苒，本书第 1 版出版至今，三年已经过去了。一切都在改变，不变的是我们的理想：积极推动内部控制与风险管理在中国落地、生根、成长……

本书的出版及修订，得到了很多人的支持。非常感谢李静、杨洪军两位编辑的辛勤努力，特别感谢江湖号称"财务杀手"的郑朝晖和王大力两位前辈，腾讯集团内审总经理陶蕾，于百忙之中为本书作序，使本书增色不少。路漫漫其修远兮，吾将奋力而求索。

谨以此书献给我的母亲粟连玉！

梁晟耀

2013 年 6 月

推荐序一

手中无剑，心中亦无剑

认识梁晟耀先生至今已有7年，交往越久，越敬佩他在风险管理和内部控制方面独到的见解、务实的作风、执著的态度和不懈的努力，他是国内同行中难得的良师益友。

三年前看过第1版的《〈企业内部控制基本规范〉合规实务指南》，我曾笑谈：你有不少保留；很荣幸看到再版，我相信推荐富有意义。

首先，企业的风险管理和内部控制的发展离不开现代企业管理意识和水平的提升，而目前国内企业现代管理所处阶段，决定了国内企业风险管理和内部控制的发展水平，比如理解参差不齐、运用千差万别，即使借鉴类似的理论和方法，也出现实施效果的失之千里。2008年中国的《企业内部控制基本规范》已出台，但市面上鲜见对理论有深刻论述、对实践有参考意义、术道兼明的资料供大家学习和参考，而这本书既从实务的角度给予了全面介绍，又丰富了不少鲜活的实例佐证供大家思考，相信能给读者不同维度的启发。

其次，在过往与不同的企业从事风险管理和内部控制的人交往中，经

常能感受到理解企业独特的自身特点、掌握企业发展的真实规律是做好这项工作的基石，但达到这样的程度却不容易，往往不是一个规范能解决的，同时，我们越来越能体会到只有更合适企业的具体实践，却没有所谓最好的企业风险管理和内部控制模式。因此在实践中借鉴和运用这本书所提到的内容时，需要我们求实的精神和不凡的智慧，而本书于此提供不少的精神食粮。

最后，我相信无论风险管理还是内部控制，扎根业务，服务企业，才不会失去她蓬勃生长和开花结果的土壤与环境；拿捏平衡，因地制宜，才不会丧失她妩媚动人和婀娜多姿的魅力和风采。越来越多的同行都认同在实践中加强风控建设的同时，考虑到更为广泛的因素，风控并非目的，不会为风控而风控，基业长青的路上既要走得快又要走得远还要健康地走。这本书所提到的内容给予读者的仅仅是参考和借鉴，不是终结而是开始。

感谢晟耀创作的一次知识饕餮！这是手中无剑、心中亦无剑的开始。

陶　蕾

2013年6月

推荐序二

公司基业长青的内部控制指南

前段时间，曾与一位投资银行的朋友探讨尽职调查，其言工作中曾涉及一些内部控制的相关内容，由于专业知识等方面的局限，往往流于形式而仅能实现“纸上合规”。恰巧此时，有幸拜读梁晟耀先生所编著的《〈企业内部控制基本规范〉合规实务指南》书稿。该书不仅可解朋友之惑，也使自己受益匪浅。

之于内部控制，往往存在以下两种有些对立的认知。

一是认为内部控制只是会计分工、内部牵制等方面内容，属公司财务部门的自娱自乐，或者是财务部门与其他部门的协调配合。其实，目前内部控制理论与实践已得到极大发展，已经历五个阶段，从初级的“内部牵制”发展至第五阶段的“企业风险管理整合框架”。

尽管更侧重于实务层面，但梁晟耀先生也在书中对内部控制理论进行了梳理概括，在介绍美国内部控制理论和实践发展的基础上，重点讨论了我国的情况。

没有理论指导的实践是盲目的。书中讲述的内部控制理论可谓恰到好

处，能够使读者茅塞顿开，进而从更宏观的层面了解和理解内部控制的发展历程与概念内核，以便更精准地指导实践。

二是言及内部控制则肃然起敬，复杂理论与烦琐规则不绝于口，置人于云雾之中。其实，内部控制并非深不可测，它只是人们在经营管理实践中的一种科学总结，也可以从几个要素来把握，如控制环境、风险评估、控制活动、信息与沟通及监控。

