第 2 章　内部控制体系框架

【本章导读】

- 新旧 IC-IF 框架
- 新旧 ERM 框架
- 其他内部控制架构
- 萨班斯-奥克斯利法案对内部控制的要求

2.1　IC-IF 框架（1992）

20 世纪 90 年代以前，美国关于内控制度的研究分散于不同的组织机构，如美国注册会计师协会、内部审计师协会、财务经理协会等。从 1991 年开始，美国关于内部控制的研究由 COSO 承担，该组织旨在通过对商业道德、有效的内部控制和公司治理的研究来改善财务报告的质量。

2.1.1　COSO 组织及其发布的报告

COSO 是反虚假财务报告委员会的发起组织委员会（The Committee of Sponsoring Organizations of the Treadway Commission，COSO）。Treadway 委员会（Treadway Commission，即反虚假财务报告委员会，National Commission on Fraudulent Financial Reporting，由于其首任主席的名为 James C. Treadway，因此此协会简称为 Treadway 委员会）1985 年由美国注册会计师协会（AICPA）、美国会计协会（AAA）、财务经理人协会（FEI）、内部审计师协会（IIA）、管理会计师协会（IMA）联合创建，旨在探讨财务报告中舞弊产生的原因，并寻找解决之道。两年后，基于该委员会的建议，其赞助机构成立 COSO 委员会，专门研究内部控制问题，COSO 成立的目的是为风险管理、内部控制、舞弊防范三个方面提供全面完整的框架和指导意见，以促进企业的业绩提升，完善公司治理架构，以减少组织中舞弊的程度。COSO 的愿景是在全球市场上成为风险和控制领域方面的公认的思想领袖，以促进公司治理和减少欺诈舞弊。

自成立以来，COSO 发布了不同的研究报告和指导性的框架意见。1987 年，COSO 发布了《反欺诈性财务报告全国委员会报告》，该报告对财务欺诈的研究和分析没有简单地局限于独立审计师的查错作用，而是密切关注企业法律、金融和其他咨询顾问在财务欺诈中的角色，分析了企业经理班子价值观念和会计、内审与审计委员会的作用，触及了政府管制和大学会计课程设置是否充分有效等问题。报告分别向公众公司、注册会计师、证券委员会以及其他法律部门、教育部门等提出了约 100 条建议。1996 年，COSO 发表了《金融衍生工具使用中的内部控制问题》，该报告模型认为，“风险管理过程需要理解实体的目标和经营活动，

识别市场风险和测度承担的风险，然后决定是否使用衍生产品将风险降低到可以承受的水平。只要简单地忽略与衍生产品有关的部分并代之以其他合适的降低风险行为，这个过程就具有普遍性。”报告为衍生工具用户建立、评估和改善内部控制，提供了指导性建议。1999年，COSO 利用 1987—1997 年欺诈性财务报告公司样本，在归纳其公司特征、控制环境特征、欺诈特征的基础上，发布了《欺诈性财务报告：1987—1997——美国公众公司分析》。报告探讨了三个欺诈高发行业（信息技术、保健和金融服务业）的欺诈特点，发现三个行业的欺诈手段存在显著差异，如信息技术业最常见的欺诈手段是收入欺诈，而金融服务业最常见的手段是资产欺诈和资产盗用，并且研究了财务报告欺诈与公司治理之间的关系，发现欺诈样本公司与其所在行业标准相比，具有相当弱的公司治理机制。至今为止，COSO 发布了一系列关于内部控制的报告（见表 2-1），可以看出，近年来 COSO 一方面致力于原有框架更新（IC-IF 框架于 2013 年更新，ERM 框架于 2017 年更新），另一方面针对新的经济形势和市场环境，强调内控框架的应用环境的适应及对风险的控制和平衡。

表 2-1　COSO 发布的报告一览表

年份	报　　告
1987	Report of the National Commission on Fraudulent Financial Reporting（反欺诈性财务报告全国委员会报告）
1992	Internal Control—Integrated Framework（内部控制——整体框架）
1996	Guidance on Monitoring Internal Control Systems Internal Control Issues in Derivatives Usage（金融衍生工具使用中的内部控制问题）
1999	Fraudulent Financial Reporting：1987－1997—An Analysis of U.S. Public Companies（欺诈性财务报告：1987—1997——美国公众公司分析）
2004	Enterprise Risk Management—Integrated Framework（企业风险管理——整体框架）
2006	Internal Control over Financial Reporting—Guidance for Smaller Public Companies（财务报告的内部控制——对小企业的指南）
2009	Guidance on Monitoring Internal Control（监管内部控制的指南）
2009	Effective Enterprise Risk Oversight：The Role of the Board of Directors（有效的企业风险监督：董事会的作用）
2009	Strengthening Enterprise Risk Management for Strategic Advantage（为策略优势而加强风险管理）
2010	Fraudulent Financial Reporting：1998－2007—An Analysis of U.S. Public Companies（欺诈性财务报告：1998—2007——美国公众公司分析）
2010	Board Risk Oversight—A Progress Report：Where Boards of Directors Currently Stand in Executing their Risk Oversight Responsibilities（董事会风险监控进展报告：董事会如何执行他们的风险监控责任?） COSO's 2010 Report on ERM：Current State of Enterprise Risk Oversight and Market Perceptions of COSO's ERM Framework（COSO 2010 关于风险管理报告：企业风险监控和 COSO 的 ERM 框架的接受度的现状分析）
2011	Embracing Enterprise Risk Management：Practical Approaches for Getting Started（企业风险管理的实务操作方法） Developing Key Risk Indicators to Strengthen Enterprise Risk Management（发展主要风险显示指标以加强企业风险管理）
2011	COSO Releases Internal Control-Integrated Framework for Public Comment（COSO 颁布新的内部控制整体框架的征求意见稿）

续表

年份	报　　告
2012	Enterprise Risk Management—Understanding and Communicating Risk Appetite（企业风险管理——理解并且沟通风险偏好）
2012	Thought Paper on Enhancing Board Oversight by Avoiding and Challenging Traps and Biases in Professional Judgement（加强风险监督以避免专业判断中的陷阱和偏差）
2012	Managing Risks of Cloud Computing the Focus of COSO's Latest Thought Leadership（COSO 框架中云计算的风险管理研究）
2012	COSO Releases for Comment Internal Control Over External Financial Reporting（COSO 颁布对外部财务报告内部控制的征求意见稿）
2012	Risk Assessment in Practice（风险评估实践）
2013	2013 Internal Control-Integrated Framework（2013 版的内部控制整体框架）
2013	The 2013 COSO Framework SOX Compliance—One Approach To An Effective Transition（ 2013 版内控框架与萨班斯法案——一种有效的过渡方法）
2013	Integrating the Triple Bottom Line into An Enterprise Risk Management Program（把三重底线融入风险管理框架）
2014	Demonstrating How Frameworks Improve Organizational Performance and Governance（框架如何改善公司业绩和治理结构）
2015	COSO in The Cyber Age（网络时代的 COSO 框架）
2015	Leveraging COSO Across The Three Lines of Defense（三重防线平衡 COSO 框架）
2016	Fraud Risk Management Guide（欺诈风险管理指南）
2017	Enterprise Risk Management — Integrating with Strategy and Performance.（企业风险管理框架——战略与业绩的整合）
2018	COSO Enterprise Risk Management - Integrating with Strategy and Performance: Compendium of Examples（企业风险管理框架的实例概要）
2018	Applying enterprise risk management to environmental, social and governance-related risks（应用企业风险管理框架于环境、社会和治理相关的风险）
2019	2013 COSO Integrated Framework: An Implementation Guide for the Healthcare Provider Industry.（2013 内控整合框架：医疗健康行业的实施指南）
2019	Managing Cyber Risk in a Digital Age（数字化时代管理网络风险）

2.1.2　IC-IF 框架（1992）的内容

1992 年，COSO 在进行了深入研究之后发布了一份关于内部控制的纲领性文件，即《内部控制——整体框架》（*Internal Control—Integrated Framework*，IC-IF），它标志着内部控制理论与实践进入了整体框架的阶段。COSO 内部控制报告分为四部分：

第一部分“管理层总结”，是对内部控制总体构架的高度总结，是针对总裁和高级管理人员、董事会成员、律师和监管当局而写的。

第二部分“总体构架”，对内部控制进行了定义，阐述其构成要素，为管理层、董事会及他人提供了评估内部控制有效性的准则。

第三部分“外部团体报告”，对那些已经或准备公开披露其对编制财务报表进行内部控制的企业提供了指导。

第四部分“评估工具”，提供了对内控系统进行评估的有用资料。

COSO 以一个独立的机构对内部控制进行专门的研究，无疑提高了研究的系统性与深度。1992 年 COSO 发布的《内部控制——整体框架》，不仅被美国的企业，也被世界上其他国家的不少企业和经济组织所接受，并融入各种规章制度之中，用以控制经营活动，实现企业既定的经营目标。在内控整体框架中，COSO 对内部控制的定义为：内部控制是受企业董事会、管理当局和其他职员的影响，旨在取得经营效果与效率；财务报告的可靠性；遵循法规等目标而提供合理保证的一种过程。第一类针对主体的基本经营目标，包括业绩、盈利目标和对资源的保护。第二类与编制可靠的公开财务报表（published financial statements）有关，包括中期和简要财务报表，以及从盈余披露等公开发布的报表中摘引的选定财务数据。第三类涉及遵循主体适用的那些法律和法规。这三类目标——经营目标、报告目标和合规目标，相互区别而又彼此交叉，体现了不同的需求，也可能是不同管理人员的职责，这一分类还利于区分每类控制的可能结果。内部控制目标，是决定内部控制运行方式和方向的关键，也是评价内部控制实施效果的最终标准。然而内控的几个目标有它固有的特点：从企业自身角度来看，经营目标是企业主观非常乐意付出努力去实现的，但实现的情况受客观环境的制约，如竞争的激烈程度、产品的受欢迎程度、是否有例外事件的发生等；而合规性目标和报告目标是企业被动地遵守，很大程度上是外界施加的，企业只要愿意实现就一定会实现的，其实现程度受着企业主观意愿的影响。

报告提出了内部控制的五个重要组成要素：控制环境、风险评估、控制活动、信息与沟通、监控，深化了内部控制的理念和应用。这些内控要素源自管理层经营企业的方式，并与管理过程融为一体。报告中也提出，尽管这些构成要素适用于所有的主体，但是它们在中小型公司的实施可能与大型公司有所不同。尽管小型公司也会拥有有效的内部控制，但是其内部控制可能不太正式、不太健全。这些构成要素如下。

1. 控制环境

控制环境（control environment）设定了一个组织的基调，影响其员工的控制意识。它是内部控制的其他所有构成要素的基础，提供了秩序和结构。控制环境的要素包括：员工的诚信、道德价值观和胜任能力；管理层的理念和经营风格；管理层分配权力和责任、组织和开发其员工的方式；以及董事会给予的关注和指导。

2. 风险评估

每个主体都面临来自外部和内部的必须加以评估的多种风险。风险评估（risk assessment）的前提是确立在不同层次上的相互衔接、内在一致的目标。风险评估就是识别和分析与实现目标相关的风险，从而为确定应该如何管理风险奠定基础。由于经济、行业、监管和经营条件将会持续变化，因此需要有识别和应对与这些变化有关的特殊风险的机制。

3. 控制活动

控制活动（control activities）是指那些有助于保证管理层的指令得到贯彻执行的政策和程序。它们有助于确保采取必要的措施来处置实现主体目标的风险。控制活动发生在整个组织之中，遍及所有的层级和所有的职能。它们包括诸如审批、授权、验证、调节、经营业绩评价、资产保护和职责分离等一系列活动。

4. 信息与沟通

企业主体必须以适当的方式在一定的时间范围内识别、获取和沟通有关的信息（information and communication），以便员工能够履行其责任。信息系统生成包含经营、财务以及与合规有关信息的报告，从而使经营和控制企业成为可能。它们不仅处理内部生成的信息，还处理与经营决策和对外报告所需的外部事项、行为和情形有关的信息。有效的沟通还必须是广义的，即信息必须在组织内自上而下、平行以及自下而上地传递。所有员工都必须从最高管理层那里获得控制责任必须严格履行的明确信息。他们必须了解自己在内部控制体系中的作用，以及个人的活动与其他人的工作之间的关联。他们应该有向上传递重要信息的途径。此外，与外部各方，如客户、供应商、监管者以及股东之间也需要有效的沟通。

5. 监控

需要对内部控制体系进行监控（monitoring），这是一个不断对内部控制体系的运行质量进行评估的过程。它可以通过持续监控活动、个别评价或两者的结合来实现。持续监控发生在经营过程中。它包括日常的管理和监控活动，以及员工在履行其职责过程中所采取的其他行动。个别评价的范围和频率主要取决于对风险的评估和持续监控程序的有效性。对于内部控制的缺陷，应该自下而上进行汇报，性质严重的应该向最高管理层和董事会报告。

