# 前言

在当今复杂多变的世界中，组织的生存和发展离不开有效的内部控制和风险管理。良好的内部控制体系是组织稳健运行和高效运作的关键因素，有效的风险管理是组织保持竞争力、抵御潜在风险的基础。本教材是对2016年教材的修订再版，旨在应对全球经济的不断变化，反映最新的研究成果和实践经验及政策法规的要求，提供关于内部控制和风险管理的全面、深入的理解。

内部控制与风险管理课程是高校财务管理、会计学、审计学等财经类专业的专业核心课程。本教材的内容包括总论、内部控制与风险管理框架、内部环境、风险评估、控制活动、信息与沟通、业务活动(含资金活动、采购业务、资产管理、销售业务、研究与开发、工程项目、担保业务、业务外包、财务报告)、内部监督、内部控制评价和内部控制审计，共11章。能满足本科层次和研究生层次的教学需要，也为企业管理者、风险管理人员以及其他相关人士提供参考。本教材的再版力争体现以下特点：

1.思政引领

将思政教育理念贯穿于教材的始终。每一章章前结合学习目标凝炼专业知识中所蕴含的思想价值和精神内涵，强化职业道德和诚信意识，培养团队协作精神，提高风险应对能力，增加法律意识和合规意识，以实现人才培养的知识传授、能力培养与价值塑造的有机融合。

2.知识新颖

为反映国内外关于内部控制与风险管理理论与实务发展的前沿动态，本教材对内部控制与风险管理的发展、理论框架等相关内容进行了修订和补充，特别是补充了COSO于2017年发布的风险管理框架内容及与2004版风险管理框架比较和我国2017年以来有关内部控制与风险管理的最新规章制度的主要精神，包括2017年财政部发布的《行政事业单位内部控制报告管理制度（试行）》和《小企业内部控制规范（试行）》及2019年以来国务院国资委印发的《关于加强中央企业内部控制体系建设与监督工作的实施意见》（国资发监督规〔2019〕101号）、《关于做好2020年（2021年、2022年、2023年）中央企业内部控制体系建设与监督工作有关事项的通知》（国资厅发监督〔2019〕44号、国资厅监督〔2020〕307号、国资厅监督〔2021〕299号、国资厅监督〔2023〕8号）、《关于加强中央企业资金内部控制管理有关事项的通知》（国资发监督〔2021〕19号）等。

3.内容全面

本教材涵盖内部控制与风险管理的各个方面，包括内部控制的目标、要素、原则、方法、流程、评价和审计，以及风险的识别、评估、应对和监督等。同时，还注重与其他学科的交叉融合，如会计、审计、法律、管理学等，以提供对内部控制和风险管理的全面理解，帮助读者建立一套适合自己的内部控制和风险管理机制。

内部控制与风险管理工作在我国目前仍处于探索与完善阶段，相关教材的编写也难免存在种种不足，恳请广大读者及时批评指正，以便我们不断完善和改进教材内容。

编　者

# 目　录

CONTENTS

# 第一章

# 总　论

## 学习目标

1.理解内部控制与风险管理产生的历史必然性；

2.理解和掌握内部控制与风险管理的概念及其特征；

3.熟悉国内外内部控制与风险管理理论的演变及发展过程；

4.结合国资委 2022 年 8 月出台的《中央企业合规管理办法》，理解合规管理与法务管理、内部控制、风险管理的协同关系；

5.熟悉并理解内部控制建设的现实意义及固有局限性。

## 课程思政

1.通过熟悉国内外内部控制与风险管理的发展历程，培养历史思维和辩证思维；

2.通过对比国内外内部控制与风险管理的发展历程，增强爱国情怀，坚定道路自信、理论自信、制度自信、文化自信；

3.培养坚持不懈、坚韧不拔的斗争精神，不断提升自我，努力成为德才兼备的优秀人才。

## 第一节　内部控制与风险管理的发展历程

内部控制是管理现代化的产物。它是在早期内部牵制的基础上，伴随着单位内部科学管理的压力和外部审计开展的动力，由单位管理人员在经营管理的实践中创造，并经审计人员理论总结而逐步发展完善的。内部控制存在于各类经济单位。

内部控制是随着人类社会发展而演变的，其在社会发展的各个阶段具有不同的内涵和外延。一般认为，内部控制理论产生与发展经历了五个阶段，达到了从会计控制到财务控制、管理控制、再到风险管理的层次。

### 一、内部控制萌芽时期——内部牵制阶段

内部牵制阶段体现于公元前 3600 年—20 世纪 40 年代。内部控制起源于内部牵制。“内部牵制制度”

规定有关经济业务或事项的处理不能由一个人或一个部门总揽全过程。1912 年 R.H.蒙哥马利在其出版的《审计——理论与实践》一书中指出，所谓内部牵制是指一个人不能完全支配账户，另一个人也不能独立地加以控制的制度，某位职员的业务与另一位职员的业务必须是相互弥补、相互牵制的关系，即必须进行组织上的责任分工和业务的交叉检查或交叉控制，以便相互牵制，防止发生错误或弊端。

内部牵制的提出主要基于两个设想：一是两个或两个以上的人或部门无意识地犯同样的错误的机会是很小的；二是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。这种设想为建立内部牵制提供了理论基础，从纵向看，每项经济业务的处理，至少要经过上下级有关人员之手，使下级受上级监督，上级受下级制约，促使上下级均能忠于职守，不可疏忽大意；从横向看，每项经济业务的处理，至少要经过彼此不相隶属的两个部门的处理，使每一部门工作或记录受另一个部门的牵制，不相隶属的不同部门均有完整的记录，使之互相制约、自动检查，防止或减少错误和弊端；同时，通过交叉核对也能及时发现错误和弊端。

内部牵制的执行大致可分为以下四类：实物牵制、机械牵制、体制牵制和簿记牵制。实物牵制指由两个以上人员共同掌管必要的实物工具，共同才能完成一定程序的牵制，如双人保管保险柜钥匙、付款清单等重要物品；机械牵制指只有按正确的程序操作机械，才能完成一定过程的牵制，如不按照程序操作的业务无法继续进行；体制牵制是把每项业务的作业交由不同的部门或个人去分别处理，以防止错误和舞弊的一种牵制，如采用双人记账等双重控制措施来预防错误和舞弊的发生；簿记牵制指会计原始凭证与记账凭证、会计凭证与账簿、账簿与会计报表之间核对的牵制，如采用账目核对等复式记账、借贷平衡的平行登记、总账和明细账定期核对等。

在内部牵制阶段，内部控制活动的主线是查错防弊，即防止记录差错和财货被侵吞，其主要方法是账户核对和职务分工。在现代企业内部控制中，仍然闪耀着古代内部牵制的思想和方法的光芒。比如，现代会计记录依然沿用的是意大利复式记账方法；西周时期要求财赋管理应做到“一毫财赋之出入，数人耳目之通焉”，演绎至现代即是“四眼原则”。

## 二、内部控制形成时期——内部控制制度阶段

内部控制制度阶段体现于 20 世纪 40 年代至 70 年代。“内部控制”一词最早见诸文字，是作为审计术语出现在审计文献中的。1934 年美国针对经济危机中发现的种种控制问题而制定的《证券交易法》，首先提出了“内部会计控制”（Internal accounting control system）的概念。1936 年，美国会计师协会发布的《注册会计师对财务报表的审查》文告，以及 1947 年《审计准则暂行公告》（TSAS），出于改进审计方式的需要，提出了以内部控制（Internal control）为基础的审计程序。

1949 年，美国职业会计师协会所属的审计程序委员会在《内部控制，一种协调制度要素及其对管理当局和独立注册会计师的重要性》的特别报告中，第一次提出了内部控制的概念，即：内部控制包括经济单位的计划及经济单位为保护其财产、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。该定义认为，内部控制系统已远远超出了财务、会计的范围。此定义及其相应的解释，当时被普遍认为是对认识内部控制这一概念的重大贡献，因为在此之前内部控制概念从未受到如此的重视。

1950 年美国将“内部控制”列入政府法令，这是世界上首次，标志着内部控制制度的产生；日本在《审计标准》中把内部控制组织划分为内部牵制组织和内部审计组织；1951 年日本《企业内部控制大纲》定义了内部控制；1958 年 10 月美国《审计程序公告第 29 号》对内部控制的定义重新表述，将内部控制划分为会计控制和管理控制，前者指与财产安全和会计记录正确性相关的程序和方法，后者指与贯彻管理方针和提高经济效益相关的程序和方法。这就是我们目前所熟知的内部控制的“制度二分法”的由来。

1963 年和 1972 年两次重新定义内部会计控制和内部管理控制，使内部管理控制的含义进一步具体化。

## 三、内部控制发展时期——内部控制结构阶段

内部控制结构阶段体现于20世纪80年代至90年代。进入20世纪80年代以后，内部控制的研究重点逐步从一般含义研究转向具体内容的深化。

1988年5月，美国注册会计师协会发布《审计准则公告第55号》，首次以“内部控制结构”概念取代了“内部控制制度”概念。该公告认为内部控制结构是指为企业特定目标提供合理保证而建立的各种政策与程序，包括控制环境、会计制度和控制程序三个要素，如图1-1所示。其中会计制度是内部控制结构的关键要素，控制程序是保证内部控制结构有效运行的机制。

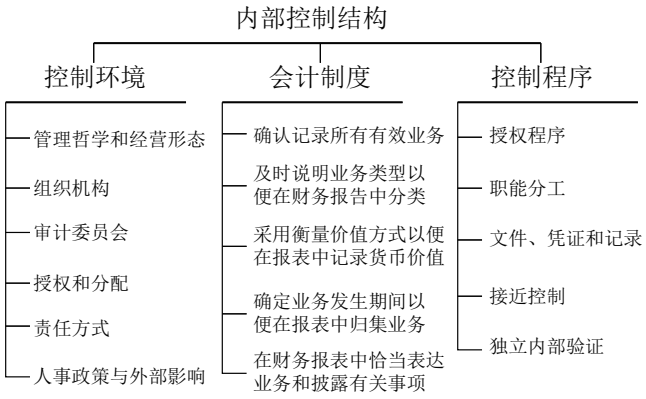


**图1-1 内部控制结构**

这一概念跳出了“制度二分法”的圈子，特别强调了管理者对企业内部控制的态度、认识和行为等控制环境的重要作用，指出这些环境因素是实现企业内部控制目标的环境保证，要求审计师在评估控制风险时不仅要关注会计控制制度与控制程序，还应对企业所面临的内外环境进行评估。

## 四、内部控制成熟时期——内部控制整合框架阶段

内部控制整合框架阶段体现于20世纪90年代至21世纪，1985年，由美国注册会计师协会（AICPA）、美国会计学会（AAA）、财务执行官协会（FEI）、国际内部审计师协会（IIA）、管理会计师协会（MAA）共同赞助成立反虚假财务报告委员会（Treadway委员会），该委员会旨在探讨财务报告中的舞弊产生的原因，并寻找解决措施。该委员会虽然未对内部控制提出结论，但其研究指出50%的财务舞弊事件可全部或部分归因于内部控制不健全。

基于该委员会的建议，其赞助机构成立COSO委员会（Committee of Sponsoring Organization），专门研究内部控制问题。

1992年9月，COSO委员会提出了报告《内部控制——整合框架》（1994年进行了增补），即COSO内部控制框架。该框架指出“内部控制是受企业董事会、管理层和其他人员影响，为经营的效率效果、财务报告的可靠性、相关法规的遵循性等目标的实现而提供合理保证的过程”。1996年年底美国审计委员会认可了COSO的研究成果，并修改相应的审计公告内容。该报告提出了内部控制的五大要素，即控制环境、风险评估、控制活动、信息与沟通、监控。

COSO发布的《内部控制——整合框架》，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。

在美国建立COSO内部控制框架后，加拿大特许会计师协会的CoCo委员会（Criteria of Control Board，控制标准委员会）1995年11月提出了“控制原则标准”（the Criteria of Control Principles，即CoCo框架）。CoCo框架提出了目标、承诺、能力、学习和监督四大类控制标准，也即四个基本要素。这四个基本要素通过“行动”联结成一个循环。英国的Cadbury委员会也提出了一个与COSO相似的内控框架。

我国2012年1月1实施的《中国注册会计师审计准则第1211号——通过了解被审计单位及其环境识别和评估重大错报风险》准则、2011年1月1日实施的《国家审计准则》和2003年6月1日实施

的《内部审计具体准则第 5 号——内部控制审计》准则，均采纳了 COSO 的内部控制框架。

为帮助企业适应越趋复杂和快速的环境变化，应对阻碍企业目标实现的风险，并提供可靠的信息以助做出明智决策。2013 年 5 月 14 日，COSO 发布了《2013 年内部控制整体框架》及其配套指南，并要求 2014 年 12 月 15 日以后用该框架取代 1992 年发布的旧框架，新框架涵盖内容摘要、具体内容、多份附录、一份应用指南（提供解释性工具）以及一份概要（提供方法和示例说明在财务报告内部控制上的应用）。

## 五、内部控制的新发展——企业风险管理阶段（ERM）

企业风险管理阶段（ERM）体现于 21 世纪以来，2001 年 11 月，安然公司财务丑闻曝光，6 个月后，世通公司再度爆发丑闻，美国这一期间有 338 家上市公司，总计 4 093 亿美元的资产申请破产保护。投资者、员工和其他利益相关者遭受了巨大的损失。为了应对这一系列上市公司财务欺诈事件所造成的美国股市危机，重树投资者对股市的信心，美国国会出台了《2002 年公众公司会计改革和投资者保护法案》，即《2002 年萨班斯—奥克斯利法案》（SOX 法案）。SOX 法案对美国《1933 年证券法》《1934 年证券交易法》做了不少修订，其中的第 302 款和第 404 款对所有在美国上市的公司的内部控制体系建设提出了要求。

《萨班斯—奥克斯利法案》第 302 款要求公司首席执行官和财务总监对呈报给 SEC 的财务报告“完全符合证券交易法，以及在所有重大方面公允地反映了财务状况和经营成果”予以签字保证。第 404 款要求公众公司年度报告中应包含内部控制报告，包括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，以及对最近财政年度末的内部控制体系及控制程序有效性评价，并要求独立审计师对公司管理层做出的内部控制评价出具鉴证报告。

作为对 SOX 法案的积极反应，2004 年 9 月，COSO 委员会颁布了《企业风险管理—整合框架》（以下简称 2004 年版 COSO－ERM 框架）该风险管理框架就是在 COSO1992 年的研究成果《内部控制——整合框架》报告的基础上，结合 SOX 法案的要求，进行扩展研究提出来的，被公认是目前满足 SOX 法案所要求的企业内部控制体系的最佳实践依据。

