中国银河证券博士后科研工作站
CHINA GALAXY SECURITIES POSTDOCTORAL PROGRAMME

博 研 周 报

2011 年 10 月 20 日 第 12 期

ISO31000 风险管理标准与全面风险管理

王曙明 ☎：（8610）8357 1403

✉：wangshuming@chinastock.com.cn

全面风险管理已经成为目前国际风险管理的大趋势，继美国 COSO 委员会（Committee of Sponsoring Organizations of the Treadway Commission）于 2004 年发布《企业风险管理一整合框架》(《Enterprise Risk Management Integrated Framework》)后，国际标准化协会(International Organization for Standardization，以下简称 ISO）于 2009 年正式发布了一项各领域通用的风险管理国际标准——《ISO31000:2009 - 风险管理：原则与指引》。ISO31000 结合了各种全面风险管理框架和标准的精华，在强调简单实用的同时，对风险管理模式做出了一系列创新性的改进，它是风险管理发展过程中的重要里程碑。本文首先简要介绍全面风险管理的发展，进而对 ISO31000 的创新性和实用性加以探讨。

全面风险管理的发展

全面风险管理兴起于本世纪初，是目前风险管理发展的主流趋势。全面风险管理是一种站在整个组织角度所进行的整体化风险管理方式，其核心思想是：一个组织的风险来自很多方面，最终对组织产生影响的不单单是某一种风险，而是所有风险联合作用的结果，所以只有从组织整体角度进行风险管理才是最有效的。通过全面风险管理，组织能够更加明确自身的经营目标，更好地聚焦管理信息，更好地理解风险-收益平衡，从而提升企业的各种决策基础。

2004 年 9 月，美国 COSO 委员会（Committee of Sponsoring Organizations of the Treadway Commission）在其 1992 年发布的《内部控制整体框架》基础上，吸收各方面风险管理研究成果，

正式发布《企业风险管理一整合框架》(《Enterprise Risk Management-Integrated Framework》)，这是全面风险管理理念在运用上的重大突破。《企业风险管理一整合框架》认为“企业风险管理是一个过程，它由一个主体的董事会、管理层和其他人员实施，应用于战略制订并贯穿于企业之中，旨在识别可能会影响主体的潜在事项，管理风险以确保风险处在该主体的风险偏好之内，并为主体目标的实现提供合理保证。”同时，它提出了风险管理框架的八大要素：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。该框架拓展了内部控制，更有力、更广泛地关注于企业风险管理这一更加宽泛的领域。

同年，澳大利亚和新西兰标准组织联合发布了澳大利亚/新西兰风险管理标准（AS/NZS 4360），其对风险概念进行了拓展并对风险管理流程各环节做了清晰的定义，随即成为国际广泛认可的全面风险管理标准之一。

2009 年 11 月，在融合了一系列全面风险管理框架（其中包括加拿大标准协会（CSA）指引 CAN/CSA-Q850、COSO 委员会的《企业风险管理一整合框架》、澳大利亚/新西兰风险管理标准（AS/NZS 4360））的最佳实践基础上，国际标准化协会（International Organization for Standardization，以下简称 ISO）正式发布了一项各领域通用的风险管理国际标准——《ISO31000:2009 - 风险管理：原则与指引》（以下简称 ISO31000）。ISO 31000 是 ISO 于 2004 年着手开始制定，历经 5 年打造出的一套极其精炼的风险管理标准。该标准的核心内容由“原则”、“框架”及“流程”三部分构成。ISO 31000 提出，全面风险管理的首要原则是：它必须要为企业创造价值。换句话说，提升正面风险和降低负面风险对组织的净影响（net effect）要大于管理和控制风险的花费。此外，ISO31000 认为，全面风险管理是以一种相容性的、机构化的、增值性的方式来处理风险，它通过风险识别、风险分析、风险评价来决定这些风险是否需要处置以满足风险准则，而在整个风险管理流程中，都应当与利益相关方保持定期的沟通与协商。

同时，为了更好地支持 ISO31000 的应用，国际电工委员会(International Electrotechnical Commission，IEC)和 ISO 联合发布了《IEC/ISO 31010:2009 风险管理：风险评估技术》。这项技术标准从操作性的角度详细阐述了 ISO31000 标准中的风险管理流程中各环节（建立环境、风险识别、风险分析、风险评价、分险处置、监控与评审以及沟通与交流）的各项要点，并介绍了适用于风险评估流程各环节（风险识别、风险分析、风险评价）的 31 种较为成熟的风险评估技术，同时对各项风险评估技术进行了适用性比较分析。

ISO 31000 的发布，促使许多国家和风险管理组织相继参照该标准修改了其原有的或发布了新

的风险管理标准或规定。事实上，早在 2008 年 ISO31000 的委员会稿（Committee Draft）发布后，澳大利亚/新西兰风险管理标准联合技术委员会主席 G. Purdy 就指出 COSO《企业风险管理一整合框架》的一些缺陷（如风险评估流程的含糊不清），并认为其应当根据 ISO31000 加以改进（参见 Purdy 2008）; 2009 年，加拿大标准协会（CSA）根据 ISO31000 对 CAN/CSA-Q850 指引作了修改，形成了 2009 修订版（R2009）;中国政府也在同年正式发布了国家标准 GB/T 24353 —— 2009《风险管理原则与实施指南》，作为我国各组织实施风险管理的最高级标准，而该标准正是参照 ISO 31000 编制的（参见安泰环球技术委员会 2010）；2010 年，英国三大风险管理组织：保险与风险经理人协会（Insurance and Risk Managers）/公共风险管理协会 ALARM (ALARM-The Public Risk management Association)/风险管理研究所（Institute of Risk Management）联合发布了一项指引——《实现 ISO31000 与企业风险管理的结构化方法》，该指引基于 ISO31000 的框架和流程详细阐述了企业如何实现全面风险管理。

