审计新视野丛书

Auditing the Risk Management Process

K. H. SPENCER PICKETT

风险管理过程审计

(英) K. H. 斯宾塞·皮克特 著

王义华 译

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

WILEY

审计新视野丛书

Auditing the Risk Management Process

K. H. SPENCER PICKETT

风险管理过程审计

(英) K. H. 斯宾塞·皮克特 著

王义华 译

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

WILEY

大连

图书在版编目（CIP）数据

风险管理过程审计／（英）皮克特（Pickett，K. H. S.）著；王义华译. —大连：东北财经大学出版社，2010. 11
（审计新视野丛书）
书名原文：Auditing the Risk Management Process
ISBN 978-7-5654-0168-8

Ⅰ. 风… Ⅱ. ①皮… ②王… Ⅲ. 风险管理-审计 Ⅳ. F239. 6

中国版本图书馆 CIP 数据核字（2010）第 205217 号

辽宁省版权局著作权合同登记号：图字 06-2006-34 号

K. H. Spencer Pickett: Auditing the Risk Management Process

东北财经大学出版社出版
（大连市黑石礁尖山街 217 号 邮政编码 116025）
教学支持：（0411）84710309
营 销 部：（0411）84710711
总 编 室：（0411）84710523
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 东北财经大学出版社发行

幅面尺寸：170mm×240mm 字数：230 千字 印张：11 1/2 插页：1
2010 年 11 月第 1 版 2010 年 11 月第 1 次印刷

责任编辑：刘东威 王 玲 刘 佳 责任校对：那 欣 毛 杰
封面设计：冀贵收 版式设计：钟福建

ISBN 978-7-5654-0168-8

定价：28. 00 元

前　言

“审计新视野丛书”是以内部审计师为主要读者的系列丛书。本丛书同时适于从事治理、风险和控制系统复核的外部审计人员、合规性小组、财务主管、咨询师及其他人员。本丛书也适于执行官、经理和职员，其正越来越多地被要求复核内部控制系统，以确保各种类型的组织均有健全的风险管理过程。本丛书的各分册均涉及与审计和复核有关的重要问题及相关概念。本系列丛书将与时俱进，威立（John Wiley & Sons）公司将同内部审计师协会（IIA）一道以确保每册的新题目均可以反映时下的最新进展。“审计新视野丛书”的框架如图 P—1 所示。

