

目 录

管理层概述	1
总体构架	11
1 定义	13
2 控制环境	23
3 风险评估	33
4 控制活动	49
5 信息和沟通	59
6 监控	69
7 内部控制的局限	79
8 作用和职责	83
附录	
A 学习本文的相关事项及背景知识	93
B 方法体系	99
C 对定义的看法和使用	105
D 反馈意见	111
E 术语	119

内部控制——整体构架

➤ 管理层概述

构架

对外界的报告

“对外界的报告”附录

管理层概述

高层管理人员一直在探求更好的企业经营控制之道。内部控制致力于促使企业向着赢利和完成自身使命的目标运行，并使这一过程中的意外最小化。内部控制使管理层能够应对瞬息万变的经济和竞争环境，客户不断变换的需求和偏好，并进行重组以利于公司的未来发展。内部控制有利于提高企业经营效率，降低资产损失风险，有助于保证财务报表的可靠性、企业经营活动的合法合规性。

鉴于内部控制具有上述的重要性，因此对提高内控系统及其报告质量的需求日益增加。内部控制日益被视为诸多潜在问题的解决方案。

什么是内部控制

内部控制对不同的人有不同的含义。这一概念在商业界人士、法律界人士、监管当局和其他人士之间容易引起混淆。由此造成的误解和期望值的差异往往给企业带来问题。一旦内部控制这一名词未经清楚定义就写入法律、规章或规则，问题便复杂化了。

本文是针对管理层的需要和期望而写的。本文对内部控制的定义服务于以下目的：

- 确立一个满足各方需要通用的定义。
- 提供一个标准——无论规模大小、公用和私人性质、赢利和非赢利，使各类企业都能以此对其内部控制制度进行评估和改进。

内部控制广义上可定义为一个受企业董事会、经理层和其他人员影响的，为达到下列目标提供合理的保证的程序：

- 经营的效果和效率
- 财务报告的可靠性
- 法律法规的遵循性

第一类目标指企业的基本经营目标，包括业绩、赢利指标和资源保护。第二类目标指编制可靠的公开财务报表的，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）。第三类目标指企业经营必须符合相关的法律法规。以上三类目标既相互独立又相互联系，分别代表不同的需求，需要

对它们作专门研究。

内部控制制度依据其运行的有效性程度而有所不同。因此，这三类目标又可根据此进行划分，如果董事会和经理层能够合理的保证：

- 他们清楚地知道企业经营目标实现的程度
- 公开财务报表的编制是可靠的
- 企业适用的法律得到遵守

虽然内部控制是一个过程，它的效果却表现为在某一时点上这一过程的状态。

内部控制包括五个相互联系的要素。它们源自管理层的经营方式，并与管理过程紧密相连。尽管此五项要素适用于各类企业，但是中小企业对其应用可能不同于大型企业。中小企业的内部控制可能不及大型企业正式、组织性强，但其内部控制也可能是有效的。内部控制的五项要素为：

- 控制环境——控制环境决定了企业的基调，直接影响企业员工的控制意识。控制环境提供了内部控制的基本规则和构架，是其他四要素的基础。控制环境包括员工的诚信度、职业道德和才能；管理哲学和经营风格；权责分配方法、人事政策；董事会的经营重点和目标等。
- 风险评估——每个企业都面临诸多来自内部和外部的有待评估的风险。风险评估的前提是使经营目标在不同层次上相互衔接，保持一致。风险评估指识别、分析相关风险以实现既定目标，从而形成风险管理的基础。由于经济、产业、法规和经营环境的不断变化，需要确立一套机制来识别和应对由这些变化带来的风险。
- 控制活动——控制活动指那些有助于管理层决策顺利实施的政策和程序。控制行为有助于确保实施必要的措施以管理风险，实现经营目标。控制行为体现在整个企业的不同层次和不同部门中。它们包括诸如批准、授权、查证、核对、复核经营业绩、资产保护和职责分工等活动。
- 信息和沟通——公允的信息必须被确认、捕获并以一定形式及时传递，以便员工履行职责。信息系统产出涵盖经营、财务和遵循性信息的报告，以助于经营和控制企业。信息系统不仅处理内部产生的信息，还包括与企业经营决策和对外报告相关的外部事件、行为和条件等。有效的沟通从广义上说

是信息的自上而下、横向以及自下而上的传递。所有员工必须从管理层得到清楚的信息，认真履行控制职责。员工必须理解自身在整个内控系统中的位置，理解个人行为与其他员工工作的相关性。员工必须有向上传递重要信息的途径。同时，与外部诸如客户、供应商、管理当局和股东的之间也需要有效的沟通。

- 监控——内部控制系统需要被监控，即对该系统有效性进行评估的全过程。可以通过持续性的监控行为、独立评估或两者的结合来实现对内控系统的监控。持续性的监控行为发生在企业的日常经营过程中，包括企业的日常管理和监督行为、员工履行各自职责的行为。独立评估活动的广度和频度有赖于风险预估和日常监控程序的有效性。内部控制的缺陷应该自下而上进行汇报，性质严重的应上报最高管理层和董事会。

这五项要素既相互独立又相互联系，形成一个有机统一体，对不断变化的环境自动作出反应。内部控制制度与企业的经营行为紧密相连，因基本的商业动机而存在。内部控制成为企业内部构架的核心部分和基本理念时最为有效。这时内部控制可以支持经营质量和主动的授权，避免不必要的花费，并对环境的变化迅速作出反应。

内部控制的三类目标之间具有直接联系，他们代表了企业努力的目标；而五项要素代表了实现这些目标所需元素。所有五项要素都与每一类目标相联系。为实现每一类目标——如经营的效率和效果——需要五项要素共同发挥作用，以说明经营的内部控制是有效的。

内部控制的定义——受人为因素影响、提供合理保证的过程，这一内在基本的概念——及其不同类型的目标、内部控制要素、内控有效性评价准则、与之相关的讨论，构成这本内部控制基本构架的内容。

内部控制能做什么

内部控制有助于企业实现其业绩和利润目标，防止资源损失，提高财务报告的可靠性，督促企业遵守相关法律法规，避免企业名誉受到损害以及受到其他不良影响。总之，内部控制有利于企业在即定轨道中前进，避免走弯路和遭遇突然袭击。

内部控制不能做什么

不幸的是，一些人对内部控制有不合实际的预期，他们存在以下幻想：

- 内部控制可以确保企业的成功——它能确保企业实现基本经营目标，至少能保证企业的生存。

即使有效的内部控制也仅仅能帮助企业实现经营目标。它提供给管理层关于企业成长过程中的信息。但内部控制不能使一个内在水平糟糕的经理变得杰出。另外，政府政策的变化、竞争对手的行为或经济环境都在管理层控制之外。内部控制不能保证成功，甚至不能保证生存。

- 内部控制可以确保财务报告的可靠性和法律法规的遵循性。

此观点也是不正确的。内部控制制度，无论设计、运行多么理想，都只能就企业目标的实现向管理层和董事会提供合理的，而非绝对的保证。经营目标的实现受到任何内控系统都具有的固有局限性的影响。内控系统的内在有限性包括以下现实情况：决策判断可能失误，简单的错误可能导致大纰漏。另外，控制可能因为两个以上人的相互勾结而趋于无效，而经理层有超越内控系统的权力。还有一个局限就是内控系统的设计必须反映以下事实，即出于资源有限性的考虑，内部控制必须考虑成本收益的匹配。

因此，尽管内部控制有助于企业实现其目标，但它并非万能药。

角色和职责

企业的每位员工都应担负内部控制的职责。

- 经理层——总裁应最终负责并具有内控系统的“所有权”。与其他人相比较，总裁制定了最高基调，这将影响诚信度、道德品行以及构成一个积极的控制环境的其他因素。在大公司，总裁通过督导高层管理人员检查其经营行为来完成自身职责。高层管理人员，则向各部门负责人分配具体的控制措施和程序。在规模小些的公司，总裁常常身兼所有者和经理人双重角色，其影响也就更加直接。在任何情况下，对于金字塔式的职责分布结构，每位经理人实际就是他所辖管职责范围内的总裁。经理层中具有特殊意义的是财务总监及其下属，他们的控制行为切入企业经营的各部分。
- 董事会——经理层对董事会负责，董事会提供管理、指引和核查。高效率的董事会成员应该是实事求是、富有才华和钻研精神的。他们熟悉企业经营及环境，留出足够的时间来完成董事会职责。不诚实的经理层有可能越过

内部控制，忽视或压制下属的信息反馈，并故意误报结果以掩盖其行径。一个强有力、活跃的董事会，特别是具备了有效的信息自下而上传递的渠道，以及完善的财务、法律和内审职能后，往往能识别和纠正这样的问题。

- 内部审计人员——内审人员在评价、维护企业内控系统有效性方面起重要作用。由于在企业中的组织地位和权威性，内部审计在监控方面扮演重要角色。

- 其他人员——从某种程度上说，内部控制是企业中每个人的职责，因此应成为每个人工作职责中明示或暗示的部分。实际上，所有职员都在产出内控系统需用的信息，或在进行与内控有效运行相关的活动。而且，所有职员都有责任向上层汇报经营中存在的问题、背离准则和违规违法行为。

一些企业外部人员常常有助于企业目标的实现。独立审计师通过实施独立、客观的监控，通过直接的财务报表审计和间接的管理建议，来帮助管理层完成职责。其他能够提供对有效内部控制有用信息的外部人员，包括律师、监管当局、客户、财务分析师、债券评级师和新闻媒体等。外部人员，不属于企业内控系统的一部分，也不对企业内控系统负责。

本报告的组织结构

本报告分四部分。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”，是附件，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。

本报告目的

根据本报告所能采取的行动与当事人所处的位置和承担的职责有关：

- 高级管理人员——多数来此学习的管理人员相信其对企业能够基本控制。然而，许多人认为一些部门或控制环节的内控还处于发展阶段或需要进一步加强。没有人喜欢出漏子。本研究报告建议总裁创建一套内控系统的自我评价系统。运用此系统，总裁以及主要经营、财务管理人员就能够将注意

力集中在关键问题上。一种方法是：总裁将部门负责人和业务骨干召集在一起讨论内部控制的初始评估方案，然后指导其他职员和上司讨论本报告中的概念，各职员在其职责范围内检查初始评估方案并提出反馈意见。另一种方法则包括对公司情况的初步复核、部门控制政策和内部审计程序。不管何种形式，初始评估方案应该能够决定是否有必要，或如何进行更深层次的评估。另外，它也应能保证持续的监管到位。评价内控系统所花费的时间是一种具有高回报的投资。

- 董事会成员——董事会成员应该和高层管理人员讨论企业内部控制制度的状况并在需要时提供督导。他们应借鉴内部审计师和外部审计师的意见。

- 其他人员——经理和其他人员应该考虑自身控制职能在整体内控构架下如何执行，并和高级管理人员讨论加强内部控制的方法。内部审计师应该考虑其对内控系统的关注范围，并将比较其评估资料与评估工具。

- 立法者和监管当局——立法当局认识到对任何事件都会存在误解和不同的期望。对内部控制的理解在两方面存在不同。首先，在内部控制的作用方面存在不同。如前所述，一些人认为内控系统应该能够防止企业遭受损失，或至少能够防止企业破产。其次，即使已在内控系统所能和所不能，以及“合理保证”的概念上取得一致，对于内部控制的概念和应用仍存在分歧。公司总裁非常关注监管当局在所谓内控失败事件发生后如何分析有关“合理性保证”的公开报告。在遵守有关管理层报告其内控情况的法律法规之前，需要对包括内控局限性的内部控制基本构架取得一致。本报告所阐述概念框架有助于达成以上共识。

