

## 浅析 COSO 整合框架中的环境建立与目标设定

王曙明 ☎: (8610) 8357 1420

✉: wangshuming@chinastock.com.cn

COSO风险管理整合框架提出了风险管理的八大要素：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。在这八大要素中,建立内部环境与设定目标直接关系到企业对风险偏好及风险容忍度的设定与设置,是一切风险管理活动的基础,因此本文重点针对COSO中的这两大要素加以探讨。

### 内部环境

#### (一) 企业的风险管理哲学

企业的风险管理哲学是共同信念和态度的集合,而这些信念和态度鲜明反映了企业在上至战略发展下至日常工作的实施等一切行为中考虑风险的方式。有时,即使企业的风险管理哲学已经被很好的发展起来,仍然可能在其业务部门之间存在一定的文化差异,从而导致风险管理哲学应用的不同。这些不同的子文化(sub-culture)可能对企业产生负面影响。但是,通过协同合作,这些带有子文化的部门是完全可以很好反应企业的风险管理哲学的。

#### (二) 风险偏好与风险容忍度

风险偏好(risk appetite)是指在董事会层面上,公司在追求价值的同时所愿意接受的风险总额。风险偏好体现了整个公司风险管理哲学,并相应地影响企业文化和运作风格,同时直接和公司的战略挂钩。例如,美林证券(Merrill Lynch)的风险管理哲学“承担风险是公司开展核

心业务不可或缺的一部分”鲜明地体现了该公司在开展核心业务时高风险偏好的风险文化。风险偏好通常是在董事会的监督下由经营管理层所建立，它是战略设定的一枚路标。企业可以定性的考虑风险偏好，将其分为：高、中、低三档；也可采用量化的方式，来反映和平衡风险增加和风险回报的目标，或者表示为以风险调整下的股东所增加价值的度量。企业风险管理应用于战略设定，帮助经营管理层来选择和其风险偏好相一致的战略。如果企业战略所关联的风险与企业的风险偏好不相容，那么战略就应被修改。经营管理层旨在调整组织、全体员工、各项工作流程以及基础设施并使其保持一致来促进战略的实施，从而使整个企业处于风险偏好当中。

风险容忍度(risk tolerance)和企业的经营目标直接关联，它是企业对于实现某一特定目标时所可能发生的相关变故（如目标只能实现 90%，80%等等）的可接受水平。风险容忍度在相同的业务单元中最好是被量化为同类目标的一定容度范围。在设置风险容忍度时，企业的经营管理层应充分考虑该特定目标的相对重要性（对于公司战略目标），并将风险容忍度和风险偏好保持一致。企业在风险容忍度下运行，使管理层能更好地保证企业处于风险偏好内部稳健发展，而同时也相应地为企业实现其目标提供了较为合理的松弛空间。

当前，国内很多证券公司还没有建立风险偏好的相关机制，更没有将风险容度和公司的战略发展有机融合。当公司在制定战略方针时应充分考虑公司的风险偏好，不同的战略政策将使公司面对不同的风险环境，这时，公司的战略决策就取决于公司的风险偏好。在企业设置风险偏好与风险容忍度时，董事会及管理层必须对企业的风险状况、风险承担能力以及风险价值取向有较为深入的思考与理解，他们首先回答以下问题（参见[2]）：

- a. 董事会及管理层是否已经对公司的风险管理能力进行了评审？
- b. 从高层的高层的角度来描述公司的风险文化特征。
- c. 对风险的理解是否已经渗透到全公司上下以及公司文化中？
- d. 公司的管理层激励机制中是否涵盖了风险管理水平的要求？
- e. 公司每年需要为风险管理花费多少？而实际花费为多少？
- f. 公司的风险管理成熟度怎样？公司上下全体对该成熟度的看法一致吗？
- g. 上述问题的回答是基于实证支持，还是基于猜测？

