公司治理〃内部控制前沿译丛

企业风险管理——整合框架

（美） COSO 制定发布

方红星　　王　宏　译

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

大 连

制定发布机构简介

COSO是 Treadway委员会（Treadway Commission，即反欺诈财务报告全国委员会（National Commission on Fraudulent Financial Reporting ），通常根据其首任主席的姓名而称为 Treadway委员会）的发起组织委员会（ Committee of Sponsoring Organizations ）的简称。 Treadway委员会由美国注册会计师协会（ AICPA）、美国会计学会（ AAA）、国际财务经理协会（ FEI）、内部审计师协会（ IIA ）和管理会计师协会（IMA）等 5 个组织于 1985 年发起成立。 1987 年， Treadway委员会发布一份报告，建议其发起组织共同协作，整合各种内部控制的概念和定义。 1992 年， COSO发布了著名的《内部控制——整合框架》（ 1994 年作出局部修订），成为内部控制领域最为权威的文献之一。 2003年 7 月， COSO发布了《企业风险管理——整合框架（征求意见稿）》，经过一年多的意见反馈、研究和修改， 2004 年 9 月发布了最终的文本。本书就是按照 2004 年 9 月正式发布的文本进行翻译的。

译者简介

方红星，东北财经大学会计学院教授，博士，兼任东北财经大学出版社社长，编审，东北财经大学内部控制与风险管理研究中心研究员，三友会计研究所所长。主要学术兼职有财政部会计准则委员会咨询专家、中国会计学会理事、中国成本研究会理事、中国注册会计师审计准则组成员、中国会计学会财务成本分会常务理事及多家学术期刊编委。

王宏，西南财经大学会计学院博士研究生，现就职于财政部会计司综合处，近年来主要致力于内部会计控制等方面的理论和政策研究。

中文版前言

在内部控制和风险管理的演进过程之中，COSO 的突出贡献是举世公认的。它在1992年所发布的、并于 1994年作出局部修正的《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 7月，COSO 发布了《企业风险管理——整合框架》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的情况。诚然，企业风险管理整合框架并没有立即取代内部控制整合框架，但是它涵盖和拓展了后者。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，正式的最终文本发布之后，由于著作权保护和其他方面的原因，在国内很难取得该框架最终定稿的版本。而许多学者继续按照征求意见稿来进行转述、介绍和研究，已经显得不合适了。为此，我们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，我国也概莫能外。我国的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急迫。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的国际权威文献，无疑具有十分突出的理论价值和现实意义。

本书是框架的上卷，即内容提要和基本框架部分。书稿的翻译工作由东北财经大学方红星教授和财政部会计司王宏博士共同完成，译稿由方红星审校。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的高鹏、孙冰洁编辑对书稿的仔细审读。在 2005年 7月下旬在北京召开的“企业内部控制指引研讨会”上，财政部会计司刘玉廷司长、高一斌副司长、舒惠好处长、郜进兴处长、中国会计学会副秘书长周守华教授、东北财经大学刘明辉教授、西南财经大学赵德武教授、南京大学杨雄胜教授、清华大学于增彪教授等领导和专家对本书的翻译给予了肯定和关注，并提出了一些有益的指导和建议，在此谨致谢忱！

由于翻译这类框架文件本身就极具挑战性，加之时间紧迫和译者水平有限，书中错误和疏漏在所难免，恳请业内专家和广大读者不吝指正（接受批评、建议的电子信箱为 hxfang@dufe.edu.cn）！

译　者

2005年 7月

The Committee of Sponsoring Organizations of the Treadway Commission

企业风险管理——整合框架

内容摘要

基本框架

2004年 **9** 月

Treadway 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 有限责任合伙公司

James W. DeLoach
执行总裁， Protiviti 有限公司

John P. Jessup
副总裁兼司库，杜邦（ E. I. duPont de Nemours）公司

Mark S. Beasley
教授，北卡罗莱纳州立大学（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**）

作　者

主要撰稿人

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

序

十几年前， Treadway委员会的发起组织委员会（ **Committee of Sponsoring Organizations of the Treadway Commission**，以下简称“ **COSO** ”）发布了《内部控制——整合框架》 ，以帮助企业和其他主体评估和增进它们的内部控制制度。这份框架此后被纳入政策、规则和法规之中，并被数千家企业用来对它们为实现既定目标所采取的行动加以更好的控制。

近年来重点关注的焦点集中在风险管理上，人们越来越清楚地认识到需要一个强有力的框架以便有效地识别、评估和控制风险。 2001 年， COSO 开展了一个项目，委托普华永道（ PricewaterhouseCoopers）开发一个对于管理当局评价和改进他们所在组织的企业风险管理的简便易行的框架。

正是在开发这个框架的期间，发生了一系列令人瞩目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而遭受了巨大的损失。随之而来的便是对采用新的法律、法规和上市准则来加强公司治理和风险管理的呼吁。对一个提供关键原则和概念、共同的语言以及明晰的方向和指南的企业风险管理框架的需要变得尤为迫切。 COSO 相信这份《企业风险管理——整合框架》 满足了这个需要，并希望它能被企业和其他组织乃至所有的利益相关者和有关各方所广泛认同。

美国的做法之一是 2002 年的《萨班斯—奥克斯利法案》（ Sarbanes-Oxley Act，简称 SOX 法案），其他国家也已经通过或正在考虑类似的立法。这部法律扩充了长期持续的对公众公司保持内部控制制度的规定，要求管理当局证实、并由独立审计师鉴证这些制度的有效性。仍在继续接受时间考验的 《内部控制——整合框架》 ，成为满足这类报告要求的被广泛认可的准则。

这份《企业风险管理——整合框架》 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。尽管它并不打算、也的确没有取代内部控制框架，但是它将内部控制框架纳入其中，公司不仅可以借助这个企业风险管理框架来满足它们内部控制的需要，还可以借此转向一个更加全面的风险管理过程。

管理当局所面临的最为重要的挑战之一是确定所在的主体在为创造价值而奋斗的同时，准备承受和实际承受了多大的风险。这份报告将更好地帮助他们去迎接这种挑战。

John J. Flaherty
COSO 主席

Tony Maki
COSO 咨询委员会主席

目　录

The Committee of Sponsoring Organizations of the Treadway Commission

企业风险管理——整合框架

内容摘要

基本框架

内容摘要

企业风险管理的基础性前提是每一个主体的存在都是为它的利益相关者提供价值。所有的主体都面临不确定性，管理当局所面临的挑战就是在为增加利益相关者价值而奋斗的同时，要确定承受多大的不确定性。不确定性可能会破坏或增加价值，因而它既代表风险，也代表机会。企业风险管理使管理当局能够有效地应对不确定性以及由此带来的风险和机会，增进创造价值的能力。

当管理当局通过制订战略和目标，力求实现增长和报酬目标以及相关的风险之间的最优平衡，并且在追求所在主体的目标的过程中高效率和有效地调配资源时，价值得以最大化。企业风险管理包括：

- 协调风险容量（ **risk appetite**）[①] 与战略 ——管理当局在评价备选的战略、设定相关目标和建立相关风险的管理机制的过程中，需要考虑所在主体的风险容量。
- 增进风险应对决策 ——企业风险管理为识别和在备选的风险应对——风险回避、降低、分担和承受——之间进行选择提供了严密性。
- 抑减经营意外和损失 ——主体识别潜在事项和实施应对的能力得以增强，抑减了意外情况以及由此带来的成本或损失。
- 识别和管理多重的和贯穿于企业的风险 ——每一家企业都面临影响组织的不同部分的一系列风险，企业风险管理有助于有效地应对交互影响，以及整合式地应对多重风险。
- 抓住机会 ——通过考虑全面范围内的潜在事项，促使管理当局识别并积极地实现机会。
- 改善资本调配 ——获取强有力的风险信息，使得管理当局能够有效地评估总体资本需求，并改进资本配置。

企业风险管理所固有的这些能力帮助管理当局实现所在主体的业绩和赢利目标，防止资源损失。企业风险管理有助于确保有效的报告以及符合法律和法规，还有助于避免对主体声誉的损害以及由此带来的后果。总之，企业风险管理不仅帮助一个主体到达期望的目的地，还有助于避开前进途中的隐患和意外。

事项——风险与机会

事项可能会带来负面的影响，也可能会带来正面的影响，抑或二者兼而有之。带来负面影响的事项代表风险，它会妨碍价值创造或者破坏现有价值。带来正面影响的事项可能会抵消负面影响，或者说代表机会。机会是一个事项将会发生并对目标——支持价值创造或保持——的实现产生正面影响的可能性。管理当局把机会反馈到战略或目标制订过程中，以便制订计划去抓住机会。

[①] 也有人将其翻译为“ 风险偏好 ”、“ 风险需求 ”、“ 风险承受能力 ”等——译者注。

所定义的企业风险管理

企业风险管理处理影响价值创造或保持的风险和机会，定义如下：

企业风险管理是一个过程，它由一个主体的董事会、管理当局和其他人员实施，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，管理风险以使其在该主体的风险容量之内，并为主体目标的实现提供合理保证。

这个定义反映了几个基本概念。企业风险管理是：

- 一个过程，它持续地流动于主体之内；
- 由组织中各个层级的人员实施；
- 应用于战略制订；
- 贯穿于企业，在各个层级和单元应用，还包括采取主体层级的风险组合观；
- 旨在识别一旦发生将会影响主体的潜在事项，并把风险控制在风险容量以内；
- 能够向一个主体的管理当局和董事会提供合理保证；
- 力求实现一个或多个不同类型但相互交叉的目标。

这个定义比较宽泛。它抓住了对于公司和其他组织如何管理风险至关重要的关键概念，为不同组织形式、行业和部门的应用提供了基础。它直接关注特定主体既定目标的实现，并为界定企业风险管理的有效性提供了依据。

目标的实现

在主体既定的使命或愿景（ vision）[①]范围内，管理当局制订战略目标、选择战略，并在企业内自上而下设定相应的目标。企业风险管理框架力求实现主体的以下四种类型的目标：

- 战略 （strategic）目标——高层次目标，与使命相关联并支撑其使命；
- 经营 （operations）目标——有效和高效率地利用其资源；
- 报告 （reporting）目标——报告的可靠性；
- 合规 （compliance）目标——符合适用的法律和法规。

对主体目标的这种分类可以使我们关注企业风险管理的不同侧面。这些各不相同但却相互交叉的类别——一个特定的目标可以归入多个类别，反映了主体的不同需要，而且可能会成为不同管理人员的直接责任。这个分类还有助于区分从每一类目标中能够期望的是什么。一些主体采用的另一类目标——保护资源也包含在上述类别之内。

[①] 也有人将其翻译为“ 远景 ”、“ 远景规划 ”、“ 长远构想 ”等——译者注。

因为有关报告的可靠性和符合法律、法规的目标在主体的控制范围之内，所以可以期望企业风险管理为实现这些目标提供合理保证。但是，战略目标和经营目标的实现取决于并不一定总在主体控制范围之内的外部事项，对于这些目标而言，企业风险管理能够合理地保证管理当局和起监督作用的董事会及时地了解主体朝着实现目标前进的程度。

企业风险管理的构成要素

企业风险管理包括八个相互关联的构成要素。它们来源于管理当局经营企业的方式，并与管理过程整合在一起。这些构成要素是：

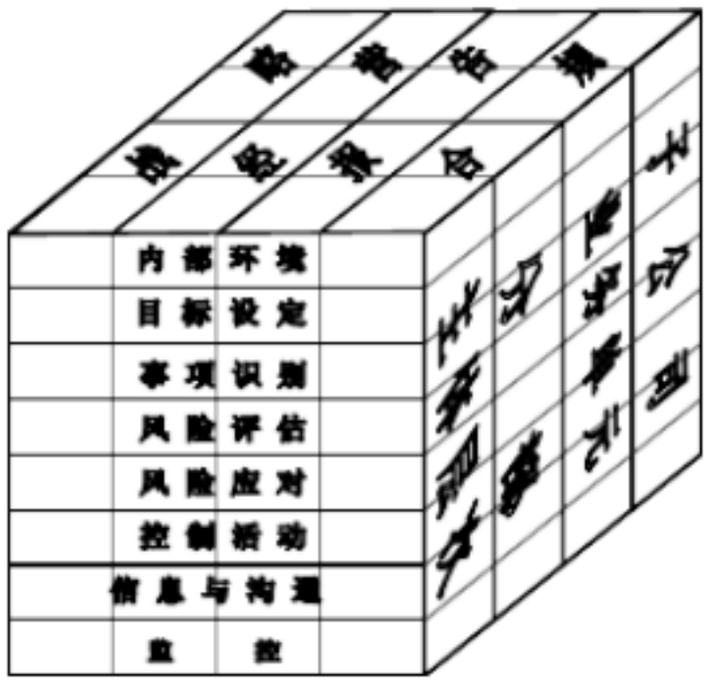
- 内部环境 ——内部环境包含组织的基调，它为主体内的人员如何认识和对待风险设定了基础，包括风险管理理念和风险容量、诚信和道德价值观，以及他们所处的经营环境。
- 目标设定 ——必须先有目标，管理当局才能识别影响目标实现的潜在事项。企业风险管理确保管理当局采取适当的程序去设定目标，确保所选定的目标支持和切合该主体的使命，并且与它的风险容量相符。
- 事项识别 ——必须识别影响主体目标实现的内部和外部事项，区分风险和机会。机会被反馈到管理当局的战略或目标制订过程中。
- 风险评估 ——通过考虑风险的可能性和影响来对其加以分析，并以此作为决定如何进行管理的依据。风险评估应立足于固有风险和剩余风险。
- 风险应对 ——管理当局选择风险应对——回避、承受、降低或者分担风险——采取一系列行动以便把风险控制在主体的风险容限（ risk tolerance）[①]和风险容量以内。
- 控制活动 ——制订和执行政策与程序以帮助确保风险应对得以有效实施。
- 信息与沟通 ——相关的信息以确保员工履行其职责的方式和时机予以识别、获取和沟通。有效沟通的含义比较广泛，包括信息在主体中的向下、平行和向上流动。
- 监控 ——对企业风险管理进行全面监控，必要时加以修正。监控可以通过持续的管理活动、个别评价或者两者结合来完成。

企业风险管理并不是一个严格的顺次过程，一个构成要素并不是仅仅影响接下来的那个构成要素。它是一个多方向的、反复的过程，在这个过程中几乎每一个构成要素都能够、也的确会影响其他构成要素。

