

**COSO**



The Committee of Sponsoring Organizations of the Treadway Commission

# 企业风险管理—— 整合框架

## ➤ 内容摘要

(简体中文翻译：中国东北财经大学方红星教授)

## 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，增进创造价值的潜力。

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 and 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) 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。

---

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）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。

---

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）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。

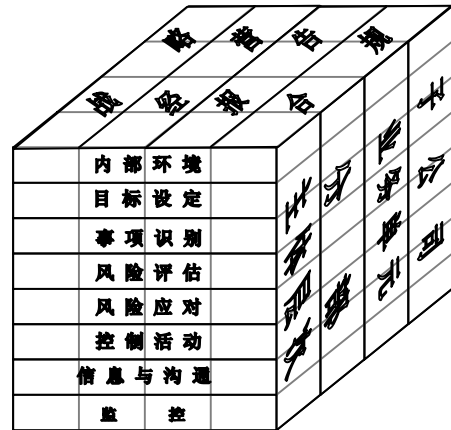
## 目标与构成要素之间的关系

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。

---

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，但是他们不但不对其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

根据本报告的提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。