

论企业风险管理 内部控制 内部审计

刘秋明

(厦门大学管理学院会计系, 福建 福州 350001)

[关键词] 企业风险管理; 内部控制; 风险导向内部审计

[摘要] 本文集中探讨了企业风险管理的概念, 企业风险管理与内部控制的融合, 以及内部审计在风险管理中的角色、风险导向内部审计计划和程序等相关问题。

[中图分类号] F234.4 [文献标识码] A [文章编号] 1005-9016(2003)11-12-03

一、企业风险管理对内部控制框架的扩展

2002年,美国 Treadway 委员会下属赞助委员会(COSO)对内部控制框架概念的基础上,提出了企业风险管理(Enterprise Risk Management, ERM)的概念,使内部控制的研究发展到一个新的阶段。COSO(2002)这样定义企业风险管理:“企业风险管理是一个过程,受企业董事会、管理当局和其他员工的影响,包括内部控制及其在战略和整个公司的应用,旨在为实现经营的效率和效果、财务报告的可靠性以及现行法规的遵循提供合理保证。”COSO(2002)认为 ERM 为公司董事会提供了有关企业所面临的重要风险,以及如何进行风险管理方面的信息,并进一步提出企业风险管理由环境、事件辨别、风险评估、反应、控制活动、信息和交流以及监督等7个方面组成。

1、环境(Environment):董事和管理当局决定企业的目标、战略和商业模式,商业模式详细说明了经营程序之间如何相互作用,以及在短期内执行战略性经营计划,这些构成了 ERM 的环境,也为 ERM 的其他组成因素提供了框架。其中特别是管理当局的风险偏好,决定了公司对可能出现的预料之外的事件的态度,管理当局和董事会必须明确战略及其执行过程中的风险和回报。

2、事件辨别(Event Identification):在对企业目标、战略和计划以及对企业所处的内部和外部环境都有深刻了解的基础上,企业风险管理要求辨别可能对实现公司目标产生负面影响的所有重要情况或事件,事件辨别的基础是将可能的风险与环境进

行对比。这一步要求综合运用各种专业知识,尽可能地了解企业当前或将来的环境和经营情况。由于未辨别的事件很可能不会出现在反应风险计划之中,因此事件辨别在 ERM 中处于十分关键的地位。

3、风险评估(Risk Assessment):一般用可能性(概率)和影响结果两个维度度量风险,前者是一定的负面影响事件发生的可能性;后者是假设事件发生,对经营、财务报告以及战略产生影响的可能结果,潜在影响一般以对经营、数量、金钱损失以及战略目标可能造成的损失进行计算。风险评估的过程中根据不同的情况,采用定性、定量以及相结合的方法,若可以获取充足的数据,一般采用定量的评估方法;若潜在的可能性及影响结果都较小,或者无法获得数据,则一般采取定性的评估方法。无论采取何种方法进行风险评估,要注意到多个事件同时发生的情形,因此需要考虑和评估两个或两个以上事件同时发生所带来的联合风险。

4、风险反应(Risk Response):企业对每一个重要的风险及其对应的回报进行评价和平衡,结果取决于成本效益分析以及企业的风险偏好。而平衡的反应包括接受、规避或缓和一些风险,后者又包括风险分离、风险转换或者减少(包括通过控制活动)等形式。风险反应是企业风险管理的整体重要组成部分。

5、控制活动(Control Activities):控制活动是管理当局设计的政策和程序,为执行特定的风险缓和反应提供合理保证。控制活动包括在整个

[收稿日期] 2003-03-17

组织中使用的批准、授权、注销、确认、观察、查证以及对经营业绩复核、资产安全、职责分离等方法。企业风险管理将控制活动的概念进行了扩展,认为它是针对所有的风险做出的反应。

6、信息和交流(Information and Communication): 风险辨别、评估、反应和控制活动在组织的各个水平层次上产生有关风险的信息,与财务信息一样,风险信息必须以一定的形式和框架进行交流,使工人、管理层以及董事履行各自的责任。风险评估的信息系统可以产生定期或“例外基础”的时时报告,报告使用趋势指标、业绩矩阵及运营或财务成果的形式,这些报告能够引导出及时的决策。在公司层次,必须对各种数据和信息流进行加工,形成关于公司风险组合轮廓的统一观点,以利于交流。通常存在自上而下式、平行式和自下而上式三种有效的交流形式。自上而下式是管理当局向员工传递风险信息;平行式是部门之间的信息交流和传递;自下而上式是一线员工向管理层汇报风险信息。员工的风险信息交流方面的意识是风险管理环境的重要组成部分,应鼓励员工就其意识到的重要风险与管理层进行交流,管理当局应当重视员工的意见。

