(2017年修订版)

公司治理·内部控制前沿译丛

美国COSO制定发布

张宜霞 译

Enterprise Risk Management — Integrated Framework

Application Techniques

企业风险管理——整合框架

应用技术

东北财经大学出版社
Dongbei University of Finance & Economics Press

国家一级出版社
全国百佳图书出版单位

(2017年修订版)

公司治理·内部控制前沿译丛

美国COSO制定发布

张宜霞 译

Enterprise Risk Management — Integrated Framework

Application Techniques

企业风险管理——整合框架

应用技术

东北财经大学出版社 Dongbei University of Finance & Economics Press | 大连

辽宁省版权局著作权合同登记号：图字06-2005-143号

图书在版编目（CIP）数据

企业风险管理——整合框架：应用技术 / （美）COSO制定发布；张宜霞译.
—2版（2017年修订版）.—大连：东北财经大学出版社，2017.4
（公司治理·内部控制前沿译丛）
ISBN 978-7-5654-2704-6

Ⅰ.企… Ⅱ.①C… ②张… Ⅲ.企业管理-风险管理-研究 Ⅳ.F272.35

中国版本图书馆CIP数据核字（2017）第026512号

东北财经大学出版社出版发行
大连市黑石礁尖山街217号 邮政编码 116025
网 址：http://www.dufep.cn
读者信箱：dufep@dufe.edu.cn
大连图腾彩色印刷有限公司印刷

幅面尺寸：170mm×240mm 字数：97千字 印张：8.5 插页：3
2017年4月第2版 2017年4月第5次印刷
责任编辑：刘东威 责任校对：孙冰洁
封面设计：冀贵收 版式设计：钟福建
定价：28.00元

教学支持 售后服务 联系电话：（0411）84710309
版权所有 侵权必究 举报电话：（0411）84710523
如有印装质量问题，请联系营销部：（0411）84710711

中文版前言

在内部控制和风险管理的演进过程中，COSO的突出贡献是举世公认的。它在1992年发布并于1994年做出局部修改的《内部控制——整合框架》，已经成为世界通行的内部控制权威文献，被国际和各国审计准则制定机构、银行监管机构和其他方面所采纳，2003年更被美国SEC指定为上市公司内部控制评价和审计的参照标准。

2003年7月，COSO发布了名为“企业风险管理框架”的征求意见稿，引起了广泛的关注，我国也有一些学者撰文介绍了相关情况。诚然，企业风险管理框架并没有立即取代内部控制整合框架，但是它涵盖并拓展了后者。因此，对新的框架进行深入研究和探讨，具有十分重要的价值。2004年9月，名为“企业风险管理——整合框架”的最终文本正式发布后，由于著作权保护和其他方面的原因，在国内很难获得最终定稿的版本。而许多学者继续按照征求意见稿来进行转述、介绍和研究，已经显得不合时宜了。为此，东北财经大学出版社通过积极联络和多方努力，最终获得了正式授权，得以将这份重要的文献翻译成中文并在国内

公开出版。

长期以来，尤其是在2001年前后，一系列令人瞩目的公司财务丑闻爆发之后，关于内部控制的研究和立法行动深受社会各界的重视和关注，我国也不例外。有关部门在几年前就已经开始了制定企业内部会计控制规范的积极尝试。目前，关于研究和制定企业内部控制指引的呼吁和探索也日益强烈。在这种背景下，认真研究和参考包括《企业风险管理——整合框架》在内的相关国际权威文献，无疑具有十分突出的理论价值和现实意义。

由方红星教授和王宏博士翻译的《企业风险管理——整合框架》是上卷，即内容提要和基本框架部分。本书是下卷，即应用技术部分。尽管在下卷中一再声明其不是框架卷的组成部分，里面例示的技术也不一定要应用，也不代表最佳实践，但是，毋庸置疑，其中例示的技术依然为有效地实施企业风险管理提供了非常有价值的借鉴和指导。书稿的翻译和校对工作由张宜霞博士完成。十分感谢美国内部审计师协会的Lucy Sheets在授权过程中的大力协助，以及东北财经大学出版社各位编辑对书稿的仔细阅读。在翻译过程中，得到了东北财经大学刘明辉教授、方红星教授的大力支持和帮助，在此谨致谢忱！

