普华经管

# 管理风险 创造价值

## ——深度解读ISO31000:2009标准

安泰环球技术委员会 编著

人民邮电出版社
POSTS & TELECOM PRESS

# 管理风险　创造价值

## ——深度解读 ISO31000：2009 标准

安泰环球技术委员会　编著

人民邮电出版社
北　京

**图书在版编目（CIP）数据**

管理风险　创造价值：深度解读ISO31000：2009标准／安泰环球技术委员会编著．—北京：人民邮电出版社，2010.10
ISBN 978-7-115-23869-6

Ⅰ.①管…　Ⅱ.①安…　Ⅲ.①风险管理—国际标准　Ⅳ.①F272.3－65

中国版本图书馆CIP数据核字（2010）第174392号

## 内 容 提 要

本书是一本关于风险管理的工具书，具体介绍了ISO31000标准制定的背景、过程，对ISO31000标准的总体认识，风险管理术语、原则，风险管理框架以及风险管理过程共五部分内容。

本书适合具体执行风险管理的企业管理人员阅读。

**管理风险　创造价值**

——深度解读ISO31000：2009标准

◆ 编　　著　安泰环球技术委员会
责任编辑　刘　盈
◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街14号
邮编 100061　　电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
三河市海波印务有限公司印刷
◆ 开本：787×1092　1/16
印张：17.5　　2010年10月第1版
字数：200千字　　2010年10月河北第1次印刷
ISBN 978-7-115-23869-6

定　价：35.00元

**读者服务热线：（010）67129879　印装质量热线：（010）67129223**
**反盗版热线：（010）67171154**

# 安泰环球技术委员会

# 序

未来充满不确定性，人人都希望自己具有“先知先觉”的特殊本领，以规避风险，抓住机会。国际标准化组织（ISO）于2009年11月15日正式发布了ISO31000:2009标准《风险管理——原则与指南》（*Risk management — Principles and Guidelines*）。明确指出“风险”是“不确定性对目标的影响”，其中的“影响”有好有坏，有机会也有威胁。风险管理就是要管理“不确定性”，减小威胁，放大机会。

ISO31000:2009标准是人类在管理学领域的又一个里程碑式的成果。ISO技术管理局（TMB）风险管理工作组（RMWG）主席凯文·W. 奈特（Kevin W. Knight）说：“ISO31000将类似于ISO9000和ISO14000标准，是最高级别的标准，它将对ISO和IEC的其他标准起指导作用。”

安泰环球风险管理技术公司作为中国最早从事风险管理研究和培训的专业机构，承载着“传播风险管理先进理念，培养风险管理专业人才，探索风险管理最佳实践，创造风险管理综合价值”的使命，在其CTO李存建博士的带领下，在公司咨询团队的帮助下，经过翻译、校对、解读、内训和公开课等过程，历时七个月，正式推出这本风险管理宝典。此举堪称中国风险管理史上一件有意义的大事，也是对中国风险管理事业的重大贡献！

《管理风险　创造价值——深度解读ISO31000:2009标准》是一本工具书，这本书融入了安泰环球咨询师和专家们多年的管理咨询经验，它的面世，将为中国企业和其他组织学习ISO31000标准、开展风险管理实践活动提供重要指导！

《管理风险　创造价值——深度解读ISO31000:2009标准》是一本哲学书，这本书将改变世人对风险纯负面的认识。ISO31000:2009标准将世界各国管理风险的先进理念及方法论融为一体，开辟了人类管理风险、管理未来的新纪元！

中国人力资源开发研究会风险管理者联谊会

中国风险管理者联谊会（CARP）

副会长兼秘书长

李素鹏

2010年6月18日 于北京

# 前　言

国际标准化组织于2009年11月15日（以正式版标准为准）发布了ISO31000:2009《风险管理——原则与指南》标准。这是世界风险管理领域的一件大事，对世界经济、政治、社会、金融和文化等都将产生重大影响，标准的颁布开启了人类标准化风险管理的新起点。在全球金融危机尚未结束，欧洲主权债务危机渐成蔓延之势的今天，更加凸显出该风险管理国际标准的重大意义。