内部控制受企业董事会、管理当局和其他职员的影响，企业组织中的每一个人都应对其承担相应的责任。

① 管理层。首席执行官负有最终的责任，其确定了“最高层的基调”。首席执行官向高级管理人员提供领导和指导，高级管理人员则把建立更为具体的内部控制政策和程序的责任分配给负责该单元各项职能的人员。对于相应层次的责任而言，每位管理人员实际就是他或她所承担的那部分责任的首席执行官。

② 董事会。管理层向董事会负责，董事会提供治理、指导和监督。有效的董事会成员应该客观、有能力，并富有质疑精神。一个强大、积极的董事会，尤其是与有效的向上沟通渠道和有能力的财务、法律和内部审计职能相结合时，通常能够最好地发现和矫正这类问题。

③ 内部审计师。内部审计师在评价控制体系的有效性方面起着重要的监控作用。

④ 其他人员。内部控制是组织中每个人的责任，因此它应该成为每个人岗位描述中明确或隐含的一部分。明确各自的职责，提供系统所需的信息，实现相应的控制；对经营中出现的问题，对不合法、违规行为有责任与上级沟通。

公司的外部人员也有助于控制目标的实现，如外部审计可提供客观独立的评价，通过财务报表审计直接向管理阶层提供有用信息；另如法律部门、监管部门、客户、其他往来单位、财务分析师、信用评级公司、新闻媒体等也都有助于内部控制的有效执行。但是，外部各方并不对主体的内部控制体系承担责任，也不是公司内部控制体系中的一部分。

2.1.3　IC-IF 框架（1992）的贡献

1992 年颁布的 IC-IF 框架蕴含了许多崭新的理念和思想，这些理念和思想，不仅对过去，而且对现在甚至未来的企业管理、财务工作和独立审计都有着重要影响，主要表现为以下几个方面。

1. 准确定位内部控制基本目标

COSO 报告将内部控制目标分为三类：经营目标、报告目标和合规目标，有利于不同的人从不同的视角，关注企业内部控制的不同方面。同时 COSO 报告指出内部控制本身不是目的，而是实现目标的手段。内部控制的目标是帮助企业奔向经营目标、完成使命和减少经营过程中的风险。

2. 内控要素之间的整合体系

COSO 报告提出内部控制由控制环境、风险评估、控制活动、信息与沟通和监控五项要素构成，这些构成要素之间存在协同和联系，从而形成一个整合的体系。内部控制系统是“嵌入于”（built in）企业经营和管理过程中的一项基础设施（infrastructure），不是后天添加物（built on），内控系统应与管理活动的计划、执行和监控职能交织融合在一起。嵌入式的控制体系能够避免不必要的成本，并能够对环境的变化迅速做出反应。

3. 内部控制对目标的实现仅仅提供的是“合理保证”

内部控制可以帮助主体实现其业绩和盈利目标，防止资源的损失，可以帮助保证财务报告的可靠性，而且有助于确保企业符合适用的法律和法规，避免对其声誉的损害以及其他后果。总之，它可以帮助主体到达它想去的地方，并避开途中的隐患和意外。即使有效的内部控制，也只能帮助主体实现这些目标。它可以向管理层提供有关主体在实现其目标方面取得的进展或者缺乏进展的信息。但是内部控制不能把一个内在素质差的经理变成一个好的经理。内部控制体系无论设计和运行得多么好，都只能就主体目标的实现向管理层和董事会提供合理而非绝对的保证。目标实现的可能性受到所有内部控制体系都存在的固有局限的影响。因此，内部控制不是解决所有问题的“灵丹妙药”。

4. 内部控制是一个“动态”的过程

内部控制不是一项制度或一个机械的规定，企业外部环境的变化必然要求企业内部控制能够不断地“与时俱进”，内部控制是一个发现问题、解决问题的循环过程。因此，需要对内部控制系统保持持续性的关注，同时内控系统应有应对不断变化的客观世界的机制。

5. 强调“人”与环境的重要性

COSO 报告指出人和环境是推动企业发展的引擎。内部控制是由人来设计和实施的，企业中的每位员工都受内部控制的影响，并通过自身的工作影响着他人的工作和整个内部控制系统。同时，在环境控制中，注重“软控制”，即指那些属于精神层面的事物，如高级管理阶层的管理风格、管理哲学、企业文化等。

6. 糅合了管理与控制的界限

在 COSO 报告中，控制不再是管理的一部分，管理和控制的职能与界限已经模糊。

2.2 IC-IF 框架（2013）

1992 年 COSO 颁布的 IC-IF 框架已成为全世界使用最为广泛的内部控制框架体系，已运行二十余年，然而随着社会的进步和经济的发展，企业或组织的业务经营环境发生了巨大的变化，如互联网的广泛使用、科学技术的进步、商业模式的改变以及全球一体化等。与此同时，利益相关者更多地参与治理过程，并且寻求更透明和更负责的内控体系来支持决策和组织的治理，这些变化都要求 IC-IF 适应环境并进行调整。COSO 于 2010 年 11 月 18 日宣布对

1992年的IC-IF框架进行修订，整个修订项目分为四个阶段：评估及构想阶段（assess & survey），构建和设计阶段（design & build），公开征求意见阶段（public exposure），以及修订、定稿阶段（finalize）。

COSO委员会委托普华永道会计师事务所（PricewaterhouseCoopers，PwC）为该项目的主持者和撰写者，COSO董事会成立了由业界、学术界、政府机构和非营利组织以及来自监管机构和标准制定机构的观察员共同组成的咨询委员会，对项目的进展进行支持——除了COSO的五个发起组织，还有公众会计公司、监管机构——美国证监会（Securities and Exchange Commission，SEC）、政府问责办公室（Government Accountability office，GAO）、联邦存款保险公司（The Federal Deposit Insurance Corporation，FDIC）、美国公众公司会计监督委员会（Public Company Accounting Oversight Board，PCAOB），以及其他一些协会的参与——国际会计师联合会（International Federation of Accountants，IFAC）、信息系统审计和控制协会（Information Systems Audit and Control Association，ISACA）加入该咨询委员会，同时近千名利益相关者在项目全球征求意见阶段发表了意见。

2011年12月19日COSO发布了征求意见稿，2013年5月14日公布了新的IC-IF框架体系，新框架体系包含内容摘要以及框架和附录两个部分，内容摘要是对新框架进行高度总结，包括内部控制的定义、目标、原则、内部控制的有效性和局限性等，使用对象为首席执行官和其他高级管理层、董事会成员和监管者；框架内容和附录包括内部控制的组成部分及相关的原则和关注点，并为各级管理层在设计、实施内部控制和评估其有效性方面提供了指导。附录包括词汇表、对于小型企业的特殊考虑、与1992版的变化总结和框架的非重要性附加参考。与框架同时颁布的还有两份说明文件，一份是《评估内部控制体系有效性的工具示例》（*Illustrative Tools for Assessing Effectiveness of a System of Internal Control*），为管理层在应用框架特别是评估有效性方面提供了模板和行动方案，另一份是《外部财务报告内部控制：方法与范例汇编》（*Internal Control over External Financial Reporting*（*ICEFR*）：*A Compendium of Approaches and Examples*），为在准备外部财务报告过程中应用框架中的要素和原则提供了实际的方案和示例。

2.2.1　IC-IF框架（2013）总体架构

COSO委员会本是由五家私人专业财务组织发起的，其并没有权利发布政府法规或专业组织指南类的标准。COSO的内控框架及指南，仅仅概述了一个适用于大多数企业的内部控制方法和内部控制最佳实践。然而，COSO内部控制框架的概念早已成为其他领域或美国以外很多国家制定相关标准的参考。

自IC-IF框架1992年面世以来，企业所处的商业及运营环境均发生了巨大的变化：治理监督的需求扩大；市场和运营的全球化程度增强，跨国并购活动频繁；企业商业运营方式的改变和复杂化，很多企业已突破原有的商业模式，广泛采用合资企业、战略联盟、对外合作、共享服务、外包服务等更复杂的方式；法律、法规、制度和标准变得更为复杂，合规需求扩大，传统的内控方法难以满足要求；对企业责任和组织能力的期望更多，随着新产品和服务的不断引进、新流程和技术的日益推广，组织需要具备更高的能力以承担更多的责任，企业利益相关者也更加强调商业活动中的责任和诚信问题；技术的发展、使用和更新愈发受重视，信息技术不再是批量处理交易的独立大型主机，而是一些复杂分散可移动的应用程

序，旨在实现不同系统、不同组织、不同流程和技术层面的切换，技术的变革颠覆了内部控制各个要素的实施方法；防止和检查舞弊的需求增加……因此，无论是 IC-IF 框架的制订者 COSO 委员会，还是框架的借鉴实施者，均认为非常有必要对 1992 年的框架进行修订，以适应时代的变化。

2013 年新 IC-IF 框架并不是对 1992 年版本的否定，2010 年 9 月至 2011 年 1 月，COSO 对 700 多家使用 COSO 内控框架的单位进行问卷调查。结果显示，大部分反馈意见支持对 COSO 内控框架进行修订和更新，但不建议推倒重来。新框架在基本概念、内容和结构，以及要素、评价内控体系有效性标准等方面均没有变化（见表 2-2），与其说修订，不如说成优化，并非改变内部控制的定义、评估和管理方式，而是要提供相关概念的指导和实践范例，力图提高 IC-IF 框架的易操作性，以及可以使更多的企业采纳使用，以提升整体内部控制质量。

表 2-2　2013 年 IC-IF 框架的变化与没有变化的内容

没有变化：	变化：
◇ 内部控制核心定义	◆ 商业及运营环境的变化
◇ 内部控制的三个目标和五个要素	◆ 经营目标和报告目标的扩大化
◇ 内部控制五要素有效性标准	◆ 五要素中需考虑的具体原则
◇ 设计、实施、评价内部控制中主观判断的重要作用	◆ 与经营、合规和非财务报告目标相关的额外的方法和例子

无论是 1992 年框架（见图 2-1），还是 2013 年框架（见图 2-2），都是由一个立方体的三个维面——目标、要素、主体共同构成。目标是主体所致力于实现的；要素是主体实现目标必不可少的；主体结构包括组织层面、业务部门以及职能机构，这三者之间有着直接的联系，它们的关系可以通过一个立方体来表示。

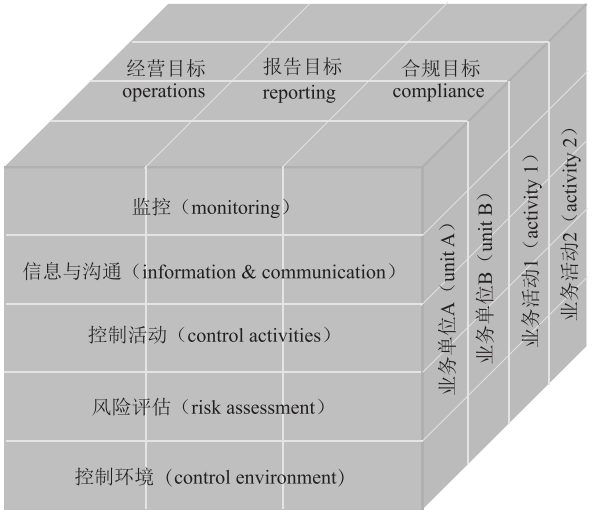

图 2-1　1992 年 IC-IF 框架结构

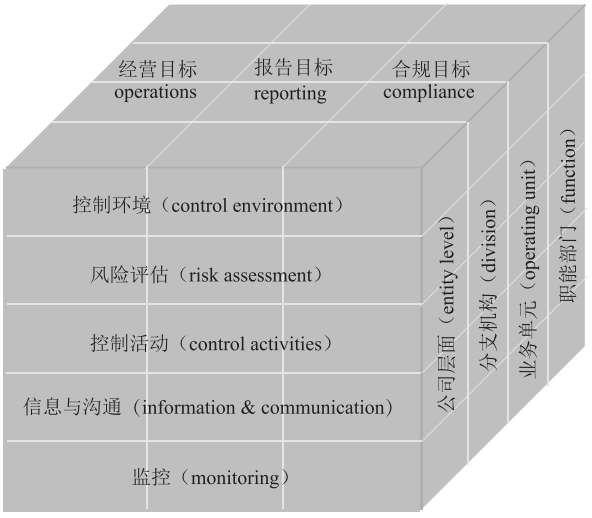

图 2-2　2013 年 IC-IF 框架结构

① 立方体从顶部开始，从左到右依次是内部控制目标的三种类别：经营、报告和合规目标。

② 立方体的正面代表内部控制的五个要素：控制环境、风险评估、控制活动、信息与沟通以及监控，内部控制一个动态、反复且整合的过程。例如，风险评估不仅影响控制环境和控制活动，而且也要求主体重新考虑信息与沟通或监控活动。因此内部控制不是上一个要素对下一个要素产生影响的线性过程，它是各个要素之间互相产生影响的整合过程。