2004 年版 COSO－ERM 框架认为：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。它包括四个目标，即战略目标、经营目标、报告目标和合规目标；八个组成要素：内部环境、目标设定、事件识别、风险评估、风险反应、控制活动、信息与沟通、监督。

简单地看，相对于内部控制框架而言，2004 年版 COSO－ERM 框架新增加了一个观念、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，该框架还要求企业设立一个新的部门——风险管理部。企业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。

2004 年版 COSO－ERM 框架在数十年的实践中暴露出一些问题，如对风险管理和内部控制的划分界限不够清晰。此外，在 ERM（2004）发布后十几年里，市场、经济环境都发生了巨大变化，新型风险层出不穷。在此背景下，美国 COSO 在 2014 年首次启动了对风险管理框架的修订工作，并于 2017 年 9 月发布了《企业风险管理—与战略和绩效的整合》（Enterprise Risk Management——Integrating with Strategy and Performance，以下简称 2017 年版 COSO－ERM 框架），该框架告别了 2004 年版的立体八要素框架，采用 5 个要素 20 项原则，更加注重对企业战略和愿景的支撑，与价值创造紧密关联，更加强调和业务活动的融合，倡导决策和目标导向，明确风险管理和战略嵌入组织的重要性。2017 年版 COSO－ERM 框架不是 2004 年版 COSO－ERM 框架的简单升级，而是大刀阔斧的重构与变革，并将其目标定位于为包括企业在内的所有主体提供一个“管理框架”而非“控制框架”。

## 第二节 我国内部控制与风险管理的起源与发展

### 一、我国内部控制的起源

在我国，内部控制制度起源于西周时期，我国社会经济发展没有经历过工业革命，所以内部控制制度没有体现在企业的制度中，而我国古代的内部控制制度体现在统治者对政权的控制中，我国西周时期内部控制的最初产生空间、手段和雏形已经具备。

组织结构方面，我国在西周时期，官厅组织结构就已经比较完善。《周礼》中有记载，西周王朝的时候，最高统治者周王，下设天官冢宰、地官司徒、春官宗伯、夏官司马、秋官司寇和冬官考工等六大官职。秦朝建立的三公九卿组织，结构更为完备。因而，从官厅内部控制的角度来讲，西周时期就具备了内部控制产生的空间条件。

会计核算方面，早在西周时期，会计组织由司会统一管理，司会的具体职责包括会计、出纳、税务、财物保管、考核（钩考）、人口与土地统计。组织内部已经构成了一个比较严密的系统，系统内部不但建立了独立的会计部门，而且会计部门与业务部门之间已分工明确。

内部牵制与内部稽核方面，《周礼》中有记载，西周时期的内部牵制包括：财物分管，也就是在天官冢宰之下分设大府、王府、内府、外府、职币等机构，分开管王朝的财物；分职核算，也就是会计记账人员、收入核算、支出核算，以及实物保管，分别由不同官员实施；内部稽核，也就是宰夫行使稽核职权，负责组织对财物保管部门年度、月度、旬度的财物出入和经济收支情况进行具体全面的稽核，这可以作为确定官吏政绩优劣的依据。

### 二、我国内部控制的发展

#### （一）古代的内部控制

在我国，古代内部控制制度始于西周，完善于唐朝，衰落于宋代。

西周时期是奴隶社会鼎盛的阶段，唐朝是封建社会的盛世时期，宋朝封建社会转衰的过程，这与我国古代的社会经济发展轨迹是相符合的。

在西周时，就闪烁着内部牵制制度的火花，例如“听出入以要会”，也就是以会计文书为依据，批准财物收支事项。当时的统治者，为防止掌管和使用财赋的官吏弄虚作假甚至贪污盗窃所采用的分工牵制和交互考核等办法，达到了“一毫财赋之出，数人之耳目通焉”的程度。这段时期上计内部控制制度已有萌芽。

秦朝时期，就已形成严密的上计制度和御史监察制度。在宋朝，已经形成知府与通判联署的做法，所以说内部控制制度在我国早已有之。中央集权的封建制度在我国的长期影响，社会经济发展及其监控主要由官府来负责，主要方式是职务牵制，民间企业发展及其监控相对薄弱。这一阶段的内部控制的着眼点在于职责的分工和业务流程及其记录上的交叉控制。内部控制主要通过人员配备和职责划分、业务流程、簿记系统等来完成。其目的主要是防止组织内部的错误和舞弊，通过保护组织财产来保障组织运转的有效运行。

#### （二）现代的内部控制

新中国成立之后，由于借鉴了苏联社会主义国家模式实行计划经济体制，对社会经济发展采取高度集中的方式，企业经营与规划完全由国家来控制，监控也由国家直接进行，以企业为主体的内部控制几乎缺失。一直到十一届三中全会确立改革开放的总方针后，市场经济的提出与全国建设才还企业以自主发展的广阔空间，发展蕴含着加强内部控制健全运营机制。这一阶段内部控制开始有了内部会计控制和内部管理控制的区分，主要是通过形成和推行一套内部控制制度来实施控制。内部控制的目标除了保护组织财产的安全之外，还包括增进会计信息的可靠性、提高经营效率和遵循既定的管理等方针。

1986 年财政部颁发《会计基础工作规范》，其中对内部控制做了明确的规定，这一阶段开始把控制环境作为一项重要内容与会计制度、控制程序一起纳入内部控制结构之中，并且不再区分内部会计

控制和管理控制。控制环境反映组织的各个利益关系主体对内部控制的态度、看法和行为；会计制度规定各项经济业务的确认、分析、归类、记录和报告方法，旨在明确各项资产、负债的经营管理责任；控制程序是管理当局所确定的方针和程序，以保证达到一定的目标。

1996 年 12 月，财政部发布了《独立审计准则第 9 号——内部控制和审计风险》，对内部控制做出了权威性解释，即“是被审计单位为了保证业务活动的有效进行，保证资产的安全完整，防止、发现、纠正错误与弊端，保证会计资料的真实、合法、完整而制定和实施的政策与程序”，并提出了内部控制“三要素”，帮助注册会计师判断是否信赖内部控制，以确定审计的性质、时间与范围。这是我国现代第一个关于内部控制的行政规定，它的发布标志着我国现代内部控制建设拉开了序幕。

1999 年修订的《中华人民共和会计法》（以下简称《公司法》）第一次以法律的形式对建立健全内部控制提出原则性要求，财政部随即连续制定发布了《内部会计控制规范——基本规范》等 7 项内部会计控制规范。2001 年 6 月财政部发布的《基本规范》和《内部会计控制规范——货币资金（试行）》，明确了单位建立和完善内部会计控制体系的基本框架和要求，以及货币资金内部控制的要求。上述两个内部会计控制规范的发布，为我国加强单位内部会计监督与控制的理论与制度建设，树立了一个具有时代意义的里程碑，同时也标志着我国会计法规建设进入到更高的新境界。

与此同时，国务院其他政府管理部门也相继出台内部控制政策和法规，如 2000 年 1 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；2002 年 6 月 13 日中国注册会计师协会制定发布了《企业内部控制审核指导意见》；2002 年 9 月 7 日中国人民银行发布《商业银行企业内部控制指引》，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。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，国资委发布《中央企业全面风险管理指引》，对内控、全面风险管理工作的总体原则、基本流程、组织体系、风险评估、风险管理策略、风险管理解决方案、监督与改进、风险管理文化、风险管理信息系统等进行了详细阐述。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，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》（以下简称《规范》），《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。《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，结束了长期以来分部门制定内部控制法规的阶段。

2010 年 4 月 26 日，政部会、证监会、审计署、银监会、保监会联合发布了《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当前实际情况、融合国际先进经验的中国企业内部控制规范体系基本建立起来了。该配套指引，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。

2011 年 10 月中国注册会计师协会发布《企业内部控制审计指引实施意见》，规范注册会计师执行

内部控制审计业务，明确工作要求，提高执业质量，维护公众利益。

2012 年 2 月财政部颁布《企业内部控制规范体系实施中相关问题解释第 1 号》，对企业内部控制规范体系的 10 个问题进行了解释，如规范体系的强制性与指导性、规范体系与其他监管部门规定的关系、内部控制与风险管理的关系、规范体系的政策盲区、内部控制的成本与效益、内部控制与其他管理体系的关系、内部控制缺陷的认定标准、内部控制机构设置、内部控制评价报告等。

2012 年 9 月财政部颁布《企业内部控制规范体系实施中相关问题解释第 2 号》，对企业内部控制规范体系的 10 个问题进行了解释，如内控组织实施、内控人才队伍培养、集团企业内部控制评价、内部控制缺陷处理、会计师事务所工作、小型企业内控建设等。

2012 年 11 月财政部发布《行政事业单位内部控制规范（试行）》，进一步提高行政事业单位内部管理水平，规范内部控制、加强廉政风险防控机制建设。

2013 年 12 月财政部发布《石油石化行业内部控制操作指南》，指导不同规模、不同产业链中的石油石化行业企业开展企业内部控制体系的建立、实施、评价与改进工作。

2014 年 1 月财政部和证监会发布《公开发行证券的公司信息披露编报规则第 21 号——年度内部控制评价报告的一般规定》，分步推进资本市场全面贯彻实施企业内部控制规范体系，规范上市公司内部控制信息披露行为，保护投资者的合法权益。

2014 年 9 月银监会印发《商业银行内部控制指引》，促进商业银行建立健全内部控制，有效防范风险，保障银行体系安全稳健运行。

2014 年 12 月财政部发布《电力行业内部控制操作指南》，供电网企业、发电企业、电力建设企业、电力设计企业和其他辅助性电力企业开展内部控制体系的建立、实施、评价与改进工作时参考使用。

2015 年 2 月中国注册会计师协会发布《企业内部控制审计问题解答》，进一步指导注册会计师更好地贯彻内部控制审计思路，解决在企业内部控制审计实务中遇到的问题，防范审计风险。

2015 年 12 月保监会印发《保险资金运用内部控制指引》及应用指引，进一步加强保险资金运用内部控制建设，提升保险机构资金运用内部控制管理水平，有效防范和化解风险。

2017 年 1 月财政部发布《行政事业单位内部控制报告管理制度（试行）》，进一步加强行政事业单位内部控制建设，规范行政事业单位内部控制报告的编制、报送、使用及报告信息质量的监督检查等工作，促进行政事业单位内部控制信息公开，提高行政事业单位内部控制报告质量。

2017 年 6 月财政部发布《小企业内部控制规范（试行）》，指导小企业建立和有效实施内部控制，提高经营管理水平和风险防范能力，促进小企业健康可持续发展。

2018 年 8 月财政部发布《管理会计应用指引第 700 号——风险管理》《管理会计应用指引第 701 号——风险矩阵》，加强企业风险管理，推动相关管理会计工具方法在风险管理领域的有效应用。

2018 年 11 月国资委颁布《中央企业合规管理指引（试行）》（国资发法规〔2018〕106 号），要求中央企业合规管理全业务、全层次、全员工、全流程，做到“四全”全面覆盖，层层强化责任制，监察、审计、内控、风险管理等工作协同联动，合规管理牵头部门客观独立履行职责，加快建立健全合规管理体系。

2019 年 10 月国资委颁布《关于加强中央企业内部控制体系建设与监督工作的实施意见》（国资发监督规〔2019〕101 号），要求企业建立健全以风险管理为导向、合规管理监督为重点，严格、规范、全面、有效的内控体系，严格落实各项规章制度，将风险管理和合规管理要求嵌入业务流程，实现“强内控、防风险、促合规”的管控目标，切实全面提升内控体系有效性。

2019 年 12 月国资委颁布的《关于做好 2020 年中央企业内部控制体系建设与监督工作有关事项的通知》（国资厅发监督〔2019〕44 号）规定，企业要高度重视内控体系建设与监督工作，加强组织领导，落实企业主要领导人员内控体系监管工作第一责任人职责，尽快明确专门职能部门或机构，配备必要专门人员，建立健全上下贯通、全面覆盖的内控工作体系。形成领导有力、职责明确、流程清晰、规范有序的工作机制。

2020 年 9 月国资委发布《关于深化中央企业内部审计监督工作的实施意见》（国资发监督规〔2020〕60 号），要求国有企业加强内控体系审计，提升企业内控体系有效性。

2020 年 10 月国资委颁布的《关于做好 2021 年中央企业内部控制体系建设与监督工作有关事项的通知》（国资厅监督〔2020〕307 号）规定。为推进中央企业管理体系和管理能力现代化，要完善中央企业内控制体系，增强中央企业抗风险能力。2021 年 3 月国资委颁布的《关于加强中央企业资金内部控制管理有关事项的通知》（国资发监督〔2021〕19 号）规定，各中央企业要高度重视资金内控管理工作，以提升资金内控有效性为目标，以强化资金内控监督为抓手，以健全资金内控制度体系为保障，落实内控部门的资金内控监管责任、工作职责与权限，明确监管工作程序、标准和方式方法，构建事前有规范、事中有控制、事后有评价的工作机制，形成内控部门与业务、财务（资金）、审计等部门运转顺畅、有效监督、相互制衡的工作体系。同时，要切实加强资金内控制度建设，持续强化资金内控关键环节监管，加快推进资金内控信息化建设，有效开展境外资金风险管控。

2022 年 1 月 7 日，国务院国资委印发《关于做好 2022 年中央企业内部控制体系建设与监督工作有关事项的通知》（国资厅监督〔2021〕299 号）（以下简称《通知》），充分总结过去两年内控体系建设短板经验，对中央企业的内控体系机制、风险管理评估和监测预警、内控制度标准化建设、内控执行专项整治、境外管控、信息化管控、监督检查评价等方面的要求更高、更细致。《通知》要求，对新兴业务、高风险业务以及风险事件频发的领域每半年至少要自评价一次，集团要制定年度监督评价方案，加强对子企业内控有效性的监督评价，在 2022 年底前完成第一轮集团监督评价“三年全覆盖”，对于集团监督评价“零缺陷”的企业，国务院国资委将纳入内控体系有效性评价重点抽查范围。国务院国资委、财政部及相关行政管理或监管部门制定、颁布、下达的一系列“指引”“规范”“指南”和“通知”，适应宏观环境、产业环境、市场环境的变化以及企业发展的内在要求，及时、适时地为各类企业牢固树立全面风险管理理念、建立健全全面风险管理体系、采用科学化和规范化的风险管理措施和手段，指明了方向和途径，提出了原则和要求。