安泰环球风险管理技术（北京）有限公司作为一家专业从事风险管理的组织，始终对ISO31000标准给予了极大关注，密切追踪了标准修订的全过程。在2008年年初，便将标准的CD稿（委员会稿）进行了全文翻译，并及时开展了研讨，向有关企业介绍了标准的制定、内容及进展情况。之后，公司对标准的DIS稿（国际标准的草案稿）、FDIS稿（国际标准的最终草案稿）、正式版标准进行了持续追踪，密切关注了在标准的各个修订阶段，标准发生的变化、标准修订的动向。在此基础上，公司对有关企业进行了十余次公开培训，介绍标准的进程和主要内容，参加培训的单位有中国海洋石油有限公司、中国五矿集团、伊利集团和中国风险管理者联谊会等。从企业的内部控制到企业所处内外部环境的不确定性，各种组织对ISO31000标准给予了极大关注和重视。可以说，正是在多次培训的基础上，又考虑到众多企业对学习、实施ISO31000标准的迫切需求，我们才萌生了编写本书的厚望，并开始付诸实施。历经数月，终于完成了本书的编写工作。

本书设计了五章内容。

**第一章介绍ISO31000标准制定的背景、过程**

近二十年来，世界范围内的风险管理理论和实践发展迅速，其中最突出的特征就是这一时期发生了风险“特定事件”和发布了风险管理“特定法规”。ISO31000标准是在世界风险管理理论和实践的基础上，在这一“特定事件”和“特定法规”的历史背景下产生的。本书第一章分国际、国内两个部分，对“特定事件”和“特定法规”进行了综述与评价，以加深读者对ISO31000标准产生和制定背景的认识。国际事件主要涉及英国巴林银行事件、亚洲金融危机、美国安然事件和世通事件等；国内事件主要涉及银广夏事件、中航油

（新加坡）事件、德隆案事件和三鹿事件等。本书第一章以这些事件为线索，对国际、国内重要的风险管理法规性文件进行了介绍。国际部分的文件主要包含《巴塞尔资本协议》（含巴塞尔资本协议Ⅱ、Ⅲ）、美国 COSO《内部控制——整合框架》、《企业风险管理——整合框架》、澳大利亚和新西兰的 AS/NZS 4360：2004 标准、美国《萨班斯—澳克斯利法案》等；国内部分的文件主要包含《证券公司内部控制指引》、《中央企业全面风险管理指引》、《企业内部控制基本规范》（含《配套指引》）、国家标准 GB/T24353——2009《风险管理原则与实施指南》等。需要说明的是，我国国家标准 GB/T24353——2009《风险管理原则与实施指南》于 2009 年 12 月 1 日开始实施。该标准制定时参考了 ISO31000 标准的 DIS 稿，所以在时间和内容上，该标准都不能被看作是 ISO31000 标准的制定“背景”。但该标准发布后成为了我国风险管理的最高层次标准，具有普遍的指导意义，在今后相当长的时间内将是我国企业实施风险管理的重要依据。因此，我们在“特定法规”中包含了该标准。为避免这一部分内容篇幅过长，又希望能给读者提供更多的信息，我们在本书中设置了附录 2、3，分别介绍并评价了重要的风险事件和风险法规。

以这些“特定事件”和“特定法规”为基础，第一章具体介绍了 ISO31000 标准起草、修订的过程。鉴于目前我国还未正式采用 ISO31000 标准，在本章的最后，我们从六个方面论述了我国及时“等同采用”ISO31000：2009 标准的必要性。

**第二章是对 ISO31000 标准的总体认识**

本章介绍了 ISO31000 标准的构成，给出了风险管理“原则、框架、过程”的总体构成图。对标准的“引言”、标准正文中的五章内容“范围”、“术语与定义”、“原则”、“框架”、“过程”进行了简要介绍。结合我国推广和实施 ISO 其他管理标准的大背景，本章从五个方面论述了 ISO31000 标准的性质：标准是“指南”、不是“管理体系”标准、不可用于第三方认证、可用于第一和第二方审核或评价、标准关注的主体是企业。标准正文前的“引言”部分是构成标准整体的重要组成部分。本章从对“风险”的认识、“一个关键特征——建立环境”等七个方面进行了说明，并重点对引言部分的“十七项”帮助进行了专题论述。

**第三章介绍风险管理术语、原则**

ISO 在发布 ISO31000 标准的同时，也发布了 ISO 指南 73：2009《风险管理——术语》标准。ISO31000 标准的第二章引用了《风险管理——术语》标准中的 29 个风险管理术语。ISO31000 标准的第三章为“原则”，给出了风险管理的 11 项原则（原则 a）→ k））。本书的第三章对标准中的“术语”和“原则”进行了介绍与论述。为叙述方便、针对性强，本