③ 立方体的侧面代表主体结构，包括公司层面、分支机构、业务单元和职能部门，如销售、采购、生产以及其他与内部控制相关的部门。没有两个主体拥有完全相同的内部控制体系。主体、目标和内部控制体系会因为行业、监管环境以及其他因素影响而有所不同。

总的来说，有效的内部控制是通过五要素的共同协作来维持的，以达到最终的内控目标。

从 1992 年和 2013 年的立方体来看，基本保持原貌，但还是有两个地方不同。一是 1992 年框架，将控制环境置于底部——是其他内部控制要素的基础。该要素在 2013 年的框架中位于内控要素的顶层，更为恰当地反映了该要素的地位。该项变化并不涉及概念上的变化。尽管控制环境的位置在图表顶层，它仍应该被看作所有其他内部控制要素的基础，它同时影响着其他三个目标以及所有业务单元和实体活动，如今顶部的新位置，将控制环境置于一个更加重要的位置，就好像企业的首席执行官出现在传统组织结构图的顶端一样。

二是立方体的侧面有变化，1992 年框架用的业务单位（unit）和业务活动（activity），2013 年框架用的公司层面（entity level）、分支机构（division）、业务单元（operating unit）和职能部门（function），可以看出新框架对于主体的确认更加细化，揭示了企业的目标既可以从整个企业的层面来设定，也可以针对企业内部具体的部门、业务单元和功能来设定（包

括销售、采购和生产等业务流程），新框架侧面则是提供目标分层的路径选择，同时新框架描绘出了大多数企业等级式的自上而下的组织结构，也反映了内部控制是全员、全部门、全业务、全流程和全面性的控制。

总之，立方体描述了以下三者之间的直接关系：企业目标（即企业所要力求实现的）；内部控制要素（即企业实现目标所需要的条件）；以及业务单元和企业内部的其他结构单元（即内部控制要素运行的各企业层面）。每个内部控制要素都跨越和适用于所有三类目标。

2.2.2 IC-IF 框架（2013）的内控目标

管理层应在董事会的监管之下，设定与主体使命、愿景和战略相协调的组织层面目标。设定目标是内部控制的先决条件，1992 年与 2013 年的 IC-IF 框架的内部控制目标设定并没有改变，依然是经营目标、报告目标、合规目标。

新框架扩展了报告目标的范围，更强调了非财务的报告目标，而且关注内控整体目标与子目标的协调与形成。

1. 经营目标

经营目标与主体基本使命和愿景的实现有关，这也是主体存在的根本理由。经营目标并不仅仅以提高公司的财务业绩为最终诉求，还可能与生产能力、产品质量、环境保护、改革创新以及客户和员工的满意度相关。这些目标适用于所有类别的主体，包括营利性组织和非营利性组织。如果一个主体的经营目标没有被恰当地制定或清晰说明，可能导致其资源的浪费。

2. 报告目标

报告目标是指编制报告，供组织和利益相关方使用。新框架认为财务报告不应局限于对外公布的财务报告，还应包括其他类别的内外部财务和非财务报告。

外部财务报告目标——主体需要实现外部财务报告目标，以履行对利益相关方的义务并满足他们的期望。财务报表对进入资本市场必不可少，并且在获得合同与供应商打交道时也可能是至关重要的。投资者、分析师和债权人往往会依赖于一个主体的财务报表，通过与同业或其他替代投资对象的对比来评估其业绩表现。管理层也可能被要求按照规则、规章及外部准则所设定的要求来公布财务报表。

外部非财务报告目标——管理层按照法律、规章、标准或其他框架的要求报告外部非财务信息。在与汇报财务报告内部控制有效性的管理报告相关的规章和标准中，会涉及非财务报告的要求，这些要求也是外部非财务报告目标的组成部分。在没有法律法规、规章、标准或框架要求的情况下，外部报告则代表外部沟通。

内部财务和非财务报告目标——给管理层和董事会的内部报告包含管理组织所必要的信息，用于支持决策及评估主体的活动和绩效。内部报告目标信赖于管理层和董事会的偏好和判断。由于主体的战略方向、运营计划和期望各不相同，因此内部报告目标也不同。

四类内部控制报告目标之间的关系见图 2-3。

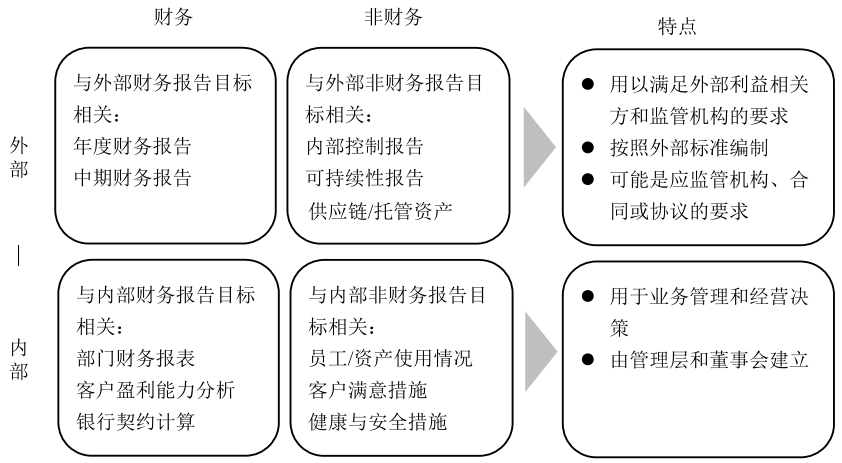

图 2-3　四类报告目标之间的关系

资料来源：COSO 委员会 2013 年 IC-IF 框架

3. 合规目标

主体必须根据相关法律、法规及规章的要求开展活动，并经常需要采取特定的行动。法律、法规及规章为主体建立了最低的行为准则要求。组织应当将这些行为准则整合在主体目标中，一些组织有可能制定比法律规定更为严格的目标，在设定这些目标时，管理层可以行使自主裁量权。

总之，有效的内部控制体系可以为主体目标的实现提供合理保证。有效的内部控制体系可以将影响目标实现的风险降低至可接受水平，这些风险可能涉及以上一种、两种或全部三种目标。1992 年框架指出，组织并非能够完全把控其运营目标的实现过程。对于运营目标，内部控制体系仅能为管理者和作为监管者的董事会提供合理的保证，使其能够及时了解到组织各个目标的实现情况。

新框架同样认为组织无法完全控制目标的实现，这与原框架的观点保持一致。同时，新框架认为如果外界状况对具体目标的实现不构成重大冲击，组织或许能够对目标的实现提供合理保证。

2.2.3　IC-IF 框架（2013）的内控原则

2013 年 IC-IF 框架的一个重大变化就是制定了支持内部控制五要素的内部控制原则（见表 2-3）。相比于 1992 年版隐晦提出了内部控制的核心原则，新版本明确列示了 17 条内部控制原则来描述与内部控制五要素有关的基础概念。这些原则广泛适用于各种类别的组织，包括营利组织、非营利组织、政府机构等，以帮助它们实现各个层面的目标。新框架提供了一种原则导向的方法，能够灵活设计、实施和推进内部控制，并留有判断空间——这些原则可在组织层面、运营层面和职能层面应用。

表 2-3　IC-IF 框架（2013）内部控制原则

控制环境
（1）诚信和道德价值观的承诺
（2）董事会独立于管理层，对内控实施监督
（3）组织架构、汇报路线、合理的权力与责任
（4）吸引、发展和保留认同组织目标的人才
（5）内部控制责任人的问责制度
风险评估
（6）设定清晰明确的目标
（7）识别、分析和管理实现目标的风险
（8）考虑潜在的舞弊行为
（9）识别并评估内部控制的重大改变
控制活动
（10）选择并执行可将风险降至可接受水平的活动
（11）针对信息技术，选择并执行控制活动以支持目标实现
（12）通过政策和程序来部署控制活动
信息与沟通
（13）获取、生成、使用高质量信息
（14）对内部控制信息进行内部沟通
（15）对内部控制信息进行外部沟通
监控
（16）进行持续和单独的内部控制评估
（17）对内部控制缺陷的评估和沟通

除了对应内部控制五要素的 17 条具体原则，2013 年版的内控框架还提出每一个原则的关注点（见表 2-4），关注点是内部控制原则的重要特征，管理层可以自行决定某些关注点不适用或不相关，也可以再识别并考虑其他关注点。关注点能够协助管理层设计、实施和执行内部控制以及评估相关原则是否存在并持续运行。

表 2-4　IC-IF 框架（2013）内部控制原则与对应的关注点

原则（principle）	关注点（points of focus）
（1）诚信和道德价值观的承诺	1. 确定“高层基调”
	2. 建立行为准则
	3. 评价对行为准则的遵守情况
	4. 及时处理行为偏差

续表

原则（principle）	关注点（points of focus）
（2）董事会独立于管理层，对内控实施监督	5. 建立监督责任
	6. 运用专业知识
	7. 保持独立运作
	8. 履行对内控体系的监督责任
（3）组织架构、汇报路线、合理的权力与责任	9. 考虑主体的所有架构
	10. 制定汇报路线
	11. 定义、分配及限制权力与责任
（4）吸引、发展和保留认同组织目标的人才	12. 建立政策及实践
	13. 评估胜任能力并改善不足
	14. 吸引、培养和留用人才
	15. 规划与准备后续人才
（5）内部控制责任人的问责制度	16. 通过组织架构、权力与责任来强化问责机制
	17. 建立绩效衡量、激励和奖励机制
	18. 评估绩效衡量、激励和奖励机制的持续相关性
	19. 考虑额外的压力
	20. 评价业绩并赏功罚过
（6）设定清晰明确的目标	21. 反映管理层的选择（运营目标）
	22. 考虑风险容忍度（运营目标）
	23. 涵盖运营和财务绩效目标（运营目标）
	24. 形成资源配置的基础（运营目标）
	25. 符合适用的会计准则（外部财务报告目标）
	26. 考虑重要性水平（外部财务报告目标）
	27. 反映主体经营活动（外部财务报告目标）
	28. 符合既定的外部标准和框架（外部非财务报告目标）
	29. 考虑所需要的精确度水平（外部非财务报告目标）
	30. 反映主体的活动（外部非财务报告目标）
	31. 反映管理层的选择（内部目标）
	32. 考虑精确度要求（内部目标）
	33. 反映主体活动（内部目标）
	34. 反映外部法律、法规及规章（合规目标）
	35. 考虑风险容忍度（合规目标）

续表

原则（principle）	关注点（points of focus）
（7）识别、分析和管理实现目标的风险	36. 涵盖主体、下属单位、分部、业务单元和职能部门层面
	37. 分析内部和外部因素
	38. 让适当层级的管理层参与
	39. 评估所识别风险的重大性
	40. 决定如何应对风险
（8）考虑潜在的舞弊行为	41. 考虑不同类别的舞弊
	42. 评估动机和压力
	43. 评估机会
	44. 评估态度和合理化
（9）识别并评估内部控制的重大改变	45. 评估外部环境变化
	46. 评估商业模式变化
	47. 评估领导层变化
（10）选择并执行可将风险降至可接受水平的活动	48. 与风险评估相结合
	49. 考虑主体特有的因素
	50. 确定相关业务流程
	51. 评估控制活动类别的组合
	52. 考虑控制活动的适用层级
	53. 强调职责分离
（11）针对信息技术，选择并执行控制活动以支持目标实现	54. 决定在业务流程中应用的信息技术和信息技术一般控制之间的关系
	55. 建立与信息技术基础设施相关的控制活动
	56. 建立与安全管理流程相关的控制活动
	57. 建立与信息技术引进、开发、维护流程相关的控制活动
（12）通过政策和程序来部署控制活动	58. 制定政策和程序以支持管理层指令的实施
	59. 确立政策和程序执行的职责和问责制
	60. 及时执行
	61. 实施整改措施
	62. 选用足以胜任的人员
	63. 重新评估政策和程序
（13）获取、生成、使用高质量信息	64. 识别信息需求
	65. 收集内外部数据
	66. 将相关数据转化为信息
	67. 在处理过程中确保信息质量
	68. 考虑成本效益原则