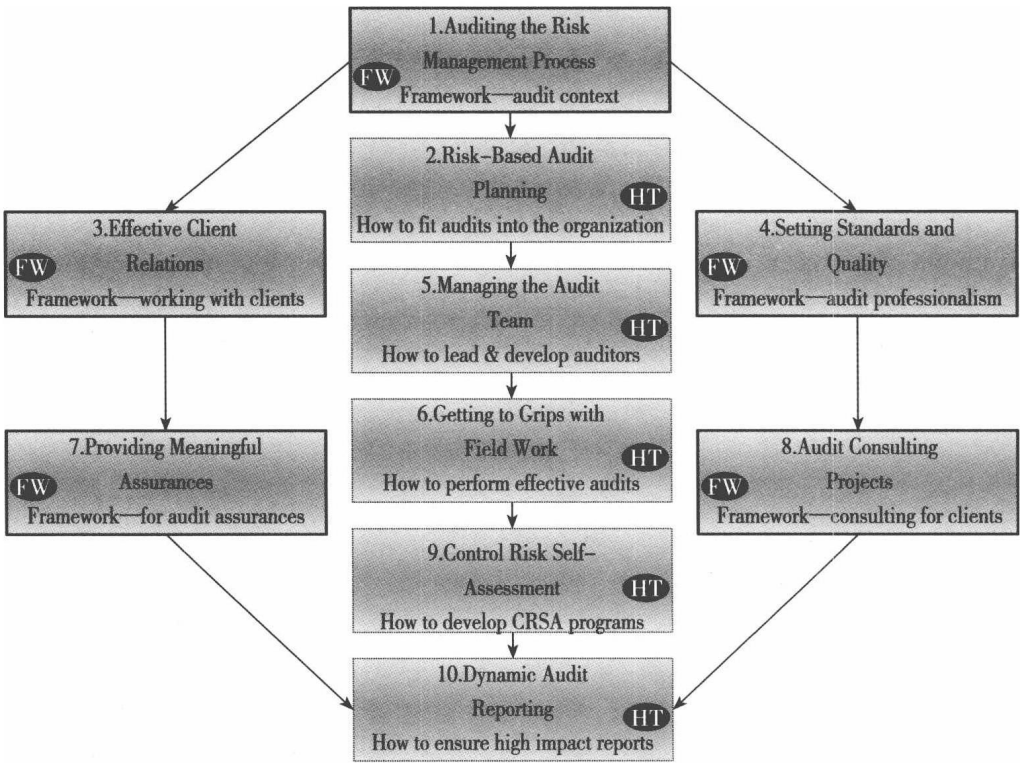

图 P—1　“审计新视野丛书”

“框架（FrameWork，FW）丛书”列示了各种模型。这些模型有参考资料的支持，以确保其可以就最佳实务指南对现行实务的影响做出评估。“如何做（HowTo，HT）丛书”也使用了同样的模型，但其更为关注的是检查表和已使用过的例子，

以此来补充说明相关支持性框架的各个方面。上述每本书均关注内部审计师协会的专业实务框架，如其所发布的准则、建议以及与之相配套的指南。因为这些丛书相当简明，所以参考其他来源的资料时也应加以限制。由于企业发展日新月异，导致目前适用的案例很快就会过时，因此本系列丛书并未引入对著名公司的详细的案例研究。然而，本丛书参考了不同组织中正在发生的许多简短的例子，以说明所持的重要观点。治理、风险及控制的动态性质，意味着“审计新视野丛书”中某些新书的名字可能会在日后有所改变。最后，衷心希望读者在阅读本丛书时可以发现其趣味性和引人入胜之处。另外，本丛书还将提供有关内部审计、外部审计及其他复核功能的部分参考文献。

书中简称列表

CAE：首席审计执行官
CEO：首席执行官
CFO：首席财务官
COSO：发起组织委员会
CRO：首席风险官
CRSA：控制风险自我评估
CSA：控制自我评估
ERM：企业风险管理
H&S：健康和安全
IIA：内部审计师协会
IS：信息系统
IT：信息技术
KPI：关键业绩指标
OECD：经济合作与发展组织
PPF：专业实践框架
PR：公共关系
RA：风险评估
RI：风险识别
RM：风险管理
RO：风险所有者
SEC：证券交易委员会
SIC：内部控制报告

译者简介

王义华，1972 年生于辽宁省，管理学（会计学）博士，现任深圳大学经济学院副教授。近年来在《特区经济》等学术期刊上先后发表论文 20 余篇，并出版学术著作、译著、教材 4 部。近期较有代表性的著作有《论现代风险导向审计》等。

目　录

第1章　为什么要有风险管理

内部审计活动应辅助组织识别和评价所面临的重大风险，并着手改善风险管理与控制系统。

IIA 准则 2110

1.1　引言

近年来内部审计迅猛发展，凸显出其在绝大部分组织中所占据的重要角色。内部审计部门不再是后勤检查小组，而是公司重要的职能部门。内部审计着眼于专业化和客观化，产生了重大的影响。这是同以往大不相同的。导致这一变化的关键是原来对雇员实施控制，而现在则运用风险评估，从而使管理当局及其雇员有能力对其经营活动实施有意义的控制。从必须去控制到主动要去控制，这种文化意识的转变，使雇员有更多创新和试验的机会。

可惜的是，风险管理在过去并非总是发挥作用。20 世纪八九十年代经济的迅速发展，意味着许多组织的加速发展已将懦弱不前者远远撇在后面。投资者希望迅速取得回报，竞争也要求我们抢先向市场提供新的或改良后的产品；或者说，至少给我们这样的印象。明确的目标或道德观对组织来说，就像铁路信号灯和刹车之于前行中的火车一样，非常有必要。而过去十年爆发的丑闻恰恰说明我们缺乏这些。

