21世纪会计系列规划教材·致用型

企业内部控制与风险管理

（第二版）

Enterprise Internal Control and Risk Management

徐凤菊　赵新娥　夏喆　编著

东北财经大学出版社
Dongbei University of Finance & Economics Press

第一章

总　论

引子一

深交所2012年11月22日发布公告，对万福生科半年报造假行为进行公开谴责。深交所发现，万福生科2012年10月26日披露的《关于重要信息披露的补充和2012年中报更正的公告》显示，万福生科2012年半年报存在虚假记载和重大遗漏，包括虚增营业收入1.88亿元，虚增营业成本1.46亿元，虚增净利润4 023.16万元。根据相关规定，深交所决定：对万福生科给予公开谴责的处分；对相关责任人给予公开谴责的处分。

2013年3月15日，深交所对万福生科及全体董事、监事和高级管理人员予以公开谴责，这是深交所对万福生科的第二次公开谴责。

深交所公告中指出，经查明，万福生科2008—2011年期间存在财务数据虚假记载情形。2013年3月2日，万福生科发布了《关于重大事项披露及股票复牌的公告》，承认其2008—2011年期间存在财务数据虚假记载情形，累计虚增收入7.4亿元左右，虚增营业利润1.8亿元左右，虚增净利润1.6亿元左右。其中，2011年度公司虚增营业收入2.8亿元，虚增营业利润6 541.36万元，虚增归属于上市公司股东的净利润5 912.69万元，分别占公司已披露2011年财务报告中三项财务数据金额的50.63%、110.67%和98.11%。经对上述虚增数据进行调整后，公司2011年营业收入、营业利润和归属于上市公司股东的净利润数额分别为2.73亿元、−630.51万元和114.17万元，与公司先前披露的相关财务数据存在重大差异。

引子二

2013年4月12日，自称是中国南车股民的网友“习惯被你惩”在天涯社区发帖“中国南车株机公司摊上假发票大事，总经理助理康意雄3个月捞44万元”，直指康意雄在100万元招待费中使用44万元假发票“捞钱”等一系列行径，引发热议。

该网友还在网上公布了康意雄的假发票明细清单、南车株机公司的财务审计报告，以及公司领导对此事的处理态度批示。其中，有资料详细记述了对该公司假发票的调查情况：通过网上发票查询显示，“假发票明细清单”中，2012年9月份消费一栏，总共23张发票，发票收款单位为北京中奥华美达大酒店、北京世纪阳光假日酒店、北京亚洲大酒店等，实际收款单位是北京朝阳公园开发经营有限公司。网友质疑：所谓的北京朝阳公园

开发经营有限公司是不是搞假发票买卖的？短短一个多月时间内，19 次提供假发票，总金额近 15 万元。

第一节　企业内部控制与风险管理的内涵

内部控制已经被公认为是企业基业长青的法宝之一。随着企业自身对规范化管理和股东掌握企业运营的准确信息的需要，以及外部审计师审计财务报表的需要，理论界和实务界对“内部控制”的关注日益密切。特别是在美国的“安然事件”和世通公司财务欺诈案之后，全球范围之内掀起了一股“内控管理”热潮。各个国家也从制度层面对企业内部控制进行了规范和要求，尤以《萨班斯-奥克斯利法案》（简称《萨班斯法案》）为代表。《萨班斯法案》是一部涉及会计职业监管、公司治理、证券市场监管等方面改革的重要法律，是美国关于会计和公司治理的一揽子改革方案。法案要求所有在美国上市的公司（包括在美国注册的上市公司和在外国注册而于美国上市的公司）都必须遵守该法案。此后，各国政府也逐渐开始积极推动内部控制领域的进程，以期减小企业的舞弊和违规行为对市场经济秩序的消极影响。

在我国，企业内部控制标准委员会于 2006 年正式成立，2006 年 6 月 6 日，国资委发布了《中央企业全面风险管理指引》，这是我国第一个全面风险管理的指导性文件，意味着中国走上了风险管理的中心舞台。2008 年 6 月 28 日，财政部、证监会、审计署、银监会、保监会五部门联合发布了《企业内部控制基本规范》，自 2009 年 7 月 1 日起先在上市公司范围内施行，鼓励非上市的其他大中型企业执行。该规范的发布，标志着我国企业内部控制规范体系建设取得重大突破，有业内人士和媒体甚至称之为中国版的“萨班斯法案”。2010 年 4 月 26 日，五部委又联合发布了《企业内部控制配套指引》。该配套指引包括 18 项《企业内部控制应用指引》、《企业内部控制评价指引》和《企业内部控制审计指引》，连同此前发布的《企业内部控制基本规范》，标志着适应我国企业实际情况、融合国际先进经验的中国企业内部控制规范体系基本建成。为确保企业内控规范体系平稳顺利实施，财政部等五部门制定了实施时间表：自 2011 年 1 月 1 日起首先在境内外同时上市的公司施行，自 2012 年 1 月 1 日起扩大到在上海证券交易所、深圳证券交易所主板上市的公司施行；在此基础上，择机在中小板和创业板上市公司施行；同时，鼓励非上市大中型企业提前执行。

那么，什么是内部控制？为什么要进行内部控制？企业如何进行内部控制？内部控制的效果如何评价？这也正是本书需要解决的几个关键问题。

一、内部控制的定义

对内部控制的内涵界定，不同的组织和学者给出了不同的答案。比较有共识的界定认为内部控制是指一个单位为了实现其经营目标，保护资产的安全完整，保证会计信息资料的正确可靠，确保经营方针的贯彻执行，保证经营活动的经济性、效率性和效果性而在单位内部采取的自我调整、约束、规划、评价和控制的一系列方法、手续与措施的总称。下面就是一些权威机构对内部控制的概念进行的不同描述：

1949 年，美国注册会计师协会（AICPA）的审计程序委员会，发布了一份题为《内部控制：一种协调组织要素及其对管理层和独立注册会计师的重要性》的报告。该报告对

内部控制提出了权威性的定义："内部控制包括组织机构的设计和企业内部采取的所有相互协调的方法和措施。这些方法和措施都用于保护企业的财产，检查会计信息的准确性，提高经营效率，推动企业坚持执行既定的管理政策。"