目标与构成要素之间的关系

目标是指一个主体力图实现什么，企业风险管理的构成要素则意味着需要什么来实现它们，二者之间有着直接的关系。这种关系可以通过一个三维矩阵以立方体的形式表示出来。

[①] 也有人将其翻译为“ 风险容忍度 ”、“ 风险承受力 ”等——译者注。



四种类型的目标——战略、经营、报告和合规——用垂直方向的栏表示，八个构成要素用水平方向的行表示，而一个主体内的各个单元则用第三个维度表示。这种表示方式使我们既能够从整体上关注一个主体的企业风险管理，也可以从目标类别、构成要素或主体单元的角度，乃至其中的任何一个分项的角度去加以认识。

有效性

认定一个主体的企业风险管理是否“有效”，是在对八个构成要素是否存在和有效运行进行评估的基础之上所作的判断。因此，构成要素也是判定企业风险管理有效性的标准。构成要素如果存在并且正常运行，那么就可能没有重大缺陷，而风险则可能已经被控制在主体的风险容量范围之内。

如果确定企业风险管理在所有四类目标上都是有效的，那么董事会和管理当局就可以合理保证他们了解主体实现其战略和经营目标、主体的报告可靠以及符合适用的法律和法规的程度。

八个构成要素在每个主体中的运行并不是千篇一律的。例如，在中小规模主体中的应用可能不太正式，不太健全。尽管如此，当八个构成要素存在且正常运行时，小规模主体依然会拥有有效的企业风险管理。

局　限

尽管企业风险管理带来了重要的好处，但是仍然存在着局限。除了前面讨论过的因素之外，局限还导源于下列现实：人类在决策过程中的判断可能有纰漏，有关应对风险和建立控制的决策需要考虑相关的成本和效益，类似简单误差或错误的个人缺失可能会导致故障的发生，控制可能会因为两个或多个人员的串通而被规避，以及管理当局有能力凌驾于企业风险管理决策之上。这些局限使得董事会和管理当局不可能就主体目标的实现形成绝对的保证。

涵盖内部控制

内部控制是企业风险管理不可分割的一部分。这份企业风险管理框架涵盖了内部控制，从而构建了一个更强有力的概念和管理工具。内部控制是在　　《内部控制——整合框架》 中加以定义和描述的。由于该框架经受了时间的考验，并且成为现行规则、法规和法律的基础，因此那份文件对内部控制的定义和框架依然有效。尽管　　《内部控

制——整合框架》 的正文中只有一部分被本框架所引用，但是本框架通过参考的方式把该框架整体融合了进来。

职能与责任

主体中的每个人都对企业风险管理负有一定的责任。首席执行官（ CEO）负有首要责任，并且应当假设其拥有所有权。其他管理人员支持主体的风险管理理念，促使符合其风险容量，并在各自的责任范围内依据风险容限去管理风险。风险官、财务官、内部审计师等通常负有关键的支持责任。主体中的其他人员负责按照既定的指引和规程去实施企业风险管理。董事会对企业风险管理提供重要的监督，并察觉和认同主体的风险容量。很多外部方面，例如顾客、卖主、商业伙伴、外部审计师、监管者和财务分析师常常提供影响企业风险管理的有用信息，但是他们不但不对主体的企业风险管理的有效性承担任何责任，而且也不是它的组成部分。

本报告的结构

本报告分两卷。第一卷包括 “ 基本框架 ” 和本部分 “ 内容摘要 ” 。“ 基本框架 ” 给企业风险管理下定义，并讲述原则和概念，为企业和其他组织中的各级管理人员提供用来评价和增进企业风险管理有效性的指导。 “ 内容提要 ” 是一个针对首席执行官、其他高级管理人员、董事会成员和监管者的高度概括。第二卷 《应用技术》（Application Techniques），讲解在应用本框架各个要素的过程中有用的技术。

本报告的使用

根据本报告的建议所可能采取的行动，取决于相关方面的地位和职责：

- 董事会 ——董事会应当与高级管理人员讨论主体企业风险管理的现状，并提供必要的监督。董事会应当确信知悉最重大的风险，以及管理当局正在采取的行动和如何确保有效的企业风险管理。董事会应当考虑寻求内部审计师、外部审计师和其他方面的参与。
- 高层管理当局 ——本项研究建议首席执行官评估组织的企业风险管理能力。方法之一是，首席执行官把业务单元（ business unit）领导和关键职能机构人员召集到一起，讨论对企业风险管理能力和有效性的初步评价。不管采取什么方式，初步评估应该确定是否需要以及如何进行更广泛、更深入的评价。
- 主体中的其他人员 ——管理人员和其他人员应该考虑如何根据本框架去履行他们的职责，并与更高层的人员讨论有关加强企业风险管理的看法。内部审计师应该考虑他们关注企业风险管理的范围。
- 监管者 ——本框架能增进有关企业风险管理的共识，包括它能干什么，以及它的局限。监管者在对他们所监管的主体采用规则或指南等形式设定期望，或进行检查时，可以参考本框架。
- 专业组织 ——为财务管理、审计和相关领域提供指南的规则制定机构和其他专业组织应该对照本框架去考虑它们的准则和指南。消除概念和术语方面的差别，对所有各方都有好处。

- 教育机构 ——本框架可以作为学术研究和分析的对象，以便探讨在哪些方面还能作进一步的改进。假设本报告能够被普遍接受的话，它的概念和术语应该设法进入大学的课程之中。

有了这个共同理解的基础，所有各方将能够用同一种语言讲话，更有效地进行沟通。企业的执行官将能够对照一套标准去评估他们公司的企业风险管理过程，强化这个过程从而使他们的企业朝着既定的目标迈进。将来的研究可以建立在一个既定的基础之上。立法者和监管者将能够获得对企业风险管理的更深入的理解，包括它的好处和局限。如果所有各方都利用共同的企业风险管理框架，这些好处都将实现。

企业风险管理——整合框架

内容摘要

基本框架

1 定义

【本章摘要】所有的主体都面临不确定性，对于管理当局的挑战在于确定在追求增加利益相关者价值的同时，准备承受多少不确定性。企业风险管理使管理当局能够识别、评估和管理面对不确定性的风险，它对于价值创造和保持而言是必不可少的。企业风险管理是一个过程，它由一个主体的董事会、管理当局和其他人员实施，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，管理风险以使其在该主体的风险容量之内，并为主体目标的实现提供合理保证。它包括八个相互关联的构成要素，它们与管理当局经营企业的方式密不可分。这些构成要素联系起来，成为确定企业风险管理是否有效的标准。

本框架的一个关键目标是帮助企业和其他主体的管理当局在实现主体目标的过程中更好地处理风险。但是企业风险管理有许多不同的称谓和解释，难以形成共同的理解，因而对于不同的人而言意味着不同的含义。因此，一个重要的目的在于把各种不同的风险管理概念整合到一个框架之中，在这个框架中构建一个共同的定义，辨别构成要素，并讲述关键概念。这个框架容纳大多数观点，为各个主体评估和增进企业风险管理、为规则制定团体和教育机构的未来行动提供一个出发点。

不确定性与价值

企业风险管理的一个基本前提是每一个主体，不管是营利性的、非营利性的，还是政府机构，存在的目的都是为它的利益相关者提供价值。所有的主体都面临不确定性，对于管理当局的挑战在于确定在追求增加利益相关者价值的同时，准备承受多少不确定性。不确定性潜藏着对价值的破坏或增进，既代表风险，也代表机会。企业风险管理使管理当局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。

在企业经营所处的环境中，诸如全球化、技术、重组、变化中的市场、竞争和管制等因素都会导致不确定性。不确定性来源于不能准确地确定事项发生的可能性以及所带来的影响。不确定性也是主体的战略选择所带来和导致的。举例来说，一个主体采取基于向其他国家拓展业务的增长战略。所选择的这个战略带来了与该国政治环境的稳定性、资源、市场、渠道、劳动力技能和成本相关的风险和机会。

从战略制订到企业的日常经营，在所有的活动中，管理当局的决策都会创造、保持或破坏价值。通过把资源，包括人、资本、技术和品牌，调配到能够产生比过去更多的利益的地方，就会发生价值创造。当创造的价值通过更高的产品质量、生产能力和顾客满意度以及其他方式得以维持时，就会发生价值保持。当由于糟糕的战略或执行导致这些目标不能达成时，价值就会被破坏。决策中伴生着对风险和机会的认识，要求管理当局考虑有关内部和外部环境的信息，调配宝贵的资源，并针对变化的环境重新校准行动。

当管理当局制订战略和目标，去追求增长和报酬目的以及相关的风险之间的最优平衡，并且为了实现主体的目标而高效率和有效地配置资源时，价值得以最大化。企业风险管理包括：

- 协调风险容量与战略　——管理当局首先要在评价备选战略的过程中考虑主体的风险容量，然后在设定与选定的战略相协调的目标的过程中，以及在构建管理相关风险的机制的过程中，也要考虑主体的风险容量。例如，一家制药公司与其品牌价值相关的风险容量较低。因此，为了保护它的品牌，它坚持了大量的规程以确保产品的安全性，并且经常性地投入巨额的资源用于早期的研究与开发以支持品牌价值创造。
- 增进风险应对决策　——企业风险管理为识别和在备选的风险应对——风险回避、降低、分担和承受——之间进行选择提供了严密性。例如，一家利用公司自有和运营的车辆的公司的管理当局认识到在其运送过程中存在的风险，包括车辆损坏和人身伤害成本。可能的选择包括通过有效的司机招聘和培训来降低风险，通过外包运送业务来回避风险，通过保险来分担风险，或者简单地承担风险。企业风险管理为这些决策提供方法和技巧。
- 抑减经营意外和损失　——主体增强了识别潜在事项、评估风险和加以应对的能力，从而降低意外的发生和由此带来的成本或损失。例如，一家制造公司调整生产部件和设备故障率和误差使其接近正常水平。该公司采用多重标准来评估故障的影响，包括维修时间、不能满足客户需要、员工安全以及预定维修与非预定维修的成本，并据此制订维护方案来加以应对。
- 识别和管理贯穿于企业的风险　——每一个主体都面临着影响组织的不同部分的无数风险。管理当局不仅需要管理个别风险，还需要了解相互关联的影响。例如，一家银行面临着贯穿于企业的交易活动的一系列风险，管理当局开发一套信息系统来分析来自其他内部系统的交易和市场数据，它与外部生成的有关信息一起，提供了关于贯穿于所有交易活动的风险的整体看法。这个信息系统可以向下追溯到部门、客户或同行、交易商和交易层次，并针对既定类别的风险容量对风险进行量化。这个系统使该银行能够把先前分隔的数据凑到一起，从而采用整体的和有目的性的看法来更加有效地应对风险。
- 提供对多重风险的整体应对　——经营过程带来许多固有的风险，而企业风险管理能够为管理这些风险提供整体解决方案。例如，一个批发配送商面临着供货过量和不足、薄弱的供货来源以及不必要的高采购价格等方面的风险。管理当局以公司战略、目标和备选的应对为背景识别和评估风险，开发了一套广泛拓展的存货控制系统。这个系统与供货商相整合，共享销售和库存信息，帮助选择战略伙伴，并通过更长期间的进货合同和改进的定价方式，避免缺货和不必要的运送成本。由供应商负责补足库存，从而进一步降低了成本。
- 抓住机会 ——通过考虑潜在事项的各个方面，而不仅仅只是风险，管理当局就能识别代表机会的事项。例如，一家食品公司考虑可能影响其收入持续增长的潜在事项。在评价这些事项的过程中，管理当局认识到该公司主要消费者的健康意识越来越强，正在改变他们的饮食偏好，对公司现有产品的未来需求呈现下降的趋势。在确定应对的过程中，管理当局明确了通过利用其现有的生产能力去开发新产品的方法，从而使公司不仅能保持来自现有消费者的收入，而且还能通过吸引更广泛的消费者来创造额外的收入。
- 改善资本调配 ——获取关于风险的有份量的信息，可以使管理当局有效地评估总体资本需求，并改进资本配置。例如，一家金融机构面临新的监管规则，除

非管理当局更加精确地计算信用和经营风险水平以及相关的资本需求，否则就要提高资本要求量。该公司根据系统开发成本以及追加的资本成本评估了风险，作出了一个有信息支持的决策。利用现有的可修改软件，该机构开发了更加精确的计算工具，避免了寻求额外资本的需要。

企业风险管理固有这些能力，它能帮助管理当局实现主体的业绩和赢利目标，并防止资源的损失。企业风险管理有助于确保有效的报告。它还有助于确保主体符合法律和法规，避免对主体声誉的损害以及由此带来的后果。总之，企业风险管理不仅帮助一个主体到达期望的目的地，还有助于避开前进途中的隐患和意外。

事项——风险与机会

事项是源于内部或外部的影响目标实现的事故或事件。事项可能有负面影响，也可能有正面影响，或者两者兼而有之。带来负面影响的事项代表风险。因此，风险可以定义如下：

风险是一个事项将会发生并给目标实现带来负面影响的可能性。

带有负面影响的事项阻碍价值创造，或者破坏现有的价值。例子包括机器设备故障、火灾和信用损失等。带有负面影响的事项可能起源于看似正面的情况，比如客户对产品的需求超过了生产能力，就会导致不能满足买方的需求，从而损害客户忠诚度和减少未来的订单。

带有正面影响的事项可以消弭负面影响，或带来机会。机会的定义如下：

机会是一个事项将会发生并给目标实现带来正面影响的可能性。

机会支持价值创造或保持。管理当局把机会反馈到战略或目标制订过程中，以便规划行动去抓住机会。

企业风险管理的定义

企业风险管理处理风险和机会，以便创造或保持价值。它的定义如下：

企业风险管理是一个过程，它由一个主体的董事会、管理当局和其他人员实施，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，管理风险以使其在该主体的风险容量之内，并为主体目标的实现提供合理保证。

这个定义反映了几个基本概念。企业风险管理是：

- 一个过程，它持续地流动于主体之内；
- 由组织中各个层级人员实施；
- 应用于战略制订；

- 贯穿于企业，在各个层级和单元应用，还包括采取主体层级的风险组合观；
- 旨在识别一旦发生将会影响主体的潜在事项，并把风险控制在风险容量以内；
- 能够向一个主体的管理当局和董事会提供合理保证；
- 力求实现一个或多个不同类型但相互交叉的目标——它只是实现结果的一种手段，并不是结果本身。

这个定义之所以比较宽泛，是出于几个方面的原因。它抓住了对于公司和其他组织如何管理风险至关重要的关键概念，为不同组织形式、行业和部门的应用提供了基础。它直接关注特定主体既定目标的实现，并为界定将在本章后文中讨论的企业风险管理的有效性提供了依据。以上所列示的基本概念将在下面各个段落中予以讨论。