- 专业组织——专业组织就企业的财务管理、审计和其他相关主题提供指引，因此必须考虑其对内控构架提出的标准和指导。一旦在概念和术语上的分歧消失，各方都会收益。

- 学术界——本内控构架可作学术研究和分析之用，以对其进一步改进。假设本报告被普遍接收，作为基础理论，其概念和专业术语有可能进入大学的课程。

我们相信本报告能带来一些益处。以此为基础达成共识，各方就有了统一的语言，能更有效地交流。商业管理人士将有一套评估内控系统的标准，以进

进一步加强内控，使企业向着既定目标前进。未来关于内部控制的研究也有了明确的基础。立法者和监管当局对内控的理解更加深刻，包括其优点和不足。只有各方运用同一个通用的内控构架，这些益处才会实现。

内部控制——整体构架

管理层概述

➤ 构架

对外界的报告

“对外界的报告”附录

第一章 定 义

本章概要：内部控制被定义为一个受企业员工行为影响，用以完成特定目标的过程。这是一个广义的概念，包含了对企业进行控制的各个方面，但却强调将重点放在特定的目标上。内部控制包括五个相互联系的要素，它们都包含在管理层经营企业的方式中。五项要素相互联系，作为评判内控系统是否有效的准则。

本次研究的主要目的在于协助管理层更好地控制企业行为。但内部控制对不同的人有不同的含义。大量的术语和释义妨碍人们了对内部控制的达成共识。因此一个重要的目标就是将形式各异的内控概念总结成一个总体构架，以确定一个通用的定义和明确各控制要素。本构架是为适应多数观点而设计的，并为企业的内控评价、立法机构的未来举措以及教学研究提供了起点。

内部控制

内部控制的定义如下：

内部控制是一个受到董事会、经理层和其他人员影响的过程，该过程的设计是为了提供实现以下三类目标的合理保证：

- 经营的效果和效率
- 财务报告的可靠性
- 法律法规的遵循性

该定义反映了以下基本概念：

- 内部控制是一个过程。它是实现目的手段，而非目的本身。
- 内部控制受人为影响。它不仅仅是政策手册和图表，而且涉及企业各层次的人员。
- 内部控制只能向企业董事会和经理层提供合理的保证，而非绝对的保证。
- 内部控制是为了实现三类即相互独立又相互联系的目标。

有两个理由使我们相信以上内部控制的定义是广泛适用的。第一，我们采访的多数经理是这样来看企业内部控制的。实际上，他们常常提及“控制”一词，而且正在“控制”。

第二，它适用于内部控制的多个子集。不同人可以有不同的侧重点，例如，可以分别侧重于财务报告和法律法规的遵循性。类似的，这一定义对企业某一部门或某一行为的内部控制也适用。

该定义同时也提供了决定内控有效性的基础，这在后面章节将会讨论到。以上基本定义将在以下小节详细讨论。

内部控制是一个过程

内部控制并非单一的事件或环境，而是针对企业行为的一系列活动。这些活动是潜移默化的，蕴含于管理层的日常经营行为中。

企业横向和纵向的经营行为都是通过计划、执行和监控这一基本过程进行的。内部控制是与这一过程密不可分的一部分，使之能够良好运行，并监督运行以保持持续的相关性。它是管理层的工具，而非管理的替代品。

这一定义与很多人不同，他们认为内部控制在企业的运营过程之外，是立法者和监管当局给企业增加的负担。内控系统与企业的运营紧密相连，因基本的商业动机而存在。只有内部控制成为企业内部构架中关键的一部分时，才最为有效。内部控制应该“嵌入”企业之中，而非“外置”在企业之外。

“嵌入式”控制直接影响企业实现其目标的能力，并支持企业的质量举措。对质量的要求直接与企业的运营和控制相联系。质量举措已成为企业运营构架的一部分：

- 高层管理人员确信质量价值蕴涵于企业的经营方式中。
- 确立质量目标与企业的信息收集、分析及其他过程相联系。
- 运用对有关竞争活动和客户期望的认知来不断推进质量的提高

以上质量要素与有效的内控系统要素相重合。实际上，内部控制不仅与质量规划紧密结合，而且对其成功起关键作用。

“嵌入式”控制对成本节约和减少反应时滞有重要作用。

- 多数企业面临高度的市场竞争和节约成本的需要。在现有的过程上增加新程序必然会增加费用。如果将重点放在当前的运营及其对有效内部控制的影响上，并将内部控制嵌入企业的日常经营中，常能使企业避免不必要的程序和成本。

- 将内部控制嵌入企业的运营构架中，有助于针对新的经营行为采取新的

控制措施。这种自动反应增加了企业的敏捷度和竞争力。

人的因素

内部控制受到企业董事会、经理层和其他人员的影响。它是通过企业员工的言行才实现的。人们确立企业的目标并将内控系统付诸实施。

同样，内部控制也影响人们的行为。人们理解、交流和行动的方式并非一成不变，每个人都有独特的背景和才干，具有不同的需求和重点。

这些现实既对内部控制产生影响也受到其影响。人们必须知道各自的职责和权限。相应的，在不同职责和执行方式之间应有明确的分工和联系，企业的各层目标也是一样。

企业员工包括董事会、经理层和其他职员。尽管董事被视为实施监管的主要人员，他们也进行工作指导，批准某些交易和政策。因此，董事会也是内部控制的一个重要元素。

合理性保证

内部控制，无论设计和执行多么理想，也只能就企业目标的实现向经理层和董事会提供合理的保证。企业目标实现的可能性受到内部控制内在局限的影响：包括人员决策上的失误；建立内部控制需考虑成本效益原则；人为错误和失误带来的内部控制失效。另外，内部控制会因两个或更多人的联合欺诈而失效。最后，经理层具有越过内控系统的权力。

目标

每个企业都有自己的使命，确立需实现的目标及相应战略。目标的设立应针对整个企业或企业内特定行为。虽然很多目标只针对特定企业，有一些还是普遍适用的，例如，几乎对所有企业普遍适用的目标是：在企业界和客户层保持良好的声誉，向股东提供可靠的财务报表，以及合法合规经营。

本报告将目标分为三类：

- 经营——关于企业资源利用的效率、效果
- 财务报告——关于编制公开财务报表的可靠性
- 遵循性——关于法律和法规的遵循性

这一分类有利于将内部控制的重点放在不同方面。这些既相互独立又相互联系的分体现了不同的需求，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。

内控系统可以为实现财务报告的可靠性和法律法规的遵循性目标提供合理的保证。这些目标（很大程度上是外界施加的）的实现有赖于企业内控系统的实施。

然而，经营目标的实现——如投资回报、市场份额、引进新产品——并非完全在企业控制能力之内。内部控制并不能阻止决策失误和意外事件的发生。只有当管理层及时了解企业向既定目标迈进的程度，内控系统才能为企业目标的实现提供合理的保证。

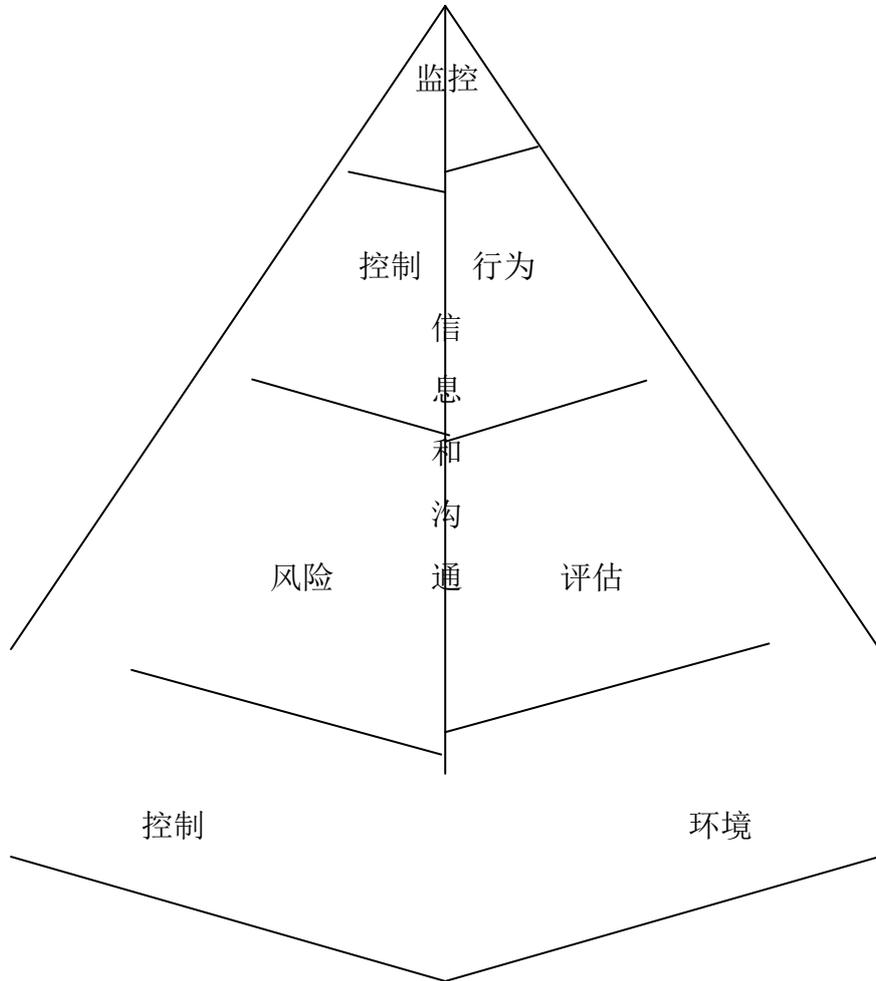
要素

内部控制包括五项相互联系的要素。它们来自管理层经营企业的方式，并融入管理过程本身。这些要素包括：

- 控制环境——企业的核心是人——员工的特性，包括诚信、道德和能力——和他们所处的环境。环境是企业发展的基础，也是推动企业发展的引擎。
- 风险评估——企业必须了解并应对其面临的风险，设定目标，包括销售、产品、营销、财务和其他行为，使之进入即定轨道运行。还必须确立识别、分析和管理的机制。

图示 1

内部控制要素



控制环境提供了员工实施(控制)活动和履行控制责任的氛围,是其他控制要素的基础。在此环境内,经理层评估实现特定目标的风险。控制活动是为了确保经理层有关减少风险的措施的顺利实施。同时,与之相关的信息被获取和在组织内部传递。整个过程都得到监控,并随着环境的改变而更新。

- 控制活动——必须确立和执行控制政策和程序,以确保那些被管理层认为必要的减少风险的措施得以执行。
- 信息和沟通——围绕在控制活动周围的是信息和沟通系统。这些系统有利于企业员工获得及交换与运作、管理和控制企业有关的信息。

- 监控——整个控制过程必须得到必要的监控和修订。这样，内控系统才能对环境的变化自动反应。

内部控制各项要素及其间联系如图示 1。该模型描述了内控系统的运行体制。例如，对风险的评估不仅影响控制行为，还可能强调需要重新考虑信息和沟通，或重新考虑企业监控行为。因此，内部控制并非一项要素影响下一项要素的顺序过程。它是一个几乎任一要素都可以影响其他要素的多方向、相互作用的过程。