续表

原则（principle）	关注点（points of focus）
（14）对内部控制信息进行内部沟通	69. 沟通内部控制信息
	70. 与董事会沟通
	71. 提供独立的沟通途径
	72. 选择相关的沟通方式
（15）对内部控制信息进行外部沟通	73. 能与外部沟通
	74. 能从外部输入沟通
	75. 与董事会沟通
	76. 提供独立的沟通途径
	77. 选择相关的沟通方式
（16）进行持续和单独的内部控制评估	78. 考虑持续评估和单独评估的组合
	79. 考虑变化率
	80. 建立对基础的理解
	81. 选用具备专业知识的人员
	82. 与业务流程整合
	83. 调整范围和频率
	84. 客观评估
（17）对内部控制缺陷的评估和沟通	85. 评价结果
	86. 沟通缺陷
	87. 监督整改措施

由政策和程序构成的控制嵌入于内部控制流程中。政策表明了管理层及董事会为实现控制有效性会如何做；而程序则是一系列保证政策落实的行动。组织应建立并执行要素中的控制，以使相关原则有效。新框架的要素与原则为管理层提供了一套评价内部控制有效性的标准，新框架要求内部控制各要素和相关原则均应存在并持续运行，且共同运行。每个关注点都与 17 个原则中的某个原则一一对应，而每个原则也都与五大要素中的某个要素一一对应。这些关注点旨在为管理层提供有用的指引，协助其设计、实施和执行内部控制，以及评估相关原则是否存在和发挥效用。正如前文所述，新框架明确了管理层可以自行决定关注点是否适合或与组织相关，另外，COSO 并没有断言这些关注点可以形成一个完整清单，管理层应当根据组织的活动和详细情况识别和考虑其他与原则相关的重要因素，管理层可以自由判断新框架所提供关注点的合适度或者相关度，然后根据企业的具体情况，来选择和考虑与某一特定原则密切相关的其他重要特点。

总之，“要素—原则—关注点”这种以原则导向的内控框架设计，为企业内部控制的设计与实施提供了一套细化的路线图，另外，新框架中也强调依赖管理层的判断，而不是像旧框架要求严格基于证据。内部控制如何实施，如何评价，如何认定有效性，如何选择关注

点，企业组织可以拥有自己的判断，管理层应通过判断去除那些失效、冗余甚至完全无效的控制。新内控框架颁布后，对于何时开始实施新框架，COSO 董事会表示，使用者应当按其具体情形，在可行的情况下尽早开始应用 2013 年版本的新框架来开展相关工作和文件记录。COSO 认为，1992 年版本框架所涵盖的重要概念和原则，基本上颇为完善且已获市场普遍认可，因此使用者在 2014 年 12 月 15 日之前仍然可以继续使用 1992 年版本，在该日期后，旧框架将作废，代之以新框架。在过渡期间，使用者在应用其 IC-IF 框架进行外部报告时，应明确披露所使用的是原始版本还是 2013 年版本。

2.3 ERM 框架（2004）

2001 年，COSO 开展了一个项目，委托普华永道开发一个评价和改进管理当局所在组织的企业风险管理的框架。正是在此期间，发生了一系列令人瞩目的企业丑闻和失败事件——安然、世通等，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。COSO 认为，对管理者来说，一个非常重大的挑战就是确定某个组织在努力创造价值的过程中准备承受多大的风险。而制定统一定义、能够提供主要原理与概念、具有明确的方向与指南的风险管理框架将有助于企业迎接这一挑战。经过两年多的时间，COSO 于 2004 年 9 月发布《企业风险管理——整体框架》（*Enterprise Risk Management—Integrated Framework*，ERM 整体框架）的研究报告。

2.3.1 企业风险管理框架概述

《企业风险管理——整体框架》共分 12 章，具体如下：定义（definition）、内控环境（internal environment）、目标设立（objective setting）、事项识别（event identification）、风险评估（risk assessment）、风险应对（risk response）、控制活动（control activities）、信息与沟通（information and communication）、监控（monitoring）、职能与责任（roles and responsibilities）、风险管理的局限（limitations of enterprise risk management）、该做些什么（what to do）。关于 ERM 与 IC-IF 的关系，COSO 在《企业风险管理——整体框架》前言中指出，企业风险管理框架是建立在内部控制整体框架基础之上的，对企业风险管理内容的关注更加广泛与深入。ERM 并非替代 IC-IF，而是包容了 IC-IF，在内控的有关概念上，两者保持了一致与连贯，ERM 比 IC-IF 更广泛，拓展和细化了内部控制。企业风险管理框架不仅可以满足企业加强内部控制的需求，也能促进企业建立更为全面的风险管理体系，ERM 框架结构如图 2-4 所示。

ERM 对风险管理的定义是：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，应用于战略制定并贯穿于企业之中，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。企业风险管理的具体含义如下。

（1）一个过程，它持续地流动于主体之内。企业风险管理并不是静止的，而是渗透于主体各种活动中的持续、反复相互影响的动态过程。这些活动渗透和潜藏于管理当局经营企业的方式之中。

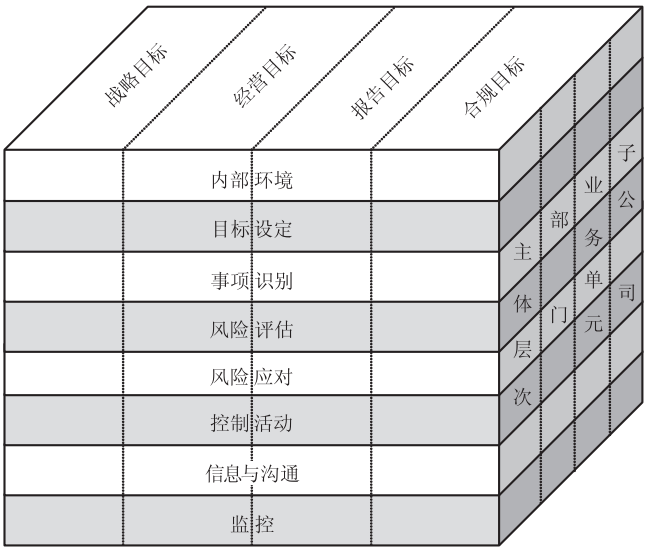

图 2-4　ERM 框架（2004）

（2）由组织中各个层级的人员实施。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及其言行来完成的。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。

（3）应用于战略制定。一个主体设定其使命与愿景，并制定战略目标，主体为了实现其战略目标而制定战略，企业风险管理应用于战略制定之中，此时管理当局应考虑与备选战略相关的风险。比如说，有两个选择，一个选择是收购其他公司以扩大市场份额，另一个是削减采购成本以实现更高的利润率。这些战略选择中的每一个都会带来许多风险，第一个选择的风险在于新市场的风险和与其他公司的协同效应的实现程度，第二个选择的风险在于新的技术和供应商的选择。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。

（4）贯穿于企业。企业风险管理要考虑组织各个层级的活动，从战略规划和资源配置等企业层次的活动，到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，都贯穿着企业的风险管理。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个人对各自的活动形成一个风险评估。

（5）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。风险容量是一个主体在追求价值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。风险容量与一个主体的战略直接相关，在战略制定过程中应予以考虑，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价值创造与主体的风险容量相协调的战略。

（6）能够向一个主体的管理当局和董事会提供合理保证。

（7）力求实现一个或多个不同类型但相互交叉的目标。

2.3.2 企业风险管理框架的构成要素和目标

同 1992 年的 COSO 报告相比，ERM 报告增加了一个目标和三个要素。在主体既定的使命或愿景（vision）范围内，管理当局制定战略目标，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。① 战略（strategic）目标。高层次目标，与使命相关联并支撑其使命。② 经营（operations）目标。有效和高效率地利用其资源。③ 报告（reporting）目标。报告的可靠性。④ 合规（compliance）目标。符合适用的法律和法规。

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。这些构成要素如下。

（1）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。

（2）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。企业风险管理能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。

（3）事项识别。必须识别影响主体目标实现的内部事项和外部事项，区分风险和机会。机会将被反馈到管理当局的战略或目标制定过程中。

（4）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。

（5）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和风险容量以内。

（6）控制活动。制定和执行政策与程序，以帮助确保风险应对得以有效实施。

（7）信息与沟通。相关的信息可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，包括信息在主体中向下、平行和向上流动。

（8）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监督活动、个别评价或者两者结合来完成。

2.3.3 ERM 框架与 IC-IF 框架的对比

一个主体中的每个人都对企业风险管理负有一定的责任。首席执行官负有最终的责任，其他管理人员支持风险管理理念，促使其符合风险容量，并且在各自的职责范围内根据风险容限去管理风险。其他人员负责根据既定的指引和规程严密进行企业风险管理。董事会提供对企业风险管理的重要监督。相对于 IC-IF 框架，ERM 强调了风险官员的责任。风险官员是指一些组织中的首席风险官或风险管理人员，由首席执行官设立并且在其支持之下，风险官员拥有资源以帮助实现跨子公司、业务、部门、职能机构和活动的企业风险管理。风险官员

的职责包括以下内容：

（1）建立企业风险管理政策，包括确定职能与责任，以及参与设定执行目标；

（2）确定各业务单元对于企业风险管理的权利和义务；

（3）提高企业风险管理能力，包括推动企业风险管理专门技术的发展，以及帮助管理人员协调风险应对和主体的风险容限，并建立恰当的控制；

（4）指导企业风险管理、其他经营计划和管理活动的整合；

（5）建立一套通用的风险管理语言，包括围绕可能性和影响共通的测度指标，以及通用的风险类别；

（6）帮助管理人员制定报告规程，包括定性和定量的下限，以及对报告过程的监控；

（7）向首席执行官报告进展和暴露的问题，并建议必要的措施。

和原有的IC-IF相比，ERM增加了一个战略目标，且处于比其他目标更高的层次。战略目标来自一个主体的使命和愿景，因而经营目标、报告目标和合规目标必须与其相协调。

ERM引入了两个概念：风险容量（risk appetite）和风险容限（risk tolerance）。风险容量是一个主体在追求价值的过程中所愿意承受的风险的数量。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，也有一些主体采用定量的方法，比如平衡增长、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。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，以便限制其短期巨额资本损失风险。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。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。

风险容量一般而言比较广泛，而风险容限是具体化可操作的，风险容限的设定有助于确保主体保持在风险容量之内。风险容限有一定的灵活度，而风险容量设置的是不能超越的风险边界。举个例子，某个组织对风险投资有着较低的风险容量（low risk appetite），愿意投资新的领域，但是只愿意承担较低的风险。这个组织的风险容限的表述为：我们期望承担不要超过5%的风险——一项新的行业投资在未来10年内经营利润的损失不超过5%。

ERM还加入了一个观念，即风险的组合观，在实现目标的过程中，从“组合”的角度考虑复合风险。

从构成要素而言，ERM把IC-IF原来的五要素扩展成八要素，即把原先风险评估的要素从风险管理的角度进行了扩展，即目标设定、事项识别、风险评估和风险应对。ERM的要素还有一个不同，就是把控制环境改成了内部环境，从概念理解上来看，内部环境的含义更广，包括了前文所述的风险容量和风险容限的概念。ERM框架与IC-IF框架的区别如表2-2所示。

表 2-5　IC-IF 内控框架与 ERM 企业风险管理框架的区别

框架类型 / 项目	IC-IF 内部控制框架	ERM 企业风险管理框架
覆盖范围	仅包括内部控制	内部控制被涵盖在企业风险管理之内，是其不可分割的一部分，企业风险管理比内部控制更广泛，拓展和细化了内部控制
目　标	经营目标、报告目标、合规目标	战略目标、经营目标、报告目标、合规目标
风险观	从一定角度评价和管理妨碍完成目标的风险	风险的组合观，除了在分别考虑实现主体目标的过程中关注风险之外，还有必要从“组合”的角度考虑复合风险，增加了两个概念：风险容量和风险容限
构成要素	控制环境、风险评估、控制活动、信息与沟通、监控	内部环境、目标制定、事项识别、风险评估、风险应对、控制活动、信息与沟通、监控
职能与责任	明确董事会、内审人员、首席执行官等企业各个层级人员在内部控制中的职能与责任	明确董事会、内审人员、首席执行官等企业各个层级人员在风险管理中的职能与责任，并增加了风险官员的职能与责任，扩充了董事的职能

2.4　ERM 框架（2017）

2014 年 10 月 21 日，COSO 委员会宣布开展修订 2004 年 ERM 框架的项目，更新将改进框架的内容，提升框架与日益复杂的商业环境之间的关联性，旨在反映风险管理理论和实践及利益相关人预期的演进，开发相关工具帮助管理层报告风险信息，检查和评估企业风险管理的实施情况。

2015 年 2 月 15 日，中国企业内部控制标准委员会与美国 COSO 委员会签署合作备忘录——《中国企业内部控制标准委员会与美国 COSO 委员会合作备忘录》的签署，标志着中美在内部控制领域的交流与合作取得重要进展，有利于我国准确了解国际内部控制标准的最新发展动向，进一步完善我国内部控制规范体系；有利于我国全面参与国际内部控制标准的制定，提高我国在国际内部控制领域的影响力和话语权；有利于打造我国全方位、多领域的会计对外交流格局。按照合作备忘录的规定，美国 COSO 委员邀请了我国参与 ERM 框架相关修订工作，这是第一次外方主动邀请我国参与国际内控标准制定工作。