2022 年 8 月 23 日，国务院国资委正式发布了《中央企业合规管理办法》（国资委第 42 号令），自 2022 年 10 月 1 日起施行。《中央企业合规管理办法》的前身为国资委 2018 年 11 月印发的《中央企业合规管理指引（试行）》。《中央企业合规管理办法》的正式版发布，充分凝结了中央企业多年合规管理工作的实践与智慧，彰显了国资委对中央企业切实有效防范合规风险、强化合规管理责任和能力的坚定决心，也为中央企业未来合规管理强化指明了方向。企业也将建立完善的企业内部管理体系，充分发挥企业合规在经营发展中的保障作用，助力企业高质量持续经营和发展。

2023 年 2 月 25 日，国务院国资委印发了《关于做好 2023 年中央企业内部控制体系建设与监督工作有关事项的通知》（国资厅监督 2023［8］号，以下简称：《通知》），对国资央企新一轮内控体系建设与监督三年工作进行部署安排，并提出了新的要求，国资央企内控管理工作迈入新阶段。切实提高质效，筑牢高质量发展安全防线，成为这一阶段国资央企内控体系建设与监督工作的主旋律。

## 三、我国企业内部控制规范体系

目前我国企业内部控制规范体系主要由 1 项基本规范、18 项应用指引、1 项评价指引和 1 项审计指引构成。其中，基本规范是内部控制体系的最高层次，起统驭作用；应用指引是对企业按照内控原则和内控“五要素”建立健全本企业内部控制所提供的指引，在配套指引乃至整个内部控制规范体系中占据主体地位；企业内部控制评价指引是为企业管理层对本企业内部控制有效性进行自我评价提供的指引；企业内部控制审计指引是为注册会计师和会计师事务所执行内部控制审计业务的执业准则。三者之间既相互独立，又相互联系，形成一个有机整体。我国企业内部控制规范体系如图 1－2 所示。

### （一）企业内部控制基本规范

基本规范在内部控制规范体系处于最高层次，起统驭作用，描绘了企业建立与实施内部控制体系必须建立的框架结构，规定了内部控制的定义、目标、原则、要素等基本要求，是制定应用指引、评价指引、审计指引和企业内部控制制度的基本依据。

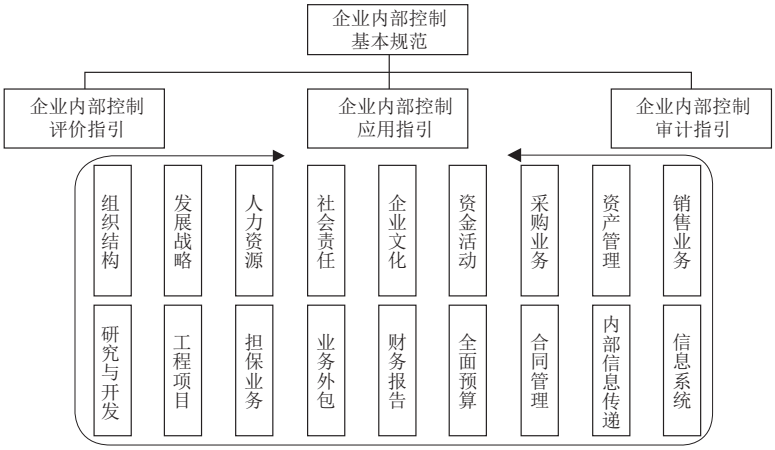


**图 1-2 内部控制规范体系图**

基本规范共七章五十条，各章分别是：总则、内部环境、风险评估、控制活动、信息与沟通、内部监督和附则。

### （二）企业内部控制应用指引

应用指引是对企业按照内部控制原则和内部控制“五要素”建立健全本企业内部控制所提供的指引，在配套指引乃至整个内部控制规范体系中居于主体地位。应用指引可以划分为三类，即内部环境类指引、控制活动类指引、控制手段类指引，基本涵盖了企业资金流、实物流、人力流和信息流等各项业务和事项。

内部环境是企业实施内部控制的基础，支配着企业全体员工的内控意识，影响着全体员工实施控制活动和履行控制责任的态度、认识和行为。内部环境类指引具有基础性地位，它们构成企业的基本条件，对企业的经营与发展起到决定性的不可或缺的作用。内部环境类指引包括组织架构、发展战略、人力资源、社会责任和企业文化等指引。

控制活动类应用指引是对各项具体业务活动实施的控制，此类指引包括资金活动、采购业务、资产管理、销售业务、研究与开发、工程项目、担保业务、业务外包、财务报告等指引。

控制手段类指引偏重于“工具”性质，往往涉及企业整体业务或管理。此类指引包括全面预算、合同管理、内部信息传递和信息系统等指引。

### （三）企业内部控制评价指引

内部控制评价指引是为企业管理层对本企业进行内部控制自我评价提供的指引和要求，包括评价内容和标准、评价程序和方法、评价报告的出具和披露等。

基本规范规定，企业应当结合内部监督情况，定期对内部控制的有效性进行自我评价，出具内部控制自我评价报告。内部控制自我评价的方式、范围、程序和频率，由企业根据经营业务调整、经营环境变化、业务发展状况、实际风险水平等自行确定，但国家有关法律法规另有规定的除外。

### （四）企业内部控制审计指引

内部控制审计指引是会计师事务所执行内部控制审计业务的执业准则。审计指引主要内容包括：审计责任划分、审计范围、整合审计、计划审计工作、实施审计工作、评价控制缺陷、出具审计报告以及记录审计工作。

基本规范要求，接受委托从事内部控制审计的会计师事务所，应当根据基本规范及其配套办法和相关执业准则，对企业内部控制的有效性进行审计，出具审计报告。负责内部控制咨询的中介机构，不得同时为同一个企业提供内部控制审计服务。

# 第三节　内部控制与风险管理的基本概念

## 一、内部控制的基本概念

控制是指控制主体按照给定的条件和目标，对控制客体施加影响的过程和行为。

### （一）COSO 内部控制框架中关于内部控制的定义

现代理论界对内部控制的定义各不相同，但被普遍接受的定义是国际权威机构美国的 COSO 委员会 1992 年对内部控制的定义。该组织认为：企业内部控制是由企业董事会、经理层以及其他员工共同实施的，为财务报告的准确性、经营活动的效率与效果、相关法律法规的遵循等目标的实现而提供合理保证的过程。在 COSO 委员会的《内部控制整合框架》中，把内部控制要素分成五大组成部分，即：控制环境、风险评估、控制活动、信息与交流和监督评审。2013 年 COSO 将内部控制定义为：内部控制是一个由主体的董事会、管理层和其他员工实施的，旨在为实现运营、报告和合规目标提供合理保证的过程。与 1992 年定义相比没有什么变化。

### （二）国内关于内部控制的定义

目前国内关于内部控制的正式定义主要是五部委发布的《企业内部控制规范——基本规范》中的表述。五部委内部控制规范中对内部控制的定义是：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。五部委内部控制规范中，把内部控制要素也分成五大组成部分，即内部环境、风险评估、控制活动、信息与交流和内部监督。

五部委对内部控制的定义基本参照或遵从了 COSO 委员会的《内部控制——整合框架》中对内部控制的定义，但结合国内的实际情况和一些前沿的研究成果进行了调整、拓展和延伸。首先，五部委关于内部控制的定义相对 COSO 委员会对内部控制的定义在实现目标上有所拓展，增加了企业战略目标和资产的安全完整目标，丰富了财务报告目标的内容；其次，五部委内部控制在形式上借鉴了 COSO 报告“五要素”框架，同时在内容上体现了风险管理“八要素”框架的实质。

### （三）对内部控制概念的理解

COSO 委员会和我国五部委对内部控制的定义反映了一些基本概念。

（1）内部控制是一个过程，它是实现目的的手段，而不是目的本身。

（2）内部控制由人员来实施，它并不仅仅是政策手册和表格，还涉及组织中各个层级的人员。

（3）内部控制贯穿于企业经营活动的各个方面。

（4）只能期望内部控制为主体的管理层和董事会提供合理保证，而不是绝对保证。

（5）内部控制被用来实现一个或多个彼此独立又相互交叉的类别的目标。

（6）有效的内部控制不仅关系到企业的各项经济目标能否实现、经济效益能否达到，也是建立现代企业制度的一项根本要求。

## 二、风险管理的基本概念

### （一）COSO 风险管理框架中关于风险管理的定义

2004 年版 COSO－ERM 框架中关于风险管理的定义是：企业风险管理是一个过程，是由企业的董事会、管理层以及其他人员共同实施的，应用于战略制定及企业各个层次的活动，旨在识别可能影响企业的各种潜在事件，并按照企业的风险偏好管理风险，为企业目标的实现提供合理的保证。该框架将全面风险管理要素分为八个，即内部环境、目标设定、事件识别、风险评估、风险对策、控制活动、信息和交流、监控。

2004 年版 COSO－ERM 框架除包括内部控制的 3 个目标之外，还增加了战略目标；全面风险管理的 8 个要素除了包括内部控制的全部 5 个要素之外，还增加了目标设定、事件识别和风险对策 3 个要素。从时间先后和内容上来看，全面风险管理是对内部控制的拓展和延伸。

2017 年版 COSO－ERM 框架简化了对 ERM 的定义：风险管理是组织在创造、保持和实现价值的过程中，结合战略制定和执行，赖以进行管理风险的文化、能力和实践。该定义包括文化和能力而不只是过程，更加强调风险与价值的相结合，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。

### （二）国内关于风险管理的定义

国资委发布《中央企业全面风险管理指引》中关于全面风险管理的定义是：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。

《中央企业全面风险管理指引》明确指出内部控制是全面风险管理体系的组成部分，同时也指出除内部控制外的其他全面风险管理组成部分。但由于五部委《内部控制基本规范》出台较晚，且借鉴了 COSO 全面风险管理框架的内容，使得其内部控制的边界扩大了不少，包括实现目标和要素都与全面风险管理差异不大。

## 三、内部控制与全面风险管理的关系

### （一）内部控制与全面风险管理关系的主要观点

理论界对内部控制与风险管理的关系有不同认识，主要观点如下。

#### 1.风险管理包含内部控制

2004 年版 COSO－ERM 框架中明确指出，企业风险管理包含内部控制；内部控制是企业风险管理不可分割的一部分；内部控制是风险管理的一种方式，企业风险管理比内部控制范围广得多。英国 Turnbull 委员会（2005）认为，风险管理对于企业目标的实现具有重要意义，公司的内部控制系统在风险管理中扮演关键角色，内部控制应当被管理者看作是范围更广的风险管理的必要组成部分。南非 KingII Report（2002）认为，传统的内部控制系统不能管理许多风险，譬如政治风险、技术风险和法律风险，风险管理将内部控制作为减轻和控制风险的一种措施，是一个比内部控制更为复杂的过程。Krogstad（1999）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。

2017 年版 COSO－ERM 框架对内部控制与风险管理的关系也做了解释。内部控制主要聚焦在主体的运营和对于相关法律法规的遵从上。企业风险管理的相关概念并没有包含在内部控制中（例如，风险偏好、风险承受度、战略和目标设定等概念，这些都是内部控制体系实施的前提条件）。为了避免重复，一些在内部控制中比较常见的概念部分，风险管理新框架并未重复叙述（例如，与财务报告目标相关的舞弊风险、与合规目标相关的控制活动、与运营目标相关的持续及独立评估）。然而，一些在内部控制中概念在该框架中被进一步的研究和深化了（例如，企业风险管理中的治理和文化部分）。在 COSO 公布的《常见问题》解释上，COSO 表明两个体系并不能相互取代，而是侧重点各不相同、相互补充。但同时也强调了内部控制作为一种经历时间考验的企业控制体系，是企业风险管理工作的一个基础和组成部分。

#### 2.内部控制包含风险管理

加拿大 COCO 报告（CICA，1995）认为，“控制”是一个组织中支持该组织实现其目标诸要素的集合体，实质上就是“内部控制”，或者说是用“控制”一词表达“内部控制”概念。COCO 报告认为，风险评估和风险管理是控制的关键要素。CICA（1998）将风险定义为，“一个事件或环境带来不利后果的可能性”，阐明了风险管理与控制的关系：“当您在抓住机会和管理风险时，您也正在实施控制。”巴塞尔委员会发布的《银行业组织内部控制系统框架》中指出，“董事会负责批准并定期检查银行整体战略及重要制度，了解银行的主要风险，为这些风险设定可接受的水平，确保管理层采取必要的步骤去识别、计量、监督以及控制这些风险……”这里显然是把风险管理的内容纳入到了内部控制框架中。加拿大注册会计师协会控制标准委员会（1999）认为，“控制应该包括风险的识别与减轻”，其中的风险不仅包括与实现特定目标相关的风险，还包括一般性的风险，如不能识别和利用机会，就

不能使企业在面临未预料到事件以及不确定信息时保持灵活性或弹性。

3.内部控制就是风险管理

Blackburn（1999）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，它们是一体化的。Laura F.Spira 等（2003）分析了内部控制是怎样变为风险管理的，并指出，“将内部控制定义为风险管理强调与战略制定的联系，刻画了内部控制作为组织支撑的特点，但是，它也掩盖了一个不争的事实：现在没有人真正明白内部控制系统是什么”。Matthew Leitch（2004）认为，理论上风险管理系统与内部控制系统没有差异，这两个概念的外延变得越来越广，正在变为同一事物。

### （二）对两者关系的理解与观点

由上面三种观点我们可以得出的基本结论是，内部控制与风险管理关系十分密切，风险管理是企业为了适应时代的变化，以内部控制为架构演变成另一种以达到某种目标的过程和手段方法。内部控制和风险管理在要素、目标、含义等方面有很多联系和相同的地方，两者是既独立又有关联的体系，是针对企业不同的需求而演变成的两种过程与目标。

我国企业内部控制基本规范中，强调了内部控制与风险管理的统一。内部控制的目标是防范和控制风险并促进企业实现发展战略，风险管理也是为促进企业实现发展战略，要求将风险控制在可承受范围之内。两者之间不是对立的，而是协调统一的整体。

国际先进研究成果和经验表明，内部控制与风险管理之间也是统一的。比如，国际风险管理协会认为，“风险管理系统与内部控制系统并没有原则性的区别；风险管理与内部控制正在趋同”。巴塞尔银行监管委员会（BCBS）在其《银行机构的内部控制制度框架》中指出，作为内部控制的一部分，风险评估应当包含银行面临的所有风险，并在银行内部各个层次上进行。南非 King II Report 英国 Tnrnbull Report 均将风险管理与内部控制并列，明确表示风险管理与内部控制并非包含关系。即使是美国的 COSO 框架，尽管在 1992 年称为内部控制整体框架，在 2004 年称为风险管理整合框架，并非是本质内容发生了重大变化，而是更加关注风险，更加强调为企业发展战略服务的控制目标。因此，尽管名称变了，但控制管理风险的本质未变，实质上仍然是内部控制。