一个过程

企业风险管理并不是静止的，而是渗透于一个主体的各种活动的持续的或反复的相互影响。这些活动渗透和潜藏于管理当局经营企业的方式之中。

企业风险管理并不像一些观察家所认为的那样是加在主体活动之上的东西。这并不是说有效的企业风险管理不要求进一步的努力，它可能会那样要求。例如，在考虑信用和货币风险时，可能需要进一步努力去开发所需的模型和进行必要的分析和计算。但是，这些企业风险管理机制与主体的经营活动交织在一起，为了基本的经营理由而存在。当这些机制被构建到主体的基础结构之中，并成为企业核心要件的一部分时，企业风险管理就会更加有效。通过建立企业风险管理，一个主体能够直接影响其执行战略和实现使命的能力。

建立企业风险管理对于抑制成本具有重要意义，尤其是在许多公司所面临的高度竞争的市场中更是如此。在现有程序之外增加新的程序会增加成本。通过关注现有的经营业务以及它们对有效的企业风险管理的贡献，并将风险管理整合到基本的经营活动之中，企业就能够避免不必要的程序和成本。而且，把企业风险管理建立在经营业务的基本框架之中的做法，可以帮助管理当局识别新的机会，以便抓住这些机会实现业务增长。

由人员来实施

企业风险管理由一个主体的董事会、管理当局和其他人员实施。它是通过一个组织中的人、通过他们的言行来完成的。人制订主体的使命、战略和目标，并使企业风险管理机制得以落实。

同样，企业风险管理也会影响人的行动。企业风险管理认识到人们并不总是始终如一地理解、沟通和行动。每个人都会给工作场所带来一个独特的背景和技术能力，他们有着不同的需要和偏好。

这些现实影响企业风险管理，同时也受到企业风险管理的影响。每个人都有一个独特的参照点，它影响他或她怎样去识别、评估和应对风险。企业风险管理提供所需的机制，帮助人们在主体目标的背景下去理解风险。人们必须知道他们的责任和权力的局限。因此，在人们的职责和他们履行职责的方式以及主体的战略和目标之间，需要有一个清晰而又密切的联系。

一个组织中的人包括董事会、管理当局和其他人员。尽管董事主要是提供监督，他们也提供指导，审批战略和特定的交易与政策。因此，董事会是企业风险管理的一个重要的要素。

应用于战略制订

一个主体设定其使命或愿景，并制订战略目标，它们是协调和支撑其使命或愿景的高层次的目的。主体为了实现其战略目标而制订战略。它还设定所希望实现的相关目标，上至战略，下至主体的业务单元、分部和流程。

企业风险管理应用于战略制订之中，此时管理当局考虑与备选战略相关的风险。举例来说，一个选择可能是收购其他公司以扩大市场份额。另一个可能是削减采购成本以实现更高的毛利率。这些战略选择中的每一个都会带来许多风险。如果管理当局选择第一个战略，就可能必须向新的和不熟悉的市场拓展，竞争者就可能会占取公司目前市场的份额，或者公司可能没有能力去有效地实施这一战略。对于第二个而言，风险包括必须利用新的技术或供应商，或者建立新的联盟。企业风险管理技术被应用在这个层次上，以帮助管理当局评价和选择该主体的战略和相关的目标。

应用贯穿于企业

在应用企业风险管理时，主体应该考虑其全部活动。企业风险管理考虑组织的各个层级的活动，从诸如战略规划和资源配置等企业层次的活动，到诸如市场营销和人力资源等业务单元的活动，再到诸如生产和新客户信用评价等经营流程。企业风险管理还应用于特殊项目和目前在主体的层级和组织结构图中还没有一个明确位置的新的活动。

企业风险管理要求主体对风险采取组合的观念。这可能要求负责一个业务单元、职能机构、流程或其他活动的每一名管理人员对各自的活动形成一个风险评估。这种评估可能是定量的，也可能是定性的。高层管理当局采用复合的观念看待组织中的所有层级，以便确定该主体的整体风险组合是否与它的风险容量相称。

管理当局从主体层次组合的角度考虑相互关联的风险。主体中单个单元的风险可能在该单元的风险容限范围之内，但是凑到一起可能会超出该主体作为一个整体的风险容量。或者刚好相反，潜在事项在一个业务单元中可能意味着不可接受的风险，但是在其他业务单元中存在抵消效应。相互关联的风险需要识别和发挥作用，以便使整体风险符合主体的风险容量。

风险容量

风险容量是一个主体在追求价值的过程中所愿意承受的广泛意义的风险的数量。它反映了主体的风险管理理念，进而影响主体的文化和经营风格。许多主体采用诸如高、适中或低之类的分类定性地考虑风险容量，而其他主体则采用定量的方法，反映和平衡增长、报酬和风险目标。具有较高风险容量的公司可能愿意把它的大部分资本配置到诸如新兴市场等高风险领域。反过来，具有低风险容量的公司可能会仅仅投资于成熟的、稳定的市场，以便限制其短期的巨额资本损失风险。

风险容量与一个主体的战略直接相关。它在战略制订过程中予以考虑，因为不同的战略会使主体面临不同的风险。企业风险管理可以帮助管理当局选择一个将期望的价值创造与主体的风险容量相协调的战略。

风险容量指导资源配置。管理当局通过考虑主体的风险容量和业务单元为实现投入资源的期望报酬而制订的计划，把资源配置到业务单元和活动之中。管理当局考虑风险容量，使其与组织、人员和流程相适应，并设计必要的基础结构以便有效地应对和监控风险。

风险容限与主体的目标相关。风险容限是相对于实现一项具体目标而言，可以接受的偏离程度，它通常最好采用那些与度量相关目标相同的单位进行度量。

在设定风险容限的过程中，管理当局要考虑相关目标的相对重要性，并使风险容限与风险容量相协调。在风险容限范围内经营有助于确保该主体能保持在它的风险容量之内，进而确保该主体将会实现其目标。

提供合理保证

设计和运行良好的企业风险管理能够为管理当局和董事会提供关于主体目标实现的合理保证。合理保证意味着与未来相关的不确定性和风险，因为没有人能够准确地预知未来。

合理保证并不意味着企业风险管理经常会失败。许多因素独自或一起加强了合理保证的概念。满足多重目标的风险应对的累积影响，以及内部控制多重目的的性质，降低了主体可能不能实现其目标的风险。而且，正常的日常经营活动和组织中各个层级人员职责的发挥，都是以实现主体的目标为目的的。事实上，在一些控制良好主体的典型样本（ cross-section）中，几乎绝大多数都会经常性地被告知朝着它们的战略和经营目标迈进，正常地实现合规目标，并且一贯地编制——期复一期，年复一年——可靠的报告。但是，不可控的事项、差错或者不当的报告偶尔也会发生。换句话说，即使是有效的企业风险管理也会遭遇失败。合理保证并不是绝对保证。

目标的实现

在既定使命的背景下，管理当局制订战略目标，选择战略，并制订贯穿于企业之中的、与战略相协调和相关联的其他目标。尽管许多目标是具体针对特定主体的，但有一些是广泛共通的。例如，在商务和消费者圈子里树立和保持正面的声誉，向利益相关者提供可靠的报告，以及遵循法律和法规开展经营，是几乎所有主体共同的目标。

本框架将主体的目标分成四类：

- 战略 ——与高层次的目的相关，协调并支撑主体的目标；
- 经营 ——与利用主体资源的有效性和效率相关；
- 报告 ——与主体报告的可靠性相关；
- 合规 ——与主体符合适用的法律和法规相关。

对主体目标的这种分类使我们可以关注企业风险管理的不同侧面。这些各不相同却又相互交叉的类别——一个特定的目标可以归入多个类别，反映了不同的主体需要，并且可能成为不同管理者的直接责任。这个分类还有助于区分从每一类目标中能够期望的是什么。

一些主体采用另一类目标，“保护资源”（safeguarding of resources），有时也称为“保护资产”（safeguarding of assets）。广义地看，它们是在防止主体的资产或资源的损失，这些损失可能是由于盗窃、浪费、低效率造成的，也可能就是由于糟糕的经营决策所造成的——例如以过低的价格销售产品，未能留住关键的员工或防止侵犯专利权，或者发生未曾预见到的债务。这些主要是经营目标，尽管保护的某些方面可以归入其他的类别。如果适用于法律或监管要求，这些就会变成合规问题。当与公开的报告联系起来考虑时，通常用的是保护资产的一个狭义的定义，防止或及时侦查未经授权的购买、使用或处置一个主体的资产，该资产可能对财务报表有重大影响。

企业风险管理可望为实现与报告的可靠性、符合法律和法规相关的目标提供合理保证。这些类型的目标的实现处于主体的控制范围之内，并且取决于主体的相关活动完成的好坏。

但是，战略目标（例如取得预定的市场份额）与经营目标（例如成功地引入一条新的产品线）的实现并不总是处在主体的控制范围之内。企业风险管理不能防止糟糕的判断或决策，或可能导致一项经营业务不能达成经营目标的外部事项。但是，它的确能够增大管理当局作出更好的决策的可能性。针对这些目标，企业风险管理能够合理地保证管理当局和起监督作用的董事会及时地了解主体朝着实现目标前进的程度。

企业风险管理的构成要素

企业风险管理包括八个相互关联的构成要素。它们源于管理当局经营企业的方式，并与管理过程整合在一起。这些构成要素是：

- 内部环境——管理当局确立关于风险的理念，并确定风险容量。内部环境为主体中的人们如何看待风险和着手控制确立了基础。所有企业的核心都是人——他们的个人品性，包括诚信、道德价值观和胜任能力——以及经营所处的环境。
- 目标设定——必须先有目标，管理当局才能识别影响它们的实现的潜在事项。企业风险管理确保管理当局采取恰当的程序去设定目标，确保所选定的目标支持和切合该主体的使命，并且与它的风险容量相一致。
- 事项识别——必须识别可能对主体产生影响的潜在事项。事项识别涉及到从影响目标实现的内部或外部原因中识别潜在的事项。它包括区分代表风险的事项和代表机会的事项，以及可能二者兼有的事项。机会被反馈到管理当局的战略或目标制订过程中。
- 风险评估——要对识别的风险进行分析，以便形成确定应该如何对它们进行管理的依据。风险与可能被影响的目标相关联。既要对固有风险进行评估，也要对剩余风险进行评估，评估要考虑到风险的可能性和影响。
- 风险应对——员工识别和评价可能的风险应对，包括回避、承担、降低和分担风险。管理当局选择一系列措施使风险与主体的风险容限和风险容量相协调。
- 控制活动——制订和实施政策与程序以帮助确保管理当局所选择的风险应对得以有效实施。

- 信息与沟通——相关的信息以确保员工履行其职责的方式和时机予以识别、获取和沟通。主体的各个层级都需要借助信息来识别、评估和应对风险。有效沟通的含义比较广泛，包括信息在主体中的向下、平行和向上流动。员工获得有关他们的职能和责任的清晰的沟通。
- 监控——对企业风险管理进行全面监控，必要时加以修正。通过这种方式，它能够动态地反应，根据条件的要求而变化。监控通过持续的管理活动、对企业风险管理的个别评价或者两者相结合来完成。

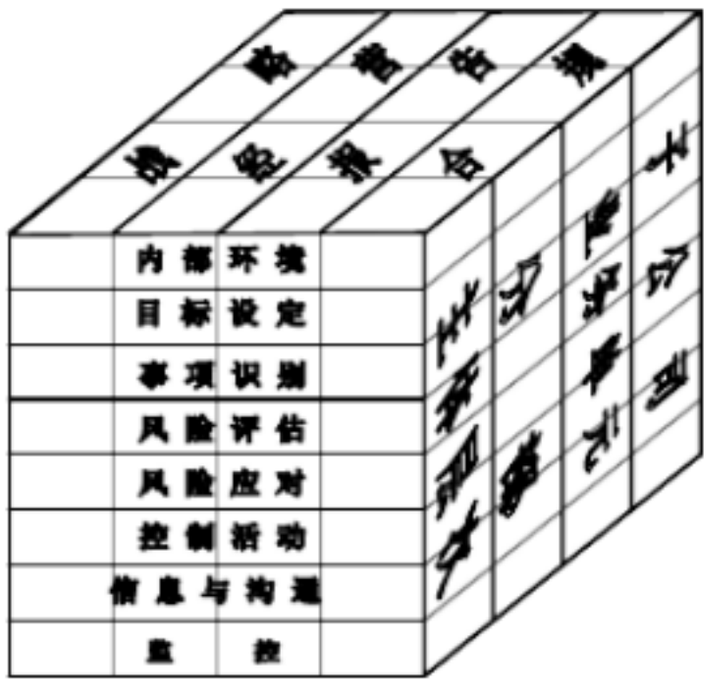
企业风险管理是一个动态的过程。举例来说，风险评估促动风险应对，它可能会影响控制活动，并凸显出考虑信息与沟通的需要或主体的监控活动的必要性。因此，企业风险管理并不只是一个构成要素仅仅影响接下来的那一个的顺次的过程。它是一个多方向的、反复的过程，在这个过程中几乎每一个构成要素都能够并且将会影响另一个要素。

任何两个主体都不可能，也不应该以同样的方式应用企业风险管理。公司和它们的企业风险管理能力和需求由于行业和规模，以及管理理念和文化的不同而大相径庭。因此，尽管所有的主体都应该具备每一个构成要素并有效运行，公司对企业风险管理的应用——包括采用的工具和技巧以及职能与责任的划分——通常会各不相同。

目标与构成要素之间的关系

目标是指一个主体力图实现什么，企业风险管理的构成要素则意味着需要什么来实现它们，二者之间有着直接的关系。这种关系通过一个三维矩阵以立方体的形状体现出来，如专栏 1-1 所示。

专栏 **1-1**



- 四种类型的目标——战略、经营、报告和合规——用垂直方向的栏来表示；
- 八个构成要素用水平方向的行来表示；
- 主体和它的单元用立方体的第三个维度表示。

每个表示构成要素的行“交叉切分”并适用于所有的四类目标。例如，来自内部和外部渠道的财务和非财务数据是信息与沟通这个构成要素的一部分，制订战略、有效地管理经营业务、有效地报告以及确定主体符合适用的法律都需要这些数据。

同样地，来看看不同类型的目标，所有的八个构成要素都和它们中的每一类有关联。以其中的一类——经营的有效性和效率为例，所有的八个要素对于它的实现不仅都适用，而且都很重要。

企业风险管理与整个企业或者它的任何单个的单元相关。这种关系通过第三个维度来体现，它表示子公司、分部和其他业务单元。这样，我们可以着眼于这个矩阵中的任何一个区间。例如，我们可以考察顶部右侧后边的那个区间，它代表一个特定的子公司与合规目标有关的内部环境。