没有两个企业会或应该具有相同的内控系统。公司的内控系统因行业和规模、文化和管理层哲学而不同。因此，尽管企业都需要这几项要素来实施对企业的控制，某一公司的内控系统常常看起来与另一公司的内控系统大相径庭。

目标和控制要素之间的关系

在企业尽力要实现的目标, 和代表实现这些目标需要什么的控制要素之间存在直接联系。它们之间的联系可用图示 2 中的三维矩阵表示：

- 三类目标——经营，财务报告和遵循性——用垂直柱条表示
- 五项要素用行来表示
- 内控系统相关的企业行为用第三维表示。

每行要素都贯穿、针对所有三类目标。图例左下角部分可以作为例子：从企业内、外部而来的财务和非财务数据，作为信息和沟通要素的组成部分，需要被用来有效管理企业运作，编制可靠财务报表和保证企业合法经营。另一例子（未单独列示），用以保证管理层规划、战略和其他指示得以贯彻的内部控制政策和程序的确立和执行——代表了控制活动这一要素——也与所有三类目标有关。

图示 2

控制目标和控制要素的关系

经营 财务报告 合法性

监控

信息和沟通

控制行为

风险评估

控制环境

左上：控制目标和要素之间具有直接联系，目标是企业尽力去实现的，而要素代表实现这些目标需要什么。

右上：内部控制与整个企业，或企业的任一部门或任一行为相关。

左下：所有三类目标都需要信息以有效管理企业、编制可靠财务报表及保证合理性。

右下：所有五项要素对经营目标的实现都适用和重要。

类似的，所有五项要素与每类目标都有关联。例如，对经营的效果和效率目标，所有五项要素都适用和重要。这在图例 2 的右下角已说明。

内部控制与整个企业或其中某一部分有关。这一关系用第三维表示，第三维代表附属公司、部门、业务单位、职能单位或诸如购买、生产、营销在内的企业行为。相应的，每个人都可以关注三维矩阵的一个单元。例如，可以考虑矩阵左下方前侧的一个单元，其代表与公司特定部门经营目标相关的控制环境。

有效性

不同企业的内控系统在不同的有效性水平上运行。类似的，特定的系统在不同的时期运行，可能具有不同的效果。当内控系统满足以下标准时，我们可以认为它是有效的：

如果董事会和经理层能够分别合理地保证在每类中任一类内部控制都可视为有效，：

- 他们了解企业经营目标可以在多大程度上实现
- 对外财务报表的编制是可靠的
- 适用的法律和法规得以遵循

尽管内部控制是一个过程，其有效性却是过程中某一时点的状态或情况。

评价某一内控系统是否有效是一种主观判断，判断来自对五项要素是否存在及有效运行的评估。内控系统的有效运行为上述某一或多项目标的实现提供了合理保证。因此，这些要素也是有效内控系统的评价标准。

尽管所有五项标准都必须满足，但并不意味着在不同企业，各项要素的功能

必须完全一致或在同一水平上。在要素间存在某种平衡。由于控制服务于多重目的，服务于目的的在某一要素中的控制也可能体现在其他要素的控制上。另外，控制防范某一特定风险的程度也有所差异，因此，加入附加的控制措施（尽管各自具有有限的影响力）可以带来令人满意的效果。

所有的要素和准则适用于整个内控系统，或适用于某一或多个分类目标。例如，当考虑到其中一类目标——对财务报告的控制时，所有五项准则都必须被满足以得出对财务报告的控制是有效的这一结论。

当评判一个内部控制制度是否有效时，应该考虑以下的章节。应该认识到：

- 由于内部控制是管理过程的一部分，因此对控制要素的讨论是在管理层如何经营企业这一背景下进行的。但并非管理层的一切行为都是内部控制的元素。例如，确立目标这一管理层重要的职责，就是内部控制的先决条件。类似的，很多管理层的决策和行为不代表内部控制。图例 3 列出了管理层的日常行为，并标出哪些被视作内部控制的要素。（该列示并非对管理层行为方式全面或唯一的归纳）
- 讨论的原则适用于所有规模的企业。一些中小型企业对要素的应用可能不同于大企业，但其仍能拥有有效的内部控制。每一章有一部分解释这样的情形。
- 每一章包含了“评估”部分，列出了评价控制要素时应考虑的因素。这些因素并非涵盖一切，也不是与每种环境都相关。它们仅提供例证用以开发一个更易理解或更具有针对性的评估模型。

图例 3

内部控制和管理过程

管理行为	内部控制
公司总体目标制定	
——使命，公司价值描述	
战略规划	
建立控制环境要素	√
操作层目标制定	

风险识别和分析	√
风险管理	
实施控制活动	√
信息甄别、获取和传递	√
监控	√
纠正行为	

第二章 控制环境

本章概要：控制环境决定了企业的基调，影响企业员工的控制意识。它是其他要素的基础，提供了基本规则和构架。控制环境因素包括：员工的诚信度、道德观和能力；管理哲学和经营风格；管理层授权和职责分工、人员组织和发展方式；以及董事会的重视程度和提供的指导。

控制环境对企业行为架构、目标设立和风险评估的方式有潜移默化的影响。它也影响控制活动、信息和沟通系统、以及监控行为。实际上控制环境不仅影响它们的设计，而且影响它们的日常运转。控制环境受企业文化和历史的影响。它影响员工的控制意识。具有有效控制的企业，尽力聘用有能力的员工，灌输诚信的企业文化和控制意识，设定一个积极的“最高基调”（完美行为规范）。它们确立适当的政策和程序，常常包括一本书面操作手册，培养共同的价值和团队精神，以期实现企业目标。

控制环境要素

控制环境包括以下讨论的要素。尽管每个要素都很重要，但根据企业的不同，侧重的程度还是有所差异。例如，一个集中经营的小作坊的总裁，也许不会建立正式的职责分工和详细的经营策略，但其仍可能有一个适当的控制环境。

诚信和道德观

企业目标及其实现方式建立在偏好、价值判断和管理风格的基础上。偏好和价值判断，转化为行为标准后，会反映出管理层的诚信度和遵行的道德观。

鉴于企业好名声的巨大价值，行为标准必然高于遵法守纪。为了把好名声奖赏给最好的公司，社会对他们的期盼比遵纪守法更多。

内部控制的有效性不可能超越创造、管理和监控这些制度的人们的诚信度和道德观。诚信度和道德观是控制环境的关键因素，它们影响其他内部控制要素的设计、管理和监控。

诚信是企业各方面活动道德行为的先决条件。正如 Treadway 委员会所报告的：在各层次上的良好公司道德氛围对公司、全体员工、顾客和公众的健康都至关重要。这一氛围对公司策略和控制系统的有效执行非常重要，也有助于影响那些即使最精细的内控系统也难以管制的行为。

因需考虑到多方面的情况，确立道德价值通常很困难。高级管理层的价值必

须与企业、雇员、供应商、顾客、竞争对手和公众的要求相协调。由于各方利益的分歧，协调可能是复杂和不令人满意的。例如，供应某种关键产品（如石油、木材或食品）可能会引起环境问题。

经营良好企业的经理日益同意“道德是有价值的”——道德行为就是好商机这一观点。有很多正面和负面的例证。医药公司对涉及某一主要产品的危机作出很好的公开处理，这一行为既合乎道德，又能带来商机。公司负面消息，如利润下滑或违法行为的缓慢释放，其对客户关系和股价的影响比起及时的披露要糟糕得多。

仅仅关注短期效应，甚至会造成短期的损害。对底线——销售或利润——的集中关注，常会引发始料不及的行为和反应。例如，高压的销售策略，冷酷无情的谈判或暗中的回扣，可能会引发具有即时（亦或持续）效果的反应。

道德行为和管理层诚信度是公司文化的产物。公司文化包括道德和行为标准及其如何传递，如何在实践中被加强。书面正式的公司政策定义了管理层希望发生什么，而公司文化决定了实际发生什么，哪些规则得到遵守、违反或忽略。从总裁开始的高层管理人员在公司文化的定位上起关键作用。总裁通常是企业的决定性人物，有责任设立企业的道德基准。

刺激和诱惑。几年前的一个研究建议，某些特定的组织因素会影响欺诈和可疑财务报告行为的可能性。同样的因素还可能影响道德行为。

个人可能仅仅因为其组织给予他们的强烈刺激和诱惑而从事不诚实、非法或不道德的行为。强调“结果”，特别短期结果，培养了失败代价很高的环境。

导致从事欺诈、可疑财务报告行为以及其他不道德行为的诱因有：

- 达到不切实际的业绩目标，特别是短期业绩的压力
- 与业绩挂钩的高回报
- 高于或低于奖金计划的奖励

研究还列出导致雇员作出不正当行为的一些“诱惑”：

- 控制不存在或失效，如敏感区域未作很好的职责分离，提供了偷窃或隐藏不良操作的诱惑。
- 组织高度分散，导致高层管理人员不清楚基层的行为，因此，减少了基层舞弊被发现的机会。

- 内部审计职能薄弱，无法发现和报告不正确的行为。
- 低效的董事会不能提供对高层管理人员的客观监管。
- 对不正确行为的惩罚力度不够或不公开，从而失去了应有的威慑力。

去掉或减少这些刺激和诱惑对减少预期外行为大有裨益。正如所建议的，只要实施合理、有利可图的商业实践，就可以取得这一效果。例如，只要业绩目标切实可行，业绩激励加之适当的控制可以成为有用的管理工具。制定现实的业绩目标是很好的激励措施；它减少了达不到预期目标的压力，同时也减少了不切实际的目标所造成的虚假财务报告的诱因。类似的，一个控制良好的报告系统可用于防范编制虚假业绩。

提供并传递道德指引。除了刚才讨论过的刺激和诱惑外，前面提及的研究发现引起欺诈和可疑财务报告的又一因素：无知。研究发现“在许多出现虚假财务报告的公司，相关人员或不知道自己做错，或错误相信他们所做的符合公司利益”。此类无知常常由缺乏的道德背景或指导造成，而并非故意欺骗。因此，不仅要传递道德价值，而且要对是非对错提供明确的指引。

在组织内传递道德行为的最有效方式是以例证方式。人们愿意模仿上司。雇员有可能形成与高级管理层类似的对错观念（包括对内部控制的态度）。得知总裁在面临艰难决策时作出合乎道德的正确选择，会给企业各层传递强烈的信息。

仅树立一个好榜样是不够的。高层管理人员应向雇员口头传递企业价值和行为标准。几年前的一个研究指出一套正式的行为准则是“向雇员传递公司关于责任和诚信预期的广泛应用的方法。”准则涵盖一系列行为，包括诚信和道德、利益冲突、非法或不正确的支付以及反竞争安排。部分受国防行业丑闻揭露的推动，许多公司最近都采纳了这样的行为准则，连同必要的信息传递途径和监控。尽管操作手册是有帮助的，它却不是向雇员、供应商和客户传递道德价值的唯一途径。

存在雇员能接收和理解的行为准则，甚至是文件，仍然不能保证其执行。高层管理人员的行为和榜样是遵行道德标准（不管道德标准是否写进行为准则）的最佳保证。对违反准则的雇员的相应惩罚；鼓励员工揭发违规行为的机制；以及对未能汇报违规行为员工的培训都具有特别重要的意义。管理层在这些情况下采取的行动所传递的信息很快便植入公司文化中。