ISO31000 的创新性与实用性

（1）创新性

ISO31000 被认为是风险管理发展历程中的里程碑，其在很多方面对全面风险管理框架作出了创新性的改进。这主要体现在以下几个方面：

第一，强调风险管理的未来性。ISO31000 强调风险管理就是管理未来可能发生的风险事件对组织（未来）目标可能产生的影响。同时，其风险管理框架也充分体现了面向未来进行设计和改进的特点，而风险管理流程中风险识别、风险分析等各个环节以及衡量风险大小的风险准则等也都带有鲜明的未来性特征。

第二，提出了正式的风险管理原则，用于衡量一个组织对风险管理的成熟程度。ISO31000 给出了管理风险的 11 项原则，并强调一个组织若想使其风险管理卓有成效，就必须在其每个层级都满足这些原则。

第三，考虑所有影响组织目标的不确定性或风险，不论其对目标实现产生的是正面的或负面的影响。之前绝大多数的风险管理框架都是从事件对目标实现的负面影响的角度定义风险，例如 COSO 委员会发布的《企业风险管理一整合框架》就将风险定义为“一个事件发生并对目标产生消极影响的可能性”。而在 ISO31000 中，风险定义为“不确定性对目标的影响”，并指出该影响可以是正面的亦可以是负面的。ISO31000 对风险的全新诠释更加完备化了对风险本质的理解，而这

也使得不确定性管理的方向更加全面，即我们不但需要降低不确定性（当不确定性不利于目标实现时），同时也需要增加不确定性（当不确定性有利于目标实现时）。更重要的是，这种新的风险定义本质上直接将风险管理和创造价值融为一体，因为风险的积极一面就是价值本身。

第四，强调组织针对自身的内部结构和治理流程特点来设计并实施与之匹配的风险管理的能力。ISO31000 在风险管理框架设计以及风险管理流程中都明确强调了风险管理要与组织的目标、结构、内外部环境以及风险状况保持一致。

第五，要求组织制定正式的、将风险管理融入所有组织流程的风险管理框架，并强调对框架的持续改进。ISO31000 明确要求使风险管理过程成为组织过程的一部分而不是与组织过程相分离，特别是要求将风险管理嵌入方针政策制定、业务与战略的规划和评审中；同时指出应当制定一套适用于全组织范围内的风险管理计划，以确保风险管理方针得以执行且被嵌入到了组织所有的实践和过程之中，并通过与内外部利益相关方的持续沟通和协商，保持框架的适用性。

第六，通过建立环境、风险评估、风险处置、沟通与协商以及正式的监控与评审来不断更新用于支持每项决策的风险管理流程。

第七，对每一项风险以及整体风险的职责都通过指定“风险责任人”加以明确，而“风险责任人”的绩效也是部分基于对风险管理的有效程度加以衡量。ISO31000 强调组织应当保证其具有管理风险的职责、权利及适当的能力，同时明确对管理风险负有责任并具有权利的风险责任人，以及组织内各个层级人员对风险管理过程应当承担的职责，并建立风险绩效指标。

（2）实用性

第一，应用的灵活性高。ISO31000 的风险管理框架和流程具有高度的通用性和未来性，这为组织根据自身特点开展符合自身发展的风险管理提供了较高的灵活性和改进空间。

第二，对行业技术、标准体系的支持性强。ISO31000 为具体领域的风险管理技术或行业标准提供了一套通用的支持性方法，使得风险管理在这些特定领域的技术体系或标准下更和谐有效地运行。

第三，具有宏观和微观的双重优势。ISO31000 作为一项各领域、各组织通用的风险管理标准，不但可以应用于公司层面的风险管理框架搭建、风险管理政策、计划制定，流程设计等，而且可以应用于业务层面甚至具体项目的的风险管理计划制定与风险管理流程设计等。

第四，为组织当前正在进行的风险管理提供评估标准。正如 ISO31000 所指出的，如果组织现有的管理实践与过程已经包含了风险管理（框架）的组成部分，或者组织已经采用了正式的风险管

理流程来处理某项特定的风险或情形，那么组织应该严格按照 ISO31000 标准对这些实践和过程加以批判性的评审和评估，以确定其充分性和有效性程度。

第五，结构清晰、内容精炼。ISO 31000 标准按照 “风险管理框架-风险管理流程-风险评估流程”三层结构的逻辑从面到点层层深入地将风险管理的各个要素与环节都清晰地进行了表达。这非常方便风险管理者根据这种层次结构将组织的风险管理框架和流程与 ISO 31000 进行差距分析（Gap-analysis）并加以改进。同时，该标准力求精练且表达通俗，通过短短的 34 页纸浓缩了风险管理的本质要素，这就方便参与风险管理的人员进行广泛的交流，并寻找出将其应用于组织的最佳办法。

第六，聚焦风险管理流程，具有较强的可操作性。ISO31000极其精练的34页内容有近一半的篇幅花在阐述风险管理流程的实施上，这充分体现了ISO31000对可操作性要求较高的风险管理流程的高度重视。为更详细地阐明风险管理流程中的核心子流程——风险评估流程，IEC和ISO还联合发布了《IEC/ISO 31010:2009 风险管理：风险评估技术》用于支持ISO31000的风险管理流程的应用，这进一步增强了ISO31000的可操作性。

中国银河证券股份有限公司 博士后科研工作站
北京市西城区金融街 35 号国际企业大厦 C 座 100033
电话：010-83571403
传真：010-66568641
中国银河证券网址：www.chinastock.com.cn
中国银河证券博士后科研工作站网址：http://www.chinastock.com.cn/yhwz/postdoc/index.shtml.chinastock.com.cn