翻译下卷——“应用技术部分”不但涉及上卷的框架部分，而且涉及很多领域的技术名词和专业术语，加之时间紧迫和译者水平有限，书中错误和疏漏在所难免。为了更加准确和完整地表述COSO企业风险管理的思想和技术，2016年译者进行了重新翻译和校对，以纠正书中存在的错误和疏漏。同时恳请业内专家和广大读者不吝指正（接受批评和建议的电子信箱为yixiazhang@163.com）。

译　者

2017年1月

反欺诈财务报告委员会发起组织委员会（Committee of Sponsoring Organizations of the Treadway Commission，COSO）

监督者	代表
COSO主席	John J. Flaherty
美国会计学会（American Accounting Association，AAA）	Larry E. Rittenberg
美国注册会计师协会（American Institute of Certified Public Accountants，AICPA）	Alan W. Anderson
国际财务经理协会（Financial Executives International，FEI）	John P. Jessup
	Nicholas S. Cyprus
管理会计师协会（Institute of Management Accountants，IMA）	Frank C. Minter
	Dennis L. Neider
内部审计师协会（The Institute of Internal Auditors，IIA）	William G. Bishop，III
	David A. Richards

COSO项目咨询委员会

指导者

Tony Maki，Chair 合伙人，Moss Adams LLP	James W. DeLoach 执行总裁，Protiviti有限公司	John P. Jessup 副总裁兼司库，E. I. duPont de Nemours公司
Mark S. Beasley 教授，北卡罗来纳州立大学（North Carolina State University）	Andrew J. Jackson 企业风险保证服务高级副总裁，美国运通（American Express）公司	Tony M. Knapp 高级副总裁兼主计长，摩托罗拉（Motorola）公司
Jerry W. DeFoor 副总裁兼主计长，Protective Life公司	Steven E. Jameson 执行副总裁，首席内部审计与风险官，Community Trust Bancorp有限公司	Douglas F. Prawitt 教授，杨伯翰大学（Brigham Young University）

普华永道有限责任合伙公司（PricewaterhouseCoopers LLP）

Richard M. Steinberg 前合伙人兼公司治理业务负责人（现Steinberg治理顾问）	Miles E. A. Everson 纽约分部合伙人兼金融服务业财务、经营、风险与合规业务负责人
Frank J. Martens 加拿大温哥华分部客户服务部高级经理	Lucy E. Nottingham 波士顿分部国内企业服务部经理

目　录

1.导论

本文献的应用

《〈企业风险管理——整合框架〉应用技术》提供了组织的不同层面在应用企业风险管理原则的过程中所用技术的实例。本书的结构与框架卷是并行的。为了提供更多的衔接，框架卷的一些段落也以斜体的形式包含在这里。那些段落也为例示的技术提供了一个基础。为了能够从本卷中获得预期的收益，使用者应当熟悉框架卷的内容。

尽管人们希望这个资料有益于那些试图应用企业风险管理技术的人，但它不是框架卷的一个组成部分。在这里介绍绝不意味着需要用例示的技术来实施企业风险管理或者在确定企业风险管理是否有效的过程中必须应用它们。也丝毫不表明这些描述或例示的技术是首选的方法或代表“最佳实践”。

我们没有试图使本卷例示的技术完整，而且它们也是不完整

的。专栏和附带的讨论只涉及在框架卷出现的和在专栏1.1中描述的某些要素。这些技术中的一些可适用于规模较小、不复杂的组织，而其他技术则与大型的复杂主体更相关。根据主体的规模、多样性和行业特色，对应用企业风险管理的技术进行更加全面的介绍超出了本书的范围。随着时间的推移，我们相信，随着职业组织、行业团体、学者、监管者和其他群体开发素材来帮助其支持者，更多的指引将会发展起来。