章将29个术语分成两组，集中论述了第一组的17个术语。第二组中12个术语被安排在了本书第四、五章的适当位置。本章对风险管理原则的论述，首先从四个方面论述了对风险管理原则的定位，然后逐一给出了每一项风险管理原则的原文，并进行了详细说明和讲解。最新的“风险”术语定义“不确定性对目标的影响”对标准的导向作用十分明显，“风险管理向目标聚焦”贯穿于整个标准。本书在此专门设置了一节内容——“对风险术语最新定义的认识”，在对“风险”一词考察的基础上，对“风险”术语的最新定义进行了详细论述。

**第四章介绍风险管理的框架**

ISO31000标准的主体是标准的第四章：风险管理“框架”。本章对标准所推荐的风险管理框架进行了详细的介绍和论述。按标准的顺序，分为六节内容：“总则”、“授权与承诺”、“管理风险框架的设计”、“实施风险管理”、“框架的监测与评审”、“框架的持续改进”。其中“授权与承诺”中有九项内容，“管理风险框架的设计”提出了七个方面的设计内容，“实施风险管理”指出要“确保本标准条款5（标准的第五章‘过程’）所描述的风险管理过程得到应用”。本章对此均进行了详细的说明和解析。

**第五章的风险管理的过程**

在ISO31000标准中，“风险管理过程”是标准中“风险管理框架”的组成部分，本章对风险管理过程进行了详细的介绍和论述。标准中的“风险管理过程”由“沟通与咨询”、“建立环境”、“风险评估”、“风险应对”、“监测与评审”五个子过程构成。其中“建立环境”要求建立四个方面的环境：“外部环境”、“内部环境”、“风险管理过程的环境”、“风险准则”。“风险评估”过程包括“风险识别”、“风险分析”和“分析评价”三个过程。标准在最后对“记录风险管理过程”提出了组织应考虑的七个方面的内容。

以下是关于本书的几点说明。

1. 本书的写作目的是向我国各种规模和类型的企业介绍ISO31000:2009《风险管理——原则与指南》标准，并对标准做出解读，希望能为企业学习、理解和实施这一标准提供帮助。因此，本书不是一本风险管理“实战”方面的书籍，而是以介绍ISO31000标准为主旨，将重点放在对标准性质、标准条款的介绍和讲解上，特别关注的是对标准中有关概念的认识和内容的理解。书中少有的举例也在于为理解标准提供补充，而不是介绍事例本身。

2. 由于ISO31000标准发布不久，按照该标准实施风险管理的案例几乎没有，我们正在尝试将部分ISO31000标准内容应用于特定的企业风险管理项目之中。目前，受实践时

间和实践事例所限，我们对标准大部分内容的认识和理解，还是来自于以往对 ISO 管理标准的学习和风险管理咨询的实践。标准中许多内容还有待深入地学习和广泛地实践。

3. 在本书的有关叙述中，我们追溯了 ISO31000 标准在不同修订阶段（标准的 CD 稿、DIS 稿、FDIS 稿、正式稿）的历史进程，对比了不同阶段的标准内容，特别是与正式版标准的差别。我们认为这样做是十分有益的，通过比较这些变化（注意：是世界范围之内的比较），可以获知标准发生了怎样的变化，思考为什么有如此变化、这些变化意味着什么，从而使我们对标准制定的思路、标准的走向有一个正确的把握，有利于我们对标准内容的深入理解。如本书对“风险管理原则”在标准制定过程中的不断突出、强化，追溯标准“引言”部分“十七项”帮助逐渐形成的历程、最新“风险”术语定义对标准的导向作用等，相信读者会受到一定的启发。

4. 我国目前尚未正式采用 ISO31000 标准，所以还没有一个官方的中文版 ISO31000：2009 标准。我们对英文版的正式标准进行了全文翻译，并尽我们的语言能力和对标准的认识、理解能力，力图忠实地再现原文的内容。在本书中，为清楚起见，将“标准原文”的内容一律以“楷体”字印刷。考虑到标准本身的篇幅较长，而在介绍和讲解中已覆盖了标准正文（包括标准的“引言”部分）的全部内容（楷体字），故未在本书之后再附以标准的全文。

5. 在本书第二章第二节“对标准的性质认识”中指出了 ISO31000 标准不是“要求”，而是“指南”，这是对标准的性质认定而言。但在本书的论述中，从语言习惯和读者易于理解的角度，我们对标准的不同内容还是并列使用了“指南”和“要求”二词。从企业的角度讲，一旦选择了该标准，就应按照标准中要求的内容实施，这时“要求”的约束力应大于“指南”。