才能

才能应反映出完成个人工作任务所需的知识和技能。这些任务需要完成到何种程度，总体上是来自于管理层决策，需要考虑到企业目标、管理层策略和实现目标的计划。在才能和成本之间经常需要权衡——例如，没有必要雇佣一名电子工程师来换一只灯泡。

管理层需要为特定的工作确定所需的才能水平，并将之具体到所需的知识和技能。而必要的知识和技能又有赖于个人的学识、培训和经验。确立知识和技能水平所需考虑的因素包括特定工作的性质和所需的职业判断。常需在监管的程度和个人所需才能水平之间取得平衡。

董事会或审计委员会

控制环境和“最高基调”受到企业董事会和审计委员会的显著影响。因素包括董事会或审计委员会相对于管理层的独立性，成员的经验 and 地位，活动的涉及面和深入程度，以及行为的适当性。另一因素是经理层关于计划和业绩的棘手问题被提出和从事的程度。董事会或审计委员会与内部和外部审计师的协同合作也是影响控制环境的因素。

鉴于其重要性，一个积极参与的董事会，监事会或其他类似机构——具有适当程度的管理、技术和其他专业技能，加之必要的地位和头脑，使其能充分行使必要的监管、指导和监控职责——对有效的内部控制至关重要。由于董事会必须对问题有所准备，仔细监察企业活动，提出可供选择的观点，具有勇气在明显的错误面前采取行动，因此必须设立外部独立董事。当然，本企业的管理人员和雇员也常是高效、重要的董事会成员，将公司情况摆上桌面。但必须取得一个制衡。尽管中小型企业有困难吸引或承担半数以上外部董事的花费，——这在大企业通常不成问题——董事会至少应包括一定量的外部独立董事，这一点非常重要。外部董事的具体数量应符合企业具体环境的需要，但通常需要超过一个的外部董事来使董事会达到必要的制衡。

董事会和审计委员会的存在必要性和其职责将在“在中小型企业的应用”和第 8 章中进一步讨论。

管理哲学和经营风格

管理哲学和经营风格影响企业管理的方式，包括企业承受的风险类型。一个

已经成功承担巨大风险的企业和一个由于冒险而面临艰难经济条件和监管结果的企业在内部控制上可能会有所不同。一个非正规管理的企业，可能大部分依赖与关键管理人员面对面的交流来实施经营控制。而正规些的公司可能更多依赖书面的政策、业绩指标和例外报告来实施控制。

其他管理哲学和经营风格要素包括对财务报告的态度、对可选会计原则保守或激进的选择，对所作会计估计的保守和尽责，以及对数据处理、会计和人事职能的态度。管理层如何实施其职责将在第 8 章中进一步讨论。

组织结构

企业的组织结构提供了一个构架，在此构架中规划、执行、控制和监督为实现企业目标而进行的活动。企业活动可能与有时所指的价值链相联系：采购（收货）的行为，运作或生产，外运（运输），市场、销售和服务。还可以有支持功能，与管理、人力资源或技术发展相关。

确立相关组织结构的主要方面包括定义关键领域的权责分工，确定合适的报告途径。例如，内审部门对高级职员应有不受限制的接触权，不直接负责编制财务报表，并有充分的授权以保证内部审计的范围，以及跟进所发现和建議的事项。

每个企业都根据自己的需要确定组织结构。一些是集权型，一些是分权型。一些具有直接的报告关系，一些则更多的是矩阵型的组织结构。一些企业按照行业或产品线，按照地理分布，按照特定的分销渠道或营销网点来组织架构。另外一些经济实体，包括国家和地方政府和非赢利机构，则按照功能来组织。

企业组织结构的适当性部分取决于规模和所从事经营活动的性质。一个结构严密的组织，包括正式的报告路线和权责分工，可能适合一个拥有很多部门分支，包括海外机构的大型企业。然而，它却可能阻挡小企业内的信息流动。不管何种组织结构，应有利于组织实施为实现特定目标而制定的策略。

权力和职责分配

这包括经营行为的权责分配，报告关系和授权协议的确立。它涉及个人和团队被鼓励主动提出和解决问题的程度以及权力限制的程度。它还涉及定义恰当的企业行为，关键人员的知识和经验，以及用以履行职责的资源政策。

将权力下放，使决策与一线人员更靠近，这样的趋势日益明显。企业可能实行这样的方针以成为更加市场推动型或质量关注型企业——可能为了消除缺陷，

缩短产品周期或提高客户满意度。为达到上述目的，企业需要认识不断变化的市场偏好、商业关系和公众期望并作出反应。所设计的授权和职责的结合通常为了鼓励在一定限制内的个人能动性。分权或授权指将某商业决策的集中权力下放到低层梯队——那些与日常交易最接近的人。这可能涉及对销售折扣的授权；长期供应合同、许可和专利的谈判；或结盟或合资。

关键的挑战是授权只到实现企业目标所需的程度。这要求确保风险承受度是建立在鉴别和最小化风险的良好实践上，包括度量风险，将潜在的风险与赢利相权衡，以进行好的决策。

另一个挑战是确保所有员工理解企业的目标。每个人都知道各自行为与目标的内在联系以及对目标的贡献，这是非常关键的。

有时日益增长的分权会伴随着或成为企业组织结构简化或扁平化的结果，而且是有目的的。有意为之的结构改变以鼓励创新、能动性、和迅速反应的能力能增强企业的竞争力和客户满意度。这种日益增长的分权可能带来对员工更高级别的管理者能力以及更大责任的内在需要。它也需要管理层实施有效的程序对结果监控。伴随着更好的市场推动型决策，授权可能增加不合需要或预期外决策的数量。如果某一地区销售经理认为，为了赢得市场份额，35%的销售折扣授权有权决定临时性的45%的折扣这一行为是正当的，管理层可能需要过问，决定这一决策是越权还是继续得以实施下去。

控制环境受到个人对各自职责认识程度的重大影响。这即便对主要管理者也是正确的，他们是企业一切活动，包括内部控制的最终负责人。

人力资源政策和措施

人力资源措施向员工传递关于预期的诚信度、道德行为和才能的信息。这些与雇佣、指导、培训、评估、咨询、提升、补偿、矫正等行为相关。例如，那些聘用最合格员工的标准，将重点放在教育背景、工作经验、过去的成就、诚信的品格和道德的行为，显示了企业对有才能和值得信赖的员工的偏好。包括正式、深入的面试，对企业历史、文化和经营风格广泛和见解深刻的演示在内的招聘活动传递了企业以人为本的理念。传达未来的职责的培训政策，包括培训学校、研讨会的实践、个案研究、角色扮演练习，这些都反映了企业预期的员工业绩和行为水平。由定期业绩评估推动的人员轮换和提升，显示了企业将合格人员及时提

升到更高级别的承诺。竞争补偿计划包括奖金激励,用于促进和增强优秀的业绩。惩罚性措施表明对预定行为的违反是不能容忍的。

部分受日新月异的科技和日趋激烈的竞争的推动,企业面临的问题也迅速变化并日趋复杂,因此人事必须准备迎接新的挑战。教育和培训,无论是课堂中的指导,自学或在职培训,必须使企业员工有准备跟上时代,有效应对环境的变化。还须加强企业影响质量能动性的能力。仅聘用能干的员工,进行一时的培训是不够的。必须进行持续教育。

差异和影响

由于管理层偏好、价值判断和管理风格的差异,企业的独立运营分部、国内外分公司的控制环境也大有差异。控制环境的差异有许多方面的原因。既然没有两个运营分部、国内外分公司以相同的方式经营,那么控制环境也不可能一样。因此,认识到不同控制环境会对控制制度的其他要素产生影响,是很重要的。

无效控制环境的影响是深远的,可能造成财务损失,公众形象受到影响或导致企业破产。以一家被公认具备有效内部控制的军工承包企业为例。该公司具有设计良好的信息系统和控制活动,众多描述内控职能的政策手册,以及广泛的协调和监控程序。它接受政府审计。然而,它的内控环境存在很大的缺陷。高层管理人员不想知道有没有发生不正当行为。即使欺诈现象非常严重,高层管理人员仍予以否认。该公司被发现在五角大楼从事欺诈活动,被判一大笔罚金,并遭到媒体的广泛披露,公众形象尴尬。

高层管理人员对有效内部控制的态度和关注必须渗透入企业内部。仅说正确的话是不够的。“我行我素”的态度必然会带来不健康的控制环境。

中小型企业的应用

虽然每个企业都应包括本章所讨论的概念,但是中小型企业对控制环境的应用会不同于大型企业。例如,小公司可以没有书面的行为准则,但这并不表示其没有强调诚信和道德行为重要性的公司文化。通过总裁或老板-经理和高级管理人员的直接参与,可以在员工会议、个人会面、和与供应商和客户打交道的过程中将对诚信和道德行为的要求以口头方式进行传达。由于雇员与他们有直接的接触,因此他们自身的信誉和行为就很重要,并应与口头宣传相符。通常的,管理的层次越少,可以接受何种行为的信息就传递得越快。

类似的，人力资源政策可能不象大公司那样正式。政策和措施仍然能够存在并被传递。总裁可以口头指示他需要招聘何种类型的人来从事某一特定工作，甚至可能积极参与招聘过程。并不一定需要正式的文件来使政策得以实行和实现有效的经营。

由于董事会或类似机构的重要性，即使小公司也需要这样的机构来获得有效的内部控制。如前所述：小企业设立大量的独立董事是有困难和不经济的，而且它可能不必要这样做。可以通过少量的独立董事来达到所需的独立性。一个重要的因素是需要存在“关键性的多数”，即足够的外部董事来保证董事会提出强硬的措施和在必要时采取一些艰难的措施。对这种需要只有一个例外。对于不需要公开筹资的私人企业，尽管独立董事也是有益的，但通常对有效内部控制不起关键作用。

评估

评判有效内部控制是否存在，评估者需要考虑到每个控制环境因素。需要重点关注的事项列示如下。这一列示并未涵盖全部，也非对每个企业都适用；它仅仅是一个起点。尽管有些具有很强的主观性，需要相当的职业判断，但总体上与控制环境的有效性相关。

诚信度和道德价值

- 行为和其他政策的指导手册的存在和应用。包括：可接受的商业行为，利益的冲突或期望的道德标准和行为。
- 与雇员、供应商、顾客、投资者、债权人、保险人、竞争对手和审计师等打交道。（例如，管理层是否在高道德标准上从事商业活动，并坚持他人也这样做，还是对道德问题很少关注）
- 实现不切实际的业绩目标的压力——尤其是短期目标——以及为了实现这些目标而所需补偿的程度

对才能的要求

- 对工作和构成工作的任务的正式或非正式的描述和定义。
- 对足够完成工作所需的知识和技能的分析。

董事会或审计委员会

- 与经理层独立，以提出必要，甚至是困难和需要查明的问题。

- 与财务总监或财务经理、内部审计师、外部审计师会晤的频率和时机。
- 信息向董事会或审计委员会传达的充分性和及时性，使管理层的目标和策略、企业财务状况和经营成果、以及重大合同的条款得到监控。
- 董事会或审计委员会得知敏感信息、调查和不正当行为的充分性和及时性。（例如，高级管理人员的差旅费、重大诉讼、监管机构的调查、贪污、挪用资产、违法内部交易规则、政治贿赂和非法支付等。）

管理哲学和经营风格

- 可承受商业风险的类型。例如，管理层是否经常从介入高风险活动，或在风险承受方面特别谨慎。
- 高级管理层和日常经营管理层之间相互交流的频率，特别是当相互之间在地理位置非常遥远时。
- 对财务报告的态度和行动，包括对会计处理应用的分歧（例如，保守或激进会计政策的选择；是否存在会计原则的错误应用、重要财务信息没有披露、或财务报告被粉饰或伪造。）

