企业内部控制与风险管理工具箱

A Complete Toolkit for Internal Control & ERM

董大胜 韩晓梅▲编著

风险基础内部审计

Risk-Based Internal Auditing

——理论·实务·案例

大连出版社
DALIAN PUBLISHING HOUSE

·企业内部控制与风险管理工具箱·

风险基础内部审计

——理论·实务·案例

董大胜　韩晓梅　编著

大连出版社

内 容 简 介

本书全面介绍了基于风险管理的内部审计的理念、方法和程序，为企业在充满风险的环境中实施风险基础内部审计、重塑内部审计职能提供指导和建议。本书共分九章，包括风险、风险管理与风险基础内部审计，风险基础内部审计的方法与流程，风险识别与评估，风险基础审计计划，风险管理审计，公司治理审计，内部控制审计，审计报告，风险基础内部审计的管理等内容。

图书在版编目(CIP)数据

风险基础内部审计：理论·实务·案例/董大胜，韩晓梅编著. —大连：大连出版社，2010.10

（企业内部控制与风险管理工具箱）

ISBN 978-7-80684-486-1

Ⅰ.①风… Ⅱ.①董… ②韩… Ⅲ.①企业—内部审计—研究 Ⅳ.①F239.45

中国版本图书馆 CIP 数据核字(2010)第 185821 号

出 版 人：刘明辉
策　　划：刘明辉　毕华书
责任编辑：姚　兰
责任校对：张丽娜　彭理文　刘丽君
封面设计：张　金
版式设计：金东秀
责任印制：史凌玲

出版发行者：大连出版社
地址：大连市西岗区长白街 12 号
邮编：116011
电话：(0411)83621349/83621049
传真：(0411)83610391/83620941
电子信箱：bhs@dlmpm.com
印 刷 者：大连美跃彩色印刷有限公司
经 销 者：各地新华书店

幅面尺寸：170mm×240mm
印　　张：19.25
字　　数：386 千字

出版时间：2010 年 10 月第 1 版
印刷时间：2010 年 10 月第 1 次印刷
印　　数：1～3000 册
书　　号：ISBN 978-7-80684-486-1
定　　价：38.00 元

如有印装质量问题，请与我社营销部联系
购书热线电话：(0411)83621349/83621049

总　序

2008年6月28日，财政部、证监会等五部委联合下发了《企业内部控制基本规范》，随后，财政部又下发了《内部控制应用指引》、《内部控制评价指引》、《内部控制鉴证指引》的征求意见稿。恰在此时，大连出版社与国内的专家学者一起筹划了这套丛书。

企业内部控制与风险管理日益受到社会各界的重视，原因有三：

首先，自美国颁布《萨班斯—奥克斯利法案》，要求公众公司的管理层发布内部控制评价报告，并由注册会计师进行鉴证，出具内部控制鉴证意见以来，内部控制已经成为公司外部治理内化的重要措施。为了保护相关者的利益，各国的证券监管部门都要求公众公司建立完善的公司治理结构。但是，如果这种外部要求不能内化为企业的增值活动，反而成为企业的一种负担，显然有悖于公司治理的初衷。内部控制与风险管理，恰恰解决了这个问题，把外部的治理要求内化为企业自身的增值活动。

其次，内部控制是现代企业重要的管理制度，内部控制制度的完善与否，关系到企业能否在变幻莫测、充满风险的经济环境中生存和发展。内部控制设计合理、执行有效，企业就能抓住机会、控制风险，在激烈的市场竞争中立于不败之地，不断发展壮大。

最后，改革开放三十年来，我国经济飞速发展，综合国力蒸蒸日上。经过三十年的发展和努力，我国经济正处于产业升级和转型的重要时期，在这个阶段，企业家的管理能力和学识，逐渐超越土地、资本等成为关键的生产要素。内部控制与风险管理理念和方法正是锐意进取的企业家们急需的。