内部控制（internal control）是指上市公司（以下简称公司）为了保证公司战略目标的实现，而对公司战略制定和经营活动中存在的风险予以管理的相关制度安排。它是由公司董事会、管理层及全体员工共同参与的一项活动。——上海证券交易所

内部控制是指上市公司（以下简称"公司"）董事会、监事会、高级管理人员及其他有关人员为实现下列目标而提供合理保证的过程。——深圳证券交易所

内部控制是由企业董事会、监事会、经理层和全体员工实施的、旨在实现控制目标的过程。内部控制的目标是合理保证企业经营管理合法合规、资产安全、财务报告及相关信息真实完整，提高经营效率和效果，促进企业实现发展战略。——我国《企业内部控制基本规范》（2008-05）

内部控制是指由企业董事会（决策、治理机构）、管理层和全体员工共同实施的，旨在合理保证企业战略实施、经营的效率和效果、财务报告及管理信息的真实可靠和完整、资产的安全完整、遵循国家法律法规和有关监管要求的一系列控制活动。——COSO报告

综上不难得出，内部控制是一个过程，是为保证组织实现特定目标的一个风险管理过程。

内部控制贯穿于企业经营活动的各个方面。有效的内部控制不仅关系到企业的各项经济目标能否达到、经济效益能否实现，也是企业建立现代企业制度的一项根本要求。

二、内部控制的分类

内部控制按照不同的标准可以分为不同的类别：

按照控制的目的分为会计控制和管理控制。会计控制是指与保护企业资产的安全性、会计信息的真实性和完整性以及财务活动的合法性有关的控制；管理控制是指与保证企业战略目标的实现和管理决策的贯彻执行，促进管理活动的经济性、效率性、效果性有关的控制。会计控制与管理控制并不是相互排斥、互不相容的，有些控制措施既可以用于会计控制，也可以用于管理控制。

按照控制的内容分为要素控制、方式控制、业务流程控制和绩效控制。

按照控制的层次分为公司治理层即所有者对决策层（董事会）的控制、董事会对管理层的控制、管理层对执行层即员工的控制，也可称为战略控制、管理控制和作业控制。

按照控制的方式分为预防性控制、发现性控制、纠正性控制。预防性控制即事前控制，通过预防性措施让错弊不要发生；发现性控制即事中控制，对已发生的错弊进行检查和发现；纠正性控制即事后控制，对已查明错弊分析原因并予以纠正。

第二节 企业内部控制的历史演进

内部控制自产生至今至少有几千年的历史，现代意义上的内部控制自20世纪初以来，伴随着市场经济的发展完善与市场竞争的加剧，基于对企业内部管理水平不断提高的要求，才越来越受到重视。自1936年美国注册会计师协会发布的《独立公共会计师对财

务报表的审查》公告中首次对内部控制做出定义以来，内部控制的建设与发展经历了内部牵制、内部控制制度（两要素阶段）、内部控制结构（三要素阶段）、COSO 内部控制整合框架（五要素阶段）及 ERM 全面风险管理（八要素阶段）五个阶段，而在这一时期，世界范围内也出现了巴林银行、安然、施乐、世通等震惊世界的财务造假引发的公司破产案件，促使了对内部控制在世界范围内的广泛关注与大量研究。

一、内部牵制阶段——20 世纪 40 年代前

内部控制，作为一个专用名词和完整概念，直到 20 世纪 30 年代才被人们提出、认识和接受。但在此前的人类社会发展史中，早已存在着内部控制的基本思想和初级形式，这就是内部牵制（internal check）。根据《柯勒会计辞典》（Kohler's Dictionary for Accountants）的解释，内部牵制是指："以提供有效的组织和经营，并防止错误和其他非法业务发生的业务流程设计。其主要特点是以任何个人或部门不能单独控制任何一项或一部分业务权力的方式进行组织上的责任分工，每项业务通过正常发挥其他个人或部门的功能进行交叉检查或交叉控制。设计有效的内部牵制以使每项业务能完整正确地经过规定的处理程序，而在规定的处理程序中，内部牵制机制永远是一个不可缺少的组成部分。"例如，在古罗马时代，对会计账簿实施的"双人记账制"，即某笔经济业务发生后，由两名记账人员同时在各自的账簿上加以登记然后定期核对双方账簿记录，以检查有无记账差错或舞弊行为，进而达到控制财物收支的目的，即是典型的内部牵制措施。

1936 年 AICPA 在《独立公共会计师对财务报表的审查》中也指出：内部牵制是指以提供有效的组织和经营，并防止错误和其他非法业务发生而采取的各种措施和方法。其目的是保证公司现金和其他资产的安全，检查账簿的准确性。

直到 20 世纪 40 年代以前，内部控制被定义为内部牵制阶段。

内部牵制基于以下假设：①两个或两个以上的人或部门无意识地犯同样错误的机会是很小的；②两个或两个以上的人或部门有意识地合伙舞弊的可能性大大低于单独一个人或部门舞弊的可能性。

内部牵制的基本内容包括：

第一，识别不相容职务，即通常不能由一个人兼任的职务，包括出纳与记账、业务经办与记账、业务经办与业务审批、业务审批与记账、财物保管与记账、业务经办与财物保管、业务操作与业务复核；

第二，合理界定不同职务的职责与权限，准确地分清责任；

第三，分离不相容职务，在进行定岗和分工时，注意将不相容职务分离开来，使其相互牵制、相互制约；

第四，必要的保障措施，如物理措施（保险柜、专用钥匙等）或技术措施（网络口令等），定期的岗位轮换等。

内部牵制按照其执行措施可分为以下四类：

（1）实物牵制。实物牵制即对核心资产实行两个或两个以上的人同时管理。例如把保险柜的钥匙交给两个以上的工作人员持有，非同时使用这两把以上的钥匙，保险柜就不能打开，可以有效防止一个人作弊。

（2）机械牵制。机械牵制即通过程序或流程机械操作，才能完成一定过程的操作，因此也称为程序牵制。它通常是将单位各项业务的处理过程，用文字说明方式或流程图的方

式表示出来，以形成制度，颁发执行。机械牵制属于典型的事前控制法，即要按牵制的原则进行程序设置，而且要求所有的业务活动都要建立切实可行的办理程序。程序控制的关键是实行以内部牵制为核心的不相容职务分离原则。例如保险柜的大门若非按正确程序操作就打不开。