2016 年 6 月 14 日，COSO 委员会公布了拟更新修订的 ERM 框架，并向公众征求意见，截止时间为 2016 年 9 月 30 日。此次更新的框架为《企业风险管理——将风险和战略、业绩结合在一起》（*Enterprise Risk Management—Aligning Risk with Strategy and Performance*），此次修订反映了企业风险管理的理论和实践的更新，并且对 2004 框架的概念进行了更清晰的阐述。此次主要的更新有：采用了元素和原则的结构；简化风险管理的定义；强调风险和价值的联系；更新企业风险管理的整体化关注；反思文化的作用；强调业绩表现与企业风险管理的关系；将风险管理融入企业决策过程；划清风险管理和内部控制的界限等。

2017 年 9 月 6 日，COSO 委员会颁布了期待已久的新 ERM 框架《风险管理框架——战略与业绩的整合》（*Enterprise Risk Management—Integrating with Strategy and Performance*）。ERM 框架的名字也经历了几番变化。如表 2-6 所示。

表 2-6　ERM 框架名称的变化

时间	框架版本	框架名称
2014 年	旧版本	Enterprise Risk Management—Integrated Framework 企业风险管理——整体框架
2016 年	征求意见稿	Enterprise Risk Management—Aligning Risk with Strategy and Performance 企业风险管理——将风险和战略、业绩结合在一起
2017 年	新版本	Enterprise Risk Management—Integrating with Strategy and Performance 企业风险管理——战略与业绩的整合

征求意见稿与正式版本名称发生了变化，从“Aligning”到“Integrating”也反映了整个框架核心理念的变化。前者强调的是协同、协调，后者意为整合、融合，表达企业风险管理和企业战略及绩效是一个有机的、密不可分的整体。仅仅一个词，将企业风险管理重新定位，从一个看似独立的风险与战略、绩效的协同的“附属工作”，强调将风险真正融入战略与绩效管理工作中去，成为一个整体，不再割裂开来。

旧版本对风险的定义：“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。”旧版 ERM 框架将事项区分为风险和机会。从表述看，虽然也提到了对机会的把握，但总体上还是偏向对负面影响的控制。新版本对风险的定义简化了很多——“风险是事项发生并影响战略和业务目标之实现的可能性”。这是一种较中立的概念，将风险和机会等同视之，试图让风险管理者从被动防御负面影响的心态转变为主动出击管理风险以创造价值的心态，让风险管理与价值创造的过程融为一体。就对企业风险管理的概念来看，新旧版本的变化也非常大，旧版本对企业风险管理的定义是：“企业风险管理是一个过程，它由一个主体的董事会、管理层和其他人员实施，应用于战略制定并贯穿于企业之中，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。”新版框架简化了对企业风险管理的定义——“组织在创造、保存、实现价值的过程中赖以进行风险管理的，与战略制定和实施相结合的文化、能力和实践”。这个概念变化更为彻底，将风险管理工作直接从“一个流程或程序”提升到“一种文化、能力和实践”，更加强调风险与价值的结合，突出价值创造而不只是防止损失，这样也避免了和内部控制定义的界限不清。

2.4.1　ERM 框架（2017）的要素

2004 年版本的 ERM 框架从某种意义上说是 1992 年 IC-IF 框架的翻版，无论是从要素、目标，还是从定义来看，只不过是从风险的视角来看内部控制，所以 2004 年的 ERM 框架与 1992 年的 IC-IF 框架同样采取了 COSO Cube（立方体）的结构，这也是近年来，无论是理论界还是实务界，企业风险管理与企业内部控制一直纠缠不清，时而暧昧、时而清晰的原因。大刀阔斧改革后的 2017 年 ERM 框架彻底对此作了个了断，放弃原来的 Cube 结构，用

一种新的类似于 DNA 螺旋的形状来展示 ERM 框架（见图 2-5），更强调了要素间的彼此融合。在 COSO 公布的《常见问题》（*Frequently Asked Questions*）解释上，COSO 表明两个体系并不是相互代替或取代，不存在孰优孰劣，两个体系侧重点不同，相互补充，虽然新 ERM 框架关注内部控制之外的领域，但是内部控制框架仍旧是一种经历时间考验的企业控制体系，为设计、执行和评估内部控制的有效性的一个可行且合适的框架。虽然框架命名中有“企业（Enterprise）”一词，但 COSO 希望这个框架应用面更广，不仅仅局限于企业，而是可以适用于任何类型、任何规模的组织，包括营利机构、非营利机构、政府部门等。

图 2-5　ERM 框架（2017）

新 ERM 框架的五个要素与 ICIF 框架的五要素迥异，而且最明显的标志是“去风险化”——要素中的“风险”一词均去除，不再一味强调风险视角下的企业治理与管理要素，而是强调将风险“嵌入”到整个企业管理中去，并与战略相结合，最后达到价值提升的目的。新 ERM 框架的五个要素分别如下。

1. 治理与文化（Governance&Culture）

治理决定了组织的基调，加强了企业风险管理的重要性和监督责任。文化与道德价值观、期望的行为以及对风险的理解有关。

2. 战略与目标设定（Strategy&Objective-Setting）

企业风险管理、战略和目标设定在战略规划过程中共同发挥作用。风险偏好的建立是与战略保持一致的；业务目标将战略付诸实施，同时作为识别、评估和应对风险的基础。

3. 绩效（Performance）

可能影响战略和业务目标实现的风险需要确定和评估。在风险偏好的背景下，风险按风全偏好的不同划分优先秩序。然后，组织选择风险应对措施并采取它所能承受风险的投资组合。这个过程的结果需要向关键风险利益相关者报告。

4. 检查与修订（Review&Revision）

通过检查绩效水平，组织可以考虑企业风险管理的各项要素在一段时间内是否正常运行，以及基于实质性变化的视角，考虑应做什么样的修订。

5. 信息、沟通与报告（Information，Communication&Reporting）

企业风险管理，需要从内部或者外部，自上而下，或者自下而上，不断地获取和分享必

要的信息。

2.4.2　ERM 框架（2017）的原则

新 ERM 框架采用了国际文件惯用的要素加原则的结构（Components&Principals），包含 5 个要素，细分为 20 个原则（见表 2-7）。2013 年 ICIF 框架也是采用这种结构，新的结构加强了新框架的可读性、可用性和一致性。

表 2-7　ERM 框架（2017）要素与原则

要素	原则
治理与文化	1. 董事会执行风险监督——董事会对战略进行监督，执行治理责任，支持管理实现战略和业务目标
	2. 建立运营机构——组织在追求战略和业务目标方面建立运营机构
	3. 定义崇尚的文化——组织定义期望的行为来描述所崇尚的文化
	4. 展示对核心价值的承诺——组织表现出对核心价值观的承诺
	5. 吸引，发展和保留有能力的个体——组织致力于建立符合战略和业务目标的人力资本
战略与目标设定	6. 分析业务环境——组织考虑业务环境对风险状况的潜在影响
	7. 定义风险偏好——组织在创造、维护和实现价值的背景下定义风险偏好
	8. 评估替代策略——组织评估替代策略，并对其潜在影响进行风险预测
	9. 制定业务目标——组织在确定协调和支持战略的各个层次的业务目标的同时，应考虑风险
绩效	10. 识别风险——组织应确定影响战略和业务目标绩效的风险
	11. 评估风险的严重程度——组织评估风险的严重程度
	12. 风险排序——组织将风险优先排序，作为选择风险应对的基础
	13. 实施风险响应——组织识别并选择风险响应措施
	14. 建立风险组合观——组织开发和评估风险组合观
检查与修订	15. 评估实质性变化——组织识别和评估可能严重影响战略和业务目标的变更
	16. 评估风险和绩效——组织评价绩效并考虑风险
	17. 企业风险管理持续改进——组织应追求企业风险管理的不断完善
信息，沟通与报告	18. 利用信息系统——组织利用信息技术系统来支持企业风险管理
	19. 沟通风险信息——组织使用沟通渠道来支持企业风险管理
	20. 风险、文化和绩效报告——组织在内部各个层次进行风险、文化和绩效的报告

2.5　其他内部控制架构

对于内部控制框架的理解，不仅仅局限于 COSO 报告，只不过我国的内控体系借鉴的是美国的 COSO 和 ERM 框架，所以理论界对这两者讨论得比较多，其实其他国家或地区也颁布了自己的内部控制的规范和体系。

2.5.1 加拿大的 COCO 报告

1992 年，加拿大特许会计师协会（Canadian Institute of Chartered Accountants，CICA）成立了控制基准委员会（The Criteria of Control Board），简称 COCO 委员会，该委员会的使命是发布有关内部控制系统设计、评估和报告的指导性文件。经过两年的研究，COCO 委员会于 1995 年 10 月正式发布了关于内部控制的框架性文件——《控制指南》（*Guidance on Control*）。

COCO 将“内部控制”的概念扩展到“控制”，其定义为“一个组织的各种要素（包括资源、系统、过程、文化、结构和任务等）聚集在一起，以支持目标的达成”。内部控制的目标为：运作的效率和效益；内部和外部报告的可靠性；法律、法规和内部政策的遵循。与 COSO 相比，COCO 框架是一种更为广泛的概念化方法。期望达到的目标，大体上是一致的，细微处的不同在于，COCO 报告增加了对内部政策（internal policy）的遵循，另外，COSO 报告强调的是财务报告的可靠性，而 COCO 强调的则是内部和外部报告的可靠性。

COCO 报告的重心是从目的、承诺、能力、监督与学习四个方面提出 20 项控制标准。这四个要素通过“行动”这个环节联结成为一个闭合的循环，COCO 框架如图 2-6 所示，COCO 框架各个要素的控制标准如表 2-8 所示。

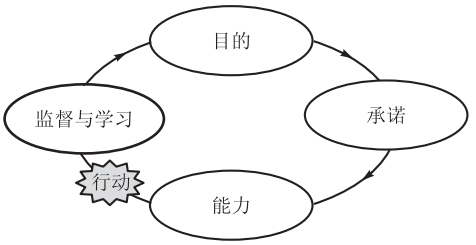

图 2-6　COCO 框架

表 2-8　COCO 要素及控制标准

COCO 要素	控　制　标　准
目　　的	拟订与沟通各种目标
	识别与评估内外风险
	制定与实施各种政策
	建立与沟通各种计划
	制定可衡量的目标与指标
承　　诺	制定与实施具有共识的道德价值观
	人力资源政策应与价值观和目标达成一致
	清楚界定权利、职责与应负责任
	加强互信气氛

续表

COCO 要素	控　制　标　准
能　　力	人员应具有必要的知识、技巧、工具
	沟通应有助于价值观和目标实现
	及时识别与沟通相关与适当的资讯
	整合组织不同的决策与行动
	控制作业应考虑目标、风险及控制因素
监督与学习	监督从内外获得的资讯
	根据特定目标监督绩效
	应注意检测目标与制度中潜在的因素
	根据变更或缺点改变资讯需要
	建立与执行稽查程序
	定期评估内控成效并进行沟通

COCO 委员会在 1999 年发布了《评估控制指南》（*Guidance on Assessing Control*），该指南描述了形成一份评估报告的 10 步程序，其中评估的重点是关于目标的信息和相关风险的管理。COCO 对内部控制的评估更多着眼于企业未来，而不是对过去的评价，如评估未来持续成功的机会和风险，审查与未来业绩表现、机遇和风险相关的信息，评价需要特殊关注和监督的控制要素信息，以及战略审查、项目批准和准备如何应付突发事件等。

无论是 COSO 报告，还是 COCO 报告，都是内部控制重要的框架结构，虽有不同之处，但两者对内部控制的某些概念的理解达成了以下共识：

（1）内部控制是一个过程；

（2）内部控制受各个层级的人的影响；

（3）内部控制只能合理保证目标的实现；

（4）内部控制要实现相应的目标，是一种手段，而非目的。

加拿大证监会认可的、可供加拿大上市公司使用的内部控制框架共有三个：美国 COSO 内控框架、英国公司治理准则和加拿大 COCO 内控框架。尽管 COCO 内控框架具有简洁易懂、实施成本低等优点，但是近年来其应用情况不容乐观。目前，大多数加拿大上市公司采用美国 COSO 内控框架；少数上市公司采用英国公司治理准则；极少数的上市公司采用加拿大 COCO 内控框架。2002 年美国萨班斯法案出台后，加拿大证监会（Canadian Securities Administrators，CSA）也着手研究制定加拿大上市公司实施内部控制的有关政策措施。2005 年至 2008 年，CSA 先后发布了公司治理指引（2005）、公司治理实践的披露（2005）、年度报告的声明（2008）等与内部控制有关的上市公司规则。其中“年度报告的声明”类似于美国萨班斯法案第 404 条款，要求加拿大上市公司的首席执行官（CEO）和首席财务官（CFO）每季度评价财务报告相关内部控制和披露控制与程序的设计有效性，以及每年度评价财务报告相关内部控制和披露控制与程序的运行有效性。相对于美国萨班斯法案的严厉实施要求，加拿大采取较为宽松的内部控制实施政策，即加拿大上市公司只需在年报中披露其