基于以上原因，我们欣然接受大连出版社的邀请，参与了这套丛书的编审工作，对丛书的体系设计和具体定位进行了把握。

从定位来看，丛书要为企业管理层理解、应用相关的内部控制与风险管理理论提供实实在在的帮助。体现在体例安排和写作风格上，丛书将理论阐释、方法应用

和实例讲解相结合，将专家对内部控制理论的理解和实务经验用生动的案例、细致的讲解展现在广大的读者面前；力求摆脱理论知识的抽象和授人以鱼的诟病。

从体系设计来看，丛书体系完整、安排科学，从内部控制设计、建立、评价、鉴证和完善的视角，提出内部控制设计、内部控制评价、内部控制鉴证和企业风险管理等选题，清晰地给出了内部控制在企业发挥作用的机制和路径；从各业务环节和流程建立完善内部控制的视角，提出了成本费用内部控制，购货与付款内部控制，固定资产与存货内部控制，预算控制与风险管理，投资、筹资与担保内部控制，销货与收款内部控制，人力资源内部控制等选题，着眼于如何在具体项目上建立健全内部控制。

本丛书既可以作为企业管理层学习企业内部控制与风险管理的教材，也可以作为日常工作中的案头工具书。

受业务水平和专业阅历所限，丛书的缺憾和不足之处在所难免，敬请广大读者批评指正！

“企业内部控制与风险管理工具箱”

丛书编审委员会

前　言

德国社会学家卢曼说过，我们生活在一个“除了冒险别无选择的社会”。风险已经成为我们生产、生活的组成部分，无处不在，无时不在。能否对面临的风险进行有效的管理，成为区分成功的企业和不成功的企业的重要标准。在竞争激烈、变幻莫测、充满不确定性的当今时代，建立有效的风险管理系统，高效地预测企业可能面临的风险并采取适当的应对措施，是企业的管理层实现既定目标的重要手段。风险管理是内部控制的基础，也是公司治理的关键要素。随着管理重心不断前移，内部审计也逐步从早期的账项基础审计和控制基础审计发展到风险基础审计，通过确认企业是否已将风险降低至可以接受的水平并抓住了重要的机遇，促进企业风险管理系统的不断完善和企业目标的实现。

根据国际内部审计师协会（IIA）的定义，内部审计是一种独立、客观的确认和咨询活动，旨在为企业增加价值并改善企业的运营。它通过应用系统的、规范的方法，评价并改善风险管理、公司治理和内部控制过程的效果，帮助企业实现其目标。正如该定义所述，内部审计深深根植于风险管理、公司治理和内部控制事项中，是风险管理审计、公司治理审计和内部控制审计的融合。本书全面介绍了基于风险管理的内部审计的理念、方法和程序，为企业在充满风险的环境中实施风险基础内部审计、重塑内部审计职能提供指导和建议。本书共分九章。第一章分析了风险管理与内部审计的联系及风险基础内部审计的由来。第二章阐述了风险基础内部审计的方法并简要介绍了开展风险基础内部审计的基本流程。第三章介绍了风险基础内部审计的第一个阶段，即风险识别与评估。第四章介绍了风险基础内部审计的第二个阶段，即在风险识别与评估的基础上制订审计计划。第五章到第七章针对风险基础内部审计的具体实施，分别介绍了风险管理审计、公司治理审计和内部控制审计的开展。第八章着重阐述了审计报告的形成、报送与跟踪。第九章则试图探索如何更好地组织和管理内部审计工作。

本书是分工协作和集体智慧的成果。其中，第一章由中国内部审计协会杨莉

执笔，第二章由南京理工大学韩晓梅、徐玲玲执笔，第三章、第四章由南京理工大学郭威执笔，第五章、第六章由南京理工大学韩晓梅执笔，第七章由南京理工大学邓德强执笔，第八章由南京审计学院倪慧萍、南京理工大学徐玲玲执笔，第九章由南京理工大学邓德强、韩晓梅执笔。国家审计署董大胜、赵圣伟，南京理工大学韩晓梅对全书进行了总纂和修改。南京理工大学郭威、陈晨对全书进行了校正。南京理工大学郭威、徐玲玲、赵翠、华娟承担了本书的资料整理和翻译等基础工作。

本书体现了全球内部审计理论和实践的最新发展，对推动我国内部审计工作的进一步发展具有重要的参考价值。但是，风险基础内部审计仍处于探索和实验阶段，本书关于风险基础内部审计的理论研究和实务指南难免存在局限，敬请广大读者批评指正。

国家审计署　董大胜

2010年8月16日

目　录

第一章　风险、风险管理与风险基础内部审计

第一节　风险与风险管理

对风险的定义，通常有两种，一种是强调事件发生损失的不确定性，另一种是强调事件发展本身的不确定性。前者属于狭义的定义，是早期的通俗定义，而后者属于广义的定义。目前，风险一词在更多情况下体现的是后者的定义。