2017 年前，COSO 在表述两个体系的关系时有时暧昧、有时清晰，2017 年 COSO－ERM 框架给两个体系的关系做了个“了断”，随着 2017 年新框架在企业的实施，二者的关系和界限会越来越清晰。

## 第四节　内部控制与风险管理建设的现实意义及局限性

### 一、内部控制与风险管理建设的现实意义

一般而言，内部控制与风险管理建设具有保护资产的安全和完整，防止、发现、纠正错误与舞弊，保证会计资料的真实、合法和完整，提高经营成果的经济性和有效性，保证完成所制定的经营目标，保证遵循政策、计划、程序、法律和法规的控制目标，增强公司风险防范能力，为公司战略发展提供合理保障，确保公司协调、持续、快速发展等意义。

但内部控制与风险管理以控制分析与风险分析为基础，加强内部控制与风险管理建设的具体现实意义可简要分析如下。

### （一）加强内部控制与风险管理建设，是企业科学发展、贯彻战略管理的需要

科学发展首先要求提高我国的资源配置效率，提高经济发展的质量，市场经济条件下直接融资有助于提高资源的配置效率，而提高企业直接融资比例，首先要保证资本市场的有效性。作为资本市场最基本的单元——企业的资源利用效率是资本市场有效的前提，一个有效率的成功企业，根据目前普遍认可的观念，对投资者来说是股东价值最大化的企业，对利益相关者来说是社会效益最大化的企业，这就要求我们研究企业内部控制机制，提高企业战略决策和战略风险管理水平。

企业将面临更多的战略抉择，战略工作不仅事关重大，需要企业高层重视，而且是一个系统工程，需要全员关心和配合。在环境变化迅速、竞争变数增多、员工素质和自主性日益增强的今天，要想增强企业可持续发展的能力，必须在增强高层的战略驾驭能力的同时，保证既能持续地监控、分析和反

馈内外环境变化的战略意义，提前示警；同时培养企业快速反应的能力，保证在需要做出反应时，能及时、有效地应变。

### （二）加强内部控制与风险管理建设，是融合内部控制与风险管理体系的需要

企业战略风险是企业面临的生存和发展的致命风险，企业所有的战略决策都和环境高度相关，因此企业的战略风险管理是企业不可回避的重大课题。

只有从完善企业内部控制角度入手，通过对企业面临的整体风险的分析，才能建立企业全面风险管理的控制体系，尤其要在企业整体风险管理的基础上关注企业战略风险管理。

企业风险管理框架也强调在企业日常经营管理中全员参与风险管理，这个过程中，企业内控制度可能发挥防止一般的经营风险和信用风险发生的作用，不符合企业内控规范的事得以有效避免，但企业风险管理框架更多的是要求参与者保持一种主动参与的姿态，强调在具体的领域里，实际操作者利用其工具方法管理面临的风险，为企业创造价值。

从风险管理过程看，企业应制定严密的业务操作规程及信息传输报告制度，建立一个有效的全面风险管理框架来全面管理各方面的风险，这就决定了企业风险管理最后形成的成果也是更好控制企业风险的内部控制制度或内部控制制度的完善。

企业风险管理最终以内控制度形式出现，是企业风险管理能力的提高，以后类似的风险就从企业第一次面对的风险变成了企业可以以常规管理控制的一般风险，纳入企业内控制度处理的管理规程，使企业在不断变化的环境中减少被动，增加反应和控制能力。

企业面临的风险更多的是一般的运营风险、市场风险、信用风险，但在企业战略执行过程中，一些普通的风险如果不及时防范都有可能变成危及企业战略目标的战略风险，企业的经营管理永远是一个动态的过程，可能一般的风险在企业内控制度的有效框架下可以得到有效治理，这时，企业的内部控制制度足以支持企业风险管理的要求，但一旦环境变化或个别环节的内控失效导致危及企业战略目标的风险发生，可能内控制度无法胜任化解风险的要求，必然要企业管理当局从企业战略高度调动企业可以控制的资源，研究风险的特性，度量风险的危害程度，采取规避措施或其他管理手段。

从以上企业经营中的风险管理的过程考察，企业内控制度是日常情形下企业运营监控体系，包括对普通风险的控制，企业战略风险管理是特殊情形下企业管理的手段和工具，企业决策者在战略决策过程中虽然分析战略风险管理，但对风险在企业内控体系中如何实施有效监管可能较少考虑，COSO 框架下的企业整体风险管理要求根据企业战略决策的需要完善内部控制体系，以适应企业战略规划目标的执行。

由于企业所处的环境的变化，以及企业的业务和管理活动是人所具体执行的，企业的内部控制体系无论如何完美都不可能一劳永逸地解决企业可能面临的全部风险，所以企业风险管理，特别是企业战略风险管理，是企业应对企业动态环境和资源变化、化解风险捕捉机会的必备工具；同时，企业可以在风险管理的实践中不断增强抗风险能力，不断完善企业的内部控制体系，这将是一个不断循环往复的过程，每一个循环，企业的内部控制体系都将得到一次完善和提高。

### （三）加强内部控制与风险管理建设，是企业进行管理转型以适应战略转型的需要

伴随着世界经济危机的发生，自 2008 年以来，我国许多企业进入了战略转型阶段。企业战略转型是指企业长期经营方向、运营模式及其相应的组织方式、资源配置方式的整体性转变，是企业重新塑造竞争优势、提升社会价值，达到新的企业形态的过程。中国大多企业的转型主要是属于企业战略转型。

适应战略转型的需要，新形势下的企业风险管理和内部控制应该有如下变化。

#### 1.从“要我控制”向“我要控制”转变

假如说实施企业内控以前更多的是来自监管部门或者股东的压力，现在主要应该是企业自我生存和自我发展的压力。

#### 2.由“会计控制”向“管理控制”转变

以前谈及“内控”，大家都认为是财务部门的事情，或者最多是内部审计部门的事情，其他部门可以对其评头论足却不承担具体义务。但现在企业的管理控制、风险控制是从企业的董事会到管理层到全体员工的，是全员的管理过程控制。

3.从“部门的控制”向“全员的控制”转变

从上级对下级的控制转变为对人对事的全面控制是一大转变。

现代内部控制是由企业董事会、经理层和全体员工实施的，旨在实现控制目标的过程。内部控制在层次上应当涵盖企业董事会、管理层和全体员工，在对象上应当覆盖企业各项业务和管理活动，在流程上应当渗透到决策、执行、监督、反馈等各个环节，避免内部控制出现空白和漏洞。

4.从“结果控制”向“过程控制”转变

如采购付款的安全性问题，这个过程需要进行大量的工作：是否建立了资金的管理制度，是否建立了资金的管理人员，是否有一系列的岗位责任制，是否有预算或者资金的一系列信息管理系统，等等，如果这些工作过程的控制与风险分析都没有，资金安全就成了空话。

5.从“标准控制”向“风险管理”转变

我国许多企业往往为了内控而内控，仅仅将内控当成一种程序系统，没有把内控当成一个防范风险、堵塞漏洞、提倡管理效率的必要推动力，故大都敷衍了事，而现在企业内控以风险管理为导向，使企业能更好地发展。

## 二、内部控制的局限性

内部控制制度在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方面具有一定的作用，但内部控制仅仅为以上目标的实现提供合理保证，而不是绝对保证，原因就在于内部控制本身具有一定的局限性。

### （一）越权操作

内部控制制度的重要实施手段之一是授权批准控制，授权批准控制使处于不同组织层级的人员和部门拥有大小不等的业务处理和决定权限，但是当内部人控制的威力超过内部控制制度本身的力量时，越权操作就成为可能。

越权操作的危害极大，不仅打乱了正常的工作秩序和工作流程，还会为徇私舞弊、违法违规创造一定的条件。

### （二）合谋串通

内部控制制度源于内部牵制的理念：因为相互有了制衡，在经办一项交易或事项时，两个或两个以上人员或部门无意识地犯同样的错误的概率要大大小于一个人或部门。

串通的结果则完全破坏了内部牵制的设想，削弱了制度的约束力，使内部控制制度无效。

### （三）成本限制

根据成本效益原则，内部控制的设计和运行是要花费代价的，企业应当充分权衡实施内部控制带来的潜在收益与成本，运用科学、合理的方法，有目的、有重点地选择控制点，实现有效控制。

内部控制的实施受制于成本与效益的权衡。内部控制的根本目标在于服务于企业价值创造，如果设计和执行一项控制带来的收益不能弥补其所耗费的成本，就应该放弃该项控制。

## 复习思考题

1.内部控制的产生与发展历经几个阶段？每一阶段有何特点？

2.简要概括我国企业内部控制规范的框架体系。

3.如何理解内部控制与风险管理的关系？

4.内部控制有哪些局限性？

5.请对“《企业内部控制基本规范》是中国版的萨班斯法案”这一说法进行评述。

# 第二章

# 内部控制与风险管理框架

## 学习目标

1.理解和掌握 COSO 委员会内部控制整合框架与企业风险管理整合框架的内容及其变化；

2.理解和掌握我国企业内部控制基本规范规定的内部控制目标和要素，及其与 COSO 委员会内部控制框架的区别；

3.理解和掌握我国企业内部控制基本规范与中央企业全面风险管理指引的区别；

4.理解和掌握我国内部控制体系建设应遵循的基本原则、思路和方法；

5.理解和掌握企业各有关方在内部控制建设中的主要职责。

## 课程思政

1.通过了解中国企业内部控制制度体系，树立中国标准、传播中国声音，塑造系统思维和创新思维；

2.通过学习全面奉献管理框架的演变及完善，学会用历史思维分析问题和解决问题；

3.通过理解内部牵制、内部控制制度、内部控制结构、内部控制整合框架、全面风险管理框架中异同要素之间的联系，领会马克思主义唯物辩证法中关于普遍联系的观点；全面培养历史思维能力、辩证思维能力，创新思维能力，战略思维能力。

4.通过学习企业各有关方在内部控制中的职责作用，培养对企业使命及社会责任的认识，树立正确的人生观和价值观，努力成为德才兼备、符合国家和社会需要的高级专门人才。

国际上较有影响的内部控制和风险管理的准则和指南有很多，本章重点介绍美国 COSO 的《内部控制——整合框架》和《企业风险管理——整合框架》及中国五部委的《内部控制基本规范》和国资委的《中央企业全面风险管理指引》。

# 第一节　COSO 委员会内部控制整合框架

## 一、1992 年 COSO《内部控制——整合框架》

1992 年 COSO《内部控制——整合框架》的核心内容包括内部控制定义、三项目标和五要素。

### （一）内部控制定义

该框架将内部控制定义为：内部控制是由企业董事会、管理当局和其他员工实施的，为达成经营活动的效率和效果、财务报告的可靠性、相关法律法规的遵循性等目标提供合理保证的过程。这个定义反映了一些基本概念：内部控制是一个过程，它是实现目的的手段，而不是目的本身；内部控制由人员来实施，它并不仅仅是政策手册和表格，还涉及组织中各个层级的人员；只能期望内部控制为主体的管理层和董事会提供合理保证，而不是绝对保证；内部控制被用来实现一个或多个彼此独立又相互交叉的类别的目标。

### （二）内部控制目标

该框架提出内部控制由三大目标构成，即经营活动的效率和效果、财务报告的可靠性、相关法律法规的遵循性。经营活动的效率和效果是企业的基本经营目标，包括业绩、盈利指标和资源保护；财务报告的可靠性是指编制可靠的公开的财务报表，包括中期和简略财务报表，以及从这些财务报表中摘出的数据（如利润分配数据）；法律法规的遵循性要求企业经营必须符合相关的法律法规。

### （三）内部控制要素

该框架还明确内部控制的五大要素，即控制环境、风险评估、控制活动、信息与沟通、监督活动。

#### 1.控制环境

控制环境是指一个企业进行内部控制的基调、氛围，直接影响企业员工的控制意识。包括：员工的诚实性和道德观，如有无描述可接受的商业行为、利益冲突、道德行为标准的行为准则；员工的胜任能力，如雇员是否能胜任质量管理要求；董事会或审计委员会，如董事会是否独立于管理层；管理哲学和经营方式，如管理层对人为操纵的或错误的记录的态度；组织结构，如信息是否到达合适的管理阶层；授予权利和责任的方式，如关键部门的经理的职责是否有充分规定；人力资源政策和实施，如是否有关于雇佣、培训、提升和奖励雇员的政策。

#### 2.风险评估

风险评估指管理层识别并采取相应行动来管理对经营、财务报告、符合性目标有影响的内部或外部风险，包括风险识别和风险分析，以实现既定目标，是风险管理的基础。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。风险分析涉及估计风险的重大程度、评价风险发生的可能性、考虑如何管理风险等。

#### 3.控制活动

控制活动指对所确认的风险采取必要的措施，以保证单位目标得以实现的政策和程序。实践中，控制活动形式多样，可将其归结为以下几类：

（1）业绩评价。指将实际业绩与其他标准，如前期业绩、预算和外部基准尺度进行比较；将不同系列的数据相联系，如经营数据和财务数据，对功能或运行业绩进行评价。这些评价活动对实现企业经营的效果和效率非常有用，但一般与财务报告的可靠性和公允性相关度不高。

（2）信息处理。指保证业务在信息系统中正确、完全和经授权处理的活动。信息处理控制分为一般控制和应用控制。一般控制与信息系统设计和管理有关，如保证软件完整的程序、信息处理时间表、系统文件和数据维护等；应用控制与个别数据在信息系统中处理的方式有关，如保证业务正确性和已授权的程序。

（3）实物控制。也称为资产和记录接近控制，这些控制活动包括实物安全控制、对计算机以及数据资料的接触予以授权、定期盘点以及将控制数据予以对比。实物控制中防止资产被窃的程序与财务

报告的可靠性有关，如在编制财务报告时，管理层仅仅依赖于永续存货记录，则存货的接近控制与审计有关。

（4）职责分离。指将各种功能性职责分离，以防止单独作业的雇员从事或隐藏不正常行为。一般来说，下面的职责应被分开：业务授权（管理功能）、业务执行（保管职能）、业务记录（会计职能）、对业绩的独立检查（监督职能）。

#### 4.信息和交流

信息与沟通，指为了使职员能执行其职责，企业必须识别、捕捉、交流外部和内部信息。外部信息包括市场份额、法规要求和客户投诉等信息。内部信息包括会计制度，即由管理当局建立的记录和报告经济业务和事项，维护资产、负债和所有者权益的方法和记录。有效的会计制度应是：包括可以确认所有有效业务的方法和记录；序时详细记录业务以便于归类，提供财务报告；采用恰当的货币价值来计量业务；确定业务发生时期以保证业务记录于合理的会计期间，在财务报告中恰当披露业务。

