内部控制框架的新发展——企业风险管理框架

2007年1月12日

——COSO委员会新报告《企业风险管理框架》简介

朱荣恩 贺 欣

［摘要］2003年7月美国CA)SO委员会颁布了企业风险管理框架的讨论稿，并将于2004年4月颁布正式稿。该讨论稿是在1992年COSO委员会颁布的内部控制框架基础上，吸收各方风险管理研究成果基础上提出的，本文将主要讨论其与内部控制框架的区别及其主要内容。

［关键词］风险管理框架 内部控制框架 风险管理 内部控制

一、企业风险管理框架与内部控制框架的联系与区别

自1992年美国CDSO委员会发布《内部控制框架》（简称COSO报告)以来，该内部控制框架已经被世界上许多企业所采用，但理论界和实务界纷纷对内部控制框架提出一些改进建议，强调内部控制框架的建立应与企业的风险管理相结合。新的企业风险管理框架就是在1992年的研究成果——《内部控制框架》报告的基础上，结合《萨班斯一奥克斯法案》(Sarbanes—Oxley Act)在报告方面的要求，进行扩展研究得到的。普华永道的项目参与者认为，新报告中有60%的内容得益于COSO1992年报告所做的工作。但由于风险是一个比内部控制更为广泛的概念，因此，新框架中的许多讨论比92年报告的讨论要更为全面、更为深刻。此外，COSO在其风险管理框架讨论稿中也说明，风险管理框架建立在内部控制框架的基础上，内部控制则是企业风险管理必不可少的一部分。风险管理框架的范围比内部控制框架的范围更为广泛，是对内部控制框架的扩展，是一个主要针对风险的更为明确的概念。

概括地看，相对于内部控制框架而言，新的 COSO报告新增加了一个观念、一个目标、两个概念和三个要素，即“风险组合观”、“战略目标”、“风险偏好”和“风险容忍度”的概念以及“目标制定”、“事项识别”和“风险反应”要素。对应风险管理的需要，新眶架还要求企业设立一个新的部门——风险管理部。新的风险管理框架比起内部控制框架，无论在内容还是范围上都有所扩大和提高，具体表现在：

1．提出一个新的观念——风险组合观(An En tity—level Portfolio View Of Risk)

企业风险管理要求企业管理者以风险组合的观点看待风险，对相关的风险进行识别并采取措施使企业所承担的风险在风险偏好的范围内。对企业内每个单位而言，其风险可能落在该单位的风险容忍度范围内，但从企业总体来看，总风险可能超过企业总体的风险偏好范围。因此，应从企业总体的风险组合的观点看待风险。

2．增加一类目标——战略目标，并扩大了报告目标的范畴

内部控制框架将企业的目标分为经营、财务报告和合法性目标。企业风险管理框架也包含三个类似的目标，但是其中只有两个目标与内部控制框架中的定义相同，财务报告目标的界定则有所区别。内部控制框架中的财务报告目标只与公开披露的财务报表的可靠性相关，而企业风险管理框架中的报告目标的范围有很大的扩展，该目标覆盖了企业编制的所有报告。

此外，企业风险管理框架比内部控制框架增加下

一个目标——战略目标。该目标的层次比其他三个目标更高。企业的风险管理在应用于实现企业其他三类目标的过程中，也应用于企业的战略制定阶段。

3．针对风险度量提出两个新概念——风险偏好(Risk Appetite)和风险容忍度(Risk Tolerances)

针对企业目标实现过程中所面临的风险，风险管理框架对企业风险管理提出风险偏好和风险容忍度两个概念。从广义上看，风险偏好是指企业在实现其目标的过程中愿意接受的风险的数量。企业的风险偏好与企业的战略直接相关，企业在制定战略时，应考虑将该战略的既定收益与企业的风险偏好结合起来，目的是要帮助企业的管理者在不同战略间选择与企业的风险偏好相一致的战略。

风险偏好的概念是建立在风险容忍度概念基础上的。风险容忍度是指在企业目标实现过程中对差异的可接受程度，是企业在风险偏好的基础上设定的对相关目标实现过程中所出现差异的可容忍限度。在确定各目标的风险容忍度时，企业应考虑相关目标的重要性，并将其与企业风险偏好联系起来。

4．增加了三个风险管理要素，对其他要素的分析更加深入，范围上也有所扩大

企业风险管理框架新增了三个风险管理要素——“目标制定”、“事项识别”和“风险反应”。此外，针对企业将管理的重心移至风险管理，风险管理框架更加深入地阐述了其他要素的内涵，并扩大了相关要素的范围。