无情竞争下的轻率交易从 20 世纪 90 年代一直延续到 21 世纪，直到监管者开始强硬起来。在陈旧的治理模式下，选出的董事会围绕着有权力的 CEO，CEO 唯一的受托责任就是发布审计师已复核过的财务报表，而该审计师又与 CEO 关系友好。在这种环境下，法规被视为需要规避的障碍。公司的律师主要被用于设计路线图，以帮助执行者获取超越法律条款和行业法规的路径。这种陈旧的治理模式已无法跟上新的商业动态。2002 年，随着《萨班斯—奥克斯利法案》的发布，社会的关注已到了摊牌的阶段：遵守法律法规并说明应当如此，这是公司高层的个人责任。IIA 将风险管理与公司治理的关系描述为：

> 风险管理是公司治理的基本要素之一。管理当局代表着董事会，其有责任建立和运作风险管理框架。[1]

在过去，控制框架除了有助于建立标准外，更多扮演的是基本标尺的角色，并停留在符合性测试的检查、归档阶段，直到下一年度的同一时间。然而，时至今日，无论是企业、执行官还是利益相关者，都将焦点集中到风险上来。事实上，社

会普遍关注风险理念的最前沿，其涉及如下诸多方面：

- 发布的会计账户信息是容易令人产生误解的。
- 业绩信息是捏造的。
- 监管披露没有良好的证据支持。
- 有关对财务报告及合规性程序是否实施了充分控制的问题，高级管理者声明其并不知情。
- 公司的资产没有得到正确的保护，以使其免于浪费、损失、遭受攻击或自然灾害。
- 公司的声誉将影响到顾客的忠诚度。
- 运营及程序是低效的且缺乏灵活性。
- 提拔和招聘了不当的人员。
- 组织无法迎合顾客、市场以及利益相关者不断变化的期望。

为了解决这些问题，组织应该遵循企业风险管理（ERM）的指导。ERM 是一种系统方法，其从战略的高度来识别和管理存在于企业的各方面的风险。由于各项风险在影响力和紧迫性方面都会随时发生变化，因此组织必须及时做出应对，以保证新风险所带来的损失是有限的，带来的机会却已被发掘。事实上，成功企业的主要特征即在于，能够比其他类似的企业更有效地预测并应对全球风险。在如此高风险的环境里，内部审计师的角色也就变得更加重要起来。如果说 ERM 是成功的关键助推器，那么 ERM 框架的各个组成部分也就成为了我们要考虑的基本要素，而 ERM 框架正是为了应对整个业务流程中的风险而建立的。当各方都具有明确的职能时，有必要解除各职能所具有的明确责任。任何不足都将导致问题的出现。首席审计师关于 ERM 审计方法的选择至关重要，不能抱任何侥幸心理。

如果组织没有面临风险，则没有必要雇用内部审计人员。如果组织始终处于完全的控制之中，则没有必要实施复核、调整以及重新组合，甚至没有必要实施内部控制。然而，之所以存在审计人员，是因为计划并非总是按照预想的方式发展，事情也并非总是像其外表那样看似真实。因此，我们需要审计人员来确保组织理解它的风险，采取步骤来应对可预见的问题并抓住潜在的机遇。为了将风险提上议事日程，并确保已对风险给予了恰当的考虑，审计师可以采用建议、帮助、劝导和发布警告等辅助工具。为成为对风险敏感的工作团队所共同做的这些努力，意味着审计师正快速成为执行官、管理者和雇员的重要朋友。

在开始第一个模型的讲述之前，我们有必要给出 IIA 对内部审计的正式定义：

> 内部审计是一项独立客观的鉴证和咨询活动，用以增加价值和改善组织的经营。它通过应用系统的、受过训练的方法，来评价和改善风险管理、控制及治理过程的效果，帮助组织实现其目标。[2]

从这个定义中我们可以清晰地看出，内部审计植根于风险管理、控制和治理。IIA 主席戴夫·理查兹（Dave Richards）出席了 2004 年 9 月于内华达州拉斯维加斯召开的“IIA 企业风险管理和控制的自我评估”会议，有报道称：