#### 5.监控

监控指评价内部控制质量的过程，即对内部控制设计、运行的合理性、有效性进行评价，包括内部审计和与单位外部人员、团体进行交流。

### （四）目标和构成要素之间的关系

目标和构成要素之间有着直接的关系，目标是主体努力争取实现的东西，构成要素则代表着要实现这些目标需要什么，每个构成要素行都“贯穿”并适用于所有三类目标，所有五个构成要素与每一类目标都有关联。内部控制与整个企业相关，或与它的某一部分（子公司、分部或其他业务单元，或者职能或诸如购买、生产、营销等其他活动）相关。

如果董事会和管理层能够合理保证以下三个方面，则内部控制可以在三类目标中任何一类上被判断为有效：他们了解主体的经营目标得以实现的程度；公布的财务报表被可靠地编制；适用的法律和法规得到了遵循。确定特定的内部控制体系是否有效是一种主观判断，它来自对五个构成要素是否存在并有效运行的评估。目标与构成要素关系如图 2－1 所示。

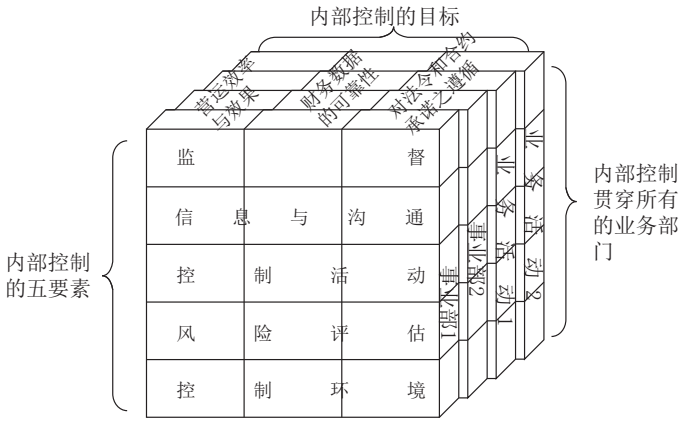


图 2－1　内部控制目标与构成要素关系图

## 二、2013 年 COSO 内部控制整合框架

### （一）新框架发布的背景

1992 年，美国 COSO 委员会首次发布《内部控制——整体框架》（以下简称旧框架），为企业内部控制的实施提供了践行标杆，在世界范围内得到广泛认可。这一框架可以看作是内部控制领域的纲领性文件，在内部控制方面为企业的经营管理层提供了指导和参考，一直沿用至今。

随着经济的快速发展，资本市场、运营环境、商业模式等发生了巨大的变化，科技创新也使环境更加复杂化。此时，企业内外部的利益相关者对经营过程的透明度要求越来越高，更加致力于寻找透明的、权责分明的和完整有效的内部控制体系，以此来帮助其做出正确的经营决策，并进行有效的公司治理。

在商业和经营环境发生变化以及利益相关者要求更高的背景下，2010 年，美国 COSO 委员会开始了对《内部控制——整体框架》的更新工作，并于 2013 年 5 月 14 日正式发布《内部控制——整体框架》（以下简称新框架）及其配套指南。新框架适用于所有类型主体，包括大、中、小型主体，营利和非营利主体，以及政府机构。

COSO 委员会发布了新的内部控制框架后，要求使用者们能够尽快地从旧框架向新框架进行转换和过渡。过渡期一直到 2014 年 12 月 15 日。在过渡期内，将继续保持旧框架的可行性，在此期间任何涉及外部报告的整合框架的应用，应该清晰披露是旧框架还是新框架。在过渡期结束以后，COSO 委员会将采用新版的内部控制框架。

### （二）新框架的内容

#### 1.内部控制定义

内部控制是一个由主体的董事会、管理层和其他员工实施的，旨在为实现运营、报告和合规目标提供合理保证的过程。这个定义强调内部控制是：旨在实现目标，这些相互独立但又互有重叠的目标类别包括运营、报告和合规；一个持续不断的过程，此过程包括持续的任务和活动，是达到目的的手段，而非目的本身；由人来实施，不仅仅是单纯的政策、流程手册、系统和表单，而且包括组织中各层级人员以及他们所实施的可能影响内部控制的行动；可以提供合理保证，向组织的高级管理层和董事会提供合理保证，但非绝对保证；与组织的结构相适应，可灵活应用于整个组织或其中一个下属单位、分部、业务单元或业务流程。

内部控制的定义之所以被设计得很宽泛，是因为它需要体现如何设计、实施和执行内部控制，以及开展内部控制体系有效性评估这些最为基本的重要概念，才能为那些不同类别、行业和地区的组织在应用本框架时提供基础。

#### 2.内部控制目标

该框架列举了三种类别的目标，使组织可以关注于内部控制的不同方面。内部控制的目标有三个，一是运营目标，即组织运营的效果和效率，包括运营和财务业绩目标、保护资产以避免损失；二是报告目标，即内外部的财务和非财务报告的可靠性、及时性、透明度，以及监管者、标准制定机构和组织政策所要求的其他方面；三是合规目标，即遵守组织所适用的法律法规及规章。

#### 3.内部控制要素

（1）控制环境。控制环境是一套标准、流程和结构，能够为组织实施内部控制提供基础。董事会和高级管理层应在高层建立基调，强调内部控制的重要性（包括期望的行为准则），并应在组织的各个层级强化这种要求。控制环境包括了组织的诚信和道德价值观；促成董事会行使治理监督职责的各种要素；组织结构以及权力与责任的分配；吸引、培养和留用人才的程序；用以实现绩效问责的严密的绩效衡量、激励和奖励机制。控制环境会对整个内部控制体系产生深远的影响。

（2）风险评估。每个主体都面临着来自内、外部的各类风险。风险是指某项事件将发生并对组织实现其目标产生负面影响的可能性。风险评估应通过动态和反复的过程，以识别和评估影响组织目标实现的风险。在考虑影响主体目标实现的各个方面风险时，应与已建立的各项风险容忍度相关联。由此，风险评估为形成如何管理风险的决策奠定基础。风险评估的先决条件是已建立了各种目标，并联接到主体内不同的层级。管理层应充分明确运营、报告和合规三大类具体目标，以便识别和评估与这些目标相关的风险。管理层也应考虑这些目标对于主体的适用性。风险评估还要求管理层考虑可能导致内部控制失效的外部环境和内部商业模式变化带来的影响。

（3）控制活动。控制活动是通过政策和程序所确立的行动，旨在协助确保管理层关于降低影响目标实现的风险的方针已经落实。在主体的各个层级、业务流程的各个环节，以及技术环境中都应实施控制活动。控制活动在性质上，可以是预防性的，也可以是发现性的；可能涵盖一系列的人工和自动化控制，如授权和批准、核查、对账和企业绩效评估等。不相容职责分离就是典型的应选择和执行的控制活动。如果不相容职责分离对主体来说难以实施，管理层应选择并执行替代性的控制活动。

（4）信息与沟通。信息对于主体履行内部控制责任以促进目标实现而言是非常必要的。管理层应

从内外部来源获取或生成和使用高质量的、相关的信息，以支持内部控制的持续运行。沟通是提供、共享和获取所需信息的持续和不断重复的过程。内部沟通是让信息在整个组织内向上、向下和横向传递的手段，它使员工能清晰获得高层要求其认真履行控制职责的讯息。外部沟通则是双重的，即将外部的相关信息引入，以及向外部提供信息以回应相关方的要求和期望。

（5）监督活动。主体应通过持续评估、单独评估或者两者的组合，以确认内部控制的五个要素（包括实现每个要素中原则的控制活动）是否存在并持续运行。持续评估应被嵌入主体不同层级的业务流程中，以提供及时的信息。单独评估应定期开展，其评估范围和频率因风险评估结果、持续评估的有效性以及管理层的其他考虑而有所不同。主体应依据监管机构、标准制定机构，或管理层和董事会所设定的标准，对各种发现进行评估，必要时应当向管理层和董事会报告各项缺陷。

#### 4.内部控制原则

该框架详细说明了 17 项代表着与要素相关基本概念的原则。由于这些原则是从各要素中直接得出的，主体可以通过应用所有的原则从而实现有效的内部控制。所有原则均适用于运营、报告及合规目标。支持各要素的原则如表 2－1 所示。

**表 2－1　新框架内部控制要素与原则**

| 五大要素 | 基本原则 |
| --- | --- |
| 控制环境 | 1.组织应展现对诚信和道德价值的承诺 |
| | 2.董事会应展现出其独立于管理层，并对内部控制的开展与成效实施监督 |
| | 3.管理层为实现目标，应在董事会的监督下确立组织架构、汇报路线、合理的权力与责任 |
| | 4.组织应展现出其对吸引、培养和留用符合组织目标要求的人才的承诺 |
| | 5.组织为实现目标，应要求员工承担内部控制的相关责任 |
| 风险评估 | 6.组织应设定清晰明确的目标，以识别和评估与目标相关的风险 |
| | 7.组织应对影响其目标实现的风险进行全范围的识别和分析，并以此为基础来决定应如何管理风险 |
| | 8.组织应在评估影响其目标实现的风险时，考虑潜在的舞弊行为 |
| | 9.组织应识别并评估对其内部控制体系可能造成重大影响的改变 |
| 控制活动 | 10.组织应该选择并执行那些可以将影响其目标实现的风险降至可接受水平的控制活动 |
| | 11.针对信息技术，组织应选择并执行一般控制活动以支持其目标的实现 |
| | 12.组织应通过政策和程序来实施控制活动。政策是建立预期，程序是将政策付诸行动 |
| 信息与沟通 | 13.组织应获取或生成和使用高质量的、相关的信息来支持内部控制的持续运行 |
| | 14.组织应在内部对内部控制目标和责任等必要信息进行沟通，从而支持内部控制持续运行 |
| | 15.组织应就影响内部控制发挥作用的事项，与外部进行沟通 |
| 监督活动 | 16.组织应选择、开展并实施持续和单独评估，以确认内部控制的各要素存在并持续运行 |
| | 17.组织应评价内部控制缺陷，并及时与整改责任方沟通，必要时还应与高级管理层和董事会沟通 |

### （三）有效内部控制体系的要求

该框架阐明了有效内部控制体系的要求。有效的内部控制体系可为主体目标的实现提供合理的保证，并将影响主体实现其目标的风险降低至可接受的水平，这些风险可能涉及一种、两种或全部三种目标类别。这就要求：

（1）内部控制五个要素中的每个要素以及相关原则必须同时存在并持续运行。“存在”是指在内部控制体系的设计和实施以实现特定目标的过程中，应确定各要素和相关原则存在。“持续运行”是指在内部控制体系的执行以实现特定目标的过程中，应确定各要素和相关原则持续存在。

（2）五个要素以整合的方式共同运行。“共同运行”是指确定五个要素共同持续运行，以将影响目标实现的风险降低至可接受的水平。五个要素作为一个整合的体系共同运行，不应仅考虑单个要素。

各要素是相互依存的，这是由于彼此间存在大量关联和联系，特别是通过各原则在相关要素内以及各要素之间互动的方式。

若存在一项重大缺陷，而该缺陷与某要素或相关原则的存在并持续运行相关，或与各要素未以整合的方式共同运行相关，组织就不能得出其已满足有效内部控制体系所有要求的结论。

当内部控制体系被确定为有效时，可以就其在主体结构内的应用向高级管理层和董事会提供如下合理保证：当外部事件对目标的实现不太可能造成重大影响，或组织可以合理地预测外部事件的性质和发生时间，并将其影响降低到可接受水平时，组织可以实现运营目标的效果和效率；当外部事件可能对目标实现造成重大影响，且组织不能将其影响降低到可接受水平时，需要知晓运营目标的效果和效率被控制的程度；编制报告，以遵照各项适用的规章及标准，或主体特定的报告目标；组织遵守适用的法律法规、规章及外部标准。

该框架要求在设计、实施和执行内部控制及评估其有效性时，应进行判断。运用判断可以协助管理层在相关法律法规、规章及标准所限定的范围内更好地做出内部控制方面的决策，但并不能保证达到完美效果。

### （四）内部控制整合框架的使用

如何使用这个报告取决于当事方的不同角色。

#### 1.董事会

董事会应与高级管理层商讨组织内部控制体系的现状，并进行适当的监督。高级管理层就内部控制情况向董事会负责，同时董事会应针对其成员如何对内部控制实施监督设定相关的政策和期望。董事会应被告知如下信息：实现主体目标的各种风险、对内部控制缺陷的评估、管理层为应对这些风险和缺陷而部署的行动，以及管理层如何评估内部控制体系的有效性。在必要时，董事会应挑战管理层、提出尖锐的问题，并从内、外部审计人员或其他渠道获取信息并寻求支持。董事会下设的委员会通常可以协助董事会行使一些监督的职责。

#### 2.高级管理层

高级管理层应根据该框架对内部控制体系进行评估，并关注于组织是如何应用 17 项原则来支持内部控制要素的。如果曾应用了 1992 年版框架，管理层在应用该框架时需先了解该框架中的更新内容（如第二部分“框架和附录”中附录 F 所载），并考虑这些更新对主体内部控制体系的影响。管理层在初步比较的过程中可考虑使用工具示例，并将其用于对主体内部控制体系的持续评估中。

#### 3.其他管理层及人员

各级经理或其他人员应对此版本较上一版本的变动进行查阅，并评估这些变动对主体内部控制体系的影响。此外，他们也需要考虑如何在该框架的要求下行使其职责，并与更高级别的人员就如何加强内部控制进行探讨。具体而言，他们应考虑现有的控制是如何在内部控制五要素中对相关原则产生影响的。

#### 4.内部审计人员

内部审计人员应对其运用 1992 年版框架的情况进行回顾，并对内审计划进行审阅。同时，内部审计人员还需要对新版框架中的变动进行详细审阅，并考虑这些变动对于主体现有内部控制体系相关的审计计划、评估及其他报告的影响。

#### 5.独立审计人员

在某些司法管辖地区，独立审计人员不仅会审计主体的财务报表，也会对客户的财务报告相关内部控制的有效性进行审计或核查。审计人员会参照该框架针对主体的内部控制体系进行评估，并关注组织如何选择、执行及部署影响内部控制要素相关原则的控制。同管理层一样，审计人员也可以将工具示例应用于对内部控制体系整体有效性的评估中。