(1)目标制定(Objective Setting)。在风险管理框架中，由于要针对不同的目标分析其相应的风险，因此目标的制定自然就成为风险管理流程的首要步骤，并将其确认为风险管理框架的一部分。

(2)事项识别(Event Identification)。企业风险管理和内部控制框架都承认风险来自于企业内、外部各种因素，而且可能在企业的各个层面上出现，并且应根据对实现企业目标的潜在影响来确认风险。但是，企业风险管理框架深入探讨了潜在事项的概念，认为潜在事项是指来自于企业内部和外部资源的，可能影响企业战略的执行和目标实现的一件或者一系列偶发事项。存在潜在的积极影响的事项代表机遇，而存在潜在负面影响的事项则称为风险。企业风险管理框架采用一系列技术来识别有关事项并考虑有关事项的起因，对企业过去和未来的潜在事项以及事项的发生趋势进行计量。

(3)风险反应(Risk Response)。企业风险管理框架提出对风险的四种反应方案：规避、减少、共担和接受风险。作为风险管理的一部分，管理者应比较不同方案的潜在影响，并且应在企业风险容忍度范围内的假设下，考虑风险反应方案的选择。在个别和分组考虑风险的各反应方案后，企业管理者应从总体的角度考虑企业选择的所有风险反应方案组合后对企业的总体影响。

(4)风险评估。内部控制框架和风险管理框架都强调对风险的评估，但风险管理框架建议更加透彻地看待风险管理，即从固有风险和残存风险的角度来看待风险，对风险影响的分析则采用简单算术平均数、最差的情形下的估计值或者事项的分布等技术来分析。最好能够找到与风险相关的目标一致的计量单位进行计量，将风险与相关的目标联系起来。风险评估的时间基准应与企业的战略和目标相一致，如果可能，也应与可观测到的数据相一致。企业风险管理框架还要求注意相互关联的风险，确定单一的事项如何为企业带来多重的风险。

正如前面所说，企业风险管理需要管理者建立一种企业总体层面上的风险组合观。在风险评估方面体现为，对各业务单位、职能部门、生产过程或相应的其他活动负责的各层管理者对其负责的部门或单位的风险应进行复合式评估，而企业高层管理者也应从企业总体层面上考虑相互关联的风险和企业的总风险。

(5)信息和沟通。企业风险管理框架扩大了企业信息和沟通的构成内容，认为企业的信息应包括来自过去、现在和未来潜在事项的数据。企业的信息系统的基本职能应以时间序列的形式收集、捕捉数据，其收集数据的详细程度则视企业风险识别、评估和反应的需要而定，并保证将风险维持在风险偏好的范围内。

总的来讲，新的框架强调在整个企业范围内识别和管理风险的重要性，强调企业的风险管理应针对企业目标的实现在企业战略制定阶段就予以考虑，而企业在对其下属部门进行风险管理时，应对风险进行加总，从组织的顶端、以一种全局的风险组合观来看待风险。此外，根据风险管理的需要，对企业目标进行重新的分类，明确战略目标在风险管理中的地位。

二、企业风险管理框架的主要内容

COSO发布企业风险管理框架的目的与当初发布内部控制框架的目的相似，是由于实务界存在对统一的概念性指南的需要。COSO希望新框架能够

成为企业董事会和管理者的一个有用工具，用来衡量企业的管理团队处理风险的能力，并希望该框架能够成为衡量企业风险管理是否有效的一个标准。

对风险的持续确认，与确定抓住什么机遇一样，对保护和提高企业利益相关者的价值是至关重要的。不确定性既代表风险，也代表机遇，既存在使企业增值的可能，也存在使企业减值的风险。在实现企业目标的过程中，企业风险管理框架是一个帮助企业管理者有效处理不确定性和减少风险进而提高企业创造价值的能力的框架。

1．企业风险管理的定义

企业风险管理是一个由企业的董事会、管理层和其他员工共同参与的，应用于企业战略制定和企业内部各个层次和部门的，用于识别可能对企业造成潜在影响的事项并在其风险偏好范围内管理风险的，为企业目标的实现提供合理保证的过程。

这是一个广义的风险管理定义，适用于各种类型的组织、行业和部门。该定义直接关注企业目标的实现，并且为衡量企业风险管理的有效性提供了基础。该定义强调：

(1)企业的风险管理是一个过程，其本身并不是一个结果，而是实现结果的一种方式。企业的风险管理是渗透于企业各项活动中的一系列行动。这些行动普遍存在于管理者对企业的日常管理中，是企业日常管理所固有的。