组织结构

- 企业组织结构的恰当性及提供必要的信息流以管理其行为的能力。
- 主要经理人员职责的充分定义及其对自身权责的理解。
- 与职责相对应的主要经理人员的知识和经验的充分性。

权力和职责的分配

- 权力和职责的分解，以应对组织目标，经营职能和法规要求，包括关于信息系统的责任和应对变化的授权。
- 与控制相关的标准和程序的适当性，包括雇员工作描述。
- 员工的合适数量，尤其对于数据处理和会计部门，需要与企业规模和工作、系统性质和复杂性相符的技能水平。

人力资源政策和措施

- 雇佣、培训、提升和补偿员工的政策措施到位的程度。
- 对偏离经批准的政策程序进行补救的措施的适当性。
- 对拟聘雇员背景调查的充分程度，尤其是有关那些企业不能接受的过往行为。

- 员工对标准的保持和提升的充分程度和信息收集技巧（如业绩评估）以及与行为准则或其他行为指南的关系。

第三章 风险评估

本章概要：每个企业都面临来自内部和外部的风险，这些风险必须进行评估。风险评估的前提是确立目标，这些目标在不同的层次上相互联系并具有内在的一致性。风险评估指对相关风险进行鉴别和分析，以实现目标，形成风险管理的基础。由于经济环境、行业、法规和经营状况不断变化，需要一个确认和处理与这些变化相关风险的机制。

所有企业，无论规模、结构、行业性质，在其各级组织结构内都面临着风险。风险影响企业生存的能力；在行业内成功竞争；保持财务实力和公众形象；保持产品、服务和人员的总体质量。没有一个实际的办法可以将风险减少至零。实际上，有经营就有风险。管理层必须确定能够谨慎地接受多少风险，并尽力将风险保持在这一水平。

风险评估的前提条件是设立目标。只有先确立了目标，管理层才能针对目标确定风险并采取必要的行动来管理风险。设立目标是管理过程重要的一部分。尽管其并非内部控制要素，它是内部控制得以实施的先决条件。本章先讨论目标，再讨论风险。

目标

设立目标可以是一个被很好组织的或非正式的过程。目标可以明示，也可以暗示，如继续保持过去的业绩水平。在公司层面上，目标常常表示为企业的使命和价值。伴随着对企业强势和弱势、机会和威胁的分析，目标最终表现为企业整体战略。总体而言，战略规划是广泛意义上的，与高层次资源的分配和优先利用相关。

更加专门化的目标来自企业的整体战略。企业层面的目标与针对企业不同“活动”更加专门化的目标，如销售、生产和工程，是紧密相关的，以保证彼此的统一。这些低层次目标，或称为操作层面的目标，包括确立目的和实现产品线、市场、财务和利润指标。

通过设立企业层面和操作层面的目标，企业能够确定关键的成功因素。这些是实现目标的关键。关键的成功因素存在于一个企业、商业单位、一项职能、一个部门、或个人。设立目标有利于管理层将重点放在关键的成功因素上，确立业绩衡量的标准。

目标的种类

尽管目标多种多样，还是能确定几个大的分类：

- 经营目标——这些与企业经营的效果和效率有关，包括业绩、赢利目标和保护资产避免损失。它们根据管理层有关组织结构和业绩选择的不同而不同。
- 财务报告目标——这些与编制可靠的公开财务报表有关，包括防止公开财务报告的欺诈。它们主要受外部要求的驱动。
- 遵循性目标——这些与遵守企业适用的法律和法规有关。它们依赖于外部因素，如环境法规，在某些方面对于全企业、或全行业是类似的。

某些目标与企业所从事的业务相关。共同基金必须每日评估净值，而另一个企业只需每季度这样做。所有上市公司必须符合证券交易管理委员会（SEC）的规定。这些外加的目标是通过法律或法规规定的，可归于遵循性目标，或财务报告目标。

反之，经营目标则更多地建立在偏好、判断和管理风格的基础上。它们在各个企业中大有差异，只是因为同样见多识广、能干和诚实的人们可能选择不同的目标。例如，对于产品的发展，有的企业可能选择成为早期的改进者，有的可能是反应迅速的跟随者，还有的可能是反应迟缓的落后者。这些选择会影响研发部门的结构、技能、人事和控制。因此，没有一个对于所有企业都是最优的目标公式。

经营目标。 经营目标与实现企业的基本使命——存在理由——相关。它们包括相关的经营子目标，旨在增强经营效果和效率，推动企业实现最终目标。

经营目标需反映企业经营的特定业务、行业和经济环境。例如，这些目标需与质量的竞争压力、缩短从产品到市场的运做周期或技术变化相关。管理层必须保证目标建立在现实和市场需求的基础上，并用专门术语表示，以利于业绩的衡量。

一套清楚的经营目标和策略，与子目标相联系，是成功的基础。它们提供了企业配置资源的重点。如果一个企业的经营目标不甚清晰，企业资源可能就会被误导。

财务报告目标。 财务报告目标与编制可靠的公开财务报表有关，包括中期

和简略财务报表以及从中提取的公开数据，如利润分配。企业需要实现财务报告目标，来履行外部义务。可靠的财务报表是获得自有资本和债权资本的前提，并对获得补偿合同和应对供应商十分关键。投资者、债权人、顾客和供应商通常借助财务报表来评估管理层业绩并将之与同行业和其他投资机会相比较。

财务报告的“可靠性”这一术语涉及依据公认的或其他相关和适用的会计原则和法规要求来编制公允披露的财务报表，以用于外部目的。公允披露的定义如下：

- 所选择和应用的会计原则已被公认，
- 会计原则应用的环境是恰当的，
- 财务报表对影响其运用、理解和解释的事项已作说明，
- 信息披露以合理的方式进行归类和汇总，既不过分详细，也不过分简略。
- 财务报表应披露出关联的交易和事项。在可接受的范围内披露财务状况、经营成果和现金流量，该范围应在财务报表中合理且实际的得以反映。

公允披露还包括财务报表的重要性概念。

支持以上目标的是企业财务报表中包含的一些声明：

- 存在或发生——在某一时点存在的资产，负债和所有者权益，已记录的交易反映了在一定时期内确实发生的事件。
- 完整性——在一段时期内所有发生的交易和事项都应被确认并已实际被记录。
- 权利和义务——资产是某一时点的权利，负债是某一时点的义务。
- 估价或分摊——资产、负债、收入和费用应按照相关和适当的会计原则正确记录其金额。交易的数量正确，并被正确地汇总和记录在企业的帐表中。
- 披露和揭示——报表中的事项已被正确描述、分类和汇总。

财务报告目标与其他类目标一样，还存在一系列目标和相关子目标。有关财务报表公允披露的要素可视为基本财务报告目标。这些基本目标可得到财务报表声明所代表子目标的支持，而这些子目标又得到企业各种操作目标的支持。

虽然以上关于公允披露和声明的定义是为财务报表而设，但它们至少在概念上也适用于其他公开发行、源自财务报表的财务报告，如期中财务信息和利润分配报告等。当然有些要素对其他公开财务报告并不适用，如披露和揭示要素一般

对利润分配不适用。

遵循性目标。 企业在从事经营和其他特定活动时必须遵守适用的法规。这些要求可能与市场、定价、税务、环境、员工福利和国际贸易相关。法律和法规确定了企业在遵循性目标中规定的最低标准。例如，职业安全和健康法规可能使公司这样定义目标：“依法包装和标注所有药品”。在此例中，政策和程序将与信息传递程序、实地检查和培训有关。

企业遵纪守法的记录——无论是正面的，还是负面的——都会极大地影响企业在社会上的形象。

目标的交迭

一类目标可能与另一类目标之间有交叉，或为其提供支持。例如，“每季度在 10 个工作日内总结”，可能主要是一个经营目标，——用于管理层定期会晤，核查企业业绩。但它也支持定期财务报告和及时向监管机构递送报表。“向车间管理层及时提供原材料生产订单的准确数据”的目标，可能与所有三类目标相联系。这一数据支持关于改变生产订单的决策（经营），促进监督危险的浪费（遵循性），提供成本核算的原始数据（财务报告和经营）。

另一类目标与“资源保护”相关。尽管这些主要是经营目标，某些方面的保护可能归在其他类下。企业资产和其他资源的有效利用，避免资源因偷盗、浪费、无效利用或决策失误（如贱卖资产，信用扩张到高风险水平，未能留住核心人员或专利受到侵占，或发生了预算外的负债）而受到损失，这些都属经营目标。但只要适用了法律和法规要求，这些就可以归属遵循性目标。另一方面，确保任何资产损失都已在财务报表中正确披露的目标又可归属财务报告目标。

一项目标的归类有时取决于环境。继续关于资产保护的讨论，防止资产被偷盗的控制——如在存货周围进行隔离，商品移动的授权得到保管的确认——归属经营目标。这些控制一般与财务报表编制的可靠性不相关，因为任何存货损失可以根据定期实物盘点和与账面记录进行核对来发现。然而，如果出于财务报告的目的，管理层完全依赖永续盘存制记录，通常中期报告都是如此，实物保护控制也归属财务报告类目标。这是因为实物保护控制，连同永续盘存制记录的控制，都被用作保证财务报告的可靠性。

目标分类间的区别和联系可用银行的商业借贷行为进一步表示出来。出于举

例目的，假设存在控制以保证信贷文件包含现有客户的信用历史和业绩数据。在此例中进一步假设银行信贷员在作出借贷决定时并不应用这一信息。相反的，对超过最高信贷额借款的批准，甚至是限制的增加都通过直觉进行。然而，财务管理通过定期复核以确定贷款损失准备的合适水平。在此案例中，对经营的控制存在很大缺陷，而对财务报告的控制却非如此。实际上，这类经营上松散的控制将会导致难以接受的利润成果。最初的端倪可能显示在业绩指标上，然后是较低的利润水平抑或损失——这需要向管理层，如果十分严重，还须向董事会提出调查和行动的需求。这样，财务报告控制可能有利于发现经营缺陷，表明它们的关系，但是缺陷仅存于经营控制中。

联系

目标之间应该是互补和相互联系的。企业层面的目标不仅应该与企业的潜能和未来发展相符，而且必须与各业务部门和职能单位的目标相一致。企业层面的目标须分成一些子目标，这些子目标应与总体策略相符、且和贯穿企业的操作层目标相联系。

只要企业层面的目标与以前的实践和业绩相符，企业操作层目标之间的联系就一目了然。然而，如果目标偏离企业过去的实践，管理层必须注意目标间的联系或承受更大的风险。鉴于目标偏离企业过去的实践，需要一些与新方向相符的业务部门或职能单位子目标就更加重要了。

“通过内部提升来充实更多的管理人员”这一目标很大程度依赖于相互联系的人力资源程序（如接任计划、评估、培训和发展）中的子目标。如果过去的实践大部分依赖外部招聘，那么这些子目标可能要大幅修改。

操作层目标应很清楚，易于理解，以便从事该操作的人能实现其目标。这些目标还必须是可衡量的。人事部门和管理层必须对需要实现什么达成一致，并有方法确定目标被完成的程度。