#### 6.其他专业机构

其他提供运营、报告及合规相关指引的专业机构可将其制定的标准和指引与该框架进行比较，并在一定程度上通过消除概念与术语上的分歧来使所有相关方都能够从中受益。

### 三、新旧框架的变化

COSO 委员会认为，旧框架中关于内部控制的基本原则和核心要素在现有环境下仍然有效，所以新框架在内部控制的定义、内部控制五大要素、评估内部控制体系有效性的标准以及专业判断的运用等方面与旧框架保持了一致。针对内部控制的认知和实践方面，旧框架的重点在于“知悉与建立”，新框架的重点在于“承诺与落实”，新框架的变化主要呈现在以下几个方面。

#### （一）着重“原则导向”的方法

新框架最显著的变化是在旧框架的基础上，提出基于内部控制五大要素的 17 项总体原则和 82 个相关属性，其内容为部分延续、部分新增、部分修改和部分删除。

#### （二）明确“目标设定”在内部控制中的角色

旧框架将目标设定作为一个管理过程，认为目标设定是风险评估要素的前提条件，并且 COSO 委员会 2004 年发布的《企业风险管理整体框架》将目标设定作为内部控制的八大要素之一。新框架同样强调目标设定是内部控制的风险评估的前提，但明确指出目标设定不是内部控制的组成部分。

#### （三）强化“公司治理”的理念

新框架包括了更多的公司治理中有关董事会及其专业委员会（包括审计委员会、薪酬委员会、提名与治理委员会等）的内容。这与台湾金管会制定有关公司治理的规定相一致。

#### （四）扩大“财务报告的范畴”

旧框架在内部控制目标设定中仅仅关注于财务报告目标，目的是确保编制可靠的公开发表财务报告，主要是企业面临主管机关的要求。新框架在报告对象和报告内容两个部分，提出扩大范围的要求。在报告对象方面，既要面向外部的投资者、债权人和监管机关，确保报告符合有关监管要求；又要面向内部的董事会和管理阶层。在报告内容方面，除了包括传统的财务报告，还涵盖了市场调查报告、资产使用报告、人力资源分析报告、内部控制评价报告等非财务报告。

#### （五）考虑了不同“商业模式和组织结构”的内部控制

随着经济全球化的发展、技术的不断进步和人才竞争的激烈，近年来企业的商业模式和组织结构发生了巨大变化，企业在营运过程中更多地使用第三方提供的产品或服务，管理阶层更加需要注意包括供应商和客户在内的价值链管理。为此，新框架分析了不同商业模式和组织结构下内部控制的有效性问题。

总之，新框架并没有改变旧框架关于内部控制的基本概念和核心内容，而是对旧框架的某些概念和指引进行更新和改进，以期适应近年来企业经营环境的演变、监管机构的要求和其他利益关系人的期望。COSO 委员会主席大卫·兰德斯蒂尔（David L. Landsittel）表示：“各类组织可以继续沿用旧框架，因为它是历经时间考验的。新框架无意改变内部控制原有的定义、评估方法或管理模式，而是给使用者提供了更加全面、准确的内部控制概念、指引和案例。”

## 第二节　COSO 委员会企业风险管理整合框架

### 一、2004 年 COSO 的《企业风险管理——整合框架》

2004 年 COSO 委员会发布的《企业风险管理——整合框架》既是对 1992 年《内部控制——整合框架》的超越，也标志着内部控制的转型，在内涵界定、目标体系、构成要素等方面都进行了拓展和延伸。

#### （一）企业风险管理的定义

##### 1.风险管理的定义

COSO 在其《企业风险管理——整合框架》报告中指出：“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，管理风险以使其限制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。”该定义反映风险管理的理念：企业风险管理是一个过程，它持续流动于企业之内；企业风险管理是由组织中各个层级的人员来实施的；企业风险管理应用于战略制定的过程中；企业风险管理贯穿企业整体，在各个层级和单元应用，还包括采取企业整体层级的风险组合观；企业风险管理旨在识别那些一旦发生将会影响企业的潜在事项，并把风险控制在风险容量以内；企业风险管理能够向一个企业的管理当局和董事会提供合理保证；企业风险管理力求实现一个或多个不同类型但相互交叉的目标。

#### 2.与内部控制框架定义的比较

与内部控制相比，企业风险管理补充了两个内容：一个是战略目标；一个是风险控制。

### （二）企业风险管理整合框架的目标体系

#### 1.目标体系的内容

企业风险管理框架提出了四类目标：①战略（Strategy）目标，即高层次目标，与使命相关联并支撑使命；②经营（Operations）目标，高效率地利用资源；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。

#### 2.与内部控制框架目标的比较

在这个目标体系中，增加了内部控制整合框架中所没有的一类目标：战略目标。虽然是平行的方式列示，但是，战略目标在这个目标体系中是最高层次的，其他三类目标都应当从属于战略目标，都是在为战略目标服务。

此外，企业风险管理框架的报告目标也有所拓展。在内部控制框架中，报告指的是公布的财务报表，报告目标主要关注公布的财务报表的可靠性，而在企业风险管理框架中，报告包括由企业编制、向内部和外部散发的所有报告。而且，范围也从财务报表的财务信息扩展到了更广泛的非财务信息。尽管在企业风险管理框架中，并没有明确表示其遵守目标与内部控制的遵守目标有什么不同，但是，负责拟定企业风险管理框架的普华在其 2004 年的一份名为《整合——驱动绩效》（Integrity - Driven Performance）的报告中认为：“主要关注遵守法律、法规的传统合规方法是不充分的，遵守内部治理、道德与风险标准和政策在防止遭受与声誉相关的风险方面更有效。”该报告对“遵守”的内涵进行了拓展，提出了一个新视角的“遵守”，给出了一个遵守风险的新定义。遵守风险是指“由于没有能够遵守法律法规、内部规则和政策以及顾客、雇员和社会等主要利益相关者的期望而导致对组织的经营模式、声誉和财务状况产生损害的风险”。

另外，内部控制整合框架 1994 年补充的“保护资产”目标在企业风险管理框架中并没有单列，因为 COSO 认为，这个目标的内容已经分别包含在了上述几类目标之中。

对于目标的实现，企业风险管理与内部控制一样，只能提供合理的保证，而且对于不同的目标所提供合理保证的内容也不尽相同。对于报告目标和合规目标而言，因为有关报告的可靠性和符合法律、法规的目标在主体的控制范围之内，所以可以期望企业风险管理为实现这些目标提供合理保证。但是，对于战略目标和经营目标而言，由于这些目标的实现还取决于一些不在主体控制范围之内的外部事项，所以，企业风险管理可以提供合理保证的是对目标的实现过程进行有效的信息沟通，即管理当局以及承担监督职能的董事会能够及时地了解企业目标实现的进展情况。

### （三）企业风险管理整合框架的构成要素

企业风险管理整合框架包括八个相互关联的构成要素，它们源自管理当局的经营方式，并与管理过程整合在一起。

#### 1.企业风险管理整合框架构成要素的内容

（1）内部环境。

内部环境包含了组织的风格，它确定了组织人员如何看待和处理风险的基础，是其他要素的基础。内部环境具体包括风险管理哲学、风险偏好、董事会、诚实度和道德价值观、组织结构、胜任能力、人力资源政策与实务、权责分配。

（2）目标设定。

在管理层辨别影响其目标实现的潜在事项之前，必须有目标，企业风险管理要求管理层设定目标，选择的目标需要能够支持组织的使命并与组织使命相一致，同时与其风险偏好相一致。

（3）事项识别。

即识别那些影响组织目标实现的内外部事项，并区分为风险和机会，机会将被考虑进管理层的战略或目标设定过程中。

（4）风险评估。

必须对风险加以分析，考虑其发生的可能性以及影响，并作为确定这些风险应如何加以管理的基础，应当对固有风险和剩余风险加以评估。

（5）风险应对。

管理层应在不同的风险应对（包括回避、接受、降低、分担风险）中做出选择，从而采取一系列与组织的风险容忍度（Risk tolerances）和风险偏好相一致的行动。

（6）控制活动。

企业应建立相关的政策和程序，以确保风险应对策略得到有效的执行。控制活动通常包括两个要素：确定应从事何种活动的政策，执行政策的程序。

（7）信息与沟通。

应当按照特定的格式和时间框架来识别、捕捉相关信息，并加以传递沟通，从而使人们可以履行其职责。有效的沟通存在于较广泛的意义上，包括向下向上以及平行交互沟通。

（8）监控。

整个企业风险管理都应当加以监控，并根据需要做出调整。监督可以通过持续性的管理活动、单独评价或者二者同时来实现。

### 2.与内部控制框架要素的比较

企业风险管理框架与内部控制框架相比，在要素构成上主要有两个方面的变化：一是以“内部环境”取代“控制环境”，在“内部环境”中引入了风险管理理念、风险偏好两个概念。风险管理理念是一套共享的观念和态度，它标志着企业考虑风险时的特征，反映了企业的价值观。风险偏好反映了一个企业的风险管理理念，并影响着企业的文化和经营方式。二是企业风险管理更加关注风险，拓展了内部控制框架的风险评估要素，进一步细分为目标设定、事项识别、风险评估和风险应对四个要素。COSO 提出的企业风险管理框架与 1999 年英国制定的特恩布尔报告中的风险管理模式有一定的相似之处。

在结构方面，COSO 沿用了内部控制整合框架中通过三维矩阵表现构成要素与目标之间关系的表示方法，如图 2－2 所示。四类目标用纵向的栏表示，八个构成要素用横向的列表示，而一个主体内的各个单元则用第三个维度表示。这种表示方式让使用者既能够从整体上关注一个主体的企业风险管理，也可以从目标类别、构成要素、主体单元，甚至其中任何一个分项的角度去加以认识。企业风险管理的构成和目标既是建立健全企业风险管理过程的依据，也是评价其有效性的标准。认定一个主体的企业风险管理是否有效，是在对八个构成要素是否存在并有效运行进行评估的基础之上所做的判断。构成要素如果存在并且正常运行，那么就可能没有重大缺陷，表示风险被控制在主体的风险容量之内。当企业风险管理分别在四类目标中的每一类下都被确定为有效时，就可以合理保证董事会和管理当局了解主体实现其战略和经营目标、主体的报告可靠性以及适用的法律和法规被遵循的程度。此外，八个构成要素在每个主体中的运行也不是千篇一律的。例如，在中小规模主体中的应用可能不太正式，不太完备。尽管如此，当八个构成要素存在且正常运行时，依然表示小规模主体的企业风险管理呈有效状态。

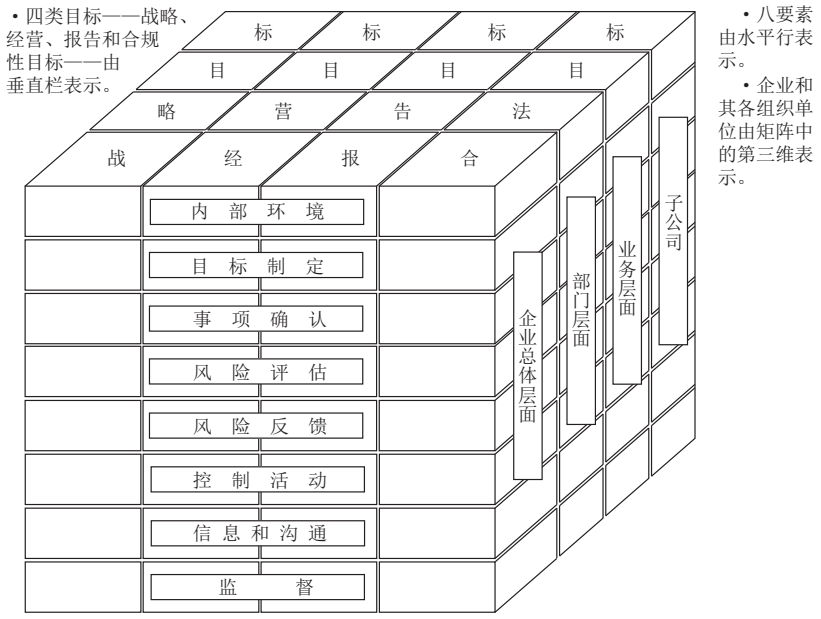


图 2-2　风险管理目标与要素关系图

## 二、2017 年版《企业风险管理—与战略和业绩的整合》

### （一）2017 年新版企业风险管理框架出台的背景

#### 1.COSO－ERM 框架（2004）在实践中暴露出一些问题

COSO－ERM 框架（2004）的初衷和定位是正确的，即从整合风险管理的角度为企业创造价值并合理保障企业战略目标的实现。但在起草 ERM 框架时采用了在 COSO 内部控制框架的基础上进行升级和扩充的做法，这直接导致了两个理论框架虽然愿景和目标各不相同，但内容的重合度非常高。企业在实践这两个理论体系时往往认为“内部控制就是风险管理”“风险管理就是内部控制”，为企业风险管理实践埋下了隐患。

另外，在 COSO－ERM 框架（2004）实施初期，由于许多企业还尚未将风险管理作为企业管理方式，风险管理更多的是运用于业务流程层面，在战略制定层面实施风险管理框架的企业并不多，加上当时美国上市企业多注重《萨班斯—奥克斯利法案》要求的合规性工作，因此 2004 年版的风险管理框架并没有得到企业的广泛接受。

#### 2.市场、经济环境发生了巨大变化，新型风险层出不穷

2004 版框架发布距今已有十几年时间，这十几年间，风险的复杂性发生了重大变化，由于新环境、新技术的不断演变，新的风险也层出不穷。利益相关方更加关心风险管理对企业价值的创造，尤其是在战略的制定和执行中风险管理价值的体现，以及增强风险管理和企业绩效之间的协同关系。特别是自 2008 年金融危机和 2011 年日本海啸发生以来，各种戏剧性风险管理失效事件频发，加上在商业环境日益复杂的共同叠加作用，在 COSO 内部控制框架的基础上进行升级和扩充的 2004 年风险管理框架已经无法满足实践需求，风险管理框架必须更新升级。

在此背景下，美国 COSO 在 2014 年首次启动了对风险管理框架的修订工作，并于 2017 年 9 月发布了《企业风险管理—与战略和绩效的整合》。

### （二）COSO－ERM 框架（2017）的内容

#### 1.风险管理的定义

风险管理是组织在创造、保持和实现价值的过程中，结合战略制定和执行，赖以进行管理风险的文化、能力和实践。新版框架简化了对 ERM 的定义，该定义包括文化和能力而不只是过程，更加强调风险与价值的相结合，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.风险管理的要素

（1）治理和文化。

治理和文化是风险管理其他四大要素的基础。治理确定了组织的基本基调，强化风险管理的重要性并确立风险管理的监督责任。文化则是组织的价值观、行为准则和对风险的理解。治理和文化是确保组织风险管理行之有效的强大基石。