建议那些思考企业风险管理应用技术的读者也要参考《内部控制——整合框架》的评价工具卷以获得更多的指导。它介绍了评价一个主体的内部控制系统所要用到的工具，包括一套空白工具、根据一家假定公司填写完毕的工具和一本参考手册。

企业风险管理的主要组成内容

为提供现有的背景，专栏1.1列示了每一企业风险管理构成要素的主要组成内容。

专栏1.1　每一构成要素的主要组成内容

内部环境

风险管理理念—风险容量—董事会的监督—诚信和道德价值观—对胜任能力的承诺—组织结构—权力和职责的分配—人力资源准则

目标设定

战略目标—相关目标—选定的目标—风险容量—风险容限

事项识别

事项—影响因素—事项识别技术—事项相互依赖性—事项类别—区分风险和机会

风险评估

固有风险和剩余风险—确定可能性和影响—数据来源—评估技术—事项之间的关系

风险应对

评价可能的应对措施—选择的应对策略—组合观

控制活动

与风险应对整合—控制活动的类型—政策与程序—信息系统的控制—主体的特殊性

信息与沟通

信息—沟通

监控

持续监控活动—专门评价—报告缺陷

一个实施过程

如前所述，本书举例说明了企业风险管理框架的具体要素要用到的多种技术。一个更高阶的、“第一位的”问题涉及管理层在最初考虑如何在组织内实施这个框架时所采取的方法。

主体的规模、复杂性、行业、文化、管理风格和其他特性将会对如何最有效果、最有效率地实施这个框架的概念和原则产生影响。因为有许多可用的方法和选择，即使是相似的组织在实施企业风险管理时也是不同的——无论是首次应用这个框架的概念和原则，还是判断其现有的企业风险管理程序（它可能是长期发展起来的）是否真的有效。然而，经验表明存在某些共性。下面

简略地描述了那些已经成功地完成企业风险管理实施的管理层所采用的常见的、应用广泛的步骤：

• 核心小组筹备——成立一个由来自业务单元和主要支持部门（包括战略规划）的代表组成的核心小组是重要的第一步。这个小组要非常熟悉这个框架的组成要素、概念和原则。这种熟悉为设计和实施有效应对主体特定需要的企业风险管理过程提供了一种通用的理解、语言和一个基本依据。

• 执行官倡议——虽然执行官倡议的时机和形式因组织而异，但执行官倡议及早开始并随着实施的进行得以巩固却很重要。执行领导层要清楚地说明企业风险管理的好处，并建立和传达相关资源投资的业务实例。CEO 支持，而且通常至少初始直接和明显的参与会促进成功。

• 制订并实施计划——初始计划是为接下来的步骤制订的，它设定了主要的项目阶段，包括已定义的工作流、主要管理节点（milestone）、资源和时机。确定了职责，从而一个项目管理系统就运行起来了。这个计划充当了与小组领导层一贯地进行沟通和协调的手段，还充当了沟通和确定不同单元和员工期望的基础以及讨论预计通过采用企业风险管理带来的主体层面变化的依据。

• 当前状态评估——这包括评估当前在主体内正如何应用企业风险管理的构成要素、概念和原则。这通常涉及确定组织内已经发展了何种风险管理理念，并确定对主体的风险容量是否存在一致的理解。核心小组既要确定组织应用该框架原则和概念已具备的能力，也要确定当前在用的正式和非正式的政策、程序、惯例和技术。

• 企业风险管理愿景——核心小组设定一个愿景，陈述企业风险管理未来将会如何继续应用以及如何在组织内整合以实现其目标——包括组织如何将其企业风险管理的努力集中在协调风险

容量与战略、增进风险应对决策、识别和管理贯穿企业的风险、抓住机会和改善资本配置上。

• 能力发展——当前状态评估和企业风险管理愿景为确定已到位并发挥作用的人员、技术和流程能力提供了所需要的洞察力，也为需要发展的新能力提供了洞察力。这包括确定职能和责任，改进组织模式、政策、流程、方法、工具、技术、信息流和工艺。