真知往往存在于实践之中。内部控制实务则是梁晟耀先生这本书的重头戏，也是能够答疑解惑的关键所在。甚至，更见体贴入微之处的是，在内部控制与全面风险管理体系建设方案的探讨里，提出了一些技巧性的具体做法。

例如，在《企业内部控制基本规范》合规的头一年，建议采用项目管理办公室的办法，在董事会及审计委员会的领导下，由公司高层担任“内部控制建设项目”负责人，在其领导下成立“内部控制建设项目指导委员会”，全面负责协调整个项目的顺利实施；又如，对于大型企业，下属公司繁多，可以采取先试点、后推广的方法。

其实，梁晟耀先生对书稿内容的定位是煞费苦心的。内部控制往往涉及方面众多，而基本规范则是最基础的，纲举目张，只有基础打牢了，才能成就内部控制的屹立百年的高楼大厦。同时，由于目前我国企业规模与发展阶段的局限，经营管理往往缺乏主动性。这样，以合规这一基础性要求为第一要务，不仅能够使企业更快地切入内部控制建设上来，也有可能在实践过程中逐渐认识内部控制的重要性，进而上升到更高层次的主动性管理。

企业内部控制做不好就不能基业长青。这不仅仅局限于中大型公司或上市公司，众多民营中小企业也同样如此。企业在内部控制构建中，需把

握其核心理念——风险管理。大公司面临风险，中小企业更面临风险。风险管理的理念贯彻于本书中，与此相应，书中将风险评估作为单独一章来专门阐释，足见其充分的内在逻辑。

如果说内部控制体系建设工作应贯彻于企业始终的话，那么对内部控制理论与实践的思考也将成为梁晟耀先生一生的追求。期待梁晟耀先生未来能有更多的如本书般有价值的优秀作品，也期待能有更多鲜活生动的案例与广大读者分享。

拙以为，梁晟耀先生书中所探讨的，不仅仅利于广大企业进行内部控制制度建设实践，也是上市公司合规经营的指导手册，更值得证券界、审计界及学界等各方面借鉴。喜读之余，乐于推荐。

王大力

郑朝晖

2010 年 4 月

目 录

第 1 章 《企业内部控制基本规范》解读 …… 1

1.1 美国内部控制理论和实践的发展 ……2

1.2 中国内部控制理论和实践的发展 ……7

1.3 内部控制的规定及相关人员的责任 ……20

第 2 章 风险评估 …… 28

2.1 风险概述 ……29

2.2 风险评估的一般程序 ……37

第 3 章 合规范围 …… 55

3.1 自上而下基于风险的方法 ……57

3.2 范围界定的步骤 ……60

第 4 章 内部控制体系建设 …… 78

4.1 内部控制体系建设概述 ……79

4.2 公司层面内部控制建设 ……91

4.3 IT 一般控制建设 ……136

4.4 业务层面内部控制建设 ……178

4.5 IT 应用控制建设 ……200

第 5 章 内部控制执行与维护 …… 211

5.1 内部控制执行 ……212

5.2 内部控制维护 ……221

第 6 章 内部控制评价 ……225

6.1 内部控制测试 ……227

6.2 缺陷评估 ……247

6.3 评价报告 ……261

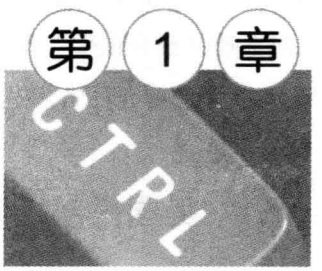
附录 A COSO 新框架（COSO—IC/2013）17 项总体原则简要说明 ……277