（2）战略和目标设定。

风险管理通过制定战略和业务目标的过程与组织的战略计划融合在一起。通过对商业环境的理解，组织可以得到对内在和外在因素的看法以及它们对风险的影响。组织在战略制定中确定其风险偏好，而业务目标使得战略得以实践并形成组织日常的运营。

（3）绩效。

组织识别并评估可能影响其实现战略和业务目标的风险，结合企业的风险偏好，对风险按照其严重程度排分优先次序，组织选择风险应对的方法并对绩效进行监控以做出调整。这样，企业对追求战略和业务目标时所面临的风险量建立起一个组合的观念。

（4）审阅与修订。

组织应如何对风险管理绩效，以及风险管理职能各大要素的长期有效性进行监控，尤其是在发生重大变更的情况下。有效的监控流程使组织领导得以深入了解风险和绩效之间的关系，以及战略风险会如何影响绩效，并且识别与实现战略有关的新兴风险。

（5）风险信息、沟通和报告。

沟通是在组织中不断迭代地取得并分享信息的过程。管理层利用从内部和外部取得的有效信息来支持组织风险管理工作，组织利用信息系统来捕捉、处理和管理数据和信息。通过利用应用于所有组成部分的信息，组织就风险、文化和绩效做出报告。该流程可以为关键利益相关方提供必要的信息和洞见。

### 3.风险管理的原则

该框架在的整体结构上使用了 2013 年 COSO 构成元素＋原则的结构，包括 5 个构成元素，细分为 20 条原则，该结构加强了该框架的可读性、可用性和一致性。支持各要素的原则如表 2－2 所示。

**表 2－2　COSO－ERM 框架（2017）风险管理要素与原则**

| 五大要素 | 基本原则 |
| --- | --- |
| 治理和文化 | 1.加强董事会对风险的监督。董事会通过对组织的风险监督和执行治理责任，以支持管理层实现战略和业务目标 |
| | 2.建立运营结构。组织在追求战略和业务目标的过程中建立运营结构 |
| | 3.定义期望的组织文化。组织通过定义其期望的行为来具体化组织所期望的文化的特点 |
| | 4.展现对核心价值的承诺 |
| | 5.吸引、开发并留住优秀个体。组织承诺按照战略和业务目标来构建人力资本 |
| 战略和目标设定 | 6.分析业务环境。组织分析业务环境对风险图谱的潜在影响 |
| | 7.定义风险偏好。组织在创造、保存和实现价值的过程中定义风险偏好 |
| | 8.评估可供选择的战略。组织评估可供选择的战略及其对风险图谱的潜在影响 |
| | 9.形成业务目标。组织在建立不同层次的、与战略一致和支持战略的业务目标过程中考虑风险 |
| 绩效 | 10.识别风险。组织识别影响战略和目标实现的风险 |
| | 11.评估风险的严重程度 |
| | 12.区分风险的优先次序。组织通过区分风险的优先次序为风险反应的选择提供基础 |
| | 13.执行风险反应 |
| | 14.建立风险组合观。组织建立和评估组织风险 |

续表

| 五大要素 | 基本原则 |
| --- | --- |
| 审阅与修订 | 15.评估重大的风险。组织识别和评估可能对战略和业务目标的重大影响的变化 |
| | 16.审阅风险与绩效 |
| | 17.持续改进企业的风险管理 |
| 风险信息、沟通和报告 | 18.升级信息系统。组织应充分发挥主体的信息和技术系统以支持企业风险管理 |
| | 19.沟通风险信息。组织利用沟通渠道以支持企业风险管理 |
| | 20.对风险、文化和绩效进行报告。组织在各个层次、各个方面对风险、文化和绩效做出报告 |

## （三）2017 年 COSO－ERM 框架与 2004 年 COSO－ERM 框架相比，主要发展与变化

### 1.修订了风险的定义

2004 年版 ERM 框架中对风险的定义为：风险是一个事项将会发生并给目标实现带来负面影响的可能性。2017 年版 ERM 框架将风险的定义为：事项发生并影响战略和商业目标实现的可能性。由此，2004 年版 ERM 框架中风险的定义只强调了负面影响，而 2017 年版 ERM 框架中的定义的兼顾了正面和负面的影响，这和国际风险管理标准 ISO 31000 及中国风险管理标准 GB－T24353 是一致的，这在 2006 年国务院国资委发布的《中央企业全面风险管理指引》文件中就有体现。

### 2.凝炼、简化了风险管理的含义

2004 年版 ERM 框架对风险管理的定义为：风险管理是一个过程，它由一个组织的董事会、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组织的潜在事项，管理风险以使其在该组织的风险容量之内。并为组织目标的实现提供合理保证。而 2017 年版 ERM 框架对风险管理的定义为：组织在创造、保持和实现价值的过程中，结合战略制定和执行，赖以进行管理风险的文化、能力和实践。2017 年版 ERM 框架简化了对风险管理的定义以方便所有读者的理解，而不只是风险管理从业者，其内容不只是过程还包括文化和能力，更加强调风险与价值的相结合，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。

### 3.2017 年版 ERM 框架采用了国际文件惯用的要素加原则的结构

2017 年版 ERM 框架采用“要素＋原则”的框架结构，其中包含五大要素和二十项原则。2013 年 COSO 组织更新了企业内部控制框架的部分内容，在文章的整体结构上就是采用的这种结构，2017 年版的结构加强了 2017 年版框架的可读性、可用性和一致性。

### 4.强调风险与价值的关系

2017 年版 ERM 框架中，风险管理被视为战略制定的重要组成和识别机遇、创造和保留价值的必要部分。该框架中风险管理不再是组织的一个额外的或是单独的活动，而是融入组织的战略和运营当中的有机部分。

### 5.加强了企业风险管理与战略、绩效的联系

2004 年版 ERM 框架开始在风险管理之中思考战略的作用，2017 年版 ERM 框架继承了 2004 版风险管理框架的优点，提出当前企业风险管理应当与企业总体战略相整合，并且从新的风险视角出发，将战略实施中的风险（绩效实施）列为五方面之一。

通过 2017 版框架与 2004 版框架的对比可知，2017 版框架探讨了企业风险管理工作如何识别、评估影响绩效的各种风险，在进行风险管理的过程中，更加注重风险管理与战略和绩效的整合，更加适应目前的市场环境。

总之，2017 版 ERM 以崭新的视角、思路与框架，首次提出或强调了企业风险管理与企业战略、价值、绩效以及企业所有业务流程的关联性、统一性、相容性，实现了风险管理思想和理论的又一次飞跃。

## 第三节 我国企业内部控制框架

我国企业内部控制框架主要体现在五部委发布的《企业内部控制基本规范》中。

### 一、内部控制的定义

《企业内部控制基本规范》所称的内部控制，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。该定义强调了企业领导者尤其是董事会、监事会、经理层和全体员工在建设与实施内部控制中的重要作用；明确了内部控制是全体员工的共同责任；指明了内部控制是一个过程，内部控制不仅是对企业生产经营过程的控制，也是对实现企业发展目标过程的控制，更是一个不断优化完善的过程。

该定义基本参照 COSO 委员会的《内部控制——整合框架》中对内部控制的定义，但也充分考虑到我国公司法及相关法规的要求，明确了监事会在内部控制建立与实施中的作用。

### 二、内部控制的目标

《企业内部控制基本规范》第三条第二款规定，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。

#### （一）合法合规目标

合法合规目标是指内部控制要合理保证企业在国家法律法规允许的范围内开展经营活动，严禁违法经营、非法获利。经营管理合法合规是企业生存和发展的客观前提，是内部控制的基础性目标，是实现其他内控目标的保证。

#### （二）资产安全目标

资产安全目标是指内部控制合理保证企业资产安全完整，防止资产流失。即一方面要确保企业的各项存款等货币资金的安全，防止被挪用、转移、侵占、盗窃；另一方面还要保护实物资产，防止低价出售，要充分发挥资产效能，提高资产管理水平。

#### （三）报告目标

报告目标是指内部控制要合理保证企业提供了真实可靠的财务报告及其他信息。它是内部控制目标体系的基础目标。这里的信息既包括财务信息，也包括非财务信息；既包括对内提供的信息，也包括对外提供的财务报告等方面的信息。财务报告目标是经营目标的成果反映，其实现程度又在一定程度上影响经营目标的实现程度。

#### （四）经营目标

经营目标是指内部控制合理保证企业经营效率与效果，使企业的经营活动更加有效地进行，更富有成果。经营目标是企业实现战略目标的核心和关键，战略目标是与企业使命有关的总括性目标，它的实现需要通过分解和细化为经营目标才能得以落实，没有经营目标，战略目标制定得再好也没有任何意义。但经营目标的实现需要合法目标、资产目标和报告目标的支持。

#### （五）战略目标

战略目标是指企业在一定时期内，执行其使命所预期要达到的成果。促进企业实现发展战略是内部控制的最高目标，也是终极目标。但战略目标需转化为企业具体的经营目标才能得以实现。

上述五个目标是一个完整的内部控制目标体系的不可或缺的组成部分，即通过内部控制，要保证企业在合法经营的前提下，保障资产的安全完整，提供真实可靠的财务报告及其他信息，保证其经营既有效果又有效率，从而实现其战略目标。

### 三、内部控制要素

《企业内部控制基本规范》第五条规定了内部控制的五要素，即内部环境、风险评估、控制活动、

信息与沟通和内部监督。

### （一）内部环境

内部环境是企业实施内部控制的基础，一般包括治理结构、机构设置及权责分配、内部审计、人力资源政策、企业文化等。内部环境影响着企业内部控制的方方面面，是内部控制其他四个构成要素的基础，在企业内部控制建立与实施中发挥着基础性作用。

### （二）风险评估

风险评估是企业及时识别、系统分析经营活动中与实现内部控制目标相关的风险，合理确定风险应对策略。风险评估由目标设定、风险识别、风险分析和风险应对构成。

### （三）控制活动

控制活动是企业根据风险评估结果，采用相应的控制措施，将风险控制在可承受度之内。《企业内部控制基本规范》第二十八条规定，企业应当结合风险评估结果，通过手工控制与自动控制、预防性控制与发现性控制相结合的方法，运用相应的控制措施，将风险控制在可承受度之内。控制措施一般包括：不相容职务分离控制、授权审批控制、会计系统控制、财产保护控制、预算控制、运营分析控制和绩效考评控制等。

### （四）信息与沟通

信息与沟通是企业及时、准确地收集、传递与内部控制相关的信息，确保信息在企业内部、企业与外部之间进行有效沟通。信息与沟通贯穿于内部控制体系的内部环境、风险评估、控制活动和内部监督四个基本要素，是四个基本要素的重要工具，为企业内部控制的有效运行提供信息保证，从而有助于提高企业内部控制的效率和效果。

### （五）内部监督

内部监督是企业对内部控制建立与实施情况进行监督检查，评价内部控制的有效性，发现内部控制缺陷，应当及时加以改进。内部监督与内部控制其他要素相互联系、互为补充，共同促进企业实现控制目标。

## 第四节　我国中央企业全面风险管理框架

### 一、全面风险管理的定义

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。这一定义明确了全面风险管理的三个要素，即风险管理基本流程、风险管理文化和风险管理的组织体系；强调了全面风险管理是一种过程和方法。

### 二、全面风险管理的目标

《中央企业全面风险管理指引》第七条规定了企业开展全面风险管理要努力实现的风险管理总体目标。

（1）确保将风险控制在与总体目标相适应并可承受的范围内。

（2）确保内外部，尤其是企业与股东之间实现真实、可靠的信息沟通，包括编制和提供真实、可靠的财务报告。

（3）确保遵守有关法律法规。

（4）确保企业有关规章制度和为实现经营目标而采取重大措施的贯彻执行，保障经营管理的有效性，提高经营活动的效率和效果，降低实现经营目标的不确定性。

（5）确保企业建立针对各项重大风险发生后的危机处理计划，保护企业不因灾害性风险或人为失误而遭受重大损失。

## 三、全面风险管理的要素

### （一）风险管理的基本流程

风险管理基本流程包括以下主要工作。

#### 1.收集风险管理初始信息

《中央企业全面风险管理指引》第十一条规定，实施全面风险管理，企业应广泛、持续不断地收集与本企业风险和风险管理相关的内部、外部初始信息，包括历史数据和未来预测。应把收集初始信息的职责分工落实到各有关职能部门和业务单位。

收集风险管理初始信息是整个风险管理的第一步，在企业开展风险评估工作之前，首先需要收集风险和风险管理相关的内部、外部初始信息，包括历史数据和未来预测，作为风险评估的准备。收集风险管理初始信息的目的在于协助企业业务单位及职能部门于主要风险领域内清楚了解企业的目标、相关业务流程、各重大业务流程的关键成功因素及绩效指标，行业竞争优势，以及企业及行业竞争对手的重大损失事件案例分析等。这些信息与潜在风险驱动因素有着重大关系。

#### 2.进行风险评估

《中央企业全面风险管理指引》规定，企业应对收集的风险管理初始信息和企业各项业务管理及其重要业务流程进行风险评估。风险评估包括风险辨识、风险分析、风险评价三个步骤。风险评估应由企业组织有关职能部门和业务单位实施，也可聘请有资质、信誉好、风险管理专业能力强的中介机构协助实施。

进行风险评估的工作可以提高管理层和员工的风险意识，并明确风险管理的职责。评估风险应涵盖企业的战略、财务、市场、运营及法律风险层面，并确定这些风险会给企业带来的影响，评估能影响企业实现其战略目标的最重大的风险，评估任何能损害企业名声的“突发事件”，决定企业“下一步”该如何管理及监督重大风险的风险。

#### 3.制定风险管理策略

风险管理策略指企业根据自身条件和外部环境，围绕企业发展战略，确定风险偏好、风险承受度、风险管理有效性标准，选择风险承担、风险规避、风险转移、风险转换、风险对冲、风险补偿、风险控制等适合的风险管理工具的总体策略，并确定风险管理所需人力和财力资源的配置原则。

企业应定期总结和分析已制定的风险管理策略的有效性和合理性，结合实际不断修订和完善。其中，应重点检查依据风险偏好、风险承受度和风险控制预警线实施的结果是否有效，并提出定性或定量的有效性标准。

#### 4.提出和实施风险管理解决方案

企业应根据风险管理策略，针对各类风险或每一项重大风险制定风险管理解决方案。方案一般应包括风险解决的具体目标，所需的组织领导，所涉及的管理及业务流程，所需的条件、手段等资源，风险事件发生前、中、后所采取的具体应对措施以及风险管理工具（如关键风险指标管理、损失事件管理等）。