> 理查兹强调了ERM和CSA的主要趋势，其包括：世界各地应采取法律行动以强调风险管理的必要性，以及有迹象表明内部审计师在使用风险评估的程序中正变得越来越主动。尽管CSA尚未完全植根于许多企业，但是ERM正日益成为良好治理的关键组成部分。内部审计师应促进组织接纳ERM并取得进展。最后，理查兹还鼓励与会人员："现在是从事内部审计职业的最佳时间"，他激励与会人员在各自的组织中倡导风险管理流程，以及在审计活动的前沿遵循内部审计准则和基本原则。[3]

当管理者在组织中努力实施良好的风险管理时，要帮助和支持管理者；同时，还应确保严格遵循审计准则的条款，这对内部审计师来说仍是一个挑战。IIA将风险管理定义为：

> 一个过程，即识别、评估、管理和控制潜在的事件或情况，以提供关于实现组织目标的合理保证。[4]

组织包括所有的公共组织和私人组织，企业风险管理被描述为：

> 一个过程，它贯穿于整个组织之中，旨在识别、评估、确定应对措施以及报告影响组织实现目标的机会和威胁。该过程是有组织的、一致的、连续的。[5]

我们也要花点时间来看看关于ERM的权威性文件——2004 COSO框架，该文件由发起组织委员会（COSO）于2004年9月29日发布。1985年，由反欺诈财务报告全国委员会发起，美国五大会计职业组织共同成立了COSO。本书中所有关于COSO框架的进一步参考都与2004 COSO框架有关。关于COSO的详细资料及其出版物，请参考网址www. coso. org。在ERM指南的前言中，COSO评论道：

> 人们迫切需要一个企业风险管理框架，以提供关键原则和概念、共同的语言、明晰的方向和指南。COSO相信《企业风险管理——整合框架》满足了这个需要，并希望它能得到公司和其他组织乃至所有利益相关者和有关方的广泛认同。[6]

1.2 风险管理框架模型：阶段I

我们第一个模型关注风险管理在组织中的存在方式。模型的起点为企业上层——CEO和董事会——的职责以及为确保良好的公司治理而采取的应对压力的方式，如图1—1所示。

接下来，将描述模型的各个方面。

1.2.1 企业外部的全球和市场发展

风险与影响全球经济的事件是内在相关的，这些事件包括利率变动、国际发展和资本转移的波动。同时，随着消费者需求的变化和竞争者的加入或离开，市场也在不断变化。公共服务也会因社会需求和期望的不断变化而受到影响。COSO将这