一、风险

（一）风险的概念

企业在实现其目标的经营活动中，会遇到各种不确定性事件，这些事件发生的概率及其影响程度是无法事先预知的，这些事件将对经营活动产生影响，从而影响企业目标实现的程度。这种在一定环境下和一定限期内客观存在的、影响企业目标实现的各种不确定性事件就是风险。一般来说，风险具有客观性、普遍性、必然性、可识别性、可控性等特点。风险的形成过程涉及风险因素、风险事故和损失三个方面。其中，风险因素是指能够引起风险事件发生或增加风险事件发生机会或影响损失严重程度的因素，通常包括物理因素、道德因素、心理因素等；风险事故是指在风险的形成过程中直接或间接造成损失的事故，也就是导致损失的直接媒介；损失则是指非故意的、非计划的和非预期的价值减少，通常为经济上的价值减少。

风险并不仅仅指负面的影响或作用。事件发生的不确定性，既代表着出现不利结果的风险，也代表着机遇；既可能损害企业的价值，也可能增加企业的价值。有时表面上看起来有利的环境或条件也可能引发不利的后果。如客户的需求超过了企业的生产能力，一方面说明企业的产品很适销，供不应求，但从另一方面看，由于不能满足客户的需求，影响了客户的满意度和忠诚度，客户可能转向其他供应商采购，从而影响了企业未来的部分订单，那么影响是负面的。

（二）风险的来源与类型

企业在经营过程中，由于不确定因素的影响，遭受损失或影响企业目标实现的

可能性来源于很多方面。以企业为例，现代企业面临的主要风险通常表现为政策风险、环境风险、市场风险、经营风险、投资风险、财务风险、管理风险、技术风险、法律风险等。以企业目标为中心，一般将这些风险按照来源于企业内部和企业外部来划分，可分为外部风险和内部风险。

外部风险是指外部环境中对企业目标的实现产生影响的不确定性。外部风险的主要因素包括：第一，国家法律、法规及政策的变化。其中，既有国家宏观经济政策的变化，也有政府针对不同行业的监管与调控等具体规定的变化。第二，经济环境的变化。即企业经营的外在氛围，如投资环境、经济增长水平、资本流动情况等的变化。第三，市场变化。资源的配置过程是根据市场的需求和走向不断变化的，行业竞争会导致人力、财力和物力等资源的争夺，从而给企业实现目标带来不确定因素。第四，自然灾害等难以避免的因素。

内部风险的主要因素包括：第一，公司治理结构的缺陷。有效的管理是通过权力制衡来保证的，健全的治理结构就是达到这一制衡的手段。如果公司治理结构存在缺陷，可能导致内部控制失效、监督机制流于形式，进而损害股东利益。第二，企业中员工的道德品质和职业素质不能达到要求。人力资源对企业的任何经营都具有决定性的作用，如果员工在道德品质和职业素质方面达不到要求，那么在其履行职责的过程中就可能出现错误甚至舞弊，影响企业目标的实现。第三，企业经营活动的特点。例如，企业经营活动越多样，复杂程度越高，相应的风险就越大。第四，企业信息系统的安全性。现代经济的运行对信息系统的依赖是前所未有的，信息系统安全对企业的正常运营有直接的影响，信息系统故障带来的风险也是巨大的。

二、风险管理

（一）什么是风险管理

风险管理起源于20世纪30年代的美国，并从美国向世界范围内传播，20世纪中期，利用保险的方法进行风险管理就已经成为一些行业的实践。从20世纪后期开始，由于环境的不断变化，控制手段和措施的不断丰富，风险管理的外延和内涵有了很大的扩展。随着对风险的认识不断提高，人们对风险管理也有了更多的理解和判断。对什么是风险管理，一些学者提出了自己的看法。美国学者克里斯蒂（James Cristy）认为，风险管理是企业或其他组织为控制偶然损失的风险，以保全所得能力和资产所做的一切努力；另外两位美国学者威廉姆斯（C. Arthur Williams, Jr.）和理查德·汉斯（Richard M. Heins）认为，风险管理是通过对风险的鉴定、衡量和控制，以最低的成本把风险所造成的损失控制在最低程度上的管理方法；我国的陈佳贯认为，风险管理是企业通过对潜在意外或损失的识别、衡量和分析，并在此基础上进行有效的控制，用最经济合理的方法管理风险，以实现最大的安全保障的