（3）体制牵制。体制牵制即通过组织分工来实现的防弊体制。为防止错误和舞弊，对于每一项经济业务的处理，都要求有两人或两人以上共同分工负责，以相互牵制、互相制约的机制。其基本要求是职责分离。它不仅要求划分职责，明确各部门或个人的职责和应有的权限，同时还要规定相互配合与制约的方法。

（4）簿记牵制。簿记牵制即原始凭证与记账凭证、会计凭证与账簿、账簿与账簿、账簿与会计报表之间核对的牵制。在某种意义上，它也是程序牵制的一个方面。

值得注意的是，内部牵制主要是通过分工协作来实现对舞弊行为的监控的，无论是部门之间相互制约还是上下级之间相互制约，往往是从某一环节或部门出发，强调点，忽略面，局限于内部审计的原理。

二、内部控制制度（两要素阶段）——20 世纪 50 年代至 80 年代

内部控制包括组织的组成结构及该组织为保护其财产安全、检查其会计资料的准确性和可靠性，提高经营效率，保证既定的管理政策得以实施而采取的所有方法和措施（美国注册会计师协会审计程序委员会，1949）。《审计程序公告第 29 号》将内部控制分为两大类：内部会计控制与内部管理控制（美国注册会计师协会审计程序委员会，1958）。

最早提出内部会计控制系统的是 1934 年美国发布的《证券交易法》。该法规定：证券发行人应设计并维护一套能为下列目的提供合理保证的内部会计控制系统。

1949 年，美国注册会计师协会（AICPA）的审计程序委员会，发布了一份题为《内部控制：一种协调组织要素及其对管理层和独立注册会计师的重要性》的报告。该报告对内部控制提出了权威性的定义："内部控制包括组织机构的设计和企业内部采取的所有相互协调的方法和措施。这些方法和措施都用于保护企业的财产，检查会计信息的准确性，提高经营效率，推动企业坚持执行既定的管理政策。"

1958 年，美国注册会计师协会审计程序委员会又发布了《独立审计人员评价内部控制的范围》的报告，将内部控制分为内部会计控制和内部管理控制。内部会计控制包括与财产安全和财产记录的可靠性有关的所有方法和程序，如授权与批准控制，从事财物记录与审核的职务及从事经营与财产保管的职务实行分离控制，实物控制和内部审计等。

1972 年，美国审计准则委员会（ASB）在《审计准则公告第 1 号》中，重新并且更加明确地阐述了内部会计控制和内部管理控制的定义：

内部会计控制：包括（但不限于）组织规划的所有方法和程序，这些方法和程序与财产安全和财物记录可靠性有直接的联系（财务目标）。这些控制包括授权与批准制度、从事财务记录和审核与从事经营或财产保管职务分离的控制、财产的实物控制和内部审计。

内部管理控制：包括（但不限于）组织计划以及与管理部门授权办理经济业务的决策过程有关的程序及其记录。这种授权活动是管理部门的职责，它直接与管理部门执行该组织的经营目标有关，是对经济业务进行会计控制的起点。

由于推动内部控制发展的主要是审计职业界，因此就不可避免地带上了审计的烙印。所谓的两分法也成为出于审计便利需要的产物——注意力仅集中在会计控制的测试，对管

理控制鲜有涉及。两分法未能完整地反映内部控制所涵盖的内容，也没有考虑控制环境对内部控制制度设计及实施效果的影响。尽管如此，这些概念的界定和分类为内部控制的发展奠定了一定的理论基础，有着承上启下的作用。

三、内部控制结构（三要素阶段）——20 世纪 80 年代末至 90 年代初

20 世纪 80 年代后期以来，会计界研究重点逐步从一般定义向具体内容深化。1988 年美国注册会计师协会发布《审计准则公告第 55 号》，建议从 1990 年 1 月起以该公告取代 1972 年发布的《审计准则公告第 1 号》，首次将控制环境纳入内部控制结构，不再区分会计控制和管理控制。这个公告首次以“内部控制结构”代替“内部控制制度”。明确“企业的内部控制结构”，包括为提供取得企业特定目标的合理保证而建立的各种政策和程序。内部控制结构由三个要素构成：控制环境、会计系统、控制程序。

1. 控制环境

控制环境是指良好的内部控制所需要的外部和内部影响因素。外部影响因素包括国家政策、行业法规等。内部影响因素主要表现在股东、董事会、经营者及其他员工对内部控制的态度和行为。具体包括：管理理念、经营风格、组织机构、董事会及审计委员会的职能、人事政策和程序、确定职责和责任的方法以及管理者监督控制和检查工作时所采用的方法，如经营计划、利润计划、预算和预测、责任会计和内部审计等。

2. 会计系统

会计系统规定各项经济业务的确认、计量、记录、归集、分类、分析和报告的方法，即建立企业内部会计制度。一个有效的会计制度应当包括：鉴定和登记一切合法的经济业务；对各项经济业务作适当的分类，作为编制报表的依据；计量经济业务的价值以使其货币价值能在财务报表中得以体现；确定经济业务发生的时间以确保其记录在适当的会计期间内；在财务报表中恰当地表述和揭示经济业务与有关价值变化的内容。

3. 控制程序

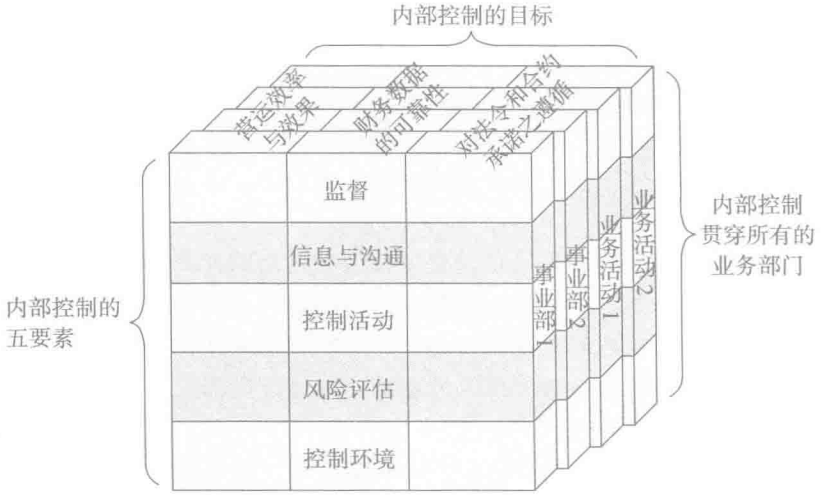
控制程序指管理层为达到控制的目标而制定的政策和程序。其中包括：经济业务和经济活动的适当授权；明确所有员工的职责分工；账簿和凭证的设置、记录与使用，以保证经济业务活动得到正确的记载；资产及记录的限制接触；对已经登记业务的记录进行复核等。