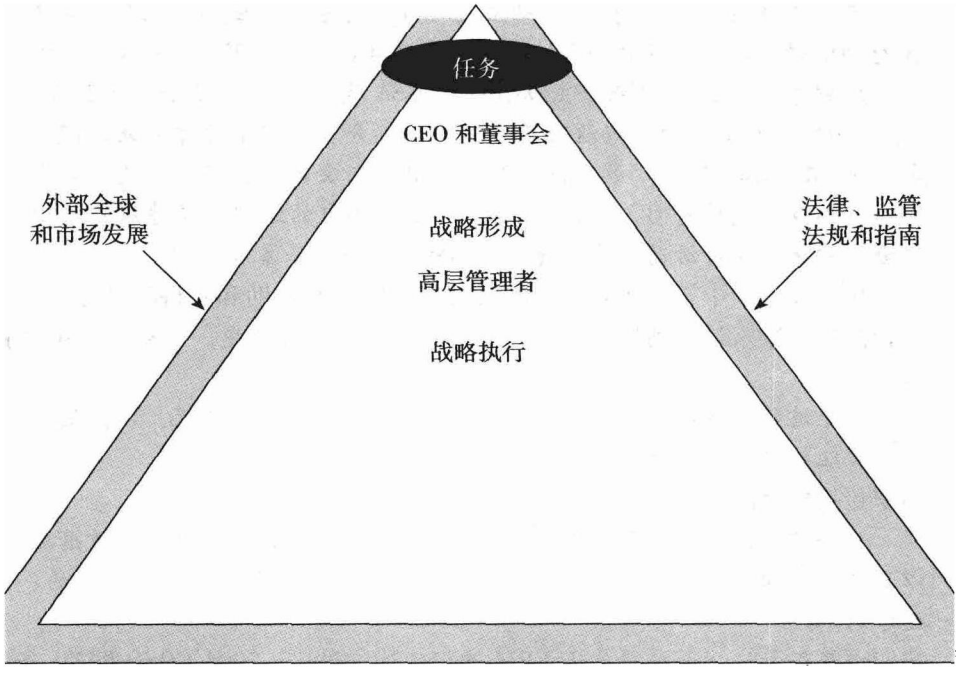

图 1—1 风险管理框架模型：阶段 I

些不确定性总结为：

> 全球化、技术、重组、市场变化、竞争和监管等因素导致了不确定性，而企业恰恰是在充斥着这些因素的环境中进行运作的。[7]

1.2.2 法律、法规、守则和指南

治理守则和公司法可以是一般性的，或者是分行业的。治理守则和公司法主要是从应对社会期望的角度对公司提出额外要求，或者是因公司丑闻所致需要对现有法律进行加强。几年前，发布了最为著名的《萨班斯—奥克斯利法案》，该法对在纽约股票交易所和纳斯达克证券交易所上市的公司产生了深远的影响。制定地方政府法律也完善了企业所必须遵循的法律框架。另外，还对某些职业（例如，法律、医疗、会计等）规定了不同的行为规范和具体法规，执业人员必须遵守。在这里，治理是指组织自身的行为方式和管理事务的方式。IIA 将治理定义为：

> 董事会所应用的程序和结构的总和，旨在通知、指导、管理和监督组织的活动，以实现组织的目标。[8]

我们应正确应对监管者所描述的日益广泛的社会需求，绝大部分组织都了解这种必要性。COSO ERM 的前言对此强调道：

> 在开发本框架期间，发生了一系列众所周知的企业丑闻和失败事件，投资者、公司员工和其他利益相关者因此遭受了巨大的损失。随之而来的便是人们纷纷呼吁采用新的法律、法规和上市公司准则来加强公司治理和

风险管理。[9]

经营业绩与法律法规的遵循情况应并重，这正如某大零售商所言：

> 我们的经营遍布全球各地，这虽然提供了非凡的机会，但是在应对不断变化的法律法规方面也带来了额外的复杂性。与监管环境的变化保持同步，这对管理者是个挑战，不过我们下决心这样做。我们继续监督法律、法规的遵循情况，并在必要的时候更新内部系统或改变经营方式，以确保遵循法律法规。[10]

1.2.3 任务

构建风险管理框架是为了实现组织最高层面上的整体任务。例如，福特汽车公司的任务被表述如下：

> 我们是一个具有光荣传统的全球大家庭，热情地致力于为全世界的人民提供汽车。我们想消费者之所想，并提供杰出的产品和服务，以改善人们的生活。[11]

同时，福特汽车公司对未来的展望是：

> 成为能够提供世界领先的汽车产品和服务的生产企业。[12]

许多公司治理守则中提出公司的目标应更加丰富，以确保其可以解决广泛的社会问题：

> 除了经营目标，公司也会努力披露与商业道德、环境和其他公共政策执行等相关的政策。[13]

私人、公共和非营利组织的环境现实意味着，我们永远都无法确定任务已被全部完成，从而使对未来的展望变为现实，而风险即是指缺乏确定性。因此，风险被界定为：

> 风险是指影响目标实现的事件发生的可能性。因此，为了确保捕捉到所有重大的风险，有必要知道所审核的组织功能或活动目标……组织的成功标准是衡量目标实现的基础，因此可运用该标准来识别和衡量风险所带来的影响或后果。[14]

1.2.4 CEO 和委员会

ERM 是由企业的 CEO 和委员会来实施的。CEO 和委员会还要做出战略决策，这些战略的实施会将任务转换成企业的成果。IIA 将委员会定义为：

> 委员会是组织的治理主体，如董事会、监事会、代理主席或立法主体、治理委员会或非营利组织的信托委员会或组织的任何其他指定主体，包括接受首席审计师向其报告的审计委员会。[15]