科学管理方法。COSO 报告则指出，企业风险管理是一个过程，受企业的董事会、管理层和其他人员的影响，应用于企业的战略制定及各个方面，旨在确定影响企业的潜在重大事件，将企业的风险控制在可接受的范围内，从而为实现企业目标提供合理保证。根据目前适用的部分法律、规定，我们把风险管理定义为，对影响企业目标实现的各种不确定性事件进行识别和评估，并采取应对措施将其影响控制在可接受范围内的过程。

正确地理解风险管理的定义，是建立有效的风险管理机制的前提。根据以上风险管理的定义，我们可以得出以下几点认识：

第一，风险管理是一个过程。风险管理不是静止、一成不变的，而是一个持续改进的过程，它与企业日常的经营活动息息相关。只有当风险管理机制嵌入企业的基本制度之中并成为企业经营中一个不可分割的部分时，才有可能发挥出最大的效用。

第二，风险管理受公司各个层级员工的影响。风险管理机制是由公司的董事会、管理层和其他员工共同建立并执行的。同时，风险管理体系也对公司员工的行为产生相应的影响。现实情况往往是，在一个企业中，由于不同的员工拥有不同的教育背景、经历和技能，也有不同的需求和偏好，因而对风险的认识、态度不一样，用以应对风险的方法也存在差异。风险管理就是要提供一种机制来帮助员工从企业目标实现这一角度来理解风险，在员工的职责、权限及工作方式与企业目标之间建立起明确而紧密的关联。

第三，风险管理应当运用于战略的制定。每个企业都有自己的使命、愿景，以及相应的战略目标。企业需要建立一系列的战略来实现其战略目标。除战略目标外，企业还应有一些相关的、具体的目标，这些目标源自企业的战略，渗透到企业的各个业务单元、分部和流程之中。风险管理应该运用于战略的制定，而战略制定就是在风险与相关替代策略之间的权衡与选择。比如企业的发展有两种战略：一种是收购其他企业扩大市场份额，另一种是通过成本控制取得更高的毛利率。每一种战略选择都会有相应的风险。收购其他企业，必须开拓新的或不熟悉的市场，竞争对手可能乘虚而入，侵蚀公司现有的市场份额，并且企业也可能缺乏实施这一战略的能力。而采用成本领先策略，则需要采用新技术、寻找新的供应商或形成新的战略联盟。风险管理技术可以帮助企业的管理层评估和选择企业相应的战略与目标。

第四，风险管理涉及企业的方方面面，也就是说，要求企业接受“组合风险”的观点。风险管理应该应用于企业的各种层面的活动，包括企业层面的战略计划、资源配置，部门层面的市场活动与人力资源管理，流程层面的生产与新客户信用的审视等。风险管理还可应用于一些特定的项目或新的举措。

第五,风险管理仅对企业目标的实现提供合理的保证(Reasonable Assurance)。设计与运行良好的风险管理系统可以对管理层和董事会在企业目标的实现方面提供合理的保证。之所以只能提供合理的保证而非绝对的保证是因为不确定性、风险与未来有关,任何人都无法准确地加以估计。合理的保证并不意味着风险管理会经常失败。风险管理实施中风险反应的累积效应、内部控制制度的加强都会减少企业目标不能实现的风险。并且,风险管理能将各级职能部门每个员工的日常经营与职责履行都指向企业目标的实现,这无疑会减少内耗,促进企业目标的实现。

第六,风险管理对不同目标的影响程度不同。在企业风险管理框架中,风险管理的目标共分为四类:一是战略目标,即企业的高层次目标,它与企业使命相一致并支持企业使命的实现。二是营运目标,涉及企业资源使用的效果与效率。三是报告目标,涉及企业业务报告和财务报告的可靠性。四是合规目标,涉及企业对法律法规的遵循。对目标进行分类有利于企业关注风险管理的不同方面。上述有些目标,如报告的可靠性、法律法规的遵循等是企业可控的,它取决于企业相关的经营活动是否适当。而企业的战略目标,如获取特定的市场份额,以及一些营运目标,如成功导入一条新的产品生产线,并不总是在企业的可控范围内。对于这些目标,企业风险管理虽然有利于管理层更好地进行决策,但并不能避免错误的判断或决策,也不能消除可能导致企业目标不能实现的一些外部因素的发生。需要特别强调的是,企业风险管理的目标不仅仅是财务报告的可靠和经营的规范,更重要的是企业战略目标的实现,以及高效率、有效果地运用资源。