涉及某一操作目标的范围和效果也是相关的。多数企业为每种操作确定一些目标，从企业层面的目标到与遵循性和财务报告目标相关的标准。例如采购，经营目标可被确定为：

- 购买符合既定工艺规格的产品；
- 谈判取得可以接受的价格和其他条件；

- 每年复核和再次确认重要的供应商。

实现为某一操作设立的所有目标，需要耗费资源；因此将某一操作的整套目标与可获得的资源联系在一起，是有益的。减轻资源限制压力的一个方法是对那些不支持企业层面目标和企业经营过程的操作目标进行提问。通常，一个职能单位可能有一些从过去实践继承的不相关目标（如编制常规的但却无用的月报）。

还有一个平衡目标和资源的方法是分出那些对实现企业层面目标至关重要的操作目标。并非所有目标的重要性都是一致的，因此一些企业将目标区分优先次序。企业可能认为某些操作目标是关键，密切关注与这些目标相关的操作。这一主张反映了前面讨论的“关键的成功因素”概念，这一概念认为“必须做正确的事”以使企业目标得以实现。

目标的实现

如前提及，确立目标是有效内部控制的前提。目标提供了指导企业活动前进的可度量的目的地。虽然企业应对某些目标的实现有合理保证，但并非对所有的目标都是如此。

如同第一章所讨论的，有效的内部控制应对企业财务报告目标的实现提供合理保证。类似的，对遵循性目标的实现也应提供合理保证。这两类目标主要建立在独立于企业目的的外部标准的基础之上，因此其实现大部分在企业控制之内。

但经营目标则有所不同。首先，它们并非建立在外部标准之上。其次，企业可能按照预期运行，却可能因竞争者而脱离运行轨迹。它还可能受不可控制的外部事件的影响——政府的变化，恶劣的天气等。企业甚至可能在目标制定的过程中考虑到这些因素，将其视为低概率因素，并准备了应急计划。然而，这样的应急计划仅仅减轻了外部事件的影响，并不能确保目标的实现。为实现目标的良好经营并不能确保成功。

在合理保证的范围内，内部控制的目标主要关注于：培养贯穿整个企业的目标的一贯性，辨别主要成功因素和及时向管理层报告业绩和期望。虽然不能确保成功，管理层应能合理保证——当目标存在不能实现的危险时可及时得到警告。

风险

识别和分析风险的过程是一个重复不断的过程，并且是有效内部控制制度的关键组成部分。管理层必须密切关注企业各层次的风险并采取行动来管理风险。

风险识别

企业的经营可能因内部或外部的因素而存在风险。而这些因素，又能影响明示或隐含的目标。如果目标日益偏离过去的表现，风险便随之增加。在一些行为领域，企业因考虑到所能接受的行为，常常不设立明示的企业层面目标。虽然在这些情况下，可能没有一个明示或书面的目标，但却有一个暗示的目标——“无变化”或“就象这样”。这不意味暗示的目标不存在内部或外部的风险。例如，一个企业可能认为其对顾客提供的服务是可以接受的，但由于竞争对手做法的改变，其服务在客户看来，却可能恶化了。

无论一个目标是明示或隐含的，企业风险评估的过程都应考虑到可能发生的风险。风险识别应是全面而复杂的，这很重要。它必须考虑企业和相关外界之间的所有重大相互影响，包括有关商品、服务和信息等。这些外界包括潜在和现有的供应商、投资者、债权人、股东、雇员、客户、买方、中介、竞争对手、公共机构和新闻媒体。

风险识别是一个重复的过程并与计划过程紧密结合。利用“白纸”法来考虑风险也是很有益的，而不仅将风险与过去的回顾相联系。

企业层面。企业层面的风险来自于外部或内部因素。包括：

外部因素

- 技术发展会影响研究的性质和时机，或带来采购的变化。
- 不断变化的客户需求和期望会影响产品开发、生产流程、客户服务、定价或保修。
- 竞争会改变企业营销或服务活动。
- 新的法律和法规可能要求经营政策和策略的改变。
- 自然灾害可能导致经营或信息系统的改变以及强调对或有损失制定应急计划的需要。
- 经济形势的变化可能对有关融资、资本支出和扩张的决策产生影响。

内部因素

- 信息系统运行的中断会对经营产生负面影响。
- 雇员的素质和培训、激励的方法可能对企业中的控制理念产生影响。
- 管理层职责的改变可能影响实施某些控制的方式。

- 企业经营活动的性质、员工对资产的接触途径可能对资源的挪用产生影响。
- 非强硬的或无效的董事会或审计委员会可能为轻率的行为提供机会。

有许多技巧被发展用于识别风险。其中多数——尤其是那些被内外部审计师发展用于确定审计业务范围的技巧——涉及将风险排列优先次序以及识别更高风险行为的定量或定性的方法。其他实践包括：对影响企业业务的经济形势和行业因素的定期复核，高层管理人员的商业计划会议以及与行业分析师的会晤。识别风险与企业的短期、长期预测和战略规划密切相关。企业选择何种方式识别风险并不特别重要。重要的是管理层必须仔细考虑那些导致或增加风险的因素。一些需要考虑的因素包括：过去未能实现目标的教训；人员素质；影响企业的变化因素，如竞争、法规、人事等；地理上业务活动的分散程度，特别是国外业务；某一业务活动对企业的重要性；以及业务活动的复杂性。

举例说明：一个服饰和鞋类的进口商确定了企业层面的目标为成为高质量时尚商品的行业带头人。在企业层面需要考虑的风险因素包括：供应商资源：国外制造商质量、数量和稳定性；外汇汇率变动的风险；运输的及时性和海关检查延误带来的影响；运输公司的有效性、可靠性和成本；国际敌视和贸易禁运的可能性；以及在外国的当地政府采取了不接受的政策时，客户和投资者抵制经营活动的压力。还有一些需考虑的更具一般性的风险，如经济条件恶化的影响，产品的市场接受度，企业市场上出现新的竞争者，以及环境或监管法规的变动等。

识别企业层面的导致风险的内、外部因素对有效的风险评估非常重要。一旦确定了主要的风险因素，管理层就可以考虑它们的重要程度，并尽可能将这些风险因素与业务活动联系起来。

操作层面。除了识别企业层面的风险外，还应识别操作层面的风险。应对这个层面的风险有助于将风险评估的重点放在重要的业务和职能部门上，如销售、生产、营销、技术发展和研究开发。对操作层面风险的成功评估还有助于将企业层面风险保持在可以接受的水平。

许多例证表明，针对明示或隐含的目标，可以识别很多不同的风险。如在采购循环中，企业可能有一个与保持充足原材料存货相关的目标。未实现这一操作目标的风险可能包括商品不符规格，或送来的订货数量不足、不及时、价格不合

理等。这些风险可能会影响与供应商沟通订货规格的方式，产品预测的适当性及其利用，确定其他供货源和进行谈判等。

未能实现目标的可能原因包括明显或模糊的、对企业潜在影响重要或不重要的风险。当然，那些对企业有重大影响、明显的风险应该识别。为了避免忽略相关风险，这类风险识别最好和风险发生可能性的评估分开。然而风险识别过程具有现实的局限性，而且划定界限、确定在哪里是很难的。考虑流星坠落到公司生产设备上的风险是荒唐的，但考虑飞机坠毁对机场跑道附近设备的影响却是合理的。

风险分析

识别企业层面和行为层面风险后，企业需要进行风险分析。风险分析的方法多种多样，主要因为许多风险难以量化。不管怎样，风险分析的过程——可能多少有些正式——通常包括：

- 估计风险的重要性程度；
- 评估风险发生的可能性（或频率）；
- 考虑如何管理风险——即评估需要采取何种措施

对企业无重大影响的风险和发生概率较低的风险通常无须仔细的考虑。相反，具有较高发生概率、影响重大的风险常需要周详的考虑。间于两者之间的情况需要较难的判断。合理而详实的分析是重要的。

有很多方法用于评估已识别的风险带来的损失成本。管理层应对之了解，并恰当地应用它们。然而，很多风险无法确定其规模。它们至多只能被描述为“大的”、“中的”、或“小的”风险。

一旦评估了风险的重要性和发生概率，管理层需要考虑如何管理风险。这涉及基于对风险假设的判断，以及对降低风险水平所需成本的合理分析。降低重大的或可能发生的风险的措施包括管理层每日做出的无数决策，从确定其他供货源或扩大产品线到获取更具相关性的经营报告或改进培训计划等。有时措施会实实在在消除风险或抵销其影响。如价值链的垂直整合以降低供应风险、金融风险的套期保值和取得充分的保险等。

注意：风险评估，作为内部控制的组成部分，与计划、程序或其他管理层认为必要来处理风险的行为是有区别的。这些行为，如同前面所讨论的，是更大范

围管理过程的一部分，而非内控系统的组成部分。

与管理风险的行动联系在一起，是确立程序使管理层能对这些行动的执行和效果予以追踪。例如，企业一项用于防范电脑服务损失风险的措施就是制定一个系统灾难恢复计划。然后实施相应的程序以确保计划制定和执行适当。这些代表“控制活动”的程序将在第四章讨论。

在制定附加的程序之前，管理层应仔细考虑现有程序对于控制已识别的风险是否合适。因为程序可能满足多重目标，管理层可能发现一些附加的行动得不到保证；现有程序可能已经足够或需要执行得更好。

管理层还应认识到可能总会存在一些残留的风险，不仅因为资源总是有限的，还因为每个内控系统都有内在局限性。这些将在第七章讨论。

风险分析并非只是理论上的。它通常对企业的成功很重要。当它涵盖了所有重大业务过程中的风险识别时，最为有效。它可能涉及过程分析，如主要依赖方面和关键控制点的识别、确定明晰的职责。有效的过程分析特别关注组织内的横向关联，对例如数据的来源、储存、如何转化为有用信息和谁使用这些信息加以识别确认。大型组织特别需要警惕公司内部和公司之间的交易和主要关联。这些过程可能会受到质量规划的积极影响，质量规划一旦被雇员广泛采纳，可成为风险防范的重要组成部分。

不幸的是，有时风险分析的重要性被认识得太晚了，正如一家知名金融服务公司的高级管理人员所说的一句名言：“我们只是没有意识到面临这么多风险。”

应对变化

经济形势、行业和法规环境不断改变，企业业务活动不断发展。在一个环境下有效的内部控制在另一环境下未必有效。风险评估的本质就是一个识别变化的环境并采取相应行动的过程。

因此，每个企业都需要一个正式或非正式的过程，来识别那些对企业实现目标的能力有重大影响的外部环境。如同第五章中进一步讨论的，该过程的关键部分涉及发现、处理和报告有关事件、活动和环境信息（这些显示了企业需要应对的变化）的信息系统。这些信息可能涉及客户偏好的变化或其他影响对公司产品和服务需求变化的因素。或者，可能涉及影响生产流程或其他业务活动的新技术，或竞争、立法、监管等方面的发展变化。一旦所需的信息系统到位，就能建立对

变化环境进行识别和反应的过程。

这一过程可能与以上讨论的企业常规的风险评估过程相平行或成为其中一部分。它涉及对已变化的条件进行辨认——这需要有一个机制来识别和传递那些影响企业目标的事件或行为——以及分析相关的机会或风险。这种分析包括识别促使目标得以完成或失败的原因，估计原因出现的概率，评估对目标实现的可能影响，以及考虑风险能被控制或机会得以利用的程度。