应该认识到四个栏代表的是一个主体目标的类型，而不是这个主体的某个部分或单元的目标。因此，举例来说，当考虑与报告有关的目标类型时，就需要了解关于主体经营的广泛的信息。但是在这种情况下，应该关注的目标类型是这个模型的中部右侧的栏——报告目标，而不是经营目标。

有效性

尽管企业风险管理是一个过程，它的有效性却是在某个时点上的一种状态或情况。确定企业风险管理是否“有效”，是在对八个构成要素是否存在和有效运行的评估的基础之上所作出的判断。因此，构成要素同时也是有效的企业风险管理的判断标准。如果这些构成要素存在且正常运行，那么就可能没有重大缺陷，而风险可能已经被控制在主体的风险容量以内。

如果确定企业风险管理在所有四类目标上都是有效的，那么就意味着董事会和管理当局对下列方面的合理保证：

- 他们了解主体实现其战略目标的程度；
- 他们了解主体实现其经营目标的程度；
- 主体的报告是可靠的；
- 符合适用的法律和法规。

尽管为了使企业风险管理被判定为有效，所有的八个构成要素都必须存在和正常运行——运用在接下来的各章中讲述的原则，但是在构成要素之间可能会存在着某些权衡。因为企业风险管理技术可以服务于许多目的，所运用的与一个构成要素相关的技术，或许能服务于通常代表另一个构成要素的技术的目的。此外，针对特定的风险而言，风险应对的程度可能有所不同，所以具有互补性的风险应对和控制，尽管各自的效果都很有限，但是结合起来可能是令人满意的。

这里所讨论的概念适用于所有的主体，无论其规模如何。尽管一些中小规模的主体在实施这些构成要素时可能与大型主体有所不同，但是它们仍然可能拥有有效的企业风险管理。比起较大的主体而言，在较小的主体中，各个构成要素的方法可能不太正式和不太健全，但是在每一个主体中这些基本的概念都应该存在。

一般把企业当作一个整体来考虑企业风险管理，其中包括考虑它在重要的业务单元中的应用。但是，也会有单独针对一个特定的业务单元去评价企业风险管理的有效性的情况。在这种情况下，为了得出这个单元的企业风险管理有效的结论，所有的八个构成要素在这个单元中必须存在且有效运行。举例来说，由于有一个具有规定特质

的董事会是内部环境的一部分，某个特定业务单元的企业风险管理，只有当该单元拥有一个恰当运行的董事会或类似机构（或者主体层次的董事会对该业务单元进行必要的监督）时，才能被判定为有效。同样地，由于对风险应对这个构成要素的描述采取了风险组合观，要想使企业风险管理被判定为有效，该业务单元也必须采取风险组合观。

涵盖内部控制

内部控制是企业风险管理不可分割的一部分。这份企业风险管理框架涵盖了内部控制，从而构建一个更强有力的概念和管理工具。内部控制是在《内部控制——整合框架》中加以定义和讲述的。因为《内部控制——整合框架》是现行规则、监管和法律的基础，而且经受了时间的检验，因此那份文件中对内部控制的定义和框架依然有效。尽管《内部控制——整合框架》的正文中只有一部分被本框架所引用，但是本框架通过参考的方式把整个《内部控制——整合框架》融合了进来。附录 C 讲述了企业风险管理与内部控制之间的关系。

企业风险管理与管理过程

因为企业风险管理是管理过程的一部分，所以企业风险管理框架的构成要素是在管理当局如何经营企业或其他主体的背景下加以讨论的。但是并不是管理当局所做的每一件事情都是企业风险管理的一部分。管理当局在决策和相关的管理活动中所运用的许多判断，尽管是管理过程的一部分，但是并不是企业风险管理的一部分。例如：

- 确保有一个恰当的目标设定过程是企业风险管理的一个重要的构成要素，但是管理当局所选定的特定目标并不是企业风险管理的一部分。
- 根据对风险的恰当评估去应对风险是企业风险管理的一部分，但是所选定的具体风险应对和主体资源的相应配置却不是。
- 确定和执行控制活动以帮助确保管理当局选择的风险应对得以有效实施是企业风险管理的一部分，但是所选定的特定的控制活动却不是。

总之，企业风险管理包括管理过程中那些保证管理当局作出知情的风险基础决策（informed risk-based decisions）的要素，但是从一系列合适的选项中选定的特定决策并不能决定企业风险管理是否有效。尽管选定的具体目标、风险应对和控制活动与管理当局的判断有关，但是这些选择必须最终把风险降低到一个可以接受的水平——这个水平取决于风险容量，以及有关实现主体目标的合理保证。

2　内部环境

【本章摘要】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、它的风险容量、董事会的监督、主体中人员的诚信、道德价值观和胜任能力，以及管理当局分配权力和职责、组织和开发其员工的方式。

内部环境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。它影响着战略和目标如何制订、经营活动如何组织以及如何识别、评估风险并采取行动。它还影响着控制活动、信息与沟通体系和监控措施的设计与运行。

内部环境受到主体的历史和文化的影响。它包含许多要素，包括主体的道德价值观、员工的胜任能力和开发、管理当局管理风险的理念以及如何分配权力和职责。董事会是内部环境的一个关键部分，它对其他的内部环境要素有重大的影响。

尽管所有要素都很重要，但是对每个要素的强调程度会因主体而异。举例来说，一家员工较少、专注化经营的公司的首席执行官可能就不会制订正式的职责划分和具体的经营政策。但是，这家公司也会有为企业风险管理提供合适基础的内部环境。

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——从战略制订和执行到日常的活动——时如何考虑风险。风险管理理念反映了主体的价值观，影响它的文化和经营风格，并且决定如何应用企业风险管理的构成要素，包括如何识别风险，承担哪些风险，以及如何管理这些风险。

成功地承担了重大风险的公司对企业风险管理的看法，似乎不同于由于在危险的地区创业而面临过严酷的经济或管制后果的公司。尽管有些主体会为了满足外部利益相关者——例如母公司或监管者的需要，而努力实现有效的企业风险管理，但是更常见的是因为管理当局认识到有效的风险管理有助于主体创造和保持价值。

当风险管理理念被很好地确立和理解、并且为员工所信奉时，主体就能有效地识别和管理风险。否则，企业风险管理在各个业务单元、职能机构或部门中的应用就可能会出现不可接受的不平衡状态。但是即使一个主体的理念被很好地确立，在它的各个单元之间仍然会存在文化上的差别，从而导致风险管理应用方面的差异。一些单元的管理者可能准备承担更大的风险，而其他的则更为保守。例如，一个有闯劲的销售职能机构可能会集中关注实现销售，而没有仔细注意对法规的遵循问题，而缔约单元的人员主要集中关注确保符合所有的相关内部和外部政策与法规。孤立地看，这些不同的次级文化都能对主体产生负面影响。但是通过很好的合作，这些单元能够恰当地反映主体的风险管理理念。

企业的风险管理理念实质上反映在管理当局在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。无论管理当局是强调书面的政策、行为准则、业绩指标和例外报告，还是更为非正式地大量通过与关键的管理者面对面的接触来进行运营，至关重要的是管理当局不仅要通过口头、而且还要通过日常的行动来强化这种理念。

风险容量

风险容量是一个主体在追求价值的过程中所愿意承担的广泛意义上的风险的数量。它反映了企业的风险管理理念，进而影响了主体的文化和经营风格。

风险容量在战略制订的过程中加以考虑，来自一项战略的期望报酬应该与主体的风险容量相协调。不同的战略会使主体面临不同程度的风险，应用于战略制订过程的企业风险管理帮助管理当局选择一个与主体的风险容量相一致的战略。

主体运用类似高、适中或低等类别，从质的角度考虑风险容量，或者运用数量化的方法，来反映和平衡增长、报酬和风险方面的目标。

董事会

一个主体的董事会是内部环境的关键部分，它对其要素有着重大影响。董事会对于管理当局的独立性、其成员的经验和才干、对活动参与和审察的程度，以及其行为的适当性都起着重要的作用。其他因素包括提出有关战略、计划和业绩方面的疑难问题和与管理当局进行商讨的程度，以及董事会或审计委员会与内部和外部审计师的交流。

一个积极的和高度参与型的董事会、托管委员会（ board of trustees）或类似的机构，应该具有适当程度的管理、技术和其他专长，以及履行监督职责所需要的思维方式。这对于一个有效的企业风险管理环境至关重要。而且，由于董事会必须准备去质疑和仔细审查管理当局的活动，提出不同的观点，并针对不当行为采取行动，因此董事会必须包含外部董事。

高层管理当局的成员可能带来他们对公司的深入了解，从而成为有效的董事会成员。但是必须有足够数量的独立外部董事，他们不但要提供合理的建议、咨询和指导，而且还要对管理当局形成必要的牵制和制衡。要想使内部环境有效，董事会中的独立外部董事必须至少占多数。

有效的董事会能确保管理当局保持有效的风险管理。尽管一家企业在过去可能没有遭受损失、没有暴露出明显的重大风险，董事会也不能天真地认定带有严重负面后果的事项“ 在这里不会发生 ”。应该认识到，尽管一家公司可能有合理的战略、胜任的员工、合理的经营流程和可靠的技术，但是它和所有的主体一样，对于风险而言都很脆弱，因此也需要有效运行的风险管理。

诚信与道德价值观

主体的战略和目标以及它们得以推行的方式建立在偏好、价值判断和管理风格的基础之上。管理当局的诚信和对道德价值观的要求影响这些转化为行为准则的偏好和判断。因为一个主体的良好声誉是如此有价值，所以行为的准则应该不仅仅只是遵循法律。经营良好的企业的管理者越来越接受这样的观点，那就是道德是值得的，道德行为就是良好的经营。

管理当局的诚信是一个主体活动的所有方面的道德行为的先决条件。企业风险管理的有效性不可能脱离那些创造、管理和监督主体活动的人的诚信和道德价值观。诚信和道德价值观是一个主体内部环境的关键要素，它影响着企业风险管理其他构成要素的设计、管理和监控。

树立道德价值观通常很困难，因为需要考虑多个方面的利益。管理当局的价值观必须平衡企业、员工、供应商、客户、竞争者和公众的利益。平衡这些利益可能是复

杂而令人沮丧的，因为利益通常是互相矛盾的。举例来说，提供一种必需的产品（石油、木材或食品）可能会导致环境方面的关切。

道德行为和管理当局的诚信是公司文化的副产品，公司文化包含道德和行为准则以及它们的沟通和强化方式。正式的政策指明了董事会和管理当局希望发生的情况。公司文化决定着实际发生的情况，以及哪些规则被遵循、扭曲或忽视了。高层管理当局——从 CEO 开始——在确定公司文化方面起着关键作用。作为主体中的居于支配地位的人员， CEO 往往确定了道德基调。

特定的组织因素也会影响出现欺诈性和可疑的财务报告行为的可能性。这些因素可能还会影响道德行为。个人可能会因为主体给了他们这么做的强烈动机或诱惑，而参与不诚实的、非法的或不道德的行为。过分地强调结果，尤其是短期结果，可能会造成一个不恰当的内部环境。仅仅关注短期结果即使在短期也可能有危害。专注于底线——不顾成本的销售收入或利润——通常会引发不希望看到的行动和反应。例如，高压销售策略、谈判的残酷或者对回扣的暗示可能会引发具有即期（以及持久）影响的反应。

参与欺诈性和可疑的财务报告行为以及其他形式的不道德行为的其他动机可能包括高度依赖于所报告的财务或非财务信息——尤其是短期结果——的报酬。

从消除或减少不恰当的动机和诱惑到消除不良行为之间要走一段很长的路。就像所建议的那样，它可以通过从事合理而又有利可图的经营活动来实现。例如，只要业绩目标切合实际，业绩激励——配以适当的控制——就能成为一个有用的管理技术。设定切合实际的目标是一项正确的激励措施，它能降低产生相反作用的压力，以及欺诈性报告的动机。同样地，一个控制良好的报告体系能够起到防止错报业绩诱惑的作用。

可疑行为的另一个原因是忽视。道德价值观不仅必须沟通，而且必须辅以关于是非对错的明确指南。正式的公司行为守则对有效的道德项目十分重要，是它的基础。守则致力于一系列的行为问题，例如诚信与道德、利益冲突、不合法或不恰当的支付以及反竞争的（ anticompetitive）协议等。向上沟通的渠道也很重要，它带来相关信息并使员工感到舒服。

仅仅有书面的行为守则、员工接受和理解的文件和适当的沟通渠道，还不能确保守则被遵守。对违反守则的员工所给予的处罚，鼓励员工报告所怀疑的违反行为的机制，以及针对知情而不报告违反行为的员工的惩戒措施，对于遵守守则而言也很重要。但是如果不能通过高层管理当局的行为和他们所作的表率提供更有效的保证的话，无论道德准则是否包含在书面的守则之中，对道德准则的遵守都没有什么区别。对于是非对错——以及对于风险与控制，员工可能会形成与高层管理当局所表现出来的一样的态度。管理当局的行为所传达的信息很快就会被包含到公司文化之中。而且，有关 CEO 在面临一个艰难的经营决策时从道德的角度讲“ 做了正确的事情 ”的认识，能够在整个主体中传达一个强有力的信息。

对胜任能力的要求

胜任能力反映实现规定的任务所需要的知识和技能。管理当局通过在主体的战略和目标与它们的执行和实现计划之间进行权衡，来决定这些任务应该完成到什么程

度。通常会存在能力与成本之间的权衡，比如说，没有必要去雇用一个电气工程师来更换灯泡。

管理当局明确特定岗位的胜任能力水平，并把这些水平转换成所需的知识和技能。而这些必要的知识和技能可能又取决于个人的智力、培训和经验。在开发知识和技能水平的过程中所考虑的因素包括一个具体岗位所运用判断的性质和程度。通常会在监督的范围和所需的胜任能力水平之间作出权衡。

组织结构

一个主体的组织结构提供了计划、执行、控制和监督其活动的框架。相关的组织结构包括确定权力与责任的关键界区，以及确立恰当的报告途径。举例来说，内部审计职能机构的结构设计应该致力于实现组织的目标，并且允许不受限制地与高层管理当局和董事会的审计委员会接触，而且首席审计官应当向组织中能保证内部审计活动实现其职责的层级报告工作。

主体建立适合其需要的组织结构。有的是集权型的，有的是分权型的。有的有着直接报告关系，而其他的则更接近于矩阵型组织。一些主体按照行业或产品线、按照地理位置或者按照特定的配送或营销网络来进行组织。而其他的主体，包括很多州和地方政府单位以及非营利机构，则按照职能进行组织。