(二)风险管理的目标

如前所述,不确定性不等于风险。不确定性是指某一事件发生的可能性,该事件可能产生积极的效果,也可能产生消极的效果。建立风险管理系统就是为了帮助管理者有效地应对不确定性,提高企业管理风险和创造价值的能力。企业风险管理使管理层能够有效地处理不确定性以及由此带来的风险和机会,从而提高主体创造价值的能力。因此,风险管理旨在为企业目标的实现提供合理的保证。良好的风险管理有助于降低决策失误的几率、避免损失的发生、相对提高企业本身的附加价值。其基本原则是以最小的成本获得最大的保障。

企业风险管理是一个过程,其有效性表现为某一时点的一种状态或条件。那么,我们如何判断一个企业的风险管理系统是否有效呢?这就需要看企业的风险管理要素是否存在,是否有效地发挥其功能。如果各要素存在且恰当地发挥着功能,就说明企业存在有效的风险管理机制,能够消除重大缺陷,将风险控制在企业的风险容量范围之内。从目标角度看,如果企业的风险管理被确认为是有效的,则企业的董事会和管理层就可以在以下方面得到合理的保证:他们了解战略目标实

现的程度、他们了解营运目标实现的程度、财务报告是可靠的、相关的法律法规得到遵循。

（三）风险管理的过程

风险管理包括识别风险和设计控制风险的方法，其核心是将没有预计到的未来事项的影响控制在可接受的范围内，从而提高企业的经济效益及社会效益。风险管理是一个系统的过程，主要包括以下三个阶段：

1. 风险识别。即根据企业的目标、战略规划等识别所面临的风险。在企业的内部和外部环境中存在各种各样的风险，尽管这些风险的轻重缓急程度以及发生的可能性各不相同，但都会影响企业目标的实现。为了确保风险管理的充分性，这一阶段必须识别所有影响企业目标实现的风险，并找出企业中高风险暴露的领域，进行重点分析。风险的识别要根据企业目标及战略规划等进行。企业目标自上而下可以分为不同的层次，如战略目标、经营目标、职能部门目标、岗位目标等。风险的识别应根据这些不同层次的目标分别进行，最终涵盖整个企业的各个层次。

2. 风险评估。对于已识别的风险，评估其发生的可能性及影响程度，同时将分析的结果与认为可接受的风险水平相比较。如前所述，企业所面临的各类风险对企业目标实现的影响程度并不相同，为了确保风险管理的针对性，要对不同的风险采取不同的控制措施加以管理。风险评估要从两方面同时进行，一是风险发生的可能性，二是风险的影响程度。这是风险的两个主要构成因素，有的风险发生的概率很大，但造成的影响却并不严重，有的风险后果很严重，但发生的可能性非常小。风险评估要针对可能性和影响程度这两方面进行，缺一不可。评估是对风险作出恰当的应对决策的基本前提。

3. 风险控制与应对。即根据风险的严重程度采取有针对性的应对措施，将风险控制在企业可接受的范围内，使企业的风险暴露水平与其所设定的目标相一致。基于成本效益原则，企业对不同程度的风险有不同的应对方式。根据风险评估结果作出的风险应对措施主要包括：回避风险，采取措施避免进行会产生风险的活动；承受风险，由于风险已在企业可接受的范围内，因而可以不采取任何措施；降低风险，采取适当的措施将风险降低到企业可接受的范围内；分担风险，采取措施将风险转移给其他企业或保险机构。

（四）风险管理中的主观因素

风险管理的过程除了一系列量化指标的对比外，还有部分主观判断的因素，这类主观因素与企业的风险容量（Risk Appetite）紧密相关。所谓风险容量，广义地讲，就是企业在追求其价值增值过程中所愿意接受的风险程度和数量。它反映了企业的风险理念和管理哲学，同时对企业的文化与经营风格产生影响。以企业为例，风险容量往往引导企业的资源配置。高风险容量的企业愿意将企业的大部分