6.ISO31000 标准引用了 ISO 指南 73《风险管理——术语》中的 29 个术语，本书在写作时，重点关注了这些风险管理术语，严格采用术语的定义进行有关论述。如在我们的日常生活和工作中，也会使用“风险管理过程”一词，但在本书中，一再强调“风险管理过程”一词特指标准第五章所描述的、由五个子过程构成的风险管理过程。重视标准中风险管理术语的正确使用，对读者学习和理解标准的内容至关重要。

7.ISO31000:2009 标准有附录 A：“强化风险管理的特性”，本书未对其进行讲解，将附录的全文置于了本书的附录 1 中，读者可参阅。

本书中 ISO31000 标准的中文全文由李存建翻译。咨询师李伟、任文、金星在翻译中提出了很多正确的建议，给予了很大帮助，并对标准的全文进行了认真校对。

全书由李存建提出整体策划，并承担了大部分内容的写作任务。第一章第一节“ISO31000 标准制定的背景”以及本书附录 2、3 由咨询师任文、李兴平、李伟完成写作。咨询师任文、李兴平、李伟、周正火、王丽洁、黄敬参与了本书的校对工作。全书由李存建最终审定。

安泰环球风险管理技术（北京）有限公司总经理对编写本书始终给予了足够的重视和关心，在人员和时间等方面给予了极大的帮助和支持，在此表示深深的谢意。

最后应特别指出，由于时间有限，作者语言能力和认识水平有限，ISO31000：2009《风险管理——原则与指南》标准还缺乏实践，本书对标准的翻译和有关概念的把握、标准条款的解读等如有不妥之处，恳请读者批评指正。

安泰环球技术委员会

二〇一〇年六月

# 目录

# 目录

# 第一章

# ISO31000 标准制定的背景、过程

## 内容提要

近二十年来，特别是进入新世纪以来，世界范围内的风险管理理论和实践发展迅速，这以在这一时期发生的风险“特定事件”和发布的风险管理“特定法规”为标志。ISO31000：2009 标准正是在这一大的历史背景下产生的。本章第一节从国际、国内两个方面对风险事件、风险法规进行了综述和评论。国际部分主要以英国巴林银行事件、亚洲金融危机、美国安然事件、世通事件和近两年的全球金融危机为线索，介绍了在国际上较为重要的风险管理法规或标准，如《巴塞尔资本协议》（含巴塞尔资本协议Ⅱ、Ⅲ）、美国 COSO《内部控制——整合框架》、《企业风险管理——整合框架》、澳大利亚和新西兰的 AS/NZS 4360:2004 标准、美国《萨班斯—澳克斯利法案》等。国内部分主要以银广夏事件、中航油（新加坡）事件、德隆案事件和三鹿事件等为线索，介绍了我国重要的风险管理法规性文件，如《证券公司内部控制指引》、《中央企业全面风险管理指引》、《企业内部控制基本规范》（含《配套指引》）、国家标准 GB/T 24353——2009《风险管理原则与实施指南》等。第二节介绍了 ISO31000 标准起草、修订的过程。第三节论述了我国等同采用 ISO31000 的必要性，从六个方面说明我国的企业实施 ISO31000 标准既有实践基础，又有现实和未来意义。

## 第一节　ISO31000 标准制定的背景

人类刚刚进入新世纪的第二个十年。

当我们跨入新世纪的门坎、叩开新世纪的大门时，我们对新世纪的到来充满了希望，憧憬着未来“一帆风顺”、“风调雨顺”。当我们在刚刚进入新世纪的第二个十年之际，回首已成为历史的第一个十年时，除了两个“梦想”（“神六飞天”和“百年奥运”）得到实现以外，“风险”、“危机”事件也在我们的记忆中留下了深深

的烙印。世纪之交，互联网泡沫破灭，加上“9·11”事件的巨大冲击，美国中央银行从2001年1月至2003年6月连续13次降息，将联邦基金利率降至近于零，试图以此来刺激美国的经济，为以后的美国次贷危机和全球性的金融危机埋下了祸根。2001年美国发生“9·11”事件，2003年“SARS”肆虐全球，公共“风险”与“危机”第一次进入人们的视野，开始受到极大的关注。此后，我国南方的重大冰雪灾害、汶川特大地震、三鹿奶粉事件等，带给人们一次又一次的重大冲击。2007年，美国爆发了源于房地产的次贷危机。次年，以雷曼兄弟投资银行破产为标志，次贷危机迅速演变成为金融危机，并海啸般地席卷全球，使得实体经济也遭受到了重创。伴随着百年不遇的世界性金融危机，新世纪的第一个十年结束了，但金融危机的影响还远未结束。