内部控制结构阶段有两个特点：一是将内部控制环境纳入内部控制的范畴；二是不再区分会计控制和管理控制。至此，在企业管理实践中产生的内部控制活动，经过审计人员的理论总结，已经完成从实践到理论的升华。

四、内部控制整合框架（五要素阶段）——20 世纪 90 年代至 21 世纪初

1992 年，由美国注册会计师协会、内部审计师协会、财务经理协会、美国会计学会、管理会计协会参与的美国反虚假财务报告委员会（National Commission on Fraudulent Reporting）所属的内部控制专门研究委员会发起机构委员会（Committee of Sponsoring Organizations of the Treadway Commission，简称 COSO 委员会）在进行专门研究后提出专题报告——《内部控制——整合框架》（Internal Control — Integrated Framework），也称 COSO 报告，并于 1994 年进行了修改。这一报告已经成为内部控制领域最为权威的文献之一。该报告系内部控制发展历程中的一座重要里程碑，其对内部控制的发展所做出的贡献可以用三句话十二个字概括，那就是“一个定义、三项目标、五种要素”。COSO 报告

提出：内部控制是一个过程，受企业董事会、管理层和其他员工影响，旨在保证财务报告的可靠性、经营的效果和效率以及现行法规的遵循。它认为内部控制整体架构主要由控制环境（control environment）、风险评估（risk assessment）、控制活动（control activities）、信息与沟通（information and communication）、监督（monitoring）五个要素构成（如图 1-1 所示）。



资料来源：COSO. 内部控制——整合框架［M］. 方红星，译. 大连：东北财经大学出版社，2008.

图 1-1 COSO 内部控制框架

1. 控制环境

控制环境主要指企业内部的文化、价值观、组织结构、管理理念和风格等。这些因素是企业内部控制的基础，将对企业内部控制的运行及效果产生广泛而深远的影响。

具体来说，包括员工的忠诚和职业道德、人员胜任能力、管理者的管理哲学和经营风格、董事会及审计委员会、组织机构、权责划分、人力资源政策及执行等方面。

2. 风险评估

风险评估是指识别和分析与实现目标相关的风险，并采取相应的行动措施加以控制。这一过程包括风险识别和风险分析两个部分。

通常，企业的风险主要来自于外部环境和内部条件的变化。其中，风险识别包括对外部因素（如技术发展、竞争、经济变化）和内部因素（如员工素质、公司活动性质、信息系统处理的特点）进行检查。风险分析则涉及估计风险的重大程度、风险发生的可能性、如何控制风险等。

3. 控制活动

控制活动是指企业对所确认的风险采取必要的措施，以保证企业目标得以实现的政策和程序。一般来说，与内部控制相关的控制活动包括职务分离、实物控制、信息处理控制、业绩评价等。

职务分离，是指为了防止单个雇员舞弊或隐藏不正当行为而进行的职责划分。通常应该分离的职责有业务授权与业务执行、业务执行与业务记录、业务记录与业务稽核等。

实物控制，指对企业的具体实物所进行的控制行为，如针对库存现金、存货、固定资

产、有价证券等所进行的控制。

信息处理控制可分为两类：一般控制和应用控制。一般控制通常与信息系统的设计和管理有关；应用控制则与个别数据在信息系统中处理的方式有关。

业绩评价是指将实际业绩与业绩标准进行比较，以便确定业绩的完成程度和质量。

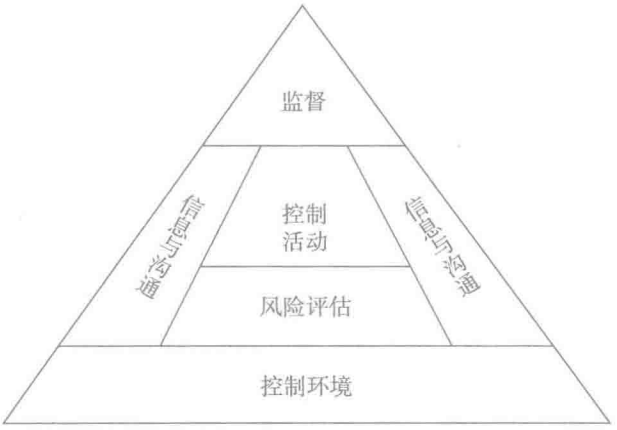
4. 信息与沟通

信息与沟通是指为了使管理者和员工能执行其职责，企业各个部门及员工之间必须沟通与交流相关的信息。这些信息既有外部的信息，也有内部的信息。信息与沟通包括确认记录有效的经济业务、采用恰当的货币价值计量、在财务报告中恰当揭示。信息沟通的目的主要是让员工了解其职责，了解其在工作中如何与他人相联系、如何向上级报告例外情况。沟通的方式一般有政策手册、财务报告手册、备查簿，以及口头交流或管理示例等。

5. 监督

监督是指评价内部控制的质量，也就是评价内部控制制度的设计与执行情况，包括日常的监督活动、内部审计等。监督活动通常是由内部审计、财务会计、人力资源等部门执行。他们定期或不定期地对内部控制制度的设计与执行情况进行检查和评估，与有关人员交流内部控制有效与否的信息，并提出改进意见，以保证内部控制能够随环境的变化而不断改进。

COSO 框架将内部控制要素以一个金字塔结构提出，其中控制环境作为金字塔的最底部，风险评估和控制活动位于上一层次，信息和沟通接近顶部，监督处于最顶端（如图 1-2 所示）。



资料来源：COSO. 内部控制——整合框架［M］. 方红星，译 . 大连：东北财经大学出版社，2008.