资本投入高风险领域，如新兴市场等。相反，低风险容量的企业可能为了限制资本短期内的巨大损失而仅仅投资于成熟、稳定的市场。风险容量也与企业的战略直接相关，不同的战略将带来不同的风险。

三、企业风险管理框架

（一）企业风险管理框架的制定背景

全面风险管理是目前风险管理发展的最新趋势，它是一种站在整个企业的角度进行的整体化风险管理。全面风险管理的核心思想是：一个企业的风险来自很多方面，比如，一个保险公司可能面对由需求变化、利率变化、资产价格变化等带来的种种不同风险，最终对公司产生影响的不是某一种风险，而是所有风险的联合作用，所以只有从企业整体角度进行的风险管理才是最有效的。目前关于全面风险管理的理论与方法主要有以下两大类：第一类是基于组织结构体系全面风险标准化度量的企业风险管理——ERM（Enterprise-Wide Risk Management）方法。ERM的概念是由美国最大的几家银行和证券公司最先提出的，其核心理念是从企业整体的角度出发，对整个企业内部各个层次的业务单位和业务环节的各种风险进行通盘管理。ERM要求对市场风险、信用风险、操作风险等各种风险，各种风险所涉及的金融资产（利率、汇率、股票、期权等）与资产组合以及承担具体风险的各个业务单位，进行全面有效的整合风险管理。第二类是基于风险决策因素的全面风险管理——TRM（Total Risk Management）理论。TRM是从风险决策角度提出的另一种全面风险管理理论，其核心思想是从系统决策的角度出发，引入风险管理策略的三要素概念。这三个要素包括概率（Probability）、价格（Price）和偏好（Preference）。概率用来估计风险（含衍生交易本身的风险）发生的可能性，价格用来确定风险防范所需支付的成本，而偏好则用来确定决策者愿意承受风险的程度和信心。风险管理的目标是谋求三因素的最优均衡。目前TRM还只是一个理论上的概念，现实生活中建立如此庞大而复杂的TRM系统现在看来似乎是不可能的。相对TRM理论而言，ERM具有良好的现实可操作性。而谈到ERM，就不能不说美国COSO发布的两个报告。

随着企业信息化的高速发展，企业运营过程中面临着越来越多的风险和挑战，内部控制结构的概念已经越来越难以满足高风险环境下的企业管理要求。因此，到20世纪90年代，对内部控制概念进一步修订和完善的呼声越来越高。1992年，美国全美反舞弊财务报告委员会（National Commission on Fraudulent Reporting）所属的内部控制专门研究委员会发起组织委员会（COSO）经过研究发布了《内部控制——整体框架》报告，并于1994年进行了修订，扩大了内部控制的范围，增加了与保障资产安全有关的控制，得到了美国审计署的认可。同时，AICPA全面接受

COSO 报告的内容，于 1995 年据以发布了《审计准则公告第 78 号》，并自 1997 年 1 月起取代《审计准则公告第 55 号》。2004 年 4 月，美国 COSO 发布了《企业风险管理——整合框架》（*Enterprise Risk Management—Integrated Framework*，下称 ERM），该报告很快受到企业界、政府监管部门和学术界的广泛关注，其中的企业风险管理框架就是在 1992 年报告的基础上发展而来的。对于企业风险管理，COSO 是这样定义的，即企业风险管理是一个过程，受企业的董事会、管理层和其他人员的影响，应用于企业的战略制定及各个方面，旨在确定影响企业的潜在重大事件，将企业的风险控制在可接受的范围内，从而为实现企业目标提供合理保证。

传统意义上的风险管理是一种在风险和收益之间找到平衡点的方法，而 ERM 视野则更加开阔，因为 ERM 涉及全部业务风险的分析和处理，既包括可保险的风险，也包括各种传统意义上不可保险的风险。这个过程从本质上来说是合作性的，多样化的技能和专业技术是必不可少的，需要企业内不同职能部门的协同努力。作为优化风险管理的一项战略，ERM 通过提供系统的、合作性的评估和风险控制来实现这个目标。它是一种在整个企业范围内识别和减轻风险相关问题的流程和方法。通过为企业提供一个分配资源和减少开支的客观基础，ERM 能改进资金效率。结果是，风险和资源之间达到更彻底的平衡，从而提升股东价值。