与内部控制相关的信息，而不要求聘请注册会计师对财务报告相关内部控制和披露控制与程序的有效性进行审计。

2.5.2 英国 Turnbull 报告

英国内部控制的发展离不开公司治理研究的推动。20 世纪八九十年代，是英国公司治理问题研究的一个高峰期，各种专门委员会纷纷成立，并发布了各自的研究报告，其中比较著名的有卡德伯利报告（Cadbury Report，1992）、拉特曼报告（Rutterman Report，1994）、格林伯利报告（Greenbury Report，1995）和哈姆佩尔报告（Hampel Report，1998）。在吸收这些研究成果的基础上，1998 年最终形成了公司治理委员会综合准则（Combined Code of the Committee on Corporate Governance）。综合准则很快就被伦敦证券交易所认可，成为交易所上市规则的补充，要求所有英国上市公司强制性遵守该准则。准则中有三条涉及公司内部控制：一是公司董事会负责建立、健全一套完整的企业内部控制制度，以保护投资者的投资和公司的资产；二是董事会负责每年检查和评价一次内部控制制度的有效性，并向股东报告，要求内部控制的检查范围应涵盖所有控制，包括财务、运营、合规、风险等方面；三是没有设立内部审计职能的公司应随时评估公司各方面对内部审计工作的需求。此外，伦敦股票交易所的“上市规则”（the listing rule）中对披露内部控制情况作了以下规定：上市公司在年报中要报告执行内部控制制度的情况，如果没有建立健全内部控制或部分建立了内部控制，要说明详细原因。

“上市规则”和“联合准则”仅对建立和披露内部控制提出了原则要求，但并没有提供建立内部控制的具体方法或模式。鉴于上市公司应提出一个内部控制方面的具体操作性的规定，伦敦股票交易所委托英国特许会计师协会（Institute of Chartered Accountants in England and Wales，ICAEW）成立了以 Turnbull 先生为主席，由董事长、总经理、财务经理、部门经理、外部审计人员、企业员工以及大学教授组成的委员会，就如何帮助在英国上市的公司贯彻执行“上市规则”和“联合准则”中的建立健全内部控制的要求进行研究。该委员会 1999 年 9 月完成了一份系统的指导企业建立内部控制的报告，即《内部控制——董事关于“联合规则”的指南》（*Internal Control—Guidance for Directors on the Combined Code*），又称 Turnbull 报告。

Turnbull 报告中指出，内部控制是指包括政策、过程、任务、行为以及公司其他方面的体系。内部控制目标在于效率和效益性，保证内外部报告的质量，遵循法律、法规和内部政策。Turnbull 报告中内部控制由四个要素组成：控制环境、控制活动、信息沟通、监控。企业管理者承担建立合理的内部控制系统、审核内部控制有效性及向股东报告有关发现的职责；对控制系统的审核应覆盖所有控制，包括经营性、合规性控制以及风险管理；同时，明确执行风险控制政策是管理层的职责，管理层应确认内部控制在风险管理方面是有效的。Turnbull 报告指出健全的内部控制应具备的基本特征：内部控制根植于公司的经营之中，形成公司文化的一部分，换言之，它不仅仅是为了取悦监管者而进行的年度例行检查，更是真正意义上的对公司既定战略目标的执行和公司治理的延伸；针对公司所面临的日新月异的风险，内部控制应具备快速反应的能力；内部控制应有对管理中存在的缺陷进行快速报告的能力，并且能及时采取纠正措施。实际上，Turnbull 报告是一种原则导向

的规定，该项指导原则并不能列举出所有内部控制的问题，各公司应根据自己的具体情况具体分析。这是因为英国的上市公司不习惯执行面面俱到的法律条文，更喜欢法规仅列出一些重要方面和需关注的问题，具体如何操作由企业自己决定。与美国 IC-IF 框架相比，英国内部控制的目标是保障股东投资与公司资产的安全，更倾向于保护股东利益，更强调风险。

2004 年，财务报告委员会（Financial Reporting Council）成立 Turnbull 工作组（Turnbull Review Group），由恒生银行集团财务总监道格拉斯·弗林特负责，审查 1999 年版本的 Turnbull 报告是否需要修订和更新。2005 年 10 月，财务报告委员会发布了新修订后的报告 *Internal Control—Revised Guidance For Directors On the Combined Code*，对原有 Turnbull 报告作了局部的修订：一是进一步强调要求将内部控制嵌入公司业务流程的各个环节和程序；二是在处理好披露内部控制与保守商业秘密的关系的前提下，要求董事会在年报中披露已经或正在采取的弥补检查过程中发现的内部控制重大缺陷的措施；三是要求在年报中增加信息量以帮助股东了解公司风险管理过程。

英国的公司治理准则（UK Corporate Governance Code）对董事会领导及有效性、薪酬、会计责任和股东联系等方面制定相应的规则，所有在英国上市的公司都必须遵守这项准则。2012 年 9 月，财务报告委员会颁布治理准则的最新版本，要求从 2012 年 10 月开始执行，新的治理准则中：C2 条款风险管理和内部控制，要求董事会对为取得策略目标所承担风险的性质和程度负有主要责任，而且应维持合理的风险管理和内部控制体系。董事每年都需要对内部控制和风险管理体系进行审视和监督，应覆盖所有的重大控制，包括财务、经营和遵循方面的控制。C3 条款审计委员会和审计师，要求董事会应建立正式且透明的制度以及如何进行应用财务报告、风险管理和内部控制原则，并应与公司的审计师保持适当的联系。虽然 Turnbull 报告被认为是风险管理和内部控制的有效框架，然而学界和理论界都认为其需要更新以适应新治理准则的要求。

2.5.3　法国内部控制框架

法国的金融业发展历史悠久，其监管体系也随着市场的发展变得较为庞大。到 20 世纪末，专门针对证券市场的监管机构就有证券交易委员会（COB）、金融市场理事会（CMF）和金融管理纪律理事会（CDGF）。2003 年颁布的《金融安全法》授权设立了金融市场监管局（AMF），取代了上述三大委员（理事）会的相关监管职能，成为证券市场的统一监管机构。《金融安全法》中有关公司内部控制的规定主要包括以下内容：上市公司的董事会主席应当在其年度报告中披露公司治理情况及相应的内部控制程序；上市公司应当在其年度报告中附上审计师对本公司财务会计信息的编制和处理的相关内控程序的观察报告；金融监管局每年应当根据各上市公司按照前两条披露的情况编写内控报告建议书。由于金融监管局每年编写的内控报告建议书是在对当年各上市公司内控披露情况进行总结的基础上提出了改良的建议，因此，虽然不属于法规规定，但也构成上市公司改进内部控制报告的要求之一。上述有关规定在发布后适用于所有有限责任公司，2005 年 7 月，金融安全法修正案将这一规定的适用范围限定于上市公司。由于该规定过于原则，缺少详尽的操作指引，金融监管局于 2005 年 1 月组建内部控制指引工作组，研究起草内部控制

指引框架。历经两年，于 2007 年 1 月 22 日发布内部控制系统框架（The Internal Control System：Reference Framework）。

法国内部控制框架中指出，内部控制是一个由所承担的责任来定义和执行的公司体系，它由一系列的资源、行为模式、过程和行动来组成。内部控制的目标为：① 法律和规定的遵守；② 由执行管理层或管理委员会所制定的规则和方向性指南被正确应用；③ 公司内部过程正确地发挥作用（特别在保护资产安全方面）；④ 财务信息的可靠。内部控制不仅仅局限于一系列的流程或财务处理的过程，它应着力于关注运作的有效性和资源的有效利用，并考虑到运作、财务和遵守法规方面的所有风险。

法国内部控制框架指出内部控制由以下五个要素构成。

（1）权责分明的组织架构系统，包括有助于实现公司目标的合适的组织架构、明确界定各组织单位的责任和权力、促使员工拥有知识和技能的人力资源管理政策、电子信息系统以及运营程序、工具和实践操作等。

（2）相关和可靠信息的内部沟通系统。使所有公司的利益相关者能够及时地获得所有可靠信息，并使得他们行使自己的相关责任。

（3）风险识别和分析系统。公司能够利用该系统识别、分析、管理公司所面临的内外风险。

（4）控制活动。控制活动发生在组织的每一个层次，它们的作用在于阻止或监视可能发生的风险，并有助于公司整体目标的实现。

（5）对内部控制程序的持续监督检查系统。为保证所有控制系统对实现公司目标是相关的和恰当的，需要对所有内部控制系统进行监督检查。一般而言，由管理部门实施这一监督检查，主要包括对所有已记录事故的分析，对控制活动执行的效果以及内部审计人员的工作等进行监督检查。

在整个内部控制框架中，除了内控的定义和要素等基本理念的阐述外，框架的第三部分是关于公司财务报告的内部控制程序，它适用于除银行和保险业以外的所有公开上市的公司的财务和会计信息的内部控制设计，其由一系列的原则和规范所组成。与财务信息的编制和处理相关的内部控制程序，主要包括会计信息生成程序、财务报表的编制和与内部有关单位的沟通。财务报告内部控制的目的是保证：① 财务和会计信息遵守了适用的准则；② 高级管理人员或管理委员会对财务信息的生成能够正确地予以指导；③ 公司的资产得到保护；④ 欺诈和财务报告问题尽可能地被发现和阻止；⑤ 所收到的信息以及用于内部监控的信息是可靠的；⑥ 财务报表及其他提供给市场的信息是可靠的。

财务报告的内部控制不仅仅包括一系列的手册和文件，其执行需要考虑人的参与，因此应充分考虑控制环境对内部控制的影响，同时，会计过程是整个财务报告内部控制的核心。会计过程将企业所有基本业务活动转换成财务或会计信息，以便于企业利益相关者的理解，同时也利于不同企业之间业务的比较，如图 2-7 所示，显示产生会计信息的过程不仅仅局限于传统的财务会计部门，应是一个更广泛参与的过程。

从以上可以看出，法国内部控制框架是以财务报告内部控制为主的，而且其框架的适用范围与对外披露财务报表的范围相配套。

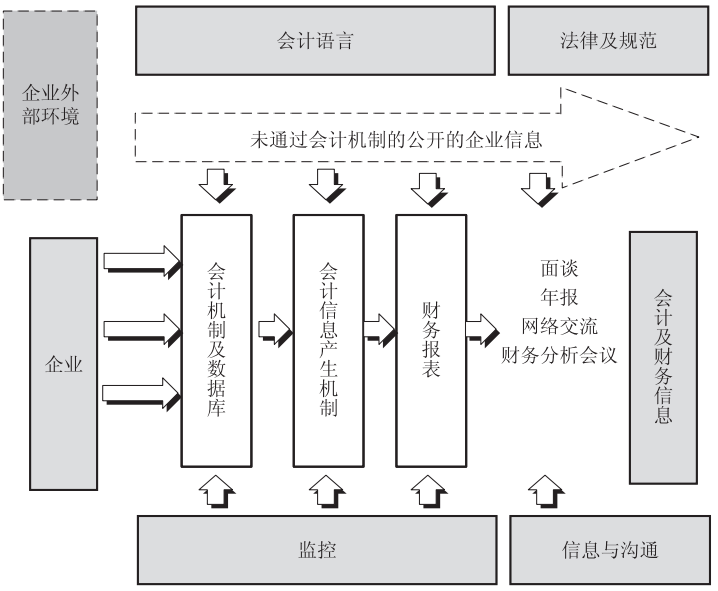

图 2-7　会计信息产生过程

资料来源：AMF . The Internal Control System：Reference Framework，2007.