图 1-2　COSO 框架五要素图

COSO 报告的出台，引起了世界会计学界的广泛研究兴趣，加深了各界对内部控制重要性的认识，基本上统一了业界的认识，这对人们进行企业内部控制的研究极具时代意义。

五、ERM 全面风险管理（八要素阶段）——21 世纪以后

2001 年 11 月下旬，帽认最大的能源企业安然公司承认自 1997 年以来，通过非法手段虚报利润 5.86 亿美元；在与关联公司内部交易中，不断隐藏债务和损失，管理层从中非法获益。消息传出，立刻引起美国金融市场的巨大动荡。安然股价从近 90 美元跌至不

足 1 美元，许多中小投资者损失惨重。自安然公司财务欺诈行为被揭露以来，美国大公司会计丑闻频频曝光，投资者信心连遭打击，美国股市因此受到重创，主要股指一度跌至 9·11 恐怖袭击事件以来的最低水平。世界通信——这只技术股中闪耀的明星，也被逐出纳斯达克市场。美国魏斯评级公司在调查了 7 000 家公司发布的财务报告后认为，有多达 1/3 的美国上市公司不同程度存在捏造盈利的问题，信用危机震惊华尔街。美国布鲁金斯学会的一项研究认为，会计丑闻使 2002 年美国经济损失了 370 亿~420 亿美元。假账丑闻使投资者对美国资本市场和会计公司的职业道德失去了信心。因此，加强金融监管以恢复投资者信心已成为当时美国国会、政府和公众的一致呼声。

另外，一系列公司假账丑闻的发生，已经不是个别公司的问题，而是美国公司制度的缺陷。这个缺陷主要表现在公司治理结构的不平衡和外部监督的缺失。

20 世纪 90 年代，美国公司制度一度被认为是最能激发人的创造力，最适合新技术发展的模式。员工股票期权激励机制和首席执行官制度被誉为美国公司近年来成功的精髓。但期权制也为公司管理层提供了抬高股价的动力，90 年代的股市繁荣，只要这些熟知公司内部情况的高级管理人员适时兑现手中的期权或股票，即使公司倒闭，其利益也能得到保证，这使得公司管理者的利益和股东利益严重脱节。

在公司治理结构上，对经营管理者的监督不力是造成假账丑闻的重要原因之一。20 世纪 90 年代是首席执行官制度的巅峰时期，名义上，首席执行官由董事会任命，但事实上，由于股权过于分散，首席执行官对董事会主席的任命有着很大影响。董事会的选举受首席执行官介绍情况的影响，并且在很多情况下，董事会主席由首席执行官兼任。这种情形的后果就是股东大会对经营管理者的控制力减弱，经营管理者为了自身利益而做出的掩盖债务、虚报利润等违法违规行为得以顺利实施，严重损害了广大投资者的利益。

在公司外部监督上，外部审计对上市公司信息披露的监督功能严重缺失。审计职能因其复杂性和专业性而从公司内部分离出来成为一个独立的行业。然而，为了谋取利益，会计师一方面对上市公司进行财务审计；另一方面又为上市公司提供会计咨询服务。因此，缺乏独立的审计，无法保证公司披露信息的真实性、公正性；一些审计公司不仅丧失了职业道德，而且干起了违法勾当，在上市公司接受司法调查时，审计公司帮助其销毁大批文件。长期以来，会计行业没有统一有效的监管，导致上市公司的外部监督失效。所以，广大投资者呼吁通过立法强化对企业会计审计监管、规范企业管理层行为。

《萨班斯-奥克斯利法案》正是这一背景下的产物。所谓《萨班斯-奥克斯利法案》，是指 2002 年 6 月 18 日美国国会参议院银行委员会以 17 票赞成对 4 票反对通过由奥克斯利和参议院银行委员会主席萨班斯联合提出的会计改革法案——《2002 上市公司会计改革与投资者保护法案》。这一议案在美国国会参众两院投票表决通过后，由布什总统在 2002 年 7 月 30 日签署成为正式法律。其主要内容以维护广大投资者利益为宗旨，对惩治公司财务欺诈、规范企业行为和加强资本市场监管做出了规定。

（一）明确了公司管理层的责任

（1）明确公司管理层对真实、全面、准确披露报告负责。公司首席执行官和财务总监必须签字对财务信息的准确性负责。公司必须实时公布任何导致公司财务健康状况发生变化的事件。

（2）明确公司管理层对内部控制体系设计、建立、运行有效负责。在披露年度报告

时，首席执行官和首席财务官就内部控制有效性发表声明。

（二）加强了会计监管

《萨班斯-奥克斯利法案》一方面加重对公司管理层违规行为的惩罚；另一方面加强对会计行业的监督。要求设立独立的上市公司会计监管委员会，负责监管执行上市公司审计的会计师事务所；特别加强执行审计的会计师事务所的独立性。

（1）美国证券交易委员会（SEC）设立独立的上市公司会计监管委员会来监督会计行业，该委员会制定清晰统一的职业标准和道德规范，并具有调查渎职和违规的权力。

（2）给美国证券交易委员会增加新资金用来对违规行为进行调查、提高员工待遇和升级电脑技术，同时赋予其禁止不诚实的管理者重新担负企业责任的权力。

（三）完善了公司审计制度

（1）内部审计制度的完善。法案第 301 条要求所有的上市公司都必须设立审计委员会，该委员会的成员必须全部是“独立董事”。法案对审计委员会的职权进行了具体的规定。

（2）外部审计监管的强化。法案明文禁止上市公司的独立审计人员同时向该上市公司提供包括保管财务数据、设计和执行财务信息制度、资产评估或估价服务等与审计无关的法律或其他专业服务在内的服务业务。

（四）强化上市公司信息披露的监控

SEC 对上市公司信息披露的审查权得到了加强。SEC 将要求上市公司达到所谓的“永久性”信息披露要求，即 SEC 必须在 3 年期限内对每个上市公司提交的信息披露进行审查，并做出审查结论。

（五）突出了舞弊防范

法案对欺诈和舞弊防范措施作了强制规定，要求建立“反舞弊程序和控制”，并要求每年进行评估，把发现高层管理人员任何程度上的舞弊行为判定为内部控制无效。

该法案第 406 条要求 SEC 制定相关规则，规定每个上市公司必须在其递交给 SEC 的定期报告的同时披露该公司是否已经制定了适用于高层财务人员的“道德法典”。“道德法典”必须包括以下内容：①诚实、道德的行为，包括私人利益与企业利益发生明显冲突时的道德准则；②在公众公司提交的报告中应包括充分、公正、准确、及时和易懂的信息披露；③要遵守政府的有关法律法规。