委员会负责形成战略，并雇用执行官、管理人员、职员以及其他适当的人员来实施战略。良好的委员会非常必要，正如下面所言：

> 安然公司存在三个主要问题：一是公司的委员会臃肿、消极；二是其

实现盈利目标的动机不良——可能这是最具杀伤力的；三是其愿意雇用最好、最聪明的雇员，并在他们创新、创新、再创新时，给予丰厚的回报。不幸的是，创新所掩盖的另一面即是欺诈。[16]

此外，委员会在监管风险管理的过程中扮演着关键的角色。COSO ERM 在描述该角色方面给予了指导，事实上，委员会的监管职责包括：[17]

- 知晓管理当局在组织中实施有效的企业风险管理的程度。
- 了解并同意主体的风险容量。
- 复核主体的风险投资，并将其同主体的风险容量进行比较。
- 知晓重大风险，以及管理者是否已做出恰当的应对。

1.2.5 战略形成

我们的模型认为，应在全球市场和相关监管框架的基础上为每个组织建立正式战略。下面是来自 CalPERS（即加利福尼亚雇员退休系统，该系统提供退休和健康福利）建立战略的简短的例子：

我们的战略计划为我们的组织绘制了蓝图，以满足 140 万成员和雇员的退休和健康福利需要。该计划为我们指引了经营关系和互动关系。我们的经营哲学是一目了然的：我们以客户为本，我们的决策过程始终遵循价值和质量。[18]

1.2.6 高级管理者

该模型的下一个方面涉及高级管理者（即负责工作顺利完成的一线管理者）。公司战略将导致各种目标的生成，以确保组织的成功（即完成整个任务）。高级管理者负责运作企业，并对实现关键的业绩目标（通常被称作关键业绩指标，即 KPIs）负责。COSO ERM 根据这一主题，将高级管理者的核心责任归纳为：

管理者在其职责范围内指导 ERM 要素的应用，以确保其应用与风险容限相一致。从这个意义上讲，存在层级责任，即每位执行者实际上都是其责任范围内的 CEO。[19]

1.2.7 战略实施

管理者负责确保其职员、系统、预算能适用于既定战略的实施。为此，管理者将长期的公司战略分解为更易管理的短期规划，并由员工和相关的工作者来完成。员工实际上是组织的动力来源。授权式的组织允许其员工在工作一线做出决策，并根据顾客和客户的需要灵活应对。关于实施方法，BASEL 在银行经营风险管理框架中列示了高级管理者的责任：

高级管理者应负责实施委员会批准的经营风险管理框架。[20]

1.3　风险管理框架模型：阶段Ⅱ

如前所述，我们已经描述了公司的整体安排。先要制定战略，然后再来实施详细计划的各个方面，从而使员工忙碌起来并富有成效。对此，我们已有了基本的了解。然而，事实上，这种近乎一维的描述需要进一步的层次化和多彩化。为了分离和理解风险，近些年又出现了其他维度。为了体现这一点，我们进一步完善了模型，如图1—2所示。