一个主体的组织结构的适当性部分地取决于它的规模和所从事活动的性质。有着正式的报告途径和职责的高度结构化的组织，可能适合于拥有很多经营分部、包括外国业务的大型主体。然而，在一家小公司中，这种结构可能会阻碍必要的信息流动。不管采取什么样的结构，主体的组织方式都应该确保有效的企业风险管理，并采取行动以便实现其目标。

权力和职责的分配

权力和职责的分配涉及到个人和团队被授权并鼓励发挥主动性去指出问题和解决问题的程度，以及对他们的权力的限制。它包括确立报告关系和授权规程，以及描述恰当经营活动的政策，关键人员的知识和经验，和为履行职责而赋予的资源。

一些主体将权力下放，以便使决策更接近于一线的人员。公司可以采取这种方式而变得更具市场驱动的特点，或者更关注质量——或许是消除缺陷、缩短周转时间或者提高客户满意度。通常通过将权力与受托责任（ accountability）相结合来鼓励个人在限定的范围内发挥主动性。权力的委派意味着将特定经营决策的核心控制权交给较低的层级——给那些更靠近日常经营业务的人员。这可能包括授权以折扣价格销售产品，商谈长期供货合同、许可或专利，或者参加联盟或合营企业。

一个关键的挑战是仅仅针对实现目标所需要的范围来进行授权。这意味着确保决策是基于合理的风险识别和评估活动，包括在确定接受何种风险以及如何对它们加以管理的过程中，估计风险的大小和权衡潜在的损失与收益。

另一个挑战是确保所有的人员都了解主体的目标。每个人都知道他们的行为彼此之间有什么关联和对实现目标有什么作用，是至关重要的。

增加授权有时候有意伴随着组织结构的简化或“扁平化”，或者是其结果。为激发创造性、发挥主动性和加快反应速度而开展的有意识的组织变革，能够提高竞争力和客户满意度。这种增加授权可能会带来对更高的员工胜任能力水平以及更大的受托

责任的隐含要求。它还要求管理当局采用有效的程序对结果进行监控，从而使决策能够根据需要被否决或接受。有了更好的、市场驱动的决策，授权能够增加非期望或非预期决策的数量。例如，如果一个区域销售经理决定授权在零售价的基础上折让 35% 来进行销售，以证实目前 45%的折扣能够获取市场份额，管理当局可能需要了解情况才能否决或者接受让这种决策进行下去。

内部环境极大地受到个人对他们将要承担责任的认识程度的影响。对于首席执行官而言，也是如此，他在董事会的监督下对主体内部的所有活动负有终极责任。

与有效的企业风险管理密不可分的各个方面的职能与责任的其他相关原则，将在“职能与责任”那一章中展开讲述。

人力资源准则

包括雇用、定位、培训、评价、咨询、晋升、付酬和采取补偿措施在内的人力资源业务向员工传达着有关诚信、道德行为和胜任能力的期望水平方面的信息。例如，强调教育背景、前期工作经验、过去的成就和有关诚信和道德行为的证据，以便雇用资质最好的个人的准则，表明了一个主体对胜任和可信任人员的承诺。当招录活动中包括正式的、深入的招聘面试和有关该主体的历史、文化和经营风格方面的培训时，也是如此。

培训政策能够通过对未来职能与责任的沟通，以及包含诸如培训学校和研习班、模拟案例研究和扮演角色练习等活动，来加强业绩和行为的期望水平。根据定期业绩评价所进行的调换与晋升，反映了主体对于提升合格员工的承诺。包括分红激励在内的竞争性的报酬计划能够起到鼓励和强化突出业绩的作用——尽管奖金制度应该严密并且有效地控制，以避免对报告结果的不实呈报产生不当的诱惑。惩戒行动所传递的信息则是对期望行为的偏离将不会得到宽宥。

随着贯穿于主体之中的问题和风险的变化和愈加复杂——部分原因在于急剧变革的技术和日益激烈的竞争，很有必要把员工武装起来以应对新的挑战。教育和培训，不管是课堂讲授、自学还是在职培训，都必须有助于个人跟上环境变革的步伐并能有效地应对。雇用胜任的人员和提供一次性培训是不够的。教育过程是持续的。

影　响

一个主体内部环境的重要性和它对企业风险管理的其他构成要素所能产生的正面或负面影响，怎么强调都不过分。一个无效的内部环境的影响会很广泛，可能会导致财务损失、损害公众形象，或经营失败。

一般认为某能源公司有着有效的企业风险管理，因为它有强有力而受人尊敬的高层管理者、声望卓著的董事会、富有创新意识的战略、设计良好的信息系统和控制活动、描述风险和控制职能的广泛的政策手册，以及全面的调整和监督途径。但是，它的内部环境却有重大缺陷。管理当局参与了十分可疑的经营业务，而董事会却视而不见。这家公司被发现曾经误报财务成果，损害了股东信心，遭遇了偿债危机，毁灭了主体的价值。最终这家公司陷入了历史上最大的破产案之一。

高层管理当局对有效企业风险管理的态度和关注必须明确而清晰，并渗透到组织之中。光说得正确是不够的。那种“按我说的去做，而不是按我做的去做”的态度，只会带来一个无效的环境。

3　目标设定

【本章摘要】设定战略层次的目标，为经营、报告和合规目标奠定了基础。每一个主体都面临来自外部和内部的一系列风险，确定目标是有效的事项识别、风险评估和风险应对的前提。目标与主体的风险容量相协调，后者决定了主体的风险容限水平。

目标设定是事项识别、风险评估和风险应对的前提。在管理当局识别和评估实现目标的风险并采取行动来管理风险之前，首先必须有目标。

战略目标

一个主体的使命从广义上确定了该主体希望实现什么。不管采用什么术语，诸如“使命”（mission）、“愿景”（vision）或是“目的”（purpose），重要的是管理当局——在董事会的监督下——明确确定了主体存在的广泛意义上的原因。由此，管理当局设定战略目标，进行战略规划，并为组织确定相关的经营、合规和报告目标。尽管一个主体的使命和战略目标一般是稳定的，但是它的战略和许多相关的目标却更多是动态的，并且会随着内部和外部条件的变化而调整。随着它们的变化，战略和相关的目标会重新调整以便与战略目标相协调。

战略目标是高层次的目标，它与主体的使命　/愿景相协调，并支持后者。战略目标反映了管理当局就主体如何努力为它的利益相关者创造价值所作出的选择。

在考虑实现战略目标的备选方式时，管理当局要识别与一系列战略选择相关联的风险，并考虑它们的影响。下文和后续章节讨论的各种事项识别和风险评估技术，可以应用到战略制订过程中。通过这种方式，企业风险管理技术被应用到制订战略和目标之中。

相关目标

相对于主体的所有活动而言，制订支持选定的战略并与之相协调的正确的目标是成功的关键。通过首先关注战略目标和战略，主体可能建立主体层次上的相关目标，它们的实现将会创造和保持价值。主体层次的目标与更多的具体目标相关联和整合，这些具体目标贯穿于整个组织，细化为针对诸如销售、生产和工程设计等各项活动和基础职能机构所确立的次级目标。

通过设定主体和活动层次的目标，主体能够识别关键成功因素（critical success factors）。要想达到目的，就必须正确处理好这些关键的事情。关键成功因素存在于主体、业务单元、职能机构、部门或分部之中。通过设定目标，管理当局能够根据对关键成功因素的关注来确定业绩的计量标准。

如果目标与以前的活动和业绩相一致，各项活动之间的联系就是已知的。但是，如果目标与主体过去的活动相背离，管理当局就必须指明这种联系或者应对更大的风险。在这种情况下，就更需要与新的方向相一致的业务单元目标或次级目标。

目标需要得到充分了解和可计量。企业风险管理要求各个层级的人员根据各自影响范围的不同对主体的目标有必要的了解。所有员工都必须对要实现什么有共同的认识，并且有办法去计量实现的情况。

相关目标的类别

尽管不同主体的目标各不相同，但是大致上可以分成以下几类：

- 经营目标——这些目标与主体经营的有效性和效率有关，包括业绩和赢利目标和保护资源不受损失。它们因管理当局对结构和业绩的选择而异。
- 报告目标——这些目标与报告的可靠性有关。它们包括内部和外部报告，可能涉及到财务和非财务信息。
- 合规目标——这些目标与符合相关法律和法规有关。它们取决于外部因素，在一些情况下对所有主体而言都很类似，而在另一些情况下则在一个行业内有共性。

特定的目标取决于主体所从事的经营业务。例如，一些公司向环境机构提交信息，而公开上市的公司则向证券监管机构申报信息。这些外部施加的要求是通过法律或法规的形式建立的，它们属于报告目标或合规目标，或者像这些例子中的那样两者都是。

相反，经营目标，以及那些内部管理报告目标，更多地建立在偏好、判断和管理风格的基础上。它们在不同的主体之间存在着广泛的区别，因为知情、胜任和诚实的人可能会选择不同的目标。例如，在产品开发方面，一个主体选择去充当早期的改进者，而另一个则选择作为一个快速的跟随者，而再另外的一个则选择迟缓的落伍者。这些选择会影响研究与开发职能机构的结构、技能、人员招录和控制。因此，对所有主体而言都是最优的目标模式是不会有的。

经营目标

经营目标关系到主体经营的有效性和效率。它们包括相关的次级经营目标，其目的在于在推动主体实现其终极目的的过程中提高经营的有效性和效率。

经营目标需要反映主体运营所处的特定的经营、行业和经济环境。例如，经营目标需要与有关质量的竞争压力、缩短将产品投入市场的周转时间或者技术的变革相关。管理当局必须确保这些目标反映了现实和市场需求，并且以有利于进行有意义的业绩计量的方式表达出来。一套与次级目标相关联的清晰的经营目标，对成功而言是至关重要的。经营目标为引导所配置的资源提供了一个焦点，如果一个主体的经营目标不清晰或者构想不完善，它的资源就可能会被误导。

报告目标

可靠的报告为管理当局提供适合其既定目的的准确而完整的信息。它支持管理当局的决策和对主体活动和业绩的监控。这类报告的例子包括市场营销计划的成果、逐日销售快报、生产质量和员工与客户满意度结果。报告还涉及到为对外传播而编制的报告，例如财务报表与附注披露、管理当局的讨论与分析（ MD&A ）以及向监管机构提交的报告。

合规目标

主体从事活动必须符合相关的法律和法规，通常还必须采取具体措施。这些要求可能涉及到市场、定价、税收、环境、员工福利和国际贸易。适用的法律和法规确定了最低的行为准则，主体将其纳入合规目标之中。例如，岗位健康和安全法规导致一家公司将其目标确定为“根据法规包装和标注所有的药品”。在这种情况下，要制订政策和程序来处理沟通项目、现场检查和培训。一个主体的合规记录可能会对它在社会和市场上的声誉产生极大的正面或负面影响。

次级分类

目标的类别是本框架所建立的共同语言的一部分，它有助于理解和沟通。但是，一个主体可能会发现讨论一个或多个目标类别的子集对于针对一个较窄的主题所进行的内部或外部沟通很有用。举例来说，一家公司可能会决定针对报告目标的一部分，比方说对外报告或者仅仅是对外财务报告的企业风险管理的有效性进行沟通。这样做能够使沟通停留在这个企业风险管理框架的范围之内，同时又允许针对各个类别的特定子集进行沟通。

目标的交叉

某一类别中的一项目标可能会与另一类中的一项目标交叉或相互支持。一项目标所归属的类别有时要视情况而定。举例来说，为业务单元的管理当局管理和控制生产活动而提供可靠的信息，可能同时为经营目标和报告目标服务。而且，从这些信息被用来向政府报告环境数据的角度来看，它又为合规目标服务。

一些主体采用另一个目标类别，“保护资源”，有时也称为“保护资产”，它与其他的目标类别有交叉。从广义的角度看，保护资产致力于防止主体的资产或资源由于盗窃、浪费、低效率或者仅仅因为糟糕的经营决策——例如以过低的价格销售产品、未能留住关键员工或未能防止专利侵权或者发生未预见到的债务等——而遭受损失。尽管保护的某些特定方面可以归入其他的类别，但是它们主要是经营目标。如果适用于法律或法规要求，它们又变成合规目标。另一方面，在主体的财务报表中恰当地反映资产损失代表着一项报告目标。

如果与公开的报告联系起来考虑，通常采用保护资产的狭义定义，即致力于防止或及时察觉对主体资产未经授权的采购、使用或出让。为了进一步讨论这类目标，应该参考《内部控制——整合框架》，它包括“向外部各方报告的附录”这个模块。

目标的实现

恰当的目标设定过程是企业风险管理的一个至关重要的构成要素。尽管目标为主体从事活动提供了可计量的基准，但是它们的重要性和优先程度各不相同。因此，虽然一个主体应该合理保证实现特定的目标，但是并不是对所有目标而言都这样。

有效的企业风险管理为主体的报告目标得以实现提供合理保证。同样，必须合理保证合规目标的实现。报告和合规目标的实现更多的是在主体的控制范围之内。也就是说，一旦确定了目标，主体对其从事满足目标所需要的活动的能力具有控制力。

但是如果说到战略目标和经营目标，就有所不同，因为它们的实现并不完全在主体的控制范围之内。主体可能像预期的那样运作，也可能会被竞争者所超越。这是由于外部事项——例如政府的变动、恶劣的天气以及类似的情况——的发生超出了它的控制范围。在目标设定过程中甚至可能已经考虑了某些这类事项，将它们当作具有较

低可能性的事项，一旦它们发生就采用一项权变计划来处理。但是，这种计划只能缓解外部事项的影响。它不能确保目标的实现。

针对经营的企业风险管理主要专注于确定贯穿于整个组织的目标和目的的一致性，识别关键成功因素和风险，评估风险并作出知情的应对，实施恰当的风险应对并建立必要的控制，以及及时报告业绩和期望。对于战略和经营目标，企业风险管理能够合理保证管理当局和履行监督职责的董事会及时地知悉主体实现这些目标的程度。

选定的目标

作为企业风险管理的一部分，管理当局不仅要选择目标并考虑它们如何支持主体的使命，而且要确保它们与主体的风险容量相协调。不协调会导致不能承受足够的风险以便实现目标，或者与之相反，承受了太多的风险。有效的企业风险管理并不是指明管理当局应该选择什么目标，而是管理当局应当制订程序来使战略目标与主体的使命相协调，并且确保所选择的战略和相关的目标与主体的风险容量相一致。

风险容量

管理当局在董事会的监督下所确定的风险容量是战略制订的指向标。公司可能将风险容量表述为增长、风险和报酬之间可接受的平衡，或者风险调整的股东增加值指标。一些主体，例如非营利组织，将风险容量表述为它们在向其利益相关者提供价值的过程中所愿意承受的风险水平。