虽然企业应对变化的过程类似于常规的风险评估过程，我们仍对其单独讨论。这是由于其对有效内部控制的重要性和因其容易被忽略或在处理日常事项的过程中未给予充分关注。

要求特别关注的情形

应对变化建立在这样的前提上：由于其潜在的影响，某些条件应给予特别考虑。当然，这些条件需要管理层关注的程度有赖于在特定环境中可能产生的影响。这些条件有：

- 已改变的经营环境——已改变的法规或经济环境会带来日益增加的竞争压力和大大不同的风险。如电信行业“垄断”废除、经纪行业佣金率解除管制等都会将企业推进大大改变的竞争环境中。
- 新人事——新来的高层管理人员可能不理解企业文化，或仅关注业绩而忽略与控制相关的企业活动。在缺乏有效培训和督导的情况下，人员的高度流动容易导致企业的瘫痪。
- 新的或经修订的信息系统——通常在发展新系统，尤其是在时间限制特别紧时，容易使控制失效——例如：为了赢得竞争优势或战术出击（而建立新的信息系统）。
- 迅速增长——当经营快速扩张，现有制度的局限可能导致控制失效；当程序变动或新人员增加时，现有的监控可能就不能保持充分的控制。
- 新技术——当新技术被运用到生产流程或信息系统中，内部控制就很可能需要修改。例如，适时（JIT）存货制造技术就需要改变成本系统和相关的控制以确保及时报告有效信息。
- 新业务、产品、活动——当企业进入新的商业领域或从事不熟悉的交易时，现有的控制可能就不足够了。例如银行，进入其少有经验的风险投资或

贷款领域时，就不清楚如何控制风险。

- 公司重组——重组——或出于杠杆收购，或出于企业业绩下滑或出于成本降低规划——可能伴随裁员和非充分监督和职责分割。或者，一项关键控制功能工作消失而替代的控制尚未到位。很多公司很晚才意识到其大规模的裁员未充分考虑控制因素。

- 海外经营——海外经营的扩张或收购带来了新的和独特的风险。例如，控制环境可能受到当地管理层文化和风俗的影响。另外，当地经济和法规环境可能带来独特的风险因素。抑或，未能建立很好的到达所有人的沟通渠道和信息系统。

机制

必须建立识别任何重要假设或条件已经或将要发生的变化机制。这些机制不一定要很精细，通常在小企业中是很不正式的。一个制造丝印机器的小公司，所有者-经理每月与销售、财务、采购、制造和工程部门负责人会谈，通过几小时的会谈，了解技术、竞争对手行为和新的顾客需求，并分析风险和机遇，为每一业务活动迅速制订行动计划。措施会立即得到执行，所有者-经理则每周和每月追踪每项业务活动，直接督导措施实施的方式，以及观察市场变化是否得到充分应对。

预见

为达到切实可行，机制必须有预见性，以使企业能预见重要的变化并作好规划。需有早期报警系统以识别那些警示新风险的数据。例如，某一商业银行，运用包含各学科的“风险委员会”来分析正在发展的新产品对银行的风险。类似的，需要有从变化的环境中早期识别机遇的机制。那些意识到客户对 8 小时外银行和交互式电子计算机系统的需求日益兴起的银行，就能通过安装对客户友好的自动银行机器网络和进行有效市场推广，来显著扩大其金融市场的客户份额。

自然，越早地识别那些影响风险和机遇的变化，就越有可能采取措施来有效地应对它们。然而，和其他控制机制一样，不得不考虑相关的成本。没有一个企业具有足够的资源来获得和全面分析所有对其产生影响的不断变化的环境信息。更进一步地说，由于没有人拥有能准确预测未来的水晶球，即使具有最具相关性的现时信息，也不能保证能够精确地预测未来的事件或获得暗示。通常很难分辨

出看似重大的信息是一个重要趋势的开始，还仅仅是一次失常。

相应地，应具备合理的机制来预测影响企业的变化，这有助于避免迫近的问题和利用将来的机遇。没有人能肯定地预测未来，但企业越能预见到变化及其影响，就越能减少不愉快的意外事件。

中小型企业的应用

小企业的风险评估过程较之大企业，更加不正式和更缺乏组织性，内部控制要素的基本概念应适用于各种规模的企业。小企业应该确立目标，尽管这些目标可能是隐含的，而非明示的。由于小企业更加集权和具有较少的权力等级，企业目标可以更易于和有效地向低层管理层传递，而且更直接和更连续。类似的，企业层面目标和操作层面目标之间的联系也常常是清晰和直接的。

识别和分析那些阻碍企业目标实现的风险的过程通常包括高层管理人员直接向雇员和外界获取信息。一个所有者-经理可通过与客户、供应商、银行、律师、独立审计师和其他外界的联系而直接获知由外部因素带来的风险。总裁可通过和各级人员的直接交流直接获知来自内部因素的风险。由于总裁和其他关键管理人员对企业的深入参与常常意味着风险是由那些既能接触到适当的信息，又能正确理解其含义的人进行评估的，因此小企业的风险评估可能特别有效。

小企业对日常风险和那些源自显著变化的环境（如新法规，经济低迷或产品线扩大）的风险的管理机制可能高度非正式却很有效。总裁与提供有助于风险识别的信息的部门负责人、外界之间的非正式会谈，也提供了分析风险和制定风险管理决策的论坛。总裁可以和有限的人员一起迅速修订行动计划。类似的，总裁或其他关键管理人员参观一些重要的部门或与顾客或供应商交谈以回应其需求，都可以使相应的措施非常迅速有效。他们进一步根据需要进行追踪，以确保必要的行动得以落实。

评估

评估者会重点关注管理层设立目标、风险分析和应对变化的过程，包括它们的联系和与业务活动的相关性。下面所列的是评估者可能会考虑的事项。这一列示并非涵盖了全部，也不是对每个企业都适用；但是，可以作为一个起点。

企业层面目标

- 企业层面目标对企业需要实现什么提供充分广泛声明和指导，且足够明确并直接与本企业相关。

- 企业层面目标向雇员和董事会传递的有效性。
- 企业层面目标和企业策略的相关性和一致性。
- 企业计划和预算与企业层面目标、战略规划和现时条件的一致性。

操作层面目标

- 操作层面目标和企业层面目标以及战略规划之间的联系。
- 操作层面目标之间的一致性。
- 操作层面目标与所有重大业务流程的相关性。
- 操作层面目标的专属性。
- 与目标相关的资源的充分性。
- 识别对实现企业层面目标的重要目标（关键成功因素）。
- 各级管理层对制定目标的参与及其对于目标的义务。

风险

- 识别来自外部风险的机制的充分性。
- 识别来自内部风险的机制的充分性。
- 识别与每个重大操作层面目标相关的重要风险。
- 风险分析过程的周详性和相关性，包括估计风险的重要性程度、发生概率和决定所采取的措施。

应对变化

- 存在机制，对影响企业或操作层面目标实现的日常事件或行为进行预测、识别和反应（通常由负责那些最受变化影响行为的经理来执行）。
- 存在机制，对那些于企业有巨大和深远影响，可能需要高层管理人员关注的变化进行识别和反应。

第四章 控制活动

本章概要：控制活动指为确保管理层指示得以执行的政策和程序。它们有助于保证采取必要措施来管理风险以实现企业目标。控制活动贯穿于企业的所有层次和部门。它们包括一系列不同的活动，如批准、授权、查证、核对、复核经营业绩、资产保护以及职责分工等。

控制活动包括政策和程序，是人们执行政策的行为，用以保证管理层进行风险管理的必要指示得以执行。控制活动依据与之相关目标的性质可分为三类：经营性，财务报告，或遵循性。

虽然一些控制活动仅与某一方面有关，但是控制活动之间常常是相互联系的。根据情况的不同，一项特定的控制活动可能有助于实现企业不止一类的目标。因此，经营控制也可能有助于保证可靠的财务报告，财务报告控制也可能对遵循性目标产生影响。

例如，一位零件分销商的销售经理，为了及时了解某些商品和地区的销售情况，每日从地区负责人那里取得最新的报告。因为销售经理会将该信息与会计系统中的销售纪录和销售员奖金相联系，所以，这一控制活动既与经营目标，又与财务报告目标相联系。又如：在一个连锁店里，顾客返回的商品贷记通知单，通过连续编号来控制，并为财务报告的目的进行汇总。这一汇总纪录还为商品经理提供了按商品分类的分析，用于未来的购买决策和存货控制。这个例子控制活动主要为财务报告的目的而设立，兼顾了经营性目标。

虽然这些分类有助于讨论内部控制，但与某一控制活动在实现某类特定行为目标时所起的作用相比，控制活动的分类并不重要。

控制活动的类型

有许多关于控制活动类型的不同描述被提出，包括防止性控制、检查性控制、手工控制、计算机控制和管理性控制等。控制活动可按照控制目标进行分类，如保证数据处理的完整性和准确性。下面介绍一些适用于组织中不同层次职员进行的通用控制活动，用来说明控制活动的范围和多样性，而非任何分类的建议。

- 高层复核——复核是指相对于预算，预测，前期和竞争对手的实际业绩情况。企业主要的行为应被追踪以衡量目标实现的程度，如营销推动，改进的生产流程、成本限制或削减计划等。同时还要对新产品开发、合资或融资

等计划的执行加以监控。管理层采取的分析和追踪这类报告的行为就代表了这一控制活动。

- 职能指导或业务管理——职能或业务部门的经理们复核业绩报告。例如：负责银行客户贷款的经理复核（间接地）按部门、地区和贷款类型分类的报告，核对汇总，辨别趋势，并将结果与经济统计数据和目标相对比。依次地，部门经理收到按贷款人员和当地客户分类的最新交易的数据。部门经理还关注遵循性事项，如复核监管机构要求出具的关于超过规定数额的新存款的报告。核对每日现金流与账面净头寸并报告中央部门，以进行隔夜拆借和投资。

- 信息处理——这类控制被用于核对交易的准确性、完整性和遵循性。记录的数据应与支票和经批准的控制文件相符。例如，客户订单，只有与经批准的客户文件和信贷限额相符，才能被接受。交易应按顺序编号记账。交易的总额应与前期的余额和控制帐户核对一致。需要追踪的例外事项应由行政职员实施，且必要时向监控者汇报。新系统的开发和现有系统的改变应进行控制，如数据、文件和程序的接触途径。下面还将进一步讨论对信息处理的控制。

- 实物控制——设备、存货、证券、现金及其他资产实物应得到保护，并定期进行盘点和帐实核对。

- 业绩指标——将不同类的数据——经营或财务的——联系起来，连同关联性分析、调查和改进行为，构成了这一控制活动。业绩指标包括，如采购价格差异，紧急订货的比重，以及退货占总订货的比重等。通过对非预期结果和非正常趋势的调查，管理层认识到主要的采购业务目标可能无法实现的具体情形。管理层运用这一信息，是仅用于经营决策，还是也追踪财务系统报告的非预期结果，决定了业绩指标的分析仅用于经营性目的，还是也用于财务报告控制目的。

- 职责分离——职责在不同人们之间进行分工或分离，是为了降低发生错误或不当行为的危险。例如，交易的授权、记录和处理相关资产的职责应予以分离。授权赊销的经理应不负责应收账款的记录或现金收入的处理。类似的，销售人员应没有修改价格文件或佣金率的权力。

以上只是企业每日实施的无数程序中的少数几种，它们用于促使企业行为符

合既定计划，保证企业向其完成目标的既定轨道中前进。

政策和程序。控制活动通常包含两类要素：确定应该做什么的政策（作为第二个要素基础）和实现该政策的程序。例如，政策可能要求证券交易商的营业部门经理复核客户交易行为。而程序是复核行为本身，必须及时进行，并关注政策里提及的因素，如所交易证券的性质和数量以及与客户证券净值和年纪之间的联系。