可喜的是，在新世纪的第一个十年之末，世界范围内还发生了一件大事——国际标准化组织（ISO）于2009年11月15日正式发布了一个可直接用于风险管理的国际标准《风险管理——原则与指南》。这一标准的发布，不仅是世界风险管理领域的大事，对世界各国政府、组织、企业等来说也是一件大事，它开启了人类标准化风险管理的新起点。我们有理由相信，该标准的实施能够提高人类管理风险的有效性，为应对不确定性、风险和危机建立起更强的信心，向着新世纪的第二个十年以及更美好的未来前进。

伴随着世界范围内的风险管理理论和实践的迅猛发展，尤其以这一历史时期发生的风险“特定事件”和发布的风险“特定法规”为重要标志，ISO31000:2009标准在这一“特定背景”下产生了。本书将对ISO31000标准进行详细介绍和解读，因此有必要对标准产生的事件背景和法规背景进行简要的梳理，以勾勒出ISO31000标准产生的大致脉络，相信此举会为读者学习和理解ISO31000标准提供有益的帮助。

## 一、国际风险事件、风险法规综述及其评价

20世纪70年代，以德国郝斯塔特银行破产、美国富兰克林国民银行破产为标志，人类步入了风险管理的新阶段。可以说，正是这一系列特定事件的接连发生，引起了风险管理在世界范围内的广泛关注。此后不久，1975年巴塞尔银行监管委员会发布了《巴塞尔协议》第一版，1979年美国发布了《反国外贿赂行为法》，风险

事件与风险管理法规相伴而生的走势逐渐形成。此后，人们追溯风险管理的历史也经常是从这一时间开始的。

鉴于全球金融环境不稳定性日益加剧，1988 年《巴塞尔资本协议》经过反复修订后正式发布。可以说，它的发布意味着资产负债管理时代开始向风险管理时代过渡。一套国际通用的、以加权方式衡量内外风险的资本充足率标准诞生了。它的实施有效扼制了与债务危机相关联的国际银行业风险。

随着关注的焦点逐步集中在风险管理上，人们越来越清晰地意识到需要提供一个强有力的风险管理框架以更好地指导风险管理实践。

1992 年，为了帮助企业及其他主体评估和增进它们的内部控制制度，美国 COSO 委员会发布了《内部控制——整合框架》。此后该《框架》被纳入政策、规则和法规中，并被数千家企业采用，以对企业为实现既定目标所采取的行动实施更好的控制。现如今《内部控制——整合框架》已成为内部控制领域最为权威的文献之一，是美国证券交易委员会（SEC）惟一推荐使用的内部控制框架。

1995 年爆发的英国巴林银行事件，堪称金融衍生工具操作失败的经典案例。从表面上看是由于在巴林银行新加坡分行既担任前台首席交易员又担任后台结算主管的尼克·里森，擅自利用“错误账户”进行违规交易而导致的恶果。但这一事件从根本上暴露出了巴林银行内部监管和外部审计监督存在重大失误。具体表现在权利制衡机制的薄弱、风险意识的缺失、领导层对财务报告不重视以及操作风险、交易风险多职合一，从而最终导致风险管控形同虚设。正是此次事件引发了全世界对金融领域风险管理的密切关注，金融衍生工具的高风险开始被广泛认识。

在英国巴林银行事件发生的同年，由澳大利亚和新西兰联合开发的 AS/NZS 4360《澳大利亚—新西兰风险管理标准》正式发布。该标准明确定义了风险管理的标准程序，是第一个企业层面的风险管理标准，也是第一个以国家名义发布的风险管理标准。

距巴林银行事件发生仅两年后的 1997 年，亚洲金融危机爆发。此次危机给了亚洲经济一记重创，它导致了全亚洲经济衰退，是继 20 世纪 30 年代大危机之后，对世界经济产生深远影响的又一重大事件。究其原因是亚洲的一些国家在国内体制还没有发展成熟、经济发展水平相对落后时，过早地开放了资本市场和金融市场，忽视了体制的不完善、监控的不完备等因素。此次亚洲金融危机也暴露出了世界和