主体的风险容量与它的战略之间存在着一种关系。通常可以设计许多不同战略中的任何一个来实现期望的增长和报酬目的，每一个都有着不同的风险。应用在战略制订过程中的企业风险管理能帮助管理当局选择一个与它的风险容量相一致的战略。如果与一个战略相关的风险与该主体的风险容量不一致，这个战略就需要修改。当管理当局先前所规划的战略超出了主体的风险容量，或者战略没有容纳使得主体实现其战略目标和使命的足够的风险时，这种情况就会发生。

主体的风险容量反映在主体的战略之中，进而指导资源配置。管理当局在考虑主体的风险容量和各个业务单元的战略计划的基础上，在业务单元之间配置资源，以使投入的资源产生一个理想的报酬。管理当局试图使组织、人员、流程与基础结构相协调，以便促成成功的战略实施，并确保主体保持在它的风险容量之内。

风险容限

风险容限是相对于目标的实现而言所能接受的偏离程度。风险容限能够被计量，而且通常最好采用与相关目标相同的单位来进行计量。

业绩计量指标可以用来帮助确保实际的结果处于既定的风险容限之内。例如，一家公司的目标是 98%按时送达，可接受的时间偏离范围是 97%～100%；它的培训目标是 90%的通过率，可接受的成绩是至少 75%；它希望员工在 24小时之内答复所有的客户投诉，但是接受最多 25%的投诉可以在 24~36小时内得到答复。

在确定风险容限的过程中，管理当局要考虑相关目标的相对重要性，并使风险容限与风险容量相协调。在风险容限之内经营能够就主体保持在它的风险容量之内向管理当局提供更大的保证，进而就主体将会实现其目标提供更高程度的慰藉。

4 事项识别

【本章摘要】管理当局识别将会对主体产生影响的潜在事项 —— 如果存在的话，并确定它们是否代表机会，或者是否会对主体成功地实施战略和实现目标的能力产生负面影响。带来负面影响的事项代表风险，它要求管理当局予以评估和应对。带来正面影响的事项代表机会，管理当局可以将其反馈到战略和目标设定过程之中。在对事项进行识别时，管理当局要在组织的全部范围内考虑一系列可能带来风险和机会的内部和外部因素。

事 项

事项是源于内部或外部的影响战略实施或目标实现的事故或事件。事项可能带来正面或负面影响，或者两者兼而有之。

在事项识别的过程中，管理当局认识到不确定性的存在，但是并不知道一个事项是否会发生，或什么时候发生，或者它所带来的确切影响。管理当局最初只考虑源于外部和内部的一系列潜在事项，而没有对它们的影响是正面的还是负面的作必要的关注。管理当局按照这种方法识别的不仅仅是具有负面影响的潜在事项，而且还包括那些代表着应该追逐的机会的事项。

事项有的很明显，有的很隐晦；所产生的影响有的微不足道，有的十分重大。为了避免忽略相关的事项，最好把识别与对事项发生的可能性和它的影响的评估区分开来，后者属于风险评估的范畴。但是，在实践中存在着局限，而且通常很难知道到底应该把界线画在哪儿。但是如果对一个重要目标的实现有重大影响的话，即使事项发生的可能性比较低，也不应该被忽略。

影响因素

无数的外部和内部因素驱动着影响战略执行和目标实现的事项。作为企业风险管理的一部分，管理当局认识到了解这些外部和内部因素以及由此可能产生的事项的类型的重要性。外部因素——以及相关事项及其影响的例子——包括：

- 与经济有关的因素——事项包括价格变动、资本的可获得性，或者竞争性准入的较低障碍，它们会导致更高或更低的资本成本以及新的竞争者。
- 自然环境因素——事项包括洪水、火灾或地震，它们会导致厂场或建筑物的损失，限制获取原材料，或者人力资本的损失。
- 政治因素——事项包括采用新的政治议程的政府官员选举，以及新的法律和监管，它们会导致诸如对国外市场的新的开放或限制进入，或者更高或更低的税收。
- 社会因素——事项包括人口统计、社会习俗、家庭结构、对工作 /生活的优先考虑的变化，以及恐怖主义活动，它们会导致对产品或服务需求的变化、新的购买场所和人力资源问题，以及生产中断。
- 技术因素——事项包括电子商务的新方式，它会导致数据可取得性的提高、基础结构成本的降低，以及对以技术为基础的服务的需求增加。

事项还来源于管理当局所作出的关于它将如何运行的选择。一个主体的能力和产能反映先前的选择，影响未来的事项，并且影响管理当局的决策。内部因素——以及相关事项及其影响的例子——包括：

- 基础结构——事项包括增加用于防护性维护和呼叫中心（call center）支持的资本配置，减少设备的停工待料期，以及提高客户满意度。
- 人员——事项包括工作场所的意外事故、欺诈行为以及劳动合同到期，它们会导致失去可利用的人员、货币性或者声誉性的损失以及生产中断。
- 流程——事项包括没有适当变更管理规程的流程修改、流程执行错误以及对外包的客户送达服务缺乏充分的监督，它们会导致丢失市场份额、低效率以及客户的不满和丢失重复性的业务。
- 技术——事项包括增加资源以应对批量变动、安全故障以及潜在的系统停滞，它们会导致订货减少、欺诈性的交易以及不能持续经营业务。

识别影响事项的外部和内部因素对于有效的事项识别是很有用的。一旦确定了起主要作用的因素，管理当局就能够考虑它们的重要性，并且集中关注那些能够影响目标实现的事项。

举例来说，一家鞋类生产商兼进口商确定了成为高质量男鞋行业领导者的愿景。为了实现这个愿景，它采用最先进的技术，并倚重于选择性的进口采购，着手制造集款式、舒适和耐用为一体的产品。这家公司考察了它的外部经营环境，并识别了社会因素和相关事项，例如它的主要消费者市场年龄的变化，以及工作着装的变化趋势。来自经济因素的事项包括外汇波动和利率变动。内部技术因素突出表现为落后的配送管理系统，而人员因素则表现为营销培训不够。

除了识别主体层次的事项之外，还要识别活动层次的事项。这样有助于将风险评估（下一章的主题）集中于主要的业务单元或职能机构，例如销售、生产、营销、技术开发以及研究与开发。

事项识别技术

主体的事项识别方法可能包含各种技术的组合，以及支持性的工具。例如，管理当局可以利用互动式的团队研讨作为其事项识别方法的一部分，利用一系列以技术为基础的工具中的任何一种来为参与者提供辅助。

事项识别技术既关注过去，也着眼于将来。关注过去事项和趋势的技术考虑诸如支付违约的历史、商品价格的变动以及浪费时间的事故等问题。着眼于未来风险暴露的技术则考虑诸如人口统计的变化、新的市场情况以及竞争者的行动等问题。

技术的复杂程度千差万别。尽管很多比较复杂的技术因行业而异，但是大多数都来源于共通的方法。例如，金融服务行业和健康与安全行业都采用损失事项追踪技术。这些技术从关注普通的历史事项入手——尽管比较先进的技术建立在可观察事项的事实性资料之上，但是比较基本的方法都根据内部员工的感知来观察事项——然后将数据纳入复杂的预测模型之中。企业风险管理比较先进的公司一般都会采用各种技术的组合，这些技术既考虑过去的事项，也考虑潜在的未来事项。

技术还因在主体内的何处应用而有所不同。一些技术关注具体的数据分析和建立对事项的自下而上的认识，而其他的则关注自上而下的。专栏 4-1 给出了事项识别技术的例子。

专栏 4-1

- 事项目录（**event inventories**）——这些是一个特定行业内的公司所共通的潜在事项或者不同行业之间所共通的特定过程或活动的详细清单。软件产品能够列出共性潜在事项的有关清单，一些主体利用它作为事项识别的出发点。例如，从事一项软件开发项目的公司编制了一份目录，详细列示了与软件开发项目有关的共性事项。
- 内部分析（**internal analysis**）——它可以作为常规性经营规划循环过程的一部分来完成，典型的是通过一个业务单元的员工会议。内部分析有时利用来自其他利益相关者（客户、供应商、其他业务单元）的信息，或者针对具体问题征询外部专家（内部或外部职能机构的专家或内部审计师）的意见。例如，一家正在考虑引入一个新产品的公司利用它自己的历史经验以及外部市场调研来识别那些曾经影响竞争者产品成功的事项。
- 扩大或底限触发器（**escalation or threshold triggers**）——这些触发器通过将现在的交易或事项与预先确定的标准进行对比，提醒管理当局关注的领域。一旦被触发，可能就需要对一个事项进行进一步的评估或者立即予以应对。例如，一家公司的管理当局针对新的营销或广告计划监控市场上的销售量，并根据其结果重新调配资源。另一家公司的管理当局追踪竞争者的定价结构，并考虑在达到一个特定的底限时变更自己的价格。
- 推进式的研讨与访谈（**facilitated workshops and interviews**）——这些技术通过经过设计的讨论，利用管理当局、员工和其他利益相关者所积累的知识和经验来识别事项。推进者主导有关可能会影响主体或单元目标实现的事项的讨论。例如，一名财务主计长与会计团队的成员一起召开了一个研讨会，来识别那些对主体的对外报告目标有影响的事项。通过结合团队成员们的知识和经验，能够识别出否则就会被遗漏的重要事项。
- 过程流动分析（**process flow analysis**）—— 这种技术考虑构成一个过程的输入、任务、责任和输出的组合。通过考虑影响一个过程的投入或其中的活动的内部和外部因素，主体能识别那些可能影响过程目标实现的事项。例如，一家医学实验室绘制了血液样本的接收和测试流程图。它利用流程图来考虑那些可能影响输入、任务和责任的因素的范围，识别与样本标注、过程中的传递以及人员换班变动有关的风险。
- 首要事项指标（**leading event indicators**）——主体通过监控与事项有相互关系的数据，来识别可能导致一个事项发生的情形是否存在。例如，金融机构很早就认识到延迟偿还贷款与最终的贷款违约之间的相互关系，以及及早干预的积极作用。对偿还方式的监控使违约的可能性得以通过及时的行动而降低。
- 损失事项数据方法（**loss event data methodologies**）——有关过去单个损失事项的数据库是识别趋势和根本原因的一个有用的信息来源。一旦确定了根本原因，管理当局就会发现它能比致力于单个事项更加有效地进行评估和处理。例

如，一家经营大型车队的公司维护了一个事故投诉的数据库，通过分析发现事故的百分比在数量和货币金额上不成比例，它与特定单元、地域和年龄结构的驾驶员工有关联。这个分析使管理当局能够确定事项的根本原因并采取行动。

事项识别的深度、广度、时机和范围因主体而异。管理当局选择符合其风险管理理念的技术，并确保主体形成所需的事项识别能力以及拥有支持工具。总之，事项识别需要强有力，因为它构成风险评估和风险应对要素的基础。

相互依赖性

事项通常并不是孤立地发生的。一个事项可能引发另一个事项，事项也可能会同时发生。在事项识别的过程中，管理当局应该明白事项彼此之间的关系。通过评估这种关系，我们可以确定风险管理活动最好指向哪儿。例如，中央银行利率的变动影响与一家公司的货币交易利得和损失有关的外汇汇率。一项缩减资本性投资的决策延迟了配送管理系统的升级，从而导致了额外的停工期和增加的经营成本。一项扩大营销培训的决策可能会提高销售能力和服务质量，从而导致重复性客户订单频率和批量的增加。一项进入一个新的经营领域的决策，以及与报告业绩挂钩的重大激励措施，可能会增加误用会计原则和欺诈性报告的风险。

事项类别

将潜在的事项归入不同的类别可能很有用。通过在主体内横向地和在业务单元内纵向地将事项汇总，管理当局形成对事项之间的关系的了解，从而获取更多的信息作为风险评估的依据。通过归集类似的事项，管理当局能够更好地辨别机会和风险。

事项分类还能使管理当局得以考虑其事项识别工作的完整性。例如，一家公司可能已经把与债款回收相关的事项归入一个名为债务违约的简单的类别。通过检查这个类别中的事项，管理当局能够推测它是否识别了所有有关债务违约的重大潜在事项。

一些公司根据对它们的目标的分类来设定事项的类别，利用一个层级，从高层次目标开始，然后逐渐向下到与组织单元、职能机构或经营过程相关的目标。

专栏 4-2 列示了一个在广义的内部和外部因素的背景下构建事项类别所采用的方法。

区分风险和机会

事项——如果它们发生——具有负面影响、正面影响，或者二者兼有。具有负面影响的事项代表风险，它需要管理当局的评估和应对。相应地，风险是一个事项将会发生并对目标的实现产生负面影响的可能性。

具有正面影响或者抵消风险的负面影响的事项代表机会。机会是一个事项将会发生并对实现目标和创造价值产生正面影响的可能性。代表机会的事项被反馈到管理当局的战略或目标制订过程中，以便规划行动去抓住机会。抵消风险的负面影响的事项在管理当局的风险评估和应对中予以考虑。

专栏 **4-2**

事项类别	
外部因素	内部因素
经济 • 资本的可利用性 • 信贷发行，违约 • 集中 • 流动性 • 金融市场 • 失业 • 竞争 • 兼并 /收购 自然环境 • 散发（ emissions）和废弃 • 能源 • 自然灾害 • 可持续发展 政治 • 政府更迭 • 立法 • 公共政策 • 管制 社会 • 人口统计 • 消费者行为 • 公司国籍 • 隐私 • 恐怖主义 技术 • 中断 • 电子商务 • 外部数据 • 新兴技术	基础结构 • 资产的可利用性 • 资产的能力 • 资本的取得 • 复杂性 人员 • 员工能力 • 欺诈行为 • 健康与安全 流程 • 能力 • 设计 • 执行 • 供应商 /依赖性 技术 • 数据的可信度 • 数据和系统的有效性 • 系统选择 • 开发 • 调配 • 维护

5 风险评估

【本章摘要】风险评估使主体能够考虑潜在事项影响目标实现的程度。管理当局从两个角度 —— 可能性和影响 —— 对事项进行评估，并且通常采用定性和定量相结合的方法。应该个别或分类考察整个主体中潜在事项的正面和负面影响。基于固有风险和剩余风险来进行风险评估。

风险评估的背景

外部和内部因素影响会发生什么事项以及事项将影响主体目标的程度。尽管一些因素对于一个行业中的公司而言是共通的，但是其他的事项对于特定的主体而言通常是独特的，其原因在于它的既定目标和过去的选择。在风险评估过程中，管理当局在决定主体风险特征的问题——例如主体的规模、经营的复杂性以及对其活动进行管制的程度——的背景下，考虑与主体及其活动相关的潜在未来事项的组合。