(2)企业风险管理是一个由人参与的过程，涉及一个企业各个层次员工。

(3)该过程可用于企业的战略制定。企业的战略目标是企业最高层次的目标，它与企业的预期和任务相联系并支持预期和任务的实现。一个企业为实现其战略目标而制定战略，并将战略分解成相应的子目标，再将子目标层层分解到业务部门、行政部门和各生产过程。在制定战略时，管理者应考虑与不同的战略相关联的风险。

(4)该风险管理过程应应用于企业内部每个层次和部门，企业管理者对企业所面临的风险应有一个总体层面上的风险组合观。一个企业必须从全局、从总体层面上考虑企业的各项活动。企业的风险管理应考虑组织内所有层面的活动，从企业总体的活动(如战略计划和资源分配)到业务部门的活动（如市场部、人力资源部），再到业务流程(如生产过程和新客户信用复核)。

(5)该过程是用来识别可能对企业造成潜在影响的事项并在企业风险偏好的范围内管理风险。

(6)设计合理、运行有效的风险管理能够向企业的管理者和董事会在企业各目标的实现上提供合理的保证。

(7)企业风险管理框架针对一类或几类相互独立但又存在重叠的目标，目的在于企业目标的实现。

总之，企业风险管理是一个过程，企业风险管理的有效性是某一时点的一个状态或条件。决定一个企业的风险管理是否有效是基于对风险管理要素设计和执行是否正确的评估基础上的一个主观判断。企业的风险管理要有效，则其设计必须包括所有的要素并得到执行。企业风险管理可以从一个企业的总体来认识，也可以从一个单独的部门或多个部门的角度来认识。即使是站在某一特定的业务部门的角度来看待风险管理，所有的要素也都应作为基准包含在内。

2．企业风险管理的构成要素

企业风险管理分为内部环境、目标制定、事项识别、风险评估、风险反应、控制活动、信息和沟通、监控等八个相互关联的要素，各要素贯穿在企业的管理过程之中。

(1)内部环境

企业的内部环境是其他所有风险管理要素的基础，为其他要素提供规则和结构。企业的内部环境不仅影响企业战略和目标的制定、业务活动的组织和对风险的识别、评估和反应，还影响企业控制活动、信息和沟通系统以及监控活动的设计和执行。董事会是内部环境的重要组成部分，对其他内部环境要素有重要的影响。企业的管理者也是内部环境的一部分，其职责是建立企业风险管理理念，确定企业的风险偏好，营造企业的风险文化，并将企业的风险管理和相关的初步行动结合起来。

(2)目标制定

根据企业确定的任务或预期，管理者制定企业的战略目标，选择战略并确定其他与之相关的目标并在企业内层层分解和落实。其中，其他相关目标是指除战略目标之外的其他三个目标，其制定应与企业的战略相联系。管理者必须首先确定企业的目标，才能够确定对目标的实现有潜在影响的事项。而企业风险管理就是提供给企业管理者一个适当的过程，既能够帮助制定企业的目标，又能够将目标与企业的任务或预期联系在一起，并且保证制定的目标与企业的风险偏好相一致。

(3)事项识别

不确定性的存在，使得企业的管理者需要对这些事项进行识别。而潜在事项对企业可能有正面的彭响、负面的影响或者两者同时存在。有负面影响约事项是企业的风险，要求企业的管理者对其进行评估和反应。因此，风险是指某一对企业目标的实观可能造成负面影响的事项发生的可能性。对企业有正面影响的事项，或者是企业的机遇，或者是可以低消风险对企业的负面影响的事项。机遇可以在企业战略或目标制定的过程中加以考虑，以确定有关行动抓住机遇。可能潜在地抵消风险的负面影响的事项则应在风险的评估和反应阶段予以考虑。

(4)风险评估

风险评估可以使管理者了解潜在事项如何影响企业目标的实现。管理者应从两个方面对风险进行评估——风险发生的可能性和影响。风险发生的可能性是指某一特定事项发生的可能性，影响则是指事项的发生将会带来的影响。对于风险的评估应从企业战略

和目标的角度进行。首先，应对企业的固有风险进行评估。确定对固有风险的风险反应模式扰能够确定对固有风险的管理措施。其次，管理者应在对固有风险采取有关管理措施的基础上，对企业的残存风险进行评估。