（六）严厉了法律制裁

《萨班斯-奥克斯利法案》针对上市公司增加了许多严厉的法律措施，成为继 20 世纪 30 年代美国经济大萧条以来，政府制定的涉及范围最广、处罚措施最严厉的公司法律。

（1）董事和高层管理人员须返还因公司虚假报表取得的激励性报酬和买卖股票收益。

（2）对于违反财务报表披露要求的行为，个人的处罚额提高到 100 万美元，并将可同时判处的监禁期限延长到 10 年，对恣意违反财务报表披露要求的公司主管处罚额高达 500 万美元，并可判处高达 25 年的监禁。

另外，按法案要求，2003 年 6 月 5 日，美国证券交易委员会颁布了《财务报告内部控制系统的管理层报告书》的“最终条例”（Final Rule）作为《萨班斯-奥克斯利法案》第 404 条款的执行细则。2004 年 3 月 9 日，美国上市公司会计监管委员会（PCAOB）最终确定了内部控制“审计标准”作为第 404 条款的审计细则。“最终条例”“审计标准”均

明确提到反虚假财务报告委员会的赞助组织委员会提出的内部控制框架可以作为企业内部控制体系建立的标准。

PCAOB 最终确定的内部控制“审计标准”要求公司管理层对内部控制的有效性实施评估，并且对所实施的评估进行记录和报告。管理层的总体责任包括：

（1）管理层必须记录与所有重要财务报表会计科目和披露事项之相关认定有关的内控设计；

（2）管理层必须测试与所有重要财务报表会计科目和披露事项之相关认定有关的内控，而且测试应当涵盖内部控制的全部要素。

（3）管理层必须执行适当程序以获得充分的证据并保留相关记录，来支持其对于公司内部控制的有效性实施的评估。

（4）管理层对内部控制实施评估是公司内部控制的一部分，它代表了公司监督内控的一个重要方面。可以使用内部审计师、公司其他人员和第三方协助其进行评估工作但不能将其对公司内部控制进行评估的责任委派给外部审计师或其他任何第三方。

（5）如果发现了一个或多个严重不合格（material weakness），管理层就不能认定公司的内部控制是有效的。

（6）404 条款管理层报告必须披露所有严重不合格（material weakness）。

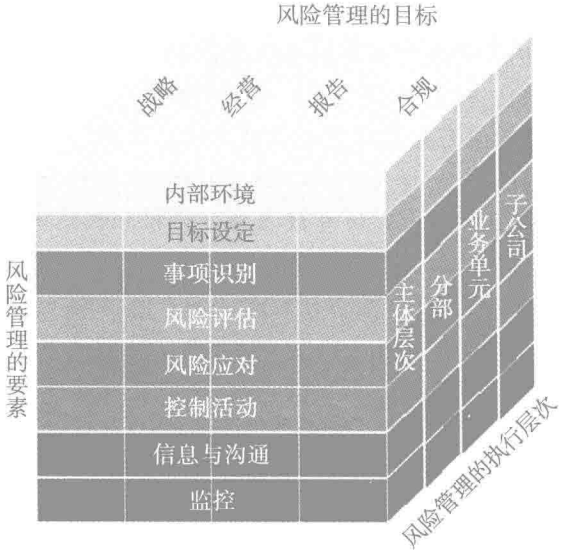
而且，法案对企业建立的内部控制活动的记录作了许多详细而严格的细节上的规定。如此一来，404 条款就成为外国公司迈入美国股市的“高门槛”。条款如此严苛，惩戒又如此严厉的法案自然令大批在美上市的外国公司不寒而栗。据悉，当时在美国上市的中国企业共有 46 家，其中不乏像网通、移动、百度这样的行业巨头。但是，中国企业此前从未经历过这样严厉的“美国规则”的考验。此次中国在美国上市的 46 家公司在应对《萨班斯-奥克斯利法案》方面的直接投入总共高达 10 亿元人民币，而大型央企由于公司治理方面相对较弱，其在人力、时间、资源方面的投入更高。有报道称，国际财务执行官组织对 321 家企业的调查显示，每家遵守《萨班斯-奥克斯利法案》的美国大型企业第一年实施 404 条款总成本平均超过 460 万美元，大名鼎鼎的通用电气公司更是花费了高达 3 000 万美元的巨款，来完善内部控制系统以符合 404 条款的要求。

综上所述，《萨班斯-奥克斯利法案》要求在美上市的公司必须建立内部控制体系；建立、运行、评估、披露内控体系的责任在管理层；美国证券交易委员会和美国上市公司会计监管委员会都推荐 COSO 框架作为企业建立内部控制体系的标准。

2004 年 10 月，COSO 委员会对《内部控制——整合框架》（Internal Control—Integrated Framework）做了进一步的延伸和扩展，提出了《企业风险管理——整合框架》（Enterprise Risk Management—Integrated Framework）。企业风险管理框架是在 1992 年 COSO 报告的基础上，结合《萨班斯-奥克斯利法案》在财务报告方面的要求，进行的扩展研究。COSO 对风险管理框架的定义是：“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的保证。”

与 1992 年 COSO 报告提出的内部控制整体架构相比，企业风险管理框架增加了一个观念（风险组合观）、一类目标（战略目标）、两个概念（“风险偏好”和“风险容忍

度”）和三个要素（“目标设定”、“事项识别”和“风险应对”），如图 1-3 所示。



资料来源：COSO. 企业风险管理——整合框架［M］. 方红星，译. 大连：东北财经大学出版社，2005.