在评估风险时，管理当局考虑预期事项和非预期事项。许多事项是常规性的和重复性的，并且已经在管理当局的计划和经营预算中提到，而其他的事项则是非预期的。管理当局评估可能对主体有重大影响的非预期的潜在事项以及——如果尚未这么做的话——预期事项的风险。

虽然“ 风险评估 ”这个术语有时与一次性活动联系起来使用，但是在企业风险管理中，风险评估这个构成要素是在整个主体中所发生的活动的一个持续性和重复性的互动。

固有风险和剩余风险

管理当局既考虑固有风险，也考虑剩余风险。固有风险是管理当局没有采取任何措施来改变风险的可能性或影响的情况下，一个主体所面临的风险。剩余风险是在管理当局的风险应对之后所残余的风险。一旦风险应对已经就绪，管理当局接下来就要考虑剩余风险。

估计可能性和影响

潜在事项的不确定性从两个方面进行评价——可能性和影响。可能性表示一个给定事项将会发生的或然率，而影响则代表它的后果。可能性和影响是通常使用的术语，尽管一些主体使用诸如概率、严重性、严重程度或后果等术语。有时这些词语有着更具体的含义，“ 可能性 ”表示一个给定的事项从定性的角度将会发生的或然率，例如高、适中、低，或其他判断性的衡量尺度；而“ 概率 ”则表示一个定量的测度，例如百分比、发生的频率或者其他的数量性尺度。

决定应该在多大程度上关注对主体所面临的一系列风险的评估很困难，而且具有挑战性。管理当局认识到发生的可能性低且潜在的影响小的风险一般毋庸多虑。另一方面，发生的可能性高且潜在影响重大的风险则需要相当关注。介于这两个极端之间的情况一般需要艰难的判断。合理而仔细的分析是很重要的。

评估风险的时间范围应该与相关战略和目标的时间范围相一致。因为许多主体的战略和目标着眼于短期到中期的时间范围，因此管理当局自然就关注与这个时间范围

相关的风险。然而，战略方向和目标的某些方面却延伸到较长的时期。因此，管理当局需要认识到较长的时间范围，并且不能忽略那些可能延伸的风险。

举例来说，一家在加利福尼亚州经营的公司可能会考虑地震破坏其经营业务的风险。如果没有一个特定的风险评估时间范围，超过里氏 6.0 级的地震的可能性很高，或许几乎是确定无疑的。另一方面，这类地震在两年内发生的可能性就特别低。通过确定一个时间范围，主体能够更深入地认识风险的相对重要性，并提高比较多重风险的能力。

管理当局在确定目标的完成程度时常常采用业绩指标，并且在考虑风险对一项特定目标实现的潜在影响时通常采用相同的或适合的计量单位。例如，一家有着一项维持特定水平的客户服务的目标的公司，将会为这项目标设计出一个排序或其他测度指标，例如客户满意度指数、投诉的数量或者对重复性业务的测度。在评估一项可能会影响客户服务的风险——例如公司的网站在一段时期内可能无法使用的可能性——的影响时，最好采用相同的指标来确定其影响。

数据来源

对风险的可能性和影响的估计值通常利用来自过去的可观察事项的数据来确定，它提供了一个比完全主观的估计值更加客观的依据。根据一个主体自己的经验内部生成的数据可能会反映较少的主观个人偏见，并提供比来自外部渠道的数据更好的结果。但是，即使在内部生成的数据是主要输入的地方，外部数据作为一个印证或者对于增进分析可能很有用。例如，一家公司的管理当局在评估由于设备故障所导致的生产中断风险时，首先看它自己的制造设备先前发生故障的频率和影响。接下来用行业基准来补充数据。这样就能够对故障的可能性和影响进行更精确的估计，从而能够制订更有效的防护性维护计划。当利用过去的事项来对未来进行预测时，应该保持谨慎，因为影响事项的因素可能随着时间的推移而发生变化。

视　角

管理人员通常对不确定性作出主观判断，在这么做时他们应该认识到固有局限。心理学研究的发现表明，不同能力的决策者，包括经营管理人员，都对他们的估计能力过度信任，而且没有认识到实际存在的不确定性的数量。研究表明存在显著的“过度信任偏差”（overconfidence bias），从而导致所应用的——例如，在风险价值（value-at-risk）方法中——估计数量或可能性存在不恰当的狭义信任差距（narrow confidence intervals）。这种在估计不确定性中过度信任的倾向可以通过有效地利用内部和外部生成的经验性数据来使其最小化。如果缺乏这些数据，对这种偏差的普遍性的敏锐察觉能够帮助降低过度信任的影响。

关于决策的人性倾向可以用另一种方法来展示，那就是对于追求利得和避免损失，人们一般都会作出不同的选择。通过认识这些人性倾向，管理人员可以定格信息以增加风险容量和强化贯穿主体的行为。如专栏 5-1 所示，如何表现或“定格”（framed）信息可能会严重影响如何理解信息以及如何看待相关的风险或机会。

专栏 **5-1**

比起潜在的利得来，个人对于潜在的损失有不同的反应。如何定格风险——关注顶部（潜在的利得）或底部（潜在的损失）——通常将会影响所作的反应。研究人类

决策的前景理论（ prospect theory）指出，个人并不是风险中性的；相反，对损失的反应比对利得的反应往往更加偏激。这样就导致了一个曲解概率和最佳解决措施的倾向。为了加以说明，假设某个人面临着两组选择：

1. 肯定的利得 240 美元，或者
   25%的机会获利 1 000 美元和 75%的机会一无所获。
2. 肯定的损失 750 美元，或者
   75%的机会损失 1 000 美元和 25%的机会不受损失。

在第一组选择中，大多数人选择“肯定的利得 240 美元”，是由于针对利得持风险厌恶态度的倾向以及积极地定格问题。相反，大多数人选择“ 75%的机会损失 1 000 美元”，是由于针对损失持风险寻求态度的倾向以及消极地定格问题。前景理论坚持认为人们并不希望承担他们已经拥有或者认为他们能够拥有的风险，但是当他们认为他们能够使损失最小化时，他们会有较高的风险容限。

评估技术

一个主体的风险评估方法包含定性和定量技术的结合。在不要求他们进行定量化的地方，或者在定量评估所需的充分可靠数据实际上无法取得或者获取和分析数据不具有成本效益性时，管理当局通常采用定性的评估技术。定量技术能带来更高的精确度，通常应用在更加复杂和深奥的活动中，以便对定性技术进行补充。

定量评估技术一般需要更高程度的努力和严密性，有时采用数学模型。定量技术高度依赖于支持性数据和假设的质量，并且与有着已知历史和允许作可靠预测的风险暴露高度相关。专栏 5-2 给出了定量风险评估技术的例子。

专栏 **5-2**

- 设定基准（ **benchmarking**） ——作为一组主体之间的协作过程，设定基准着眼于具体的事项或过程，采用共通的标准比较计量指标和结果，并且识别改进的机会。建立有关事项、流程和计量指标的数据来比较业绩。一些公司利用设定基准来在整个行业中评估潜在事项的可能性和影响。
- 概率模型 ——概率模型根据特定的假设将一系列事项以及所造成的影响与这些事项的可能性联系起来。在历史数据或反映对未来行为的假设的模拟结果的基础上，对可能性和影响进行评估。概率模型的例子包括风险价值、风险现金流量、风险盈利以及信贷和经营损失分布的计算等。概率模型可以采用不同的时间范围，以估计诸如不同时期金融工具的价值范围等结果。概率模型还可以用来评估期望的或平均的结果，以及极端的或非期望的影响。
- 非概率模型 ——非概率模型在估计没有量化相关可能性的事项的影响时，利用主观的假设。根据历史或模拟数据和对未来行为的假设对事项的影响进行评估。非概率模型的例子包括敏感性指标、压力测试以及情景分析。

为了采用定性评估技术获得有关可能性和影响的一致意见，主体可以使用与它们在识别事项时所采用的相同的方法，例如访谈和研讨。风险的自我评估过程通过使用描述性的或者数量性尺度，获取参与者对未来事项潜在的可能性和影响的观点。

一个主体不需要在所有的业务单元使用共同的评估技术。相反，对技术的选择应该反映对精确度的需要和该业务单元的文化。例如，一家公司在识别和评估一个流程层次的风险，一个业务单元采用自我评估问卷，而另一个则采用研讨会。对固有风险和剩余风险进行评估，然后按照风险类型和每个业务单元的目标进行整理和分组。尽管采用了不同的方法，它们为促进整个主体的风险评估提供了足够的一致性。

当针对某个事项的所有个别风险评估都以定量的方式表示时，管理当局就能够获得该事项在整个主体范围内的定量的影响指标。例如，分别计算出各个业务单元中能源价格变动对毛利的影响，就可以确定主体范围内的影响。在定性和定量指标相混合的领域，管理当局开发一种跨越定性和定量指标的定性评估，从而得出用定性的术语来表示的复合评估。在整个主体范围内确定共通的可能性和影响术语以及针对定量指标的共通的风险类别，有助于这些复合的风险评估。

事项之间的关系

如果潜在的事项并不相关，管理当局就对它们分别进行评估。例如，一家公司的不同业务单元面临着不同的——例如纸浆和外币——价格波动风险，它会针对与市场波动相关的风险分别进行评估。但是当事项之间存在相互关联，或者事项结合或相互影响产生显著不同的可能性或影响时，管理当局就要把它们放在一起来评估。尽管单个事项的影响可能很轻微，但是事项的次序或组合的影响可能更大。

举例来说，配送仓库中丙烷罐上的一个有缺陷的阀门会导致丙烷泄露；仓库的门保持关闭以便保持隔壁办公室的热度；一辆正在开近的卡车的司机开启遥控装置来打开仓库的门。丙烷气体的存在和车库门马达所产生的火花共同引发了一场爆炸。这些不同的事项相互影响并导致了重大的风险。在另一个例子中，一家进入一个国外市场的公司在当地新聘任了管理人员，其报告体系未经验证，总部管理当局用来判断相关业绩的依据不足，就会导致错误或欺诈性报告方面的重大风险。

如果风险可能会影响多个业务单元，管理当局可以将它们归入共通的事项类别中，并且首先分单元逐个考虑，然后再从整个主体的范围把它们放在一起加以考虑。例如，一家金融服务公司的业务单元面临着政府利率变动的风险，它的管理当局不仅从每个业务单元的角度分别评估风险，而且将它们组合起来从整个主体的角度进行风险评估。一家制造业的公司有多个业务单元，分别都面临黄金价格波动的风险；管理当局把黄金价格潜在变动的风险汇总到一个单一的指标中，以反映在它的全部黄金库存量中每盎司的价格变动 1 美元的净影响。

事项的性质以及它们是否相关联可能会影响所采用的评估技术。例如，在评估可能有极端影响的事项的影响时，管理当局可以采用压力测试（stress testing）；而在评估多重事项的影响时，管理当局可能会发现模拟或情景分析更加有用。

关注风险的可能性和影响之间的相互关系是管理当局的一项重要责任。有效的企业风险管理不仅要求针对固有风险进行风险评估，而且还要与接下来的风险应对（将在下一章中予以讨论）相结合。

6 风险应对

【本章摘要】在评估了相关的风险之后，管理当局就要确定如何应对。应对包括风险回避、降低、分担和承受。在考虑应对的过程中，管理当局评估对风险的可能性和影响的效果，以及成本效益，选择能够使剩余风险处于期望的风险容限以内的应对。管理当局识别所有可能存在的机会，从主体范围或组合的角度去认识风险，以确定总体剩余风险是否在主体的风险容量之内。

风险应对可以分为以下几种类型：

- 回避（avoidance）——退出会产生风险的活动。风险回避可能包括退出一条产品线、拒绝向一个新的地区市场拓展，或者卖掉一个分部。
- 降低（reduction）——采取措施降低风险的可能性或影响，或者同时降低两者。它几乎涉及各种日常的经营决策。
- 分担（sharing）——通过转移来降低风险的可能性或影响，或者分担一部分风险。常见的技术包括购买保险产品、从事避险交易（hedging transactions）或外包一项业务活动。
- 承受（acceptance）——不采取任何措施去干预风险的可能性或影响。

专栏 6-1 为如何应用这些风险应对给出了例子。

专栏 **6-1**

回避 ——一家非营利组织识别和评估向它的会员提供直接医疗服务的风险，并决定不承受相关的风险。它决定改为提供推荐服务。

降低 ——一家股票交割公司识别和评估它的系统超过 3个小时不能用的风险，并得出它不能承受发生这种情况的影响的结论。这家公司投资于增进故障自测和系统备份的技术，以降低系统不能用的可能性。

分担 ——一所大学识别和评估与管理学生宿舍相关的风险，并作出结论：它不具备有效地管理这些大型居住物业所必需的房间服务能力。这所大学把宿舍管理外包给了一家物业管理公司，从而更好地降低了与物业相关的风险的影响和可能性。

承受 ——一个政府机构识别和评估它在不同地理区域的基础设施发生火灾的风险，并评估通过保险分担风险影响的成本。它得出的结论是保险和相关的扣除所增加的成本超过重置成本，于是决定承受这项风险。

回避应对意味着所确定的应对方案都不能把风险的影响和可能性降低到一个可接受的水平。降低和分担应对把剩余风险降低到与期望的风险容限相协调的水平，而承受应对则表明固有风险已经在风险容限之内。

对于许多风险而言，适当的应对方案是明显的和很好接受的。比如说，对于不能计算可利用性的风险，一个典型的应对方案就是实施一项业务持续性计划。对于其他的风险，可采用的方案可能不那么明显，需要调查和分析。例如，与降低竞争者在品牌价值方面的活动的影响有关的应对方案，可能需要市场调研和分析。

在确定风险应对的过程中，管理当局应该考虑下列事项：

- 潜在应对对风险的可能性和影响的效果——以及哪个应对方案与主体的风险容限相协调；
- 潜在应对的成本与效益；
- 除了应付具体的风险之外，实现主体目标可能的机会。

对于重大风险，主体通常从一系列应对方案中考虑潜在的应对。它使应对选择更具深度，并且对“现状”（status quo）提出了挑战。

评价可能的应对

分析固有风险和评价应对的目的在于使剩余风险水平与主体的风险容限相协调。通常，某些应对中的任何一个都将带来与风险容限相一致的剩余风险，而有时应对的组合能带来最优的效果。相反，有时一个应对能够影响多重风险，在这种情况下管理当局可以决定不需要再采取其他的措施来处理某个特定的风险。