(5)风险反应

风险反应可以分为规避风险、减少风险、共担风险和接受风险四类。规避风险是指采取措施退出会给企业带来风险的活动。减少风险是指减少风险发生的可能性、减少风险的影响或两者同时减少。共担风险是指通过转嫁风险或与他人共担风险，降低风险发生的可能性或降低风险对企业的影响。接受风险则是不采取任何行动而接受可能发生的风险及其影响。对于每一个重要的风险，企业都应考虑所有的风险反应方案。有效的风险管理要求管理者选择可以使企业风险发生的可能性和影响都落在风险容忍度之内的风险反应方案。

选定某一风险反应方案后，管理者应在残存风险的基础上重新评估风险，即从企业总体的角度、或者组合风险的角度重新计量风险。各行政部门、职能部门或者业务部门的管理者应采取一定的措施对该部门的风险进行复合式评估并选择相应的风险反应方案。

(6)控制活动

控制活动是帮助保证风险反应方案得到正确执行的相关政策和程序。控制活动存在于企业的各部分、各个层面和各个部门，通常包括两个要素：确定应该做什么的政策和影响该政策的一系列程序。

(7)信息和沟通

来自于企业内部和外部的相关信息必须以一定的格式和时间间隔进行确认、捕捉和传递，以保证企业的员工能够执行各自的职责。有效的沟通也是广义上的沟通，包括企业内自上而下、自下而上以及横向的沟通。有效的沟通还包括将相关的信息与企业外部相关方的有效沟通和交换，如客户、供应商、行政管理部门和股东等。

(8)监控

对企业风险管理的监控是指评估风险管理要素的内容和运行以及一段时期的执行质量的一个过程。企业可以通过两种方式对风险管理进行监控——持续监控和个别评估。持续监控和个别评估都是用来保证企业的风险管理在企业内务管理层面和各部门持续得到执行。

监控还包括对企业风险管理的记录。对企业风险管理进行记录的程度根据企业的规模、经营的复杂性和其他因素的影响而有所不同。适当的记录通常会使风险管理的监控更为有效果和有效率。当企业管理者打算向外部相关方提供关于企业风险管理效率的报告时，他们应考虑为企业风险管理设计一套记录模式并保持有关的记录。

3．风险管理要素和企业目标、企业内各层面及部门的关系

企业的风险管理框架包括四类目标和八要素。四类目标分别是战略目标、经营目标、报告目标和合法性目标，八要素是内部环境、目标制定、事项识别、风险评估、风险反应、控制活动、信息和沟通、监控，是企业实现各类目标的保证，它们相互之间存在直接的关系。而且，新的风险管理框架还强调在整个企业范围内实行风险管理。

4．各管理层在企业风险管理中的地位和职责

(1)董事会。董事会对企业的风险管理负有监督职责，主要通过以下方式实现其职责：

——了解管理者在企业内部建立有效的风险管理的程度；

——获知并认可企业的风险偏好；

——复核企业的风险组合观并与企业的风险偏好相比较；

——评估企业最重要的风险并评估管理者的风险反应是否适当。

(2)管理者。企业的首席执行官对企业的风险管理最终负责，企业的高层确定风险管理的基调，从而影响企业内部环境中的员工操守和价值观及其他因素。

(3)风险管理员。风险管理员是指某一组织内的首席风险管理员或首席风险管理经理，他与企业内其他管理者一起，在各自的职责

范围内建立并维护有效的风险管理框架。首席风险管理员也可以担当监督风险管理进度和帮助其他管理人员在企业内向上、向下和横向报告有关风险信息的职责，并可以成为企业风险管理委员会的一员。

(4)内部审计人员。内部审计人员在企业风险管理的监控中占有重要的地位，这一职责作为其日常职责的一部分。他们可能通过对管理者风险管理过程的充分性和有效性进行监控、检查、评估、报告和提出改进建议来帮助管理者和董事会或审计委员会履行其职责。

(5)其他员工。从某种程度上讲，企业风险管理是企业内每一个员工的责任，因此，风险管理应是企业内每一个员工的工作手册的一部分内容。本质上，企业所有的员工都应提供风险管理所需的信息或者采取必要的措施管理风险。同样，企业所有的员工都有责任向上报告风险。

企业的许多外部相关方也有助于企业目标的实现。如外部审计人员，他们从一个独立、客观的角度对企业的财务报表进行审计和对企业的内部控制进行复核，直接有助于企业目标的实现。同时，外部审计人员还可以向管理者和董事会提供履行其职责有用的额外信息，间接地为企业目标的实现做出贡献。其他向企业提供风险管理的有用信息的相关方还包括行政管理部门、客户、其他与企业进行交易的各方、财务分析师、债券承销商和新闻媒介等等。但是，外部的各相关方并不对企业的风险管理负责。

打印 关闭