2.5.4　南非的 King 报告

1994 年，南非关于公司治理的 King 报告（以下简称“King Ⅰ 报告”）由公司治理 King 委员会颁布（该委员会由前高等法院法官 Mervyn King S. C 任主席），成为南非公司治理行为的最高标准。2002 年，King Ⅱ 出台，对 King Ⅰ报告进行了修订，公司治理摆脱了原有的单一底线（bottom line），即为股东的利润服务，扩展成为三重底线，包括公司行为的经济、环境和社会三个方面。2008 年南非新的公司法出台，同时伴随着公司治理新趋势的出现，2009 年 King 委员会发布了 King Ⅲ报告，该报告是由 2009 南非公司治理 King 报告（The King Report on Governance for South Africa—2009）和 2009 公司治理 King 准则（The King Code of Governance Principles—2009）共同组成的。

King Ⅲ报告关注的是内部财务控制（internal financial control，IFC），并且认为审计委员会在整个 IFC 中极其重要。一个有效的控制系统，应该能够降低财务报表的实质性风险，并且为可靠的财务报告提供坚实的基础。

然而，整个 IFC 参照的是美国 COSO 框架，需要把 COSO 的五要素包括在内，即控制活动、控制环境、风险评估、信息与沟通、监控，并且认为控制活动是整个内部控制的“熔炉”（boiler room），它们包括每日的限制、审批、核对、确认及其他管理层和工作人员维护资产安全和行为记录的企业活动。常见的记录控制活动的两种方式：一种是从上至下的方法（top-down approach），这种方法需要管理层确认财务报表账户的平衡和披露无论在量还是在质上都是显著的，从这些账户的平衡再追溯到具体披露或记录的交易过程；另一种是从下至上的方法（bottom-up approach），管理层开始以员工每天的活动为基础，从具体的交易活动再至财务报表账户。King Ⅲ报告认为最好的选择是从上至下的方法，它能够识别出财务报告中最显著的风险，并且以组织实体水平的控制（entity-level controls）为出发点，包括了 COSO 的五个要素，

并嵌入财务报告的过程中去。如果没有充分的组织实体水平的控制，控制活动不可能有效。这种方法的使用能够确保所有关键控制（包括所有重要的账户和披露）的记录和测试。

审计委员会确保整体报告和内部财务控制的完整性，监控财务报告的风险，同时 King Ⅲ报告要求：

（1）整体报告包括管理层对内部控制有效性的评价；

（2）整体报告包括审计委员会对内部财务控制的有效性的评价；

（3）审计委员会所做的评价应基于内部审计所做的测试，这些测试用来确定内部财务控制体系设计和执行的有效性；

（4）如果认为财务控制缺陷是实质性的，并会导致确切的财务损失或实质性的错误，那么这些缺陷应及时地汇报给董事会和利益相关者；

（5）审计委员会应决定正式记录下来的内部财务控制的特性和完善程度。和美国萨奥法案不同，该报告并不要求注册会计师对内部财务控制进行审计。

2.5.5 日本的内部控制架构

2004 年 10 月，日本西武铁路公司虚报持股数，结果被取消上市资格，董事长锒铛入狱，为此日本金融厅于该年年末对全部上市企业提出了对公开披露内容自我检查的要求，结果有 625 家企业（占总体的 14.3%）提交了修正报告书，日本监管当局开始重视内部控制问题，

2006 年 6 月 7 日，日本的《证券交易法》经过修改后更名为《金融商品交易法》，此法规定：从 2008 年 4 月 1 日以后开始的会计年度起，上市公司在每个营业年度提交财务报告的同时应提交企业内部控制报告，并且内部控制报告必须接受注册会计师的审计。

日本企业会计审议会在 2005 年 1 月召开的全体会议上，决定对制定管理层对财务报告内部控制有效性进行评价的标准及注册会计师审计标准开始进行审议，2005 年 2 月起内部控制专业委员会开始审议工作。该专业委员会在对各国内部控制准则标准等内容进行研究的同时，对与日本公司法规的协调等方面进行了考虑。在此基础上，内部控制标准委员会于 2005 年 7 月，对于财务报告内部控制评价与审计准则公布了公开征求意见稿，根据提到的意见，归纳整理为《财务报告内部控制评价与审计准则》，并于 2005 年 12 月 8 日对外公布。2006 年 11 月将实施准则作为征求意见稿予以公布。

2007 年 2 月 15 日，日本企业会计审议会审议发布了《关于财务报告内部控制评价与审计准则以及财务报告内部控制评价与审计实施准则的制定（意见书）》，要求适用于自 2008 年 4 月 1 日以后开始的会计年度财务报告内部控制评价与审计。日本企业会计审议会是日本金融厅下属机构。其公布的《财务报告内部控制评价与审计准则》和《财务报告内部控制评价与审计实施准则》，是为了配合《金融商品交易法》规定的内部控制报告制度的实施而制定的。

日本企业会计审议会在公布这一准则和实施准则时指出，为了充分发挥证券交易市场的功能，恰当地向投资者披露企业信息是非常必要的，但近年来发生了一系列有价证券报告披露内容方面的违法事件，因此，为确保披露制度的可靠性，通过构建内部控制制度，促进信息披露可靠性提升，并提高证券市场的可信度。

《财务报告内部控制评价与审计准则》由三部分组成："内部控制基本框架""财务报告内部控制的评价与报告""财务报告内部控制审计"。"内部控制基本框架"规定了对管理层拥有构建和运行职能与责任的内部控制的定义、概念框架。"财务报告内部控制的评价与报

告”和“财务报告内部控制审计”则表明了管理层对财务报告内部控制有效性进行评价和注册会计师进行审计的思路。

内部控制是为达到目标而提供合理保证，内含于业务活动之中，由组织内部所有人员实施的程序。日本的准则在基本沿袭 COSO 报告框架的同时，结合日本的实际情况，在 COSO 报告三个目标和五项基本要素之上各增加一项，规定为四个目标和六项基本要素。内部控制的目标为：经营的有效和效率；财务报告的可靠性；营业活动遵循相关法律；资产保全。内部控制基本要素为：控制环境、风险的评估与应对、控制活动、信息与沟通、监控、信息技术的应对。

管理层应当对财务报告的内部控制有效性进行评价。在进行评价之前，应当预先决定财务报告内部控制的构建和运行政策及程序，并记录和保存其状况。财务报告内部控制有效性评价，应当在合并基础上进行，首先对财务报告整体控制进行评价，然后对业务流程相关的内部控制进行评价。

承担财务报表审计的审计人员，对管理层进行的财务报告内部控制有效性评价结论进行审计的目的，在于对管理层编制的内部控制报告是否依据一般公认合理的内部控制评价准则，在所有要点上是否适当表明内部控制有效性的评价结论，将基于审计人员自身取得的审计证据进行判断的结果作为意见，予以表明。对内部控制报告的意见，采用关于内部控制评价的审计报告的方式表明。可以看出，日本对内部控制审计和评价是基于财务报告的内部控制，而非整体内部控制。而财务报告审计是对内部控制评价报告的结论的审计。内部控制审计人员应当和承担该企业财务报表的审计人员为同一审计人员，内部控制审计与财务报表审计应当一并进行。所谓同一审计人员不仅要求是同一审计事务所，还要求是同一执行审计业务的人员。内部控制审计报告原则上也应当与财务报表审计的审计报告一并编制。

内部控制准则于 2008 年导入，在实施过程中也遇到了一些困惑，因此，企业会计审计会内部控制分会从 2010 年 5 月开始，对内部控制准则的运用的修改等进行了审议和探讨，并于 2011 年 3 月 30 日公开发表其修订后的准则。此次修订的主要内容有：确保审计人员有效运用企业创意，对于经营者创意的内部控制评价方法，审计人员应理解和尊重，加强内部控制审计和财务报表审计一体化的效率；确立内部控制有效率运用的修改，企业的评价方法和手续尽可能简洁化和明确化；对“重大缺陷”术语的修改，有观点指出“重大缺陷”这一术语恐怕会带来企业本有缺陷的误解，修改为“应该披露的重要不完备”；同时编制面向中小上市企业的简洁化、明确化、容易理解的内部控制报告实务事例集。

2.6　萨班斯-奥克斯利法案对内部控制的要求

2001 年 12 月，曾居《财富》500 强第七位的安然公司正式申请破产，这桩当时是美国历史上最大金额的破产申请案，给市场监管部门敲响了警钟。2002 年美国国会报告称这一系列会计丑闻事件“彻底打击了投资者对美国资本市场的信心”，由此引发了一连串的后续反应，其中最重要的影响就是萨班斯-奥克斯利法案的出台。萨班斯-奥克斯利法案最初于 2002 年 2 月 14 日提交给国会众议院金融服务委员会，到 7 月 25 日国会参众两院最终通过，先后有 6 个版本：2 月 14 日、4 月 22 日、4 月 24 日、7 月 15 日、7 月 24 日、7 月 25 日（最后版本）。7 月 30 日，该法案最终由美国总统布什签字生效。总统布什在签署该法案的新闻发布会上称：“这是自罗斯福总统以来美国商业界影响最为深远的改革法案。”罗斯福总统

签署了1933年的《证券法》和1934年的《证券交易法》，形成了美国企业法规的基本框架，也就是说，萨班斯-奥克斯利法案是自《证券法》和《证券交易法》签字生效以来美国资本市场最大幅度的变革，对会计职业监管、公司治理、证券市场监管、内部控制等方面做出了不少新的规定。该法案的全名是《2002年公众公司会计改革和投资者保护法案》（*Public Company Accounting Reform and Investor Protection Act of 2002*），是由美国众议院金融服务委员会主席奥克斯利和参议院银行委员会主席萨班斯联合提出的，因此，又被称为《2002年萨班斯-奥克斯利法案》（*Sarbanes-Oxley Act of 2002*，以下简称萨奥法案）。

总体而言，萨奥法案的目的在于促进企业责任感，加强信息的公众披露，提高财务报告和审计的质量及透明度，并对违反证券法律和其他法规的行为加大惩罚力度。萨奥法案增加了对企业报告的要求和责任，明确禁止了某些上市公司的行为，显著扩大了审计委员会的责任和权威，并且创造出一个全新的会计行业监督机构——公众公司会计监察委员会（Public Companies Accounting Oversight Board，PCAOB）。

PCAOB拥有注册、检查、调查和处罚的权限，保持独立运作，自主制定预算和进行人员管理，不应作为美国政府的部门和机构，授权美国证券交易委员会对PCAOB进行监督。PCAOB由五名专职委员组成，由证券交易委员会与美国财政部长和联邦储备委员会主席商议任命，任期五年，其中两名是或曾经是注册会计师（CPA），另外三名必须是代表公众利益的非会计专业人士。主席可以由CPA中的一员担任，前提是他或她已有五年没有从事CPA业务。

PCAOB有权制定或采纳有关会计师职业团体建议的审计与相关鉴证准则、质量控制准则以及职业道德准则等。PCAOB如认为适当，将与指定的、由会计专家组成的、负责制定准则或提供咨询意见的专业团体保持密切合作，有权对这些团体建议的准则进行补充、修改、废除或否决。PCAOB需就准则制定情况每年向证券交易委员会提交年度报告。

萨奥法案与公司内部控制相关度较高的主要是302、404和906条款。

302条款：财务报告的公司责任。要求证券发行人的首席执行官和首席财务官要在审计报告后附上一份声明，保证“定期报告中的财务报表和信息披露是适当的，在所有重大方面公正地报告了公司的运营和财务状况”。任何违反这个条款的行为都被视作明知故犯，必须承担责任。这条规定实际上是要求首席执行官和首席财务官对财务报告的真实性、准确性和内部控制的有效性签订个人保证书，断绝了他们对公司财务欺诈推卸责任的退路。

404条款：管理层内部控制的评估。要求上市公司在每份年度报告里包含一份“内部控制报告”，该报告要求管理层出具对建立和维护与财务报表相关的内部控制具有责任的声明；管理层于财政年度末对内部控制体系及控制程序有效性的评价；外部审计师对管理层的评估过程和结果发表的内部控制评价报告。404条款是该法案的核心内容，要求所有在美国上市的企业、公司管理层每年需就财务报告内部控制出具评估报告，并要求独立外部审计师对管理层的报告发表声明，其内容包括建立和维护有效内部控制的责任声明、内部控制评估标准、管理层评估结论和外部审计师意见等。

404条款比302条款更加严格，302条款要求公司管理层对内部控制的有效性给予保证，而404条款还要求公司管理层对予以保证的内容拿出充分的证据。而且302条款主要是与披露有关的控制和程序，不需要外部审计师的审计；404条款主要是与财务报告有关的控制和程序，需要外部审计师的审计。从以上两个条款可以看出它们之间的联系，财务报告内部控制（由404条款规定）仅是信息披露控制及程序（由302条款规定）的一部分。证监会要

求发行人维护定期评估信息披露控制及程序的成效，该披露控制及程序的设计旨在确保证券交易法规定需纳入报告的信息能及时地记录、处理和总结。另外，也说明不定期报告及披露活动的时代已经结束。

萨奥法案还加强了对违法行为的处罚，906 条款规定，若公司违反财务报告和相关披露的责任，将受到最高达 100 万美元的罚金，最高达 10 年的监禁，或并罚；如果蓄意故犯，则将被处以最高达 500 万美元的罚金，最高达 20 年的监禁。