• 实施计划——更新和改进初步计划，增大深度和广度以涵盖更多的评价、设计和配置。规定更多的责任，而且项目管理系统也精炼为必需的内容。该计划通常包括一般项目管理规范，它是任何实施过程的一个组成部分。

• 变革管理[①]（change management）的发展和实施——制定必要的行动来实施和维持企业风险管理愿景和要求的能力——包括实施计划、培训会议、报酬强化机制以及监控实施过程的其余部分。

• 监控——管理层要不断地审查和加强风险管理能力，作为其持续管理过程的一部分。

下面的章节举例说明了一些应用企业风险管理框架每一构成要素的概念和原则的具体技术。

---

① 第一，变革管理是一个涉及改变的系统过程，从结构的观点和单独层次两者中来。对于一个有些不明确的条款，变革管理有至少三个不同的方面，包括适应变革、控制变革和影响变革。主动变革处于所有三个方面的核心地位。对于一个组织，变革管理意味着定义和实现程序和/或者在商业环境中处理变革的工艺，以及从变化的机会中获利。成功地适应变化对于一个组织的重要性与它在自然界中的重要性相同。正像植物和动物，团体和个体都在不可避免地面临他们无法控制的变革情形。越有效地应对变革，你就越有可能茁壮成长。适应可能包括建立一个在商业环境中关于回应变革的结构方法论（例如经济的起伏，或者竞争的威胁）或建立一个在工作场所中关于回应变革的应对机制（例如新政策或工艺）。《变革的保利森》的作者Terry Paulson引用叔父的教诲：按着马前进的方向骑最轻松。换句话说，不要与变革作对，试着顺应这种变革。第二，计算机系统环境的变革管理是指采用系统化方法来跟踪系统的一些细节问题，比如，每个计算机上运行的操作系统版本还有安装方式——译者注。

2.内部环境

【框架章摘要】

内部环境包含组织的基调，它影响组织中人员的风险意识，是企业风险管理所有其他构成要素的基础，为其他要素提供约束和结构。内部环境因素包括主体的风险管理理念、风险容量、董事会的监督、主体中人员的诚信、道德价值观和胜任能力，以及管理层分配权力和职责、组织和开发其员工的方式。

这一章应用技术简要描述了内部环境要素对主体的成功或失败所产生的影响，并举例说明了风险管理理念、评价风险管理理念与主体文化整合程度的技术及提高诚信和道德文化的工具。

影响

一个组织的内部环境对如何实施企业风险管理并使其持续发

挥作用具有重大影响。内部环境是应用企业风险管理其他构成要素的环境，通常具有强大的正面或负面影响。专栏2.1是具有负面影响的例子。

专栏2.1　内部环境的影响

内部环境的影响可以通过哥伦比亚事故调查委员会报告的调查结果来说明。这个委员会由国家航空航天局（NASA）组建，调查哥伦比亚航天飞机发生事故的原因。在这次事故中，航天飞机在重返大气层的途中爆炸分解。该报告陈述："哥伦比亚事故在组织方面的原因来源于航天飞机计划的历史和文化……对安全有害的文化特性和组织行为得以发展，它们包括：依赖于用过去的成功代替可靠的工程实践（例如为了了解系统为何没有按要求运行而进行的测试）、阻碍关键安全信息的有效沟通和压制专业意见分歧的组织障碍、缺少贯穿所有计划要素的整合管理以及运行在组织规则之外的非正式命令和决策过程链的形成。"

风险管理理念

一个主体的风险管理理念是一整套共同的信念和态度，它决定着该主体在做任何事情时——从战略制定和执行到日常的活动——如何考虑风险……企业的风险管理理念实际上反映在管理层经营该主体的过程中所做的每一件事情上。它可以从政策表述、口头和书面的沟通以及决策中反映出来。无论管理层是强调书面的政策、行为准则、业绩指标和例外报告，还是更为非正式地通过与关键管理者面对面的大量接触来进行经营，至关重要的