附录 B 内控体系建设 100 问 ……283

附录 C 香港《企业管治常规守则》摘录 ……331

附录 D 美国萨班斯法案（SOX）摘录 ……334

参考文献 ……338



《企业内部控制基本规范》解读

现代意义上的企业内部控制[①]是在长期的经营活动过程中，随着企业对内加强管理和对外满足社会需要，逐渐产生并发展起来的自我检查、自我调整和自我约束的系统，其中凝聚着诸多的经济思想、管理理论和实践经验。伴随内部控制实践的逐渐丰富，内部控制理论的发展也经历了一个漫长的过程，先后出现了“内部牵制”、“内部控制制度”、“内部控制结构”、“内部控制整合框架”和“企业风险管理整合框架”五个阶段。内部控制理论与实践起源于西方发达国家，特别是美国。

1.1 美国内部控制理论和实践的发展

1992年，由美国注册会计师协会（AICPA）、美国会计学会（AAA）、财务经理人协会（FEI）、国际内部审计师协会（IIA）和管理会计师协会（IMA）共同赞助成立的一个专门研究内部控制的问题委员会——COSO委员会（Committee of Sponsoring Organizations of the Treadway Commission，全美反舞弊性财务报告委员会发起组织），发布了指导内部控制实践的纲领性文件COSO研究报告：《内部控制——整合框架》（COSO—IC/1992）。该框架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。在COSO报告中，内部控制被定义为一个受企业员工行为影响，用以完成特定目标的过程。内部控制是一个受到董事会、管理层和其他人员影响的过程，该过程的设计是为了提供实现以下三类目标的合理保证：经营的效果和效率、财务报告的可靠性、法律法规的遵循性。内部控制包括控制环境、风险评估、控制活动、信息与沟通、监控五个相互联系的要素，它们都包含在管理层经营企业的方式中。五项要素相互联系，作为评

① 本书中“内控”和“内部控制”通用。

判内部控制系统是否有效的准则。

2002年，安然、世通公司突然垮台，施乐、默克等美国一系列大型企业相继出现财务丑闻，为整个金融市场敲响了警钟。这些丑闻的出现，不是偶然事件，与其对内部控制的过分疏忽有密切的关系。继这些丑闻曝光后，2002年7月30日，美国紧急出台了著名的《2002年公众公司会计改革和投资者保护法案》，又被称做2002年《萨班斯—奥克斯利法案》（简称《萨班斯法案》，SOX），同时成立了一个新的监管机构——上市公司会计监督委员会（The Public Company Accounting Oversight Board，PCAOB）取代美国注册会计师协会（AICPA）来监管会计职业界。该法案是1930年以来美国证券立法中最具影响的法案，它加重了公司主要管理者的法律责任，加强了对公司高级管理层的收入监管，对公司内部的审计委员会做出了法律规范；与此同时，该法案强化了对公司外部审计的监管，加强了信息披露制度和其他有关公司监管的规定。

《萨班斯法案》的影响已波及整个资本市场，各行各业都受到并将继续受到该法案的影响。该法案中的第404条款管理层对内部控制的评估是最棘手的部分，它要求上市公司及其外部审计师对公司财务报告内部控制的有效性进行报告。

在《萨班斯法案》颁布之后，COSO委员会于2004年9月29日正式发布了《企业风险管理——整合框架》（COSO—ERM/2004），将COSO—IC/1992（见图1-1）纳入其中，企业不仅可以借助其来满足内部控制的需要，而且拓展至与企业风险管理这一更加宽泛的领域。COSO—ERM/2004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标准。

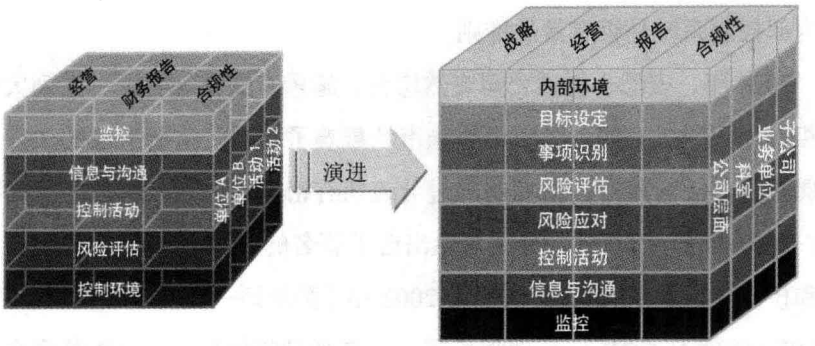


图 1-1　COSO—IC 演进到 COSO—ERM

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、事项识别、风险评估、风险应对、控制活动、信息与沟通、监控。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的运行提供了平台和结构。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。