知识链接

萨班斯-奥克斯利法案 302、404、906 条款

302：公司对财务报告的责任

（a）对制定规章的要求——SEC 应颁布规定，对于按照 1934 年的证券交易法的 13（a）或 15（d）部分编制定期报告的公司，应要求这些公司的首要官员（们）及首要财务官（们）（或担任同等职务的人员）在每一年度报告或季度报告中保证如下内容。

（1）签字的官员已审阅过该报告。

（2）该官员认为报告中不存在重大的错报、漏报。

（3）该官员认为报告中的会计报表及其他财务信息在所有重大方面，公允地反映了公司在该报告期末的财务状况及该报告期内的经营成果。

（4）签字官员：

（A）对建立及保持内部控制负责；

（B）设计了所需的内部控制，以保证这些官员能知道该公司及其并表子公司的所有重大信息，尤其是报告期内的重大信息；

（C）评价公司的内部控制在签署报告前 90 天内的有效性；

（D）在该定期报告中发布他们上述评价的结论。

（5）签字官员已向公司的审计师及董事会下属的审计委员会（或担任同等职务的人员）披露了如下内容：

（A）内部控制的设计或执行中，对公司记录、处理、汇总及编报财务数据的功能产生负面影响的所有重大缺陷，以及向公司的审计师指出内部控制的重大缺点；

（B）在内部控制中担任重要职位的管理人员或其他雇员的欺诈行为，而不论该行为的影响是否重大。

（6）签字官员应在报告中指明在他们对内部控制评价之后，内部控制是否发生了重大变化，或是其他可能对内部控制产生重要影响的因素，包括对内部控制的重大缺陷或重要缺点的更正措施。

（b）公司迁址国外不影响本法案的效力——即使发行证券的公司通过再合并或其他交易使公司的注册地或办公地迁至国外，也不能减少本节规定的法律效力。本节规定对该公司依然适用，且全部适用。

（c）最终期限——本节（a）部分的规定应在本法案颁布后 30 日内生效。

404：管理层对内部控制的评价

（a）内部控制方面的要求——SEC 应当相应地规定，要求按《1934 年证券交易法》第 13 节（a）或 15 节（d）编制的年度报告中包括内部控制报告，包括：

（1）强调公司管理层建立和维护内部控制系统及相应控制程序充分有效的责任；

（2）发行人管理层最近财政年度末对内部控制体系及控制程序有效性的评价。

（b）内部控制评价报告——

对于本节（a）中要求的管理层对内部控制的评价，担任公司年报审计的会计公司应当对其进行测试和评价，并出具评价报告。上述评价和报告应当遵循委员会发布或认可的准则。上述评价过程不应当作为一项单独的业务。

906：公司对财务报告的责任

（a）总论。——根据本法案在美国法典第 63 段第 18 章的 1349 节后加入：“§1350. 公司官员证明财务报告失败。”

（A）证明定期财务报告。——每一份由发行证券的公司根据 1934 年证券交易法第 13（a）节或 15（d）节向 SEC 申报的包含财务报告的定期报告都应包括公司首席执行官和财务总监写的声明。

（B）内容。——（a）小节中要求的声明包括财务报告的定期报告是完全按照 1934 年证券交易法第 13（a）节或 15（d）节的要求编写的，定期报告中的信息在所有重大方面都公允地反映了公司的财务状况和经营成果。

（C）罚则。——无论是谁

（1）知道包括财务报告的定期报告没有满足本节的所有要求却根据本节（a）和（b）小节签署证明的，应该被处以最多 $1 000 000 的罚款，最多 10 年的监禁，或并罚；或

（2）明知包括财务报告的定期报告没有满足本节的所有要求却根据本节（a）和（b）小节蓄意签署证明的，应该被处以最多 $5 000 000 的罚款，最多 20 年的监禁，或并罚。

（b）文字修改。——美国法典第 63 段第 18 章开始的目录中在结尾处增加：“§1350. 公司官员证明财务报告失败。”

资料来源：Public Company Accounting Reform and Investor Protection Act of 2002.

自萨班斯-奥克斯利法案颁布后，对不同类型的企业执行 404 条款设立了不同的执行期限，按照公众持股股份分为：非加速编报组（non-accelerated filer，公众持股数少于 7 500 万），加速编报组（accelerated filer，公众持股数 7 500 万至 70 000 万之间）和大型加速编报组（large accelerated filer，公众持股数在 70 000 万以上）。最初的要求是对非加速编报组的企业执行期限为 2005 年 4 月 15 日，而加速和大型加速编报组的企业执行期限为 2004 年 6 月 15 日，在执行过程中，美国的一些企业与金融业者认为该法案的一些规定过于严格，增大了企业（特别是小型企业）的审计成本，降低了其他国家企业到美国金融市场上市筹资的兴趣。随后的几年里，小企业的披露日期则一再延后（2004 年 4 月、2005 年 3 月、2005 年 9 月、2006 年 1 月、2008 年 7 月、2009 年 1 月，共延后了六次，具体执行时间见表 2-9）。2010 年 7 月 21 日美国总统奥巴马签署了被称作自金融海啸以来最彻底的金融改革法案——《华尔街改革和消费者保护法案》（*Dodd-Frank Wall Street Reform and Consumer Protection Act*），该法案结束了 404 条款备受争议的问题：小企业（公共发行股本少于 7 500 万美元）不再需要出具内部控制审计报告。

表 2-9　萨奥法案 404 条款执行时间表

			2002. 7. 30 颁布 SOX	2004. 2. 24	2005. 3. 2	2005. 9. 22	2006. 8. 9	2006. 12. 15	2008. 7. 2	2009. 10. 13	2010. 9. 15
国内	非加速编报 7 500 万以下	404（a）	2005. 4. 15	2005. 7. 15	2006. 7. 15	2007. 7. 15		2007. 12. 15			
		404（b）						2008. 12. 15	2009. 12. 15	2010. 6. 15	NO
	加速编报 ≥7 500 万	404（a）	2004. 6. 15	2004. 11. 15							
		404（b）									
国外	非加速 <7 500 万	404（a）	2005. 4. 15	2005. 7. 15	2006. 7. 15	2007. 7. 15		2007. 12. 15			
		404（b）						2008. 12. 15	2009. 12. 15	2010. 6. 15	NO
	加速 7 500 万～ 70 000 万	404（a）	2004. 6. 15	2004. 11. 15							
		404（b）					2007. 7. 15				
	大型加速 >70 000 万	404（a）									
		404（b）									

注：404 条款 a 是指出具内部控制自我评价报告，404 条 b 是指出具内部控制审计报告。

2012 年 3 月 27 日，美国国会众议院代表以压倒性投票通过了参议院修订的“创业企业融资法案”（*The Jumpstart Our Business Startups Act*，或称 JOBS Act，以下简称“JOBS 法案”），旨在使小型企业在满足美国证券法规要求的同时，更容易吸引投资者并获得投资。这项新法案将对现有证券法做出几处重要修改：① 鼓励“新兴成长型企业”首次公开募股（IPOs）；② 促进企业通过私募发行及小规模公开发行进行融资，而无须向美国证券交易委员会（SEC）注册登记，从而减少小型企业的融资成本和限制。

此项法案提出了一个新的企业类别——“新兴成长型企业”（emerging growth company，EGC），其定义如下：在最近的财务年度内总收入低于 10 亿美元的发行人。一旦被认定为新兴成长型企业，该企业将保留该资格直到以下日期中的最早日期为止：发行人首次公开发行普通股五周年后的首个财务年度截止日；发行人年度总收入达到 10 亿美元或以上的财务年度截止日；在过去三年内，发行人累计发行的不可转换债券超过 10 亿美元的日期；发行人被认定为“大型加速编报公司”的日期。以上四个日期中的最早日期即为企业“EGC 资格”的终止日期。

EGC 四个截止日期的最早日期前将得以豁免若干监管要求。这些企业无须满足《萨班斯-奥克斯利法案》（SOX）下 404（b）条款的要求，即在一段时间内（EGC 资格终止前）不再需要出具内部控制审计报告。

阅读与思考

安然事件

安然（ENRON）1985 年由美国休斯敦天然气公司和北方内陆天然气（InterNorth）公司合并而成，公司总部设在美国得克萨斯州的休斯敦，首任董事长兼首席执行官为肯尼斯·雷，他既是安然公司的主要创立者，也是安然公司创造神话并在后来导致危机的关键人物。从 1990 年到 2000 年的 10 年间，安然公司的销售收入从 59 亿美元上升到了 1 008 亿美元，净利润从 2.02 亿美元上升到 9.79 亿美元，其股票成为众多证券评级机构的推荐对象和众多投资者的追捧对象。2000 年 8 月，安然股票攀升至历史最高水平，每股高达 90.56 美元，同年，安然名列《财富》杂志“美国 500 强”中的第七，它一直是美国乃至世界最大的能源交易商。在其最辉煌的年代，掌控着美国 20% 的电能、天然气交易。安然不仅是天然气、电力行业的巨擘，还是涉足电信、投资、纸业、木材和保险业的大户。

直到破产前，公司营运业务覆盖全球 40 个国家和地区，共有雇员 2.1 万人，资产额高达 620 亿美元；安然一直鼓吹自己是“全球领先企业”，业务包括能源批发与零售、宽带、能源运输以及金融交易，连续 4 年获得“美国最具创新精神的公司”称号。

然而，这个能源帝国的倒塌却源于一位投资者吉姆·切欧斯的质疑。2001 年，吉姆·切欧斯公开对安然的盈利模式表示了怀疑。他指出，虽然安然的业务看起来很辉煌，但实际上赚不到什么钱，也没有人能够说清安然是怎么赚钱的。切欧斯还注意到有些文件涉及了安然背后的合伙公司，这些公司和安然有着说不清的幕后交易，而安然的首席执行官却一直在抛出手中的安然股票，同时不断宣称安然的股票会从当时的 70 美元左右升至 126 美元。但是按照美国法律规定，公司董事会成员如果没有离开董事会，就不能抛出手中持有的公司股票。到了 2001 年 8 月中旬，人们对于安然的疑问越来越多，并最终导致其股价下跌。

安然破产时间表：

8月9日，安然股价已经从年初的80美元左右跌到了42美元。

10月16日，安然发表2001年第二季度财报，宣布公司亏损总计达到6.18亿美元，即每股亏损1.11美元。同时首次透露因首席财务官安德鲁·法斯托与合伙公司经营不当，公司股东资产缩水12亿美元。

10月22日，美国证券交易委员会瞄上安然，要求公司自动提交某些交易的细节内容，并最终于10月31日开始对安然及其合伙公司进行正式调查。

11月1日，安然抵押了公司部分资产，获得J.P.摩根和所罗门史密斯巴尼的10亿美元信贷额度担保，但美林和标准普尔公司仍然再次调低了对安然的评级。

11月8日，安然被迫承认做了假账，虚报数字让人瞠目结舌：自1997年以来，安然虚报盈利共计近6亿美元。

11月9日，迪诺基公司宣布准备用80亿美元收购安然，并承担其130亿美元的债务。当天午盘安然的股价下挫0.16美元。

11月28日，标准普尔将安然债务评级调低至“垃圾债券”级。

11月30日，安然股价跌至0.26美元，市值由峰值时的800亿美元跌至2亿美元。

12月2日，安然正式向法院申请破产保护，破产清单中所列资产高达498亿美元，成为美国历史上最大的破产企业。当天，安然还向法院提出诉讼，声称迪诺基中止对其合并不合规定，要求赔偿。

安然事件就像多米诺骨牌一样，引起了一系列企业倒闭的连锁反应。安然破产后，一批有影响的企业舞弊案相继暴露出来，IBM、思科、施乐、J.P.摩根、大通银行等大企业也传出存在财务违规行为，同时还引发了一系列美国企业破产风暴。自2001年12月2日，安然公司申请破产后，美国又有几家大企业宣布申请破产保护：2002年1月22日，美国第二大零售商凯马特因资不抵债而申请破产保护，该公司资产总额达170亿美元；2002年1月28日，美国环球电讯公司由于债台高筑，向纽约破产法院申请破产保护，该公司在破产申请文件中列出的资产为224亿美元；2002年6月25日，全美第六大有线电视公司Adelphia宣布，该公司及其200余家子公司已在纽约申请了破产保护；2002年7月21日，美国第二大长途电话公司世界通信公司宣布申请破产保护，从而以1 070多亿美元的资产超越安然，创造了美国最新的破产案纪录。

根据美国参议院成立的调查委员会提供的报告分析，导致安然公司董事会失灵和公司破产的原因有六个方面：受托责任的失败；高风险会计政策；利益冲突；大量未披露的公司表外经营活动；行政人员的高报酬计划；董事会缺乏独立性。

资料来源：经作者综合分析整理，安然丑闻与安达信危机. http://www.china.com.cn/zhuanti2005/node_5128081.htm.

思考题

查阅相关的背景资料，从COSO框架的五要素的角度分析安然破产的原因。