风险管理解决方案分外包方案和内控方案。外包方案应注重成本与收益的平衡、外包工作的质量、自身商业秘密的保护以及防止自身对风险解决外包产生依赖性风险等，并制定相应的预防和控制措施。内控方案应满足合规的要求，坚持经营战略与风险策略一致、风险控制与运营效率及效果相平衡的原则，针对重大风险所涉及的各管理及业务流程，制定涵盖各个环节的全流程控制措施；对其他风险所涉及的业务流程，要把关键环节作为控制点，采取相应的控制措施。

#### 5.风险管理的监督与改进

企业应以重大风险、重大事件和重大决策、重要管理及业务流程为重点，对风险管理初始信息、风险评估、风险管理策略、关键控制活动及风险管理解决方案的实施情况进行监督，采用压力测试、

返回测试、穿行测试以及风险控制自我评估等方法对风险管理的有效性进行检验，根据变化情况和存在的缺陷及时加以改进。

监督和改进的实质是关注风险管理的目标，深思熟虑地对风险管理进行分析，集中发现关于重大风险、重大事件、重要管理及业务流程的风险管理的缺陷，并根据变化情况进行改进，持续提升风险管理水平。

### （二）风险管理的文化

企业应注重建立具有风险意识的企业文化，促进企业风险管理水平、员工风险管理素质的提升，保障企业风险管理目标的实现。

企业文化是企业在长期经营管理活动中，由企业经营领导者倡导的、自觉形成的，并为绝大多数员工恪守的经营宗旨、价值观念、道德行为准则，以及与这些相适应的组织和制度的综合体现。全面风险管理不是某个人或某个部门的单独的事情，而是涉及企业各个层面、各个业务领域、所有员工的事情，只有将风险意识和理念融入企业文化中，把风险意识转化为全体员工的共同认识和自觉行动，才能确保风险管理目标的实现。建立良好的风险管理文化，与建立全面风险管理体系、执行风险管理流程同等重要。企业的所有生产经营行为、所有的控制制度，最终都由具体的人来操作和完成。如果员工没有正确的风险管理意识，再好的体系和机制，也难免会出现重大风险事件。

### （三）风险管理的组织体系

企业应建立健全风险管理组织体系，主要包括规范的公司法人治理结构，风险管理职能部门、内部审计部门和法律事务部门以及其他有关职能部门、业务单位的组织领导机构及其职责。

## 第五节　全面风险管理指引与内部控制基本规范比较

### 一、全面风险管理指引与内部控制基本规范比较

全面风险管理指引与内部控制基本规范比较如表 2－3 所示。

表 2－3　全面风险管理指引与内部控制基本规范比较表

| 比较要素 | 《内部控制基本规范》 | 《中央企业全面风险管理指引》 |
| --- | --- | --- |
| 适用范围 | 境内设立的大中型企业 | 中央企业 |
| 对风险的理解 | 仅指纯粹风险 | 不仅包括纯粹风险，也包括机会风险 |
| 目标 | 五个 | 五个（包括内控的三个） |
| 关于风险管理与内控的关系 | 没有明确论述 | 明确指出内控是风险管理的一部分 |
| 风险分类 | 外部风险、内部风险 | 战略风险、财务风险、市场风险、运营风险、法律风险 |
| 风险评估 | 目标设定、风险识别、风险分析、风险应对 | 风险辨识、风险分析、风险评价 |
| 风险应对策略 | 风险规避、风险降低、风险分担、风险承受 | 除左栏四项外，还包括：风险转换、风险对冲、风险补偿 |
| 控制措施 | 较具体、细化 | 类别划分较粗，但完备 |
| 风险管理信息系统 | 简单提及 | 有专门章节明确叙述、指导 |
| 风险管理文化 | 简单提及 | 有专门章节明确叙述、指导 |

### 二、内部控制系统与全面风险管理的异同

内部控制系统是全面风险管理的重要组成部分。一般来说，内部控制系统针对的风险大多是可控纯粹风险，其控制对象是企业中的个人，其控制目的是规范员工的行为，其控制范围是企业的业务和管理流程。全面风险管理还包括对机会风险的管理，其管理目的是为企业带来价值。

# 第六节 内部控制体系的建设

## 一、内部控制体系建设的原则

《内部控制基本规范》第四条规定，企业建立与实施内部控制，应当遵循下列原则。

### （一）全面性原则

全面性原则要求内部控制应当贯穿决策、执行和监督全过程，覆盖企业及其所属单位的各种业务和事项。

### （二）重要性原则

重要性原则是指内部控制应当在全面控制的基础上，关注重要业务事项和高风险领域。

### （三）制衡性原则

制衡性原则是指内部控制应当在治理结构、机构设置及权责分配、业务流程等方面形成相互制约、相互监督，同时兼顾运营效率。

### （四）适应性原则

适应性原则要求内部控制应当与企业经营规模、业务范围、竞争状况和风险水平等相适应，并随着情况的变化及时加以调整。

### （五）成本效益原则

成本效益原则要求内部控制应当权衡实施成本与预期效益，以适当的成本实现有效控制。

## 二、内部控制体系建设的程序

内部控制体系建设大致分为准备、设计优化、运行测试、维护与更新四个阶段。

### （一）准备阶段

准备阶段主要工作包括内部控制组织搭建与人员培训、确定内部控制建设的目标与范围和诊断内部控制现状。

#### 1.内部控制组织搭建与人员培训

（1）组织保障是建立健全内控的首要条件。根据《内部控制基本规范》的定义：内控是由企业董事会、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，只有有了全员参与，内控方才能行之有效，明确各机构在内控决策、执行以及监督中的工作职责。构建内控体系最大的挑战是如何与生产经营相结合，将控制无缝嵌入企业的生产、销售、管理等各环节的工作中，所以除了成立专/兼职部门负责组织内控的建立与持续改进外，搭建内控组织很重要的一环就是在各部门指定内控人员来负责本部门的内控建立与落实。

（2）内控建设要得到企业各层级员工的大力支持与配合，宣贯与培训是必不可少的。通过宣贯让各利益方了解内控的意义，通过培训让内控人员理解和掌握内控的理念和方法，在企业内营造管控的氛围，为内控建设奠定基础。

#### 2.确定内部控制建设的目标与范围

内部控制建设终极目标是战略目标，所有内部控制体系运行必须服务于企业中长期战略规划，重点解读企业领导对战略规划的思考，从战略高度把握内部控制体系建设要点。

内部控制建设围绕企业层面、业务层面、信息系统层面三个层面展开，企业根据自身的战略规划、经营目标、基本业务类型、组织架构、职责分工来确定内部控制体系的建设范围。

企业层面建设以解读战略目标为起点，业务层面建设范围采用定量与定性相结合的方法来判断。信息系统层面建设包括系统开发与维护、访问与变更、数据输入与输出、文件储存与保管、网络安全等方面的控制。

### 3.诊断内部控制现状

通过访谈及深度研读大量的内部管理文件和外部行业资料，运用各种诊断方法对企业进行诊断，重点对内部控制缺陷进行诊断。确定内部控制设计和运行中存在的缺陷，并确定认定缺陷的标准。

## （二）设计优化阶段

以五部委 2008 年《企业内部控制基本规范》及 2010 年《企业内部控制配套指引》为理论基础进行设计优化。

### 1.基于战略的内部环境优化

内部环境优化主要内容包括：建立规范的公司治理结构和议事规则（对治理体系中的风险和内部控制进行管理优化）；明确决策、执行、监督等方面的职责权限；形成科学有效的职责分工和制衡机制；强化审计功能，专列部门，强化职能，保持独立；建立并巩固人力资源政策、企业文化、职业操守、法律观念。

### 2.基于战略的全面风险评估

全面风险评估基本步骤是：广泛收集风险初始信息；分解企业目标体系；基于目标体系的风险识别；对风险信息进行风险确认，形成风险清单；在风险识别的基础上开展风险分析；设计风险评估问卷并进行统计；通过统计风险评估问卷，绘制风险坐标地图；制定风险策略，并落实风险应对策略，使其制度化、流程化。

### 3.控制活动建设，流程及制度优化

按照控制活动设计原则，运用一般方法和特殊方法对内部控制 18 项配套指引对应的控制活动进行诊断，根据诊断结果对内部控制制度及流程体系进行优化，并按内部控制要求嵌入流程，使其具有可执行性。

### 4.基于战略的信息与沟通机制优化

企业应从以下方面进行信息与沟通的设计与优化：建立相关信息的收集、处理和传递程序，确保信息及时沟通，促进内部控制有效运行；利用信息技术促进信息的集成与共享，充分发挥信息技术在信息与沟通中的作用；建立反舞弊机制，坚持惩防并举、重在预防的原则，明确反舞弊工作的重点领域、关键环节和有关机构在反舞弊工作中的职责权限，规范舞弊案件的举报、调查、处理、报告和补救程序。

信息与沟通机制是内部控制的有效决策依据，信息与沟通机制和内控是相关联的：必须通过某种方式，在一定的时间之内明确、获得并传达沟通相关信息以确保人们能够履行其职责；信息系统提供有关财务、经营和法律法规的遵守等信息的报告，这些信息使企业的管理控制成为可能；所有员工必须从高级管理层获得明确的信息指令，即所有人都必须认真看待和履行控制职责。

### 5.内部监督机制优化

据内部控制指引，制定内部控制监督制度，明确内部审计机构（或经授权的其他监督机构）和其他内部机构在内部监督中的职责权限，规范内部监督的程序、方法和要求。建立内部控制体系有效性评价机制。

## （三）运行测试阶段

设计优化阶段形成内部控制文本规定，比如内部控制手册。在内部控制体系建立后，需要对内部控制运行的有效性进行测试，主要工作如下：制定体系分布实施工作计划；进行运行测试，反馈运行效果；根据运行测试反馈结果，调整内部控制强度，修订手册；将体系运行扩大到各部门，并制定体系运行保障机制；通过打造标杆，指导子公司开展风险与内部控制工作。

## （四）内部控制体系的维护与更新

内部控制体系建设是一个动态过程，并不是一劳永逸的。在测试整改阶段完成之后，只能说针对当前的情况，所建立的内部控制体系是有效的。但外部环境和企业自身的情况是不断变化的，业务流程与风险也是在不断更新的，这就需要随时关注内部控制体系建设，维护更新，以适应具体情况的变化。管理层每年都需要出具自我评价报告，来证明企业内部控制运行的有效性。所以，为保证建立的

内部控制体系长期有效运行，需要根据外部环境和企业内部管理状况的不断变化，持续建设企业的内部控制体系，并不断改进完善。

综上所述，企业通过以上四步的动态建设，有助于把内部控制的理念和要求融入日常的工作，从而使各岗位高效运行，各部门密切配合，充分发挥整体的作用，以顺利实现企业的目标。

## 三、有关各方面在内部控制中的职责作用

### （一）董事会

董事会是公司的常设权力机构，向股东大会负责，实行集体领导，是股份公司的权力机构和领导管理、经营决策机构，是股东大会闭会期间行使股东大会职权的权力机构。对外是公司进行经济活动的全权代表，对内是公司的组织、管理的领导机构。董事会由股东大会选出的董事组成。董事一般由本公司的股东担任，也有的国家允许有管理专长的专家担任董事，以利于提高管理水平。

董事会在内部控制中的重要职责表现为：科学选择恰当的管理层并对其进行监督；清晰了解管理层实施有效的风险管理和内部控制的范围；知道并同意单位的最大风险承受能力；及时知悉最重大的风险以及管理层是否恰当地予以应对。董事会负责单位内部控制的建立健全和有效实施。

### （二）审计委员会

审计委员会是董事会设立的专门工作机构，主要负责公司内、外部审计的沟通、监督和核查工作。审计委员会的主要职责包括：审核及监督外部审计机构是否独立客观及审计程序是否有效；就外部审计机构提供非审计服务制定政策并执行；审核公司的财务信息及其披露；监督公司的内部审计制度及其实施；负责内部审计与外部审计之间的沟通；审查公司内部控制制度对重大关联交易进行审计。

审计委员会的主要目标是督促提供有效的财务报告，并控制、识别与管理许多因素对公司财务状况带来的风险。公司面临的风险涉及竞争、环境、财务、法律、运营、监管、战略与技术等方面。审计委员会本身无法监管所有这些风险，应该由各方（包括董事会其他委员会）共同合作。

审计委员会负责人应当具备相应的独立性、良好的职业操守和专业胜任能力。

### （三）管理层

管理层直接对一个单位的经营管理活动负责。总经理在内部控制中承担重要责任，其职责包括：为高级管理人员提供领导和指引；定期与主要职能部门（营销、生产、采购、财务、人力资源等部门）的高级管理人员进行会谈，以便对他们的职责，包括他们如何管理风险等进行核查。管理层负责组织领导单位内部控制的日常运行。

### （四）风险管理部门

风险管理部门及其人员的职责包括：建立风险管理政策；确定各业务单元对于风险管理的权利和义务；提高整个单位的风险管理能力；指导风险管理与其他经营计划和管理活动的整合；建立一套通用的风险管理语言；帮助管理人员制订风险管理报告规程；向董事会或管理层等报告单位风险管理进展和暴露的问题。

### （五）财务部门

单位的财务活动应当贯穿单位经营管理全过程。财务部门负责人在制定目标、确定战略、分析风险和做出管理等决策时应扮演一个关键的角色。管理层应当赋予财务部门及其负责人参与决策的权力，并支持其关注经营管理的更广范畴，局限财务负责人的关注领域和知悉范围，会削弱、制约单位的管理能力。

### （六）内部审计部门

内部审计部门及其人员在评价内部控制的有效性，以及提出改进建议方面起着关键作用。单位应当授予内部审计部门适当的权力以确保其审计职责的履行；对内部审计部门负责人的任免应当慎重；内部审计部门负责人与董事会及其审计委员会应保持畅通沟通；应当赋予内部审计部门追查异常情况的权力和提出处理处罚建议的权力。

### （七）单位员工

所有员工都在实现内部控制中承担相应职责并发挥积极作用。管理层应当重视员工的作用，并为员工反映诉求提供信息通道。

## 复习思考题

1.COSO 报告中如何定义内部控制的概念？“过程”反映了内部控制的什么特征？

2.2013 版 COSO 的内部控制框架与 1992 年版 COSO 内部控制框架相比有哪些变化？

3.1992 年版 COSO 内部控制框架与 2004 年的风险管理框架有何告的联系与区别？

4.2017 年版 COSO 风险管理框架主要内容有哪些？与 2004 年版风险管理框架有哪些变化？

5.我国企业内部控制基本规范规定的内部控制目标和要素各有哪些？与 COSO 内部控制目标和要素有何不同？

6.比较我国企业内部控制基本规范与中央企业全面风险管理指引的不同。

7.我国内部控制体系建设应遵循哪些原则？

8.企业各有关方在内部控制建设中主要职责有哪些？