COSO—IC/1992 到 COSO—ERM/2004，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；目标设定中增加“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“事项识别”、“风险评估”和“风险应对”，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。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，对中国在美国上市公司具有直接影响，对中国市场监管也具有借鉴意义。

自 COSO—IC/1992 发布以来，企业的经营环境和管理模式经历了巨大变化，新技术和复杂组织结构的不断涌现，信息技术、互联网和电子商务迅猛发展，以及愈加严格的监管要求，促使企业在满足旧框架主要针对财务报告内控目标的基础上，越来越关注公司治理和风险管理，越来越重视非财务报告内部控制。近 20 年后，COSO 委员会于 2011 年 12 月 19 日发布新版《内部控制——整合框架》（草案），公开征求社会意见，2013 年 5 月 14 日发布了正式稿（COSO—IC/2013）及其配套指南[②]。

COSO—IC/2013 并没有改变 COSO—IC/1992 中关于内部控制的基本概念和核心内容，比如内部控制的定义、内部控制五要素（控制环境、风险评估、控制活动、信息与沟通、监控活动，见图 1-2）、评估内控体系有效性的标准以及职业判断的运用等保持了一致。

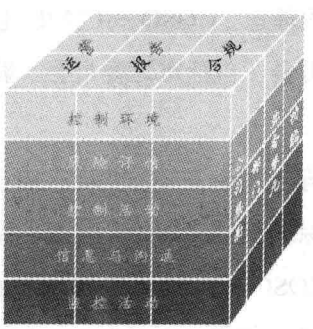


图 1-2　COSO—IC/2013 框架图

② 一份用于评估内控系统有效性的说明性工具（Illustrative Tools），一份外部财务报告内控的方法与案例概要（A Compendium of Approaches and Examples）。

COSO—IC/2013的变化主要表现在以下几个方面：

（1）注重原则（Principles）导向的方法。COSO—IC/2013提炼出内部控制五要素的17项总体原则。五项基本要素和17项总体原则[③]作为内部控制的基本概念，适用于所有的组织。每项原则都由多个关注点（Points of Focus）所支持，这些关注点代表着这些原则的相关特点。五项基本要素和17项原则组合起来就构成了内部控制的准则，而各个关注点则为管理层提供指引，协助其评估内部控制的各个要素是否存在并发挥效用。

（2）明确目标设定在内部控制中的角色。COSO—ERM/2004将目标设定作为内部控制的八要素之一。COSO—IC/2013同样强调目标设定是内部控制的前提，但明确指出目标设定不是内部控制的组成部分。

（3）反映了对信息技术越来越大的依赖性。自1992年以来，随着信息技术的广泛运用，各种技术已经从分批处理交易的大型独立主机环境，演变成高度复杂、分散式的移动应用程序，当中所涉及的多项实时活动横跨多个系统、组织和流程。技术发展的这一变化势必对内控实施带来影响。

（4）强化公司治理的理念。COSO—IC/2013包括了更多的公司治理中有关董事会及其专门委员会（包括审计委员会、薪酬委员会、提名与治理委员会等）的内容。

（5）扩大报告的范畴。COSO—IC/1992在内控目标设定中仅仅关注财务报告目标，目的是确保编制可靠的公开发表的财务报告，主要来自企业面临的外部监管要求。COSO—IC/2013在报告对象和报告内容两个维度上进行了扩展，以满足利益相关者（Stakeholder）的要求。在报告对象上，既要面向外部投资者、债权人和监管部门，确保报告符合有关监管要求；

③ 请参考附录A“COSO新框架（COSO—IC/2013）17项总体原则简要说明”。