评价对风险的可能性和影响的效果

在评价应对方案的过程中，管理当局同时考虑对风险的可能性和影响的效果，认识到一个应对可能会对可能性和影响产生不同的效果。举例来说，一家公司有一个位于强暴风雨地区的计算机中心，它制订了一个经营持续性计划，这个计划尽管对暴风雨发生的可能性起不到任何效果，但是能够减轻建筑物损坏或人员不能上班的影响。另一方面，把计算机中心迁移到另外一个地区的选择不能降低同等暴风雨的影响，但是能够降低暴风雨发生的可能性。

在分析应对的过程中，管理当局可以考虑过去的事项和趋势，以及潜在的未来情景。在评价备选的应对时，管理当局通常要利用与衡量相关目标相同的或适合的计量单位。

评估成本与效益

资源总是有约束的，因而主体必须考虑备选风险应对方案的相关成本与效益。对实施风险应对所作的成本与效益计量的精确度水平各不相同。一般说来，处理方程式的成本一方比较容易，在很多情况下可以非常精确地予以量化。通常考虑与开展一项应对相关的所有直接成本，以及可以实际计量的间接成本。一些主体还将与使用资源相关的机会成本也纳入考虑。

但是，在某些情况下很难量化风险应对的成本。量化的挑战来自估计与一个特定应对相关的时间和效果，例如，获取有关客户偏好的变化、竞争者的行动等市场信息或其他外部生成的信息，就是这种情况。

效益一方通常涉及到更多的主观评价。例如，有效的培训计划的效益一般很明显，但是难以量化。然而，在许多情况下，一项风险应对的效益可以在与实现相关目标有关的效益的背景下予以评价。

在考虑成本—效益关系时，把风险看作是相互关联的，有助于管理当局汇集主体的风险降低和风险分担应对。举例来说，在通过保险分担风险时，把风险组合到一个

险种之下可能是有利的，因为把组合后的风险投保到一个财务协议之下通常可以降低定价。

应对方案中的机会

事项识别的那一章讲述了管理当局如何识别对主体目标的实现产生正面或负面影响的潜在事项。具有正面影响的事项代表机会，并被反馈到战略或目标制订过程中。

同样，在考虑风险应对时也可以识别机会。风险应对所考虑的内容不应该仅仅限于降低已经识别出来的风险，而且还应该考虑给主体带来的新的机会。管理当局可以识别创新的应对，尽管它们仍然适用在本章前面所讲述的类别，但是对于该主体乃至一个行业来讲可能完全是新的。当现有的风险应对方案正处在到达其有效性的极限时，以及进一步的改进可能只能对风险的影响或可能性带来些许细微的变化时，这种机会可能会显现出来。一个例子是一家汽车保险公司针对在特定的道路交叉口所发生的大量事故的创造性应对，它决定投资增加交通信号灯，以降低事故投诉，进而提高毛利。

选定的应对

在评价了备选风险应对的效果之后，管理当局决定它打算如何管理风险，选择一个旨在使风险的可能性和影响处于风险容限之内的应对或者应对组合。应对并不是必须达到最低数量的剩余风险。但是如果一个风险应对会导致剩余风险超过风险容限，管理当局就要对该应对进行相应的反思和修改，或者，在特定的情形下，重新考虑既定的风险容限。因此，平衡风险与风险容限可能涉及到一个反复的过程。

评价针对固有风险的备选应对，要求考虑应对可能带来的附加风险。这也会导致管理当局在完成决策之前，需要经过一个反复的过程，它要考虑这些附加的风险，包括一些可能不会立即显现出来的。

一旦管理当局选择了一个应对，它就可能需要制订一项实施计划来执行该应对。实施计划的一个关键部分是确定控制活动（将在下一章中讨论）以确保风险应对得以实施。

管理当局认识到总是会存在一定程度的剩余风险，这不仅是因为资源是有限的，而且还因为所有的活动都固有未来的不确定性和局限。

组合观

企业风险管理要求从整个主体范围或组合的角度去考虑风险。管理当局通常所采取的方法是首先从各个业务单元、部门或职能机构的角度去考虑风险，让负有责任的管理人员对本单元的风险进行复合评估，以反映该单元与其目标和风险容限相关的剩余风险。

通过对各个单元风险的了解，一个企业的高层管理当局能够很好地采取组合观来确定主体的剩余风险和与其目标相关的总体风险容量是否相称。不同单元的风险可能处于各该单元的风险容限之内，但是放到一起以后，风险可能会超过该主体作为一个整体的风险容限，在这种情况下需要附加的或另外的风险应对，以便使风险处于主体的风险容量之内。相反，主体范围内的风险可能会自然地相互抵消，例如，一些单个

单元的风险较高，而其他的则对风险比较厌恶，这样整体风险就在主体的风险容量之内，从而不需要另外的风险应对。

风险组合观可以用多种方式来描述。组合观可以通过关注各个业务单元的主要风险或事项类别，或者该公司作为一个整体的风险，运用类似风险调整资本（ risk-adjusted capital）或风险资本（ capital at risk）等标准来获取。在计量通过盈利、增长以及有时与已配置的和可利用的资本相关的其他业绩指标表述的目标上的风险时，这种复合性指标尤其有用。这种组合观的指标能够为在业务单元之间重新配置资本和修改战略方向提供有用的信息。

一个例子是一家制造业公司对于它的经营性盈利目标采取风险组合观。管理当局采用通用的事项类别来获取各个业务单元的风险。接下来它按照类别和业务单元编制了图表，说明用一个时间范围内的频率来表示的风险可能性，以及对盈利的相对影响。其结果是对公司所面临风险的一个复合性的或组合的观点，管理当局和董事会据此考虑风险的性质、可能性和相对大小，以及它们可能对公司的盈利产生怎样的影响。

另外一个例子是一家金融机构，它号召各个业务单元都从风险调整资本报酬的角度去制订目标、风险容限和业绩指标。这个一贯应用的尺度帮助管理当局把各个单元的组合风险评估结合起来，形成把该机构作为一个整体的风险组合观，从而使管理当局能够按照目标去考虑各个单元的风险，并确定主体是否处于其风险容量之内。

如果从组合的角度看待风险，管理当局就可以考虑它是否处于既定的风险容量之内。此外，它能够重新评价它所愿意承担的风险的性质和类型。在组合观显示风险显著低于主体的风险容量的情况下，管理当局可以决定鼓励各个业务单元的管理人员去承受目标领域的更大的风险，以便努力增进主体的整体增长和报酬。

7　控制活动

【本章摘要】控制活动是帮助确保管理当局的风险应对得以实施的政策和程序。控制活动的发生贯穿于整个组织，遍及各个层级和各个职能机构。它们包括一系列不同的活动，例如批准、授权、验证、调节、经营业绩评价、资产安全以及职责分离。

控制活动是帮助确保管理当局的风险应对得以实施的政策和程序，后者是指人们直接或通过对技术的应用来执行政策的行动。控制活动可以根据与其相关的主体目标的性质——战略、经营、报告和合规——进行分类。

尽管一些控制活动仅仅与一个类别有关，但是通常是交叉的。根据情况，一项特定的控制活动可能有助于满足主体的多个类别的目标。例如，特定的经营控制也能帮助确保可靠的报告，对控制活动的报告能够帮助实现合规目标，如此等等。

与风险应对相结合

选定了风险应对之后，管理当局就要确定用来帮助确保这些风险应对得以恰当地和及时地实施所需的控制活动。

目标、风险应对和控制活动的关联可以通过下面的例子展示出来：一家公司设定的一项目标是达到或超过销售任务，并将不能获取对现在和潜在的客户需求之类的外部因素的充分了解识别为一种风险。为了降低这种风险发生的可能性和影响，管理当局建立了现有客户的购买历史记录，并开展了新的市场调研活动。这些风险应对作为确定控制活动的焦点，控制活动包括根据既定的时间表跟踪客户购买历史记录发展的进展，以及采取措施确保报告数据的准确性。从这种意义上讲，控制活动直接建立在管理过程之中。

在选择控制活动的过程中，管理当局要考虑控制活动是如何彼此关联的。在一些情况下，一项单独的控制活动可以实现多项风险应对。在另一些情况下，一项风险应对则需要多项控制活动。更有另一些情况，管理当局可能会发现现有的控制活动足以确保新的风险应对得以有效执行。

尽管控制活动一般是用来确保风险应对得以恰当实施的，但是对于特定的目标而言，控制活动本身就是风险应对。例如，对于一项确保特定的交易被恰当授权的目标而言，应对可能就是类似职责分离和由监督人员审批等控制活动。

就像对风险应对的选择要考虑它们的恰当性和残留的或剩余的风险一样，对控制活动的选择或评审应该包含对它们与风险应对和相关目标的相关性和恰当性的考虑。这可以通过单独考虑控制活动的适当性来完成，也可以通过在风险应对和相关控制活动两者的背景下考虑剩余风险来完成。

控制活动是企业致力于实现其经营目标的过程的一个重要部分。控制活动的实施并不仅仅是出于它们自身的缘故，也不仅仅是因为它看起来好像是要做的“正确的或恰当的”事情。在上面的例子中，管理当局需要采取措施来确保销售任务得以实现。控制活动充当了对该项目标的实现进行管理的机制。

控制活动的类型

前面已经列举了关于控制活动的类型的许多不同的表述，包括预防性的、侦查性的、人工的、计算机的以及管理控制。控制活动还可以根据特定的控制目标来进行分类，例如确保数据处理的全面性和准确性。

专栏 7-1 描述了通常所采用的控制活动。这些只是不同组织层级的人员所普遍实施的诸多程序中的一些，这些程序被用来强化对既定行动计划的坚持，以及保证主体在实现其目标的道路上前进。它们是用来展示控制活动的范围和多样性的，并不意味着任何特定的分类。

专栏 **7-1**

- 高层复核（**top-level reviews**）—— 高层管理当局对照预算、预测、以前期间和竞争者来复核实际的业绩。主要的活动——例如营销冲刺、改进生产流程以及成本抑制或降低计划等——被反映到任务实现程度的计量指标上。并对新产品开发、合营企业或筹资计划的执行进行监控。
- 直接的职能或活动管理（**direct functional or activity management**）—— 负责职能机构或活动的管理人员审核业绩报告。一位负责一家银行的消费者贷款的管理人员审核按分行、地区和贷款（担保）种类区分的报告，核对摘要，识别趋势，并将结果与经济统计数据和任务进行对照。分行管理人员收到按贷款官员和地区客户分片区分的新业务数据。分行管理人员还要关注合规问题，审核监管机构对规定金额的新存款所要求的报告。根据集中为隔夜转账和投资所报告的净头寸，调节每日的现金流量。
- 信息处理（**information processing**）—— 实施一系列的控制来检查交易的准确性、完整性和授权。输入的数据要经过联机编辑核对（on-line edit checks）或与经批准的控制文件相匹配。例如，一个客户的指令只有在对照了经批准的客户文件和信用限额之后才能被接受。对交易的数量化结果进行核算，对例外情况追查到底并报告给监督人员。对新系统的开发和现有系统的改变，以及对数据、文件和程序的进入都要加以控制。
- 实物控制（**physical controls**）——对设备、存货、证券、现金和其他资产进行实物性的保护，定期盘点，并与控制记录上所反映的数额相比较。
- 业绩指标（**performance indicators**）——把不同系列的——经营的或者财务的——数据彼此联系起来，与对相互关系的分析以及调查和矫正措施一起，构成了一项控制活动。例如，业绩指标包括各个单元的员工流动率。通过调查非预期的结果或异常的趋势，管理当局可以识别由于没有足够的能力去完成关键的流程而可能意味着实现目标的可能性较低的情况。管理当局如何利用这种信息——仅仅用于经营决策，或是还要追查报告系统中非预期的结果——决定着对业绩指标的分析是只能用于经营目的，还是也能同时用于报告控制目的。
- 职责分离（**segregation of duties**）——把不同人员的职责予以分开或隔离，以便降低错误或舞弊的风险。举例来说，交易授权、记录和处理相关资产的职责就要分开。一位授权赊销的管理人员不能负责记录应收账款或处理现金回款。同样，销售人员无权修改产品价格文件或佣金比率。

通常执行一个控制组合来处理相关的风险应对。例如，一家公司的管理当局设定交易限额来管理与一个投资组合相关的风险，并确定旨在帮助确保不超过交易限额的控制活动。控制活动包括在执行之前停止特定交易的预防性控制，以及及时地识别其他交易的侦查性控制。控制活动把计算机和人工控制结合起来，包括确保正确获取了所有信息的自动化控制，以及使负有责任的个人能够授权或批准投资决策的途径程序。

政策和程序

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。例如，政策可能要求证券经纪商的零售分部管理人员对客户交易活动进行复核。程序就是复核本身，及时执行并注意政策中所列举的要素，例如所交易的证券的性质和数量，以及它们与客户净财富和期限之间的关系。

在很多时候，政策是口头沟通的。如果政策是一项长期持续而且充分理解的惯例，以及在沟通渠道包括很少几个管理阶层而且对员工有密切互动和监督的较小的组织中，不成文的政策能很有效。但是不管是否成文，政策都必须仔细地、有意识地和一贯地执行。如果机械地执行，缺乏对政策所针对的情况的敏锐的持续关注的话，程序就不会有用。此外，根据所观察的程序和所采取的适当的矫正措施来辨别情况也是至关重要的。后续措施可能会因企业的规模和组织结构而异。它们的范围很广，从大公司的正式报告程序——各业务单元陈述任务为什么没有实现以及应该采取什么措施来防止再次发生，直到小企业的所有者兼管理人员穿过走廊与车间管理人员就什么出了问题以及需要做什么进行交谈。

对信息系统的控制

出于对信息系统在经营企业和满足报告和合规目标方面的普遍依赖，需要对重要的系统进行控制。可以采用两个广义的信息系统类别。第一个是一般控制，它适用于许多并非全部是应用系统的情形，并且有助于确保它们持续、适当地运行。第二个是应用控制，它在应用软件中包含计算机化的步骤，以便对处理过程进行控制。一般控制和应用控制，在必要的时候与人工实施的控制结合起来，共同起作用以确保信息的完整性、准确性和有效性。

一般控制

一般控制包括对信息技术管理、信息技术基础结构、安全管理和软件获取、开发和维护的控制。它们适用于所有的系统——从主机到客户 /服务器到桌面和手提电脑环境。专栏 7-2 为这些类别中的共通控制给出了例子。

专栏 **7-2**

- 信息技术管理 ——一个指导委员会提供对信息技术活动和改进行动的监督、监控和报告。
- 信息技术基础结构 ——将控制应用于系统的界定、获取、安装、配置、整合和维护。控制可能包括确定和强化系统表现的服务水平协议，保持系统有效性的业务持续性计划，跟踪运行失败的网络表现，以及安排计算机运行的进程。信