7、监督(Monitor): 与内部控制一样,企业应通过持续的监督和独立的评价活动,监督企业风险管理的有效性。持续监督以日常经营中发生的事件和交易为对象,包括管理当局和专门的监督人员的活动。独立评价一般以定期检查计划为基础,或者以日常监督中发现的意外为起点,由于在独立调查、风险评估和报告方面具备能力、技巧和经验,内部审计师是提供独立的评价合适人选。

在10年之后,COSO对内部控制框架的概念进行了扩展,形成了企业风险管理的概念,比较这两个概念,我们可以发现:(1)企业风险管理的定义采用了1992年内部控制框架定义的模式,认为企业风险管理与内部控制同样是一个程序,它不是静态的,而是处于不断的调整 and 变化之中,以适应组织环境的变化;(2)企业风险管理与内部控制有相同的目标,COSO仍然强调了三个目标即经营的效率和效果、财务报告的可靠性以及现行法规的遵循,这与1992年内部控制框架所强调的目标是一致的;(3)企业风险管理的组成由五要素增加到七要素,与1992年内部控制框架的五要素相比,由于对象不同,风险管理更加针对组织面临的“风险”,增加了事件辨认和风险反应两个要素,拓展了概念的深度和广度。

· 企业风险管理与内部控制的融合

内部控制与风险管理的融合很早就引发了人们的关注,但二者的关系仍无普遍认可的观点。一种观点认为内部控制从属于风险管理的范畴,是风险管理的方式之一。例如Krogstad(1999)就认为内部控制不存在于真空或暗箱之中,而存在于协助组织进行风险管理并提升有效的治理程序之中;McNamee也认为内部控制是企业管理者对企业风险的反应。另一种有代表性的观点是将风险管理纳入内部控制体系,认为控制包含了风险。例如美国的COSO(1992)报告将风险评估视为内部控制的五个要素之一;而加拿大CICA的控制委员会则认为“控制应包括对风险的确认和规避”(1999,P.9)。经过争论和实践,人们对二者关系的认识不断深化,逐渐认识到将两者关系隔离的分析方法是不可取的,内部控制与风险管理只有相融合,才能实现最佳效果。例如,Blackburn(1999)就认为“风险管理与内部控制仅是人为的分离,而在现实的商业行为中,他们是一体化的”。COSO(2002)企业风险管理概念的提出,将风险管理与内部控制的融合大大地向前推动了一步,这种融合必将极大地推进内部控制和内部审计的发展。

· 风险管理对内部审计的影响

内部控制向风险管理领域扩展,对内部审计的发展产生了深远影响,这种影响集中体现在风险基础内部审计(risk based internal audit)产生。

由于各国实务各不相同,尚未形成统一的最佳做法,国际内部审计师协会(IIA)目前还没有标准的风险基础审计定义,IIA(2002)的职业问题委员会认为:风险基础审计关注的焦点是组织对所面临影响其目标实现的风险作出的反应,与其他形式的审计不同,这种审计的出发点是风险,而非控制,其目的在于为风险管理提供独立保证,并在必要时加以引导和改进,审计业务的范围和优先次序应由组织所面临的风险所决定。

1、内部审计师在风险管理中的角色和定位

咨询:向董事会、审计委员会、高级管理人员以及其他人员提供公司治理发展、总结会议议程、就风险管理系统方面良好的实务操作提供咨询,从其他组织中吸取教训,为新公布的准则、指南和标准提供客观的解释说明。