是管理层不但要通过口头，而且要通过日常的行动来强化这种理念。

有些公司的管理层以书面的形式清楚地表述他们风险管理理念的基本内容。专栏 2.2 和专栏 2.3 是风险管理理念的实例。

专栏 2.2　描述风险管理理念的实例（一）

在全球发展和文化扩张中，我们的组织需要一个公司风险管理的综合方法来促进广泛的战略思考和分析，同时，从根本上整合组织的核心价值和信念。为了这个目标，我们力争使风险管理变成我们的竞争优势。

我们风险管理程序的起点是一个企业风险战略，它要考虑与我们有关的所有人的需求和愿望。通过促进信息流动和强化贯穿组织的沟通，风险管理程序提供了一个连续的循环风险信息模型。这个模型提供了与利益相关者需求和持续改善我们企业风险战略的愿望有关的信息。

为了确保实现我们的战略，我们的风险管理程序要为我们的员工提供工具和能力来努力克服超越预期时出现的障碍。通过认识到风险和控制是每个人的事情，我们的员工将会以一种更有效和更节省成本的方式主动地识别在向市场交付产品和服务的过程中存在的风险。我们的风险管理程序允许我们的员工从不同角度看问题，不仅识别风险抑制活动，还要预测潜在的机会并对其采取行动——从而挑战寻常的智慧以催生更好的解决办法。

我们组织的一个基本原则是对我们的员工、客户和股东要尊重和保持诚信。通过把风险管理加入到我们日常的业务活动中和实施相关的绩效指标，风险管理程序确保我们通过实行核心价值观来维持我们最高的道德标准。

专栏2.3　描述风险管理理念的实例（二）

企业风险管理将为我们的组织提供全方位识别、评估和管理风险的卓越能力，并使所有层级的员工能更好地了解和管理风险。这将使我们：

- 有合理的风险承受力。
- 支持执行官和董事会。
- 改进结果。
- 强化责任。
- 强化受托责任（stewardship）。

希望全体员工在制定战略和追逐目标的过程中表现出适当的行为准则。这个理念被下面的指导原则所支持。管理层和全体员工应该：

- 在做出决策时考虑所有形式的风险。
- 建立和评价业务单元层次和公司层次的风险概况，以便考虑对其单个业务单元和部门来说什么是最好的，对公司整体来说什么是最好的。
- 支持执行管理层建立公司层面的风险投资组合观。
- 在业务单元或影响层面的其他点保持对风险和风险管理的所有权和责任。风险管理不是把责任推给其他人。
- 在企业风险管理中努力实现最佳实践。
- 监控对政策和程序的遵循情况以及企业风险管理的状况。
- 推动（lever）现有的风险管理实践，无论它们存在于公司的什么地方。
- 记录和报告所有重大的风险和企业风险管理缺陷。
- 接受企业风险管理是强制的而不是随意的。

为了深入了解风险管理理念与主体文化的融合情况，一些公

司实施了一个风险相关文化的调查，它度量了关键风险相关特性的存在状况和强度。在这些调查中涉及的一些主要特性如专栏2.4所示。

专栏2.4　在风险相关文化的调查中度量的特性

1.领导能力和战略

- 展示道德和价值观
- 沟通使命和目标

2.人员和沟通

- 对胜任能力的要求
- 共享信息和知识

3.责任和强化

- 组织结构
- 业绩计量和报酬

4.风险管理和基础设施

- 评估和度量风险
- 系统接近和安全

一些公司根据期望的时机和置信水平定期（如每年一次）调查所有员工，更频繁地调查员工的一个代表性样本。公司每季展开这些调查，目的是更好地了解该组织持续的波动和变化趋势，尤其是在变动的时期会有所帮助。这样一些调查的结果为组织文化中的优势区域和弱势区域提供了方向性指标。专栏2.5部分地例示了如何展示和解释一个风险相关文化调查问题的结果。这些结果有助于主体识别那些为了确保有效的内部环境而需要加强的特性。