图 1-3　企业风险管理框架

1. 提出了一个观念

企业风险管理框架提出了一个观念，即风险组合观，它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，总风险可以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. 增加了一类目标，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、财务报告和合规性三类。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：既包括内部报告，也包括外部报告；既包括企业内部管理者使用的报告，也包括向外部提供的报告；既包括法定报告，也包括向其他利益相关者提供的非法定报告；既包括财务信息，也包括非财务信息。此外，企业风险管理框架比内部控制框架增加了一类新的目标——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. 增加了两个概念

企业风险管理框架增加了两个概念，即“风险偏好”和“风险容忍度”。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。风险容忍度的概念是建立在风险偏好概念基础上的，是指在企业目标实现的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

现的差异的可容忍限度。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，即“目标设定”、“事项识别”和“风险对策”。此外，企业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。在控制环境要素上，企业风险管理框架将“控制环境”扩展为“内部环境”，更加直接、广泛地关注风险是如何影响企业的风险文化。在风险评估方面，企业风险管理框架建议从固有风险和残存风险的角度来看待风险；还要求注意相互关联的风险，确定一件单一的事项如何为企业带来多重的风险。在信息与沟通方面，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。

总的来讲，新的架构强调在整个企业范围内识别和管理风险的重要性。COSO 委员会强调风险管理框架必须和内部控制框架相一致，把内部控制目标和要素整合到企业全面风险管理过程中。因此，企业风险管理框架是对内部控制框架的扩展和延伸，它涵盖了内部控制，并且比内部控制更为完整有效。

2013 年 5 月 14 日，COSO 发布了修订的《内部控制——整合框架》和相关的说明性文件。COSO 还发布了《评价内部控制系统和对外财务报告内部控制（ICEFR）有效性的说明性工具：方法和范例简编》，简称 ICEFR 简编。该说明性工具将会帮助使用者评估其内部控制系统是否符合更新版框架提出的要求。ICEFR 简编特别与按照更新版框架中提出的要求编制用于外部目的财务报表的机构相关。

COSO 建议企业根据自身情况在可行的情况下尽可能快地采用修订的框架。在转换过渡期内（2013 年 5 月 14 日至 2014 年 12 月 15 日），企业可以继续采用原来的框架，但对外报告的机构应当明确披露其采用的是原来的框架还是 2013 年的框架。在此期间，COSO 也将继续在其刊物上提供《规模较小的公共公司财务报告内部控制指引》。到 2014 年 12 月 15 日之后，COSO 开始用 2013 年的框架取代原有框架。

第三节 我国内部控制制度的发展

20 世纪 80 年代以前，我国的企业内部控制基本停留在会计控制的范畴，而且主要是以账户核对和职务分工为主要内容的牵制制度上。但总的来看，这些制度比较零散、不系统，而且很多未能真正得以执行而流于形式，致使单位内部管理低效，控制弱化。

一、我国历年的内部控制法规

20 世纪 90 年代后期开始，我国政府才开始积极推进内部控制评价的规范化建设。我们可以从历年来形成的有关内部控制的法规窥见一斑：

1986 年财政部颁发《会计基础工作规范》，其中对企业（单位）内部控制制度作了明确规定。

1997 年 1 月中国注册会计师协会实施《独立审计具体准则第 9 号——企业内部控制与审计风险》，以便于会计师事务所评估审计风险，提高审计效率，保证执业质量。

1999 年 3 月全国人民代表大会通过新《会计法》，将企业（单位）内部控制制度当作保障会计信息“真实和完整”的基本手段之一。

1996 年 12 月国家审计署实施《中华人民共和国国家审计基本准则》，其中将对企业（单位）内部控制制度的测试当作“作业准则”予以明确。

2000 年 11 月中国证监会发布《公开发行证券公司信息披露编报规则》，要求公开发行证券的商业银行、保险公司、证券公司应建立健全企业内部控制制度。

2001 年 6 月财政部发布《内部会计控制——基本规范（试行）》和《内部会计控制基本规范——货币资金（试行）》。

2002 年 2 月中国注册会计师协会制定发布了《内部控制审核指导意见》。

2002 年 9 月 7 日中国人民银行发布《商业银行内部控制指引》，指出企业内部控制是商业银行为实现经营目标，通过制定和实施一系列制度、程序和方法，对风险进行事前防范、事中控制、事后监督和纠正的动态过程和机制。

2002 年 12 月 19 日中国证监会发布《证券投资基金管理公司企业内部制度指导意见》，首次系统地提出基金公司企业内部控制的目标和要求。

2002 年 12 月财政部发布《内部会计控制规范——采购与付款（试行）》和《内部会计控制规范——销售与收款（试行）》。

2003 年 10 月财政部发布《内部会计控制规范——工程项目（试行）》。

2004 年 8 月 20 日中国银行业监督管理委员会通过《商业银行内部控制评价试行办法》，自 2005 年 2 月 1 日起施行。

2006 年 6 月 5 日上海证券交易所发布《上海证券交易所上市公司内部控制指引》，内部控制是指上市公司（以下简称公司）为了保证公司战略目标的实现而对公司战略制定和经营活动中存在的风险予以管理的相关制度安排。它是由公司董事会、管理层及全体员工共同参与的一项活动。公司内部控制通常应涵盖经营活动中所有业务环节、经营活动各环节之中的各项管理制度、信息管理、专项风险等。

2006 年 6 月 6 日国资委出台《中央企业全面风险管理指引》，本指引所称全面风险管理，指企业围绕总体经营目标，通过在企业管理的各个环节和经营过程中执行风险管理的基本流程，培育良好的风险管理文化，建立健全全面风险管理体系，包括风险管理策略、风险理财措施、风险管理的组织职能体系、风险管理信息系统和内部控制系统，从而为实现风险管理的总体目标提供合理保证的过程和方法。

2006 年 7 月 15 日，我国企业内部控制标准委员会成立大会暨第一次全体会议在北京举行。企业内部控制标准委员会成员由财政部、证监会、国资委等来自监管部门以及实务界、理论界的专家学者组成。

2008 年以前，我国发布的内部控制法律法规，具有很强的行业和部门特点，虽不乏共识之处，但更多的是各自为政，缺乏统一、规范、协调的内控框架。

2008 年 6 月，五部委联合下发《企业内部控制基本规范》，自 2009 年 7 月 1 日率先在上市公司实施，鼓励非上市的大中型企业执行。

2010 年 4 月，五部委联合下发《企业内部控制配套指引》，自 2011 年 1 月 1 日起在境内外同时上市的公司施行，自 2012 年 1 月 1 日起在上海证券交易所、深圳证券交易所主板上市公司施行；在此基础上，择机在中小板和创业板上市公司施行。鼓励非上市大中型企业提前执行。