提升:通过审计提议、建议、创新、引导、培训及开发工作小组的形式参与整个风险管理循环,并扮演领导者的角色。

参与: 审计师通过团队合作、联合技术攻关, 在系统设计、准则草拟、讨论会引导、保证说明书细化等方面, 更为积极地参与开发、执行甚至风险管理方案的实施。

评价: 对已经存在的或是处于开发过程中的风险管理方案和控制进行独立评价, 这种审计包括复核、监督和保证相关的风险管理系统。

遵循和鉴证: 对经营程序、行为是否遵循了相关准则的要求, 是否与内部控制政策、准则和程序是否一致, 以及报表和陈述提供鉴证。

技术支持: 就风险水平传授审计知识, 向别人传达风险分析技巧和技术, 如何更好地进行控制。

2、内部审计师在风险管理中的审计计划

国际内部审计师协会 2001 年修订的实务标准规定“将审计计划与风险相联系”, 要求内部审计部门的计划应该反映组织的风险战略, 组织的风险管理与内部审计程序之间应该协调一致, 使这两项工作产生协同增效的作用。(1) 应该在可能对影响组织的风险进行评估的基础上, 制定内部审计部门的审计计划, 审计的最终目的是向管理层提供信息, 以减少在实现组织目标的过程中可能带来的负面影响;(2) 审计范围可以包含组织战略性计划的组成部分, 从而考虑并反映整个公司的计划目标, 审计范围可能受到风险管理结果的影响, 制定计划时, 应考虑风险管理的结果;(3) 在评估风险优先次序的基础上安排审计工作。在对风险进行优先排序之后, 在根据风险的重要性分配相关的资源, 例如根据金额的重大性、内部控制的质量、前次审计业务开展的时间等等;(4) 在更新审计范围与相关审计计划中的内容时, 应反

映出管理层的方针、目标、工作重心出现的变化。

3、内部审计师在风险管理中的审计程序

在风险管理过程中, 内部审计师应获取足够的证据, 确认企业主要风险管理目标是否得到实现, 以形成关于风险管理过程是否充分的意见。在收集证据的过程中, 内部审计师应考虑下列审计程序。(1) 研究、评估与机构业务有关的当前发展情况、趋势、行业信息以及其他恰当的信息资源, 确定是否存在可能影响组织的风险, 以及用来解决、监督与再评估这些风险的相关控制程序;(2) 检查公司政策、董事会和审计委员会的会议记录, 确定组织的经营战略、风险管理理念和方法、对风险的偏好以及风险的接受程度;(3) 检查管理层、内部审计师、外部审计师以及其他有关方面以前发表的风险评估报告;(4) 与行政经理和业务部门经理交谈, 确定业务部门的目标、相关的风险以及管理层开展的降低风险活动和控制监督活动;(5) 收集信息, 独立评估风险降低、监督、风险报告和相关控制活动的有效性;(6) 评估针对风险监督活动建立报告专线的恰当性;(7) 评估针对风险管理结果报告的充分性和及时性;(8) 评估管理层的风险分析是否全面、评估为纠正风险管理过程中发现的问题而采取的措施的完整性, 提出改进建议;(9) 确定管理层的自我评估过程是否有效, 这可以通过以下方式进行: 实地观察、直接检测监控程序、测试监督活动所用信息的准确性以及其他恰当的技术;(10) 评估与风险有关、可能说明风险管理实务中存在薄弱环节的问题, 在适当情况下, 与管理层、审计委员会和董事会就此进行讨论。

【参考文献】

- [1] Blackburn, S(1999), "Managing risk and achieving Turnbull compliance", Accountants Digest 417, ABG.
- [2] Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2002) Enterprise Risk Management Framework Key Concepts Briefing Document.
- [3] Committee of Sponsoring Organizations of the Treadway Commission (COSO) (1992) Internal Control - Integrated Framework, AICPA, New Jersey.
- [4] David McNamee (1992), "Change and the nature of auditing", Managerial Auditing Journal, Vol. 10, 1995.
- [5] David McNamee and George M. Selim: "Risk Management: Changing the Internal Auditor's paradigm", P. 5, The Institute of Internal Auditors Research Foundation, 1998.
- [6] Krogstad, J.L., Ridley, A.J. and Rittenberg, L. E. (1999), "Where we're going", Internal Auditor, October, pp. 28 - 33.
- [7] 刘秋明. 我国上市公司内部控制信息披露问题及改进 [J]. 证券市场导报, 2002(6).
- [8] 王光远. 内向型管理审计: 从控制导向到风险导向 [J]. 财会月刊, 2002(7).
- [9] 王光远, 刘秋明. 公司治理下的内部控制与审计 [J]. 中国注册会计师, 2003(2).