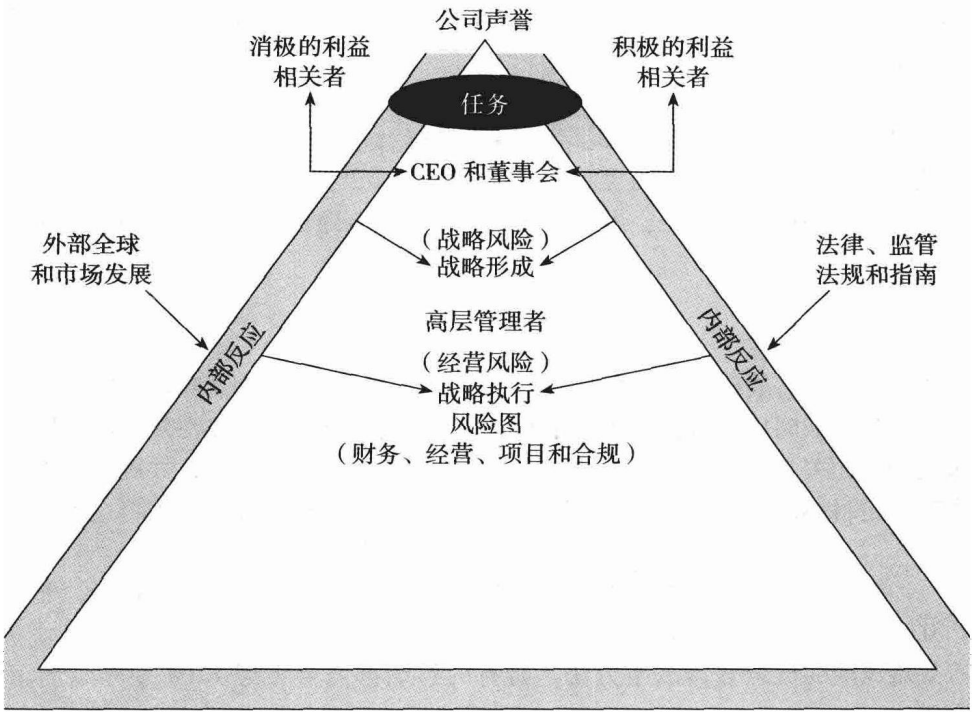

图1—2　风险管理框架模型：阶段Ⅱ

接下来，将描述该模型各个新的部分。

1.3.1　积极的利益相关者

近年来，我们逐渐接受了公司利益相关者的角色。积极的利益相关者对组织有直接的影响。在股份制公司中，积极的利益相关者包括股东，其可以投票决定董事会成员及其薪酬问题。此外，投资者、贷款人、同行、合伙人、银行、雇员以及其他方也都对组织有着重要的影响。类似地，机构投资者在许多大企业中因持有大量有投票权的股份而扮演着重要的角色。而公共部门组织则会受到公众的共同监督，以保证其良好的运作。在风险管理中，澳大利亚和新西兰的风险管理准则将利益相关者描述为：

受决策、活动或风险影响的人或组织，以及认为其自身会受决策、活动或风险影响的人或组织。[21]

1.3.2 消极的利益相关者

不与具体企业直接产生相互影响的利益相关者，被称作消极的利益相关者。此类利益相关者正越来越多。关心大型组织的地方社区、传媒、环境组织以及关心大型组织行为的人们对董事会都没有显著的影响，但其可对组织在众人眼中的整体形象发挥综合影响力并形成组织在他人眼中的整体形象。对于运作糟糕或没有充分评估其影响的企业来说，这些压力集团正影响着企业。对此，澳大利亚和新西兰的风险管理准则指出：

在风险管理过程的各个步骤，沟通和咨询都是重要的考虑因素。这涉及努力以咨询的方式与利益相关者展开对话，而不只是从决策者到其他利益相关者的单向信息流动。[22]

围绕着公司的社会责任，出现了新的主题。该主题将提升所有类型利益相关者的重要性。

1.3.3 战略风险

我们的模型将战略风险植根于公司的日程表。战略风险即意味着预定的目标可能不会实现。战略风险包括市场变化的风险、没有遵循各种法律法规的风险以及没有满足利益相关者需要的风险。公司战略应考虑这些分散的风险，并确保风险是以能实现既定目标的方式被解决的。澳大利亚和新西兰的风险管理准则将这种关系描述为：

能够有效（效果和效率）进行风险管理的组织更易于实现目标，并且其实现目标的总成本通常较低。[23]

战略风险的概念强调战略方法。所有的组织都需要考虑 ERM 中列示的下列问题：[24]

- 协调风险容量和战略。
- 加强风险应对决策。
- 降低经营意外和损失。
- 识别和管理贯穿企业的风险。
- 提供对多种风险的整体应对。
- 抓住机会。
- 改善资本配置。

各种类型的组织所面临的诸多重大风险都是无法由保险公司来承担的，如蔓延全球的恐怖主义、技术的快速更新以及优秀职员的可获得性。为了实现组织持续经营的目标，许多组织都将上述风险诉诸于内部保险，并使用良好的风险管理系统。回到 COSO ERM 上来，有些事项会影响组织，这些事项可被细分为如下外部因素