2012 年财政部财会〔2012〕21 号文颁布了《行政事业单位内部控制规范（试行）》，

指导行政事业单位内部控制活动的有序进行，并于2015年12月21日财会〔2015〕24号文颁布了《关于全面推进行政事业单位内部控制建设的指导意见》。

二、目前我国的内部控制体系

我国企业现行的内部控制体系是由财政部、审计署、银监会、证监会和保监会五部委于2008年6月28日联合下发的《企业内部控制基本规范》和2010年4月联合下发的18项《企业内部控制应用指引》、《企业内部控制评价指引》和《企业内部控制审计指引》，以及于2010年7月出台的操作应用指南。

其中，内部控制标准体系主要包括基本规范、具体规范和相关应用指南。内部控制基本规范规定了内部控制的基本目标、基本要素、基本原则和总体要求，是制定具体规范和应用指南的基本依据，在内控标准体系中起统驭作用。内部控制具体规范是根据基本规范，对企业办理具体业务与事项从内部控制角度做出的具体规定。相关应用指南是根据基本规范和相关具体规范制定的详细解释和说明，主要是为某些特殊行业、特殊企业、特定内控程序提供操作性强的指引。

我国现行的内部控制体系如图1-4所示。

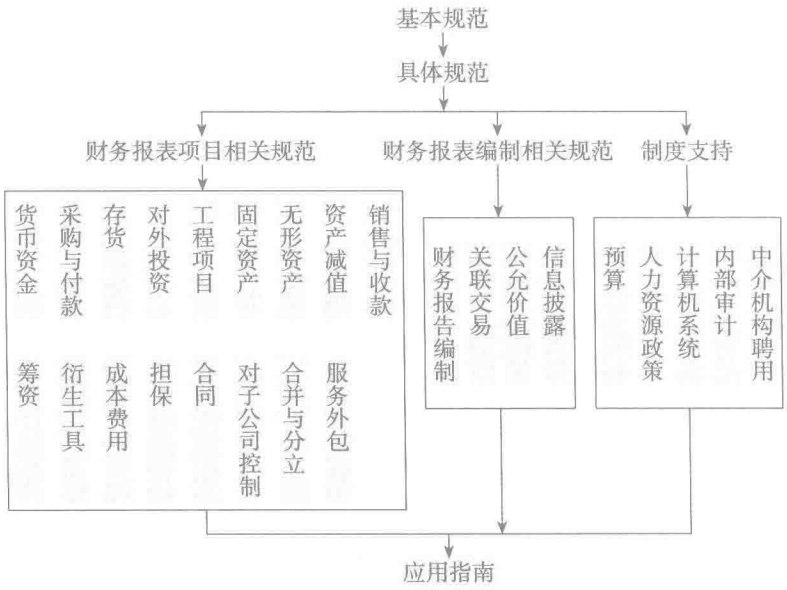


图1-4 我国现行的内部控制体系

第四节 企业内部控制的意义、相关概念与局限性

一、企业内部控制的意义

1. 企业对内部控制与风险管理的认知是解决企业现实难题的独特钥匙

如何看待企业在发展过程中效率与安全的矛盾；制度有时为何成为发展的绊脚石；为什么有健全制度仍然出现问题；保证制度有效性的主要责任在谁；如何辨别企业、业务、部门的风险；部门与企业发展战略如何切实连接；怎样确保制度的有效贯彻和执行；生产、采购、销售、投资、应收账款的管理如何全面布局；基于财务的内控体系如何构建？

面对企业这些现实难题，内部控制制度体系与风险管理框架可以为其提供有效的解决方案。

2. 强化企业的内部控制已经成为发达国家治理公司的重要手段

企业必须建立有效的内部控制体系。但什么是有效的内部控制体系？谁对企业内部控制负责？如何评价和改进企业的内部控制？这已成为企业可持续发展的关键。

企业内部控制是关系到企业发展壮大乃至生存的非常重要的一个方面。虽然企业内部控制不能保证企业成功，但是在通过对企业失败案例进行分析后我们发现，如果没有内部控制，企业失败的概率会大很多。也就是说有了内部控制不是万能的，但是没有它是万万不能的。例如：企业各部门、各岗位谁最重要？相同业务，为什么不同人操作结果会有差异？怎么解决企业每一部门、每一岗位做什么的问题？怎么解决每一部门、每一岗位怎么做的问题？指令从最高层传达至最底层为什么会完全“变味”？如何解决战略失当、决策失误、无为成本、毁损价值的现象？诸如此类的问题，正是内部控制可以解决的问题。

3. 内部控制与风险管理是提高企业运营效率的基本工具

内部控制通过构建完整的企业内控制度体系，规范企业各作业流程，明确所有员工责权利，寻找企业经营的风险事件和风险点，完善风险管理措施，可以有效地整合企业资源，提高企业资金利用效率。通过内部控制的授权和流程设计可以解决战略失当、决策失误、无效成本、低效成本、不良成本、无为成本、错误、舞弊、违法、信息失真、价值链畸变等问题。因此，随着企业间竞争环境的恶化和竞争程度的不断加剧，21 世纪企业发展的基础有赖于内部控制和风险管理技术的不同，内部控制与风险管理是提高企业运营的效率的基本工具。

4. 内部控制与风险管理已经成为财务主管的重要职责

随着全球范围内内部控制的不断推广，各个国家都分别对企业内部控制与风险管理提出了新的要求。财务主管的主要职能也在悄然发生着变化，由原来的简单记账、财务评价、企业顾问到决策支持，即由会计控制到管理控制再到资金控制然后到风险控制。全面风险管理已经成为现代企业财务主管的重要职责。

5. 防范错弊

错弊的防范是企业生存的底线，企业在盈利之前，先要保证资金的安全，不要让可能的风险发生，这就是防范错弊。在设计错弊的防范机制之前，首先要知道错弊是怎么发生的。错弊三角理论认为，任何错弊的发生都是在压力、借口和机会三个要素共同作用下形成的（如图 1-5 所示）。

图 1-5 错弊三角动因图

有压力就有寻找借口的动机，一旦存在错弊的机会时，就可能在压力之下找到各种舞弊的借口，从而进行舞弊。因此，压力、借口和机会是错弊形成的动因，也称为错弊三要素。那么，要防范错弊，就要从三要素入手，即通过进行职业道德教育让其不愿犯错；通过法律法规让其不敢犯错；通过内部控制让其不能犯错。企业内部的舞弊行为有可能是主