### （三）董事会监督

董事会是内部环境中的关键部分，并且对其它内部环境元素起到了非常重要的影响作用。

一个有效的董事会能够保证企业管理层保持有效的风险管理。

#### (四) 廉正与道德价值 (integrity & ethical value)

个体员工之所以可能从事欺骗、违法、或者其他丧失道德的行为，主要是由于企业“赋予”了它们强大的“激励因素”或“诱导因素”。过分的注重结果，尤其是短期结果，会营造出一种不得当的内部环境。一味的注重短期结果甚至在短期内都可能对企业造成伤害。消除或减少不正当“激励因素”和“诱导因素”将历经一个较长的过程才能实现完全清除不良行为。方法有：设置合理现实的目标；一个控制良好的报告系统也起到了抵制虚假行为的保护作用。正式的公司行为准则 (corporate conduct code) 对于有效规范员工行为是非常重要的，它同时也是道德规划的基础。同时，公司管理层的行为也会发出强大的信号，来影响全体员工的行为。

#### (五) 员工胜任力 (competence)

胜任力反映了员工执行所分配任务时所需要的知识与技能。管理层为特定的工作明确其对应的胜任力水平，并将这些水平转换为所需要的知识与技能。

## 目标设定

### (一) 四大目标

COSO 认为一家企业的目标主要分为战略目标、操作性目标、报告性目标及合规目标。战略目标为操作性目标、报告性目标以及合规目标建立了基础。企业的目标和其风险偏好是保持一致的，并且驱动了风险容忍水平。战略性目标反映了企业为股东创造价值而采取的管理选择。

**操作性目标：**和企业操作的效率和效果相关的目标。操作性目标需要反映企业运作所在的商务、行业以及经济环境。操作目标为引导所配置的资源提供了焦点，如果一家企业的操作性目标不明确的话，其资源就可能会被错误指引。

**报告性目标和报告的可靠性**相关联，包含了内部和外部报告，并且可能包含财务及非财务信息。可靠的报告机制为企业达到目标提供所需的正确、完备以及适当的经营管理信息，如营销表、每日销售快报、生产质量等。

**合规目标：**遵循相关的法律法规。企业的合规记录会对企业和社会或业界的声誉产生重大

的正面或负面的影响。

上述几大目标是可能出现重叠！

## (二) 目标的实现

尽管目标提供了企业实现发展规划的可度量指标，但这些目标具有不同程度的重要性和优先性，因此，对于某些目标，企业应该具有合理的把握(reasonable assurance)并使其完全实现，但是对于另外一些目标则不然。

首先，战略性目标和操作性目标并不总是企业可以掌控的。企业风险管理(ERM)并不能完全消除错误的判断或决策。此外，一些不可控的外部事件会使企业无法实现操作性目标。甚至在目标设置的过程中，企业可能已经将这些外部事件考虑了进去并赋予其较低的发生可能性，同时制定了相应的应急计划，但这些计划仅仅能减轻外部事件的影响，而不能保证战略性目标和操作性目标一定得以实现。尽管如此，企业风险管理(ERM)仍然能提升企业作出更佳决策的可能性。因此，对于这两类目标，有效的企业风险管理(effective ERM)能使得董事会和管理层能够对形势具有一种合理的掌控以清楚地理解企业目标被实现的程度。

另一方面，报告性目标和合规性目标在很大程度上取决于企业自身的控制，有效的企业风险管理使得董事会和管理层能够具备合理的把握并通过控制措施使这些目标完全得以实现。换句话说，一旦这些目标确立，企业就要对其自身能力加以控制，从而尽全力来实现目标。

## (三) 目标的选择

关于目标的选择：作为风险管理的一部分，企业经营管理层不仅要选择目标并考虑它们如何支持企业的使命，并且要保证它们和企业的风险偏好保持一致。有效的企业风险管理并不规定管理层应当选择哪些目标，而是规定了管理层应当建立将战略目标和企业使命一致化的流程，这一过程同时保证了所选择的战略及相关目标和企业的风险偏好是一致的。

## 参考文献

[1] COSO, Enterprise Risk Management - Integrated Framework, September, 2004.

[2] Institute of Risk Management, Risk Appetite and Risk Tolerance, May 2011.

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](http://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>