（二）企业风险管理框架的目标与要素

企业风险管理框架（ERM 框架）适合各种类型的企业或机构的风险管理。该框架有三个维度：第一维是企业的目标，即战略目标、经营目标、报告目标和合规目标；第二维是全面风险管理的八个要素，即内部环境、目标设定、事件识别、风险评估、风险应对、控制活动、信息与沟通、监控；第三维是企业的各个层级，包括整个企业、各职能部门、各条业务线及下属各子公司。ERM 框架三个维度的关系是，全面风险管理的八个要素是为企业的四个目标服务的，企业各个层级都要坚持同样的四个目标，都必须从以上八个方面开展风险管理活动。

ERM 框架力求实现以下四种类型的目标：战略目标，即高层次目标，它与使命相关联并支持使命；经营目标，即有效和高效率地利用企业资源；报告目标，即报告的可靠性；合规目标，即符合法律法规的要求。

ERM 框架包括八个相互关联的构成要素，这些要素来源于管理层经营企业的方式，并与企业的管理过程相互融合。这八个构成要素分别是：

第一，内部环境。内部环境影响人们的风险意识，影响战略和目标的制定、经营活动的开展，以及如何识别、评估风险并采取行动，是企业风险管理所有其他构成要素的基础。内部环境要素包括正直与道德观、胜任能力、董事会与审计委员会、管理哲学与经营风险、组织结构、权责划分方式、人力资源政策等，为员工如何看待或处理风险与内部控制问题提供了基础。

第二,目标设定。内部环境的营造只是令企业中的每个员工有了思想上的准备,如果真的要采取行动,还必须有一个明确的目标,只有这样,才会形成合力,使风险管理工作行之有效。必须先有目标,管理层才能识别影响目标实现的潜在事项。企业风险管理确保管理层采取适当的程序去设定目标,保证所选定的目标支持和切合企业的使命,并与它的风险容量相符。目标设定是事项识别、风险评估和风险应对的前提。

第三,事项识别。事项是指企业内外部影响战略实施或目标实现的事件。管理者必须识别可能对企业产生影响的潜在事项。事项可能带来正面或负面的影响,或者两者兼而有之。带来负面影响的事项代表风险,它要求管理者予以评估和应对;带来正面影响的事项代表机会,管理者可以将其反映到战略和目标设定过程之中。在对事项进行识别时,管理者要在整个企业范围内考虑一系列可能带来风险和机会的内部与外部因素。

第四,风险评估。风险评估能够使企业考虑潜在事项影响目标实现的程度。管理者通常采用定性和定量相结合的方法,从可能性和影响这两个角度对事项进行评估,考察整个企业中潜在事项的正面和负面影响,并基于固有风险和剩余风险来进行风险评估。通过考虑风险的可能性和影响来对其加以分析,并以此作为决定如何进行管理的依据。风险评估应立足于固有风险和剩余风险。

第五,风险应对。在评估相关风险之后,管理者就要确定如何应对风险。应对包括回避、降低、分担和承受等四种方式。在考虑应对风险的过程中,管理者评估风险的可能性和影响以及成本效益,并选择能够使剩余风险处于期望的风险容量以内的应对方式。管理者应识别所有可能存在的机会,从企业范围或组合的角度去分析风险,以确定总体剩余风险是否在企业的风险容量之内。

第六,控制活动。控制活动是确保管理者的风险应对方式得以实施的政策和程序。控制活动贯穿于整个企业,遍及各个层级和各个职能机构。控制活动主要包括批准、授权、验证、调节、经营业绩评价、保护资产安全以及职责分离等。控制活动一般包括两个要素:确定应该做什么的政策,以及实现政策的程序。

第七,信息与沟通。通过及时确认、获取相关的信息以及沟通使员工能够履行其职责。企业各层级都需要相关的信息来评估风险并作出适当的反应,人们也需要在其角色、职责方面进行有效的沟通。风险的存在是因为不确定性,也就是信息不明晰。因此,为使各个部门真正成为一个整体,各部门就要进行信息交换与沟通。

第八,监控。企业风险管理随着时间的推移而不断变化,曾经有效的风险应对方式可能会失灵,控制活动可能会变得无效或不再被执行,企业的目标也可能发生变化。面对这些变化,管理者需要通过控制手段来确定企业风险管理的运行是否持续有效。监控活动可以通过持续监督(如管理层对客户投诉处理的及时监督、财