很多时候，政策以口头形式传达。当政策是长期存在和被广泛接受的，以及在沟通渠道只涉及有限的管理层、人员之间联系密切、易于监管的小企业中，非书面的政策也可以是有用的。不管政策是否是书面的，必须被仔细地、尽责地、一贯地执行。如果程序只是机械地被执行，而对政策的方向没有一个敏锐、持续的关注，那么也是没有益处的。

进而，调查执行程序中发现的情况并采取适当的纠正措施，是很关键的。追踪活动由于企业规模和组织结构的不同而千差万别。它们包括：从大公司正式的报告程序——部门阐述为何目标未能实现以及采取何种措施避免这类情形重复发生——到小企业的所有者-经理走出大厅与车间经理讨论哪里出错并需要做什么。

与风险评估结合

在风险评估同时，管理层为了管理风险，应确定相应的行动并使之有效。被确定用于管理风险的行动也用于重点关注控制活动是否已经到位，以有助于确保正确、及时地执行这些行动。

例如，一公司制定了“实现或超过销售目标”的目标。已识别的风险包括对现有和潜在顾客的需求了解不充分。管理层对付风险的措施包括确定现有客户的购买历史和实施新的市场调查。这些行为也是确定控制活动的关键点。

控制活动很大程度上是企业尽力实现其商业目标的过程的一部分。控制活动不单纯出于自身的原因或因为它看上去是“正确的应该”去做的事。在此例中，管理层需要采取步骤以保证销售目标得以实现。控制活动是用于管理目标实现的机制。这些行为可能包括跟踪既定时间段的客户购买历史发展的过程，以及确保报告数据准确性的措施。在此意义上，控制直接进入了管理过程。

信息系统的控制

随着对信息系统普遍的依赖，需要对这些系统进行的全面控制：财务的、遵循性的、经营性的，大的和小的系统。

大多数企业，包括小公司或大公司的部门，都运用计算机进行信息处理。因此，下面的讨论适用于包括手工和电算化因素的信息系统。对那些严格手工操作的信息系统，需要应用不同的控制；这些控制虽然不同，却建立在相同的控制理念的基础上。

可以运用两大类的信息系统控制活动。第一类是一般性控制——适用多数应用系统并协助确保其持续、正确地运行。第二类是应用性控制，包括应用软件中的电算化步骤，以及用以控制不同种类交易处理过程的相关手工操作程序。总之，这些控制用于保证财务和其他信息系统的完整性、准确性和遵循性。

一般性控制

一般性控制通常包括对数据中心操作、系统软件的购买和维护、数据入口安全、以及应用系统开发和维护的控制。这些控制适用于所有系统——大型机、小型机和终端用户的计算机环境。

数据中心操作控制。这包括工作设定和时间安排、操作员行为、后台支持和恢复程序、以及或有事件或灾害补偿计划。在一个复杂陈旧的环境中，这些控制还涉及容量规划和资源分配与利用。在一个高科技环境中，工作时间安排是自动的，工作控制语言是在线的。储存管理工具自动将数据文件卸载到高速驱动器中，并期待下一项工作。移动网络超级用户不再需要手工记录控制台日志，因为它不是打印出来的；而是保持在系统中。在一个联合控制台上每秒钟闪现的几百条信息支持了众多的大型机。小型机则不用关照地日夜运转。

系统软件控制。这些控制包括对系统软件——操作系统、数据库管理系统、通信软件、安全软件和系统工具（具有运行系统和支持应用系统的功能）——有

效采购、运行和维护。系统活动的主要指导者，系统软件也提供系统日志、追踪和监控功能。系统软件可以报告应用工具的使用，因此如果有人进入强大的数据修改功能，至少它们的使用情况被记录下来并形成报告供复核之用。

入口安全控制。随着通信网络的成长，这类控制日益重要。系统的用户可能远在世界那端，也可能就在厅外。有效的入口安全控制能保护系统，防止不当进入和系统的非法授权使用。如果设计良好，还能拦截黑客和其他侵犯者。

充分的入口控制措施，如经常更换拨号数字，或运用回拨——该系统让潜在用户返回授权数字，而非允许直接进入系统——可以有效防止非授权的进入。入口安全控制将授权用户限制在其工作必需的应用系统或应用功能中，支持适当的职责分工。对允许或限制进入的用户界面应经常及时查看。前任或不满的职员相对黑客可能更加危险；终端雇员密码和用户代码应立即改变。通过防止非授权使用和更改系统，数据和程序的完整性得以保护。

应用系统开发和维护控制。应用系统的开发和维护对多数企业而言一度是高成本领域。全部成本包括管理信息系统（MIS）资源、所需的时间、人们完成任务所需的技巧、以及所需的硬件和软件等都必须考虑到。为控制这些成本，许多企业形成一定形式的系统开发方法论。它提供了系统设计和运用的结构，概述了特定的阶段，将需求文件化，通过设定批准和核对点来控制项目的开发或维护。该方法论应提供有关系统需求变更的适当控制，这可能包括对需求变更的必要授权、对变更的检查、批准、结果测试和实施草案，以保证正确地实施变化。

系统内部开发的另一选择是使用软件包，这一方法日渐流行。销售商提供灵活性的、集成的系统，允许通过利用系统的嵌入式选择为客户量身定制。很多系统开发方法将购买软件包视作一种开发的可选方案，并包括必要的步骤以提供有关选择和实施流程的控制。

应用性控制

如同名字所示，应用性控制被设计用于控制应用过程，协助保证交易处理的完整性、准确性、交易授权和有效性。特别需要注意应用系统的有关接口，因其常与其他系统相连，而这些系统也需要控制，以保证所有用于处理的信息适当地输入和输出。

计算机对控制的一个最有意义的贡献就是其防止错误进入系统的能力，以及

一旦错误存在，及时加以发现和改正的能力。鉴于此，许多应用性控制依赖于计算机的编辑核对功能。这包括数据的格式、存在性、合理性和其他检查，这些功能在开发应用系统时已经内置其中。如果这些系统的数据检查功能设计正确，它们就能在数据录入系统时协助提供控制。

一般性控制和应用性控制之间的关系

这两类对计算机系统的控制是相互关联的。一般性控制用于保证建立在计算机程序基础上的应用性控制得以实施。

例如，应用性控制，如计算机匹配和编辑检查功能对数据的在线录入进行测试。当数据不匹配或格式错误，它们可以提供及时的反馈，以便作出修改。它们显示出错信息，说明数据哪里出错，或编制例外事项报告以便进行跟踪。

如果没有充分的一般性控制，也就不可能依赖应用性控制，因为，应用性控制的前提是假设系统本身运行良好，与正确的文件相匹配，或所提供的出错信息准确反映了问题所在，或在例外事项报告中包括了所有的意外。

另一个表明需要在应用性控制和一般性控制之间寻求平衡的例子是完整性控制，它通常在某类涉及预先编号文件的交易中使用。这些通常是内部产生的文件，如采购订单就运用了预先编号的形式。复印件将被标出或不能被接受。为了使这种控制有效，按照其设计，系统将拒绝不正确的事项或对之悬而不决，而用户则得到一个列示所有丢失的、复制的和范围之外事项的报告。那么，那些需要依靠报告内容进行追踪调查的人，怎能知道报告中所有应该列示的项目都已经如实列示了呢？

答案就是一般性控制。对系统开发的控制要求对应用程序进行仔细的复核和测试，以保证报告程序具有严密的逻辑性，以及测试确定所有的例外事项得到报告。为了提供应用程序执行之后的控制，入口安全和系统维护控制保证了应用程序没有遭受非法进入或修改，而是得到了所需的授权修改。数据中心运行控制和系统软件控制保证了文件的正确地运用和适当地更新。

应用性控制和一般性控制之间的关系是：一般性控制用于支持应用性控制的功能，两者都用于保证信息处理过程的完整性和准确性。

正在发展的问题

出于对许多新兴技术影响的考虑，提出了新的控制问题。这包括 CASE（计

计算机辅助软件工程)开发工具,依据原型创建新系统,图像处理和电子数据交换。这些科技将影响如何实施控制的方式,但并未改变控制的基本要求。

例如,在最终用户电脑化(EUC)中,功能日渐强大的微机和日益便宜的小型机能够传送数据和具有强大的计算能力。一些部门和生产单位常常通过独立的、低成本的局域网自行进行电子处理。这些属于用户维护的系统,而非集中开发的软件。

为了提供EUC系统所需的控制,需要实施和加强有关系统开发、维护和运行的企业层面政策。局域网的处理环境应由类似于更传统的大型机环境水平的控制活动加以管理。

一个正在兴起的技术是人工智能或专家系统。将来,由于这样的系统包含在许多应用程序中,——无论是由数据处理部门或最终使用者进行开发抑或外购——问题将包括如何决定哪种应用程序最合适,应该运用哪种工具以及如何控制开发。许多人认为这类系统最终会以与目前的最终用户电脑化同样的方式进行控制。当EUC最初盛行时,人们也提出了同样的问题,但最终还是意识到控制仍以与以前同样的方式进行:即通过适当的控制活动。

企业特殊性

每个企业具有自身的一套目标和实施策略,因此在目标的结构和相关控制活动上存在不同。即使两个企业具有同一的目标和结构,其控制活动也会不同。每个企业由不同的人管理,他们在实施内部控制时会运用个人判断。而且,控制反映了企业经营的环境和行业,及其组织的复杂性、历史和文化。

企业经营的环境影响了其面临的风险,这些风险将被披露并可能应唯一的外部报告要求或特殊法规要求而呈现。例如,一家药品制造商较之一般服务性公司必须管理更大的环境风险,并在财务报告披露中考虑废物处理问题。

企业的复杂性及其活动的性质和范围,也影响其控制活动。行为多样的复杂组织较之行为单一的简单组织,可能面临更困难的控制问题。分权经营的企业将重点放在地区自治和改革上,较之高度集权的企业,具有不同的控制环境。其他影响企业复杂性和控制性质的因素包括:地区地理分布、经营的广泛性和复杂性,以及信息处理方法等。

所有这些因素影响企业的控制活动,控制活动需依不同因素相应制定,以实

现企业的目标。

对中小企业的应用

小组织中控制活动包含的概念不可能与大组织相差太远，但是控制活动实施的正式程度却有所差异。进而，由于中小企业管理层所实施的高度有效的控制，其可能发现有些类型的控制活动并非总与之相关的。

例如，总裁和其他关键管理人员直接参与新的营销计划，掌握赊销授权，重大购买和信贷额度的动用，为这些活动提供了强有力的控制，减少或消除了对更详细控制活动的要求。他们还直接了解对主要顾客的销售，仔细复核主要比率和其他业绩指标，这些控制的目的常常与大公司内典型的低层控制活动的目的相吻合。

职责的适当分离，至少在表面上，对小企业似乎有些困难。然而，即使只有几个人的公司，也通常将职责分开以实现必要的检查和制衡。如果这样做不可能——有时确实是实情——那么老板对不相容职务的直接监督，也能提供必要的控制。例如，为了对付不当的现金支付，老板作为支票的唯一授权签名人，或要求将每月银行对账单直接未拆封地寄给他，以核对已经支付的支票，这些情况在小企业中也是很常见的。

信息系统的控制，尤其是一般性电脑控制和入口安全控制，在中小型企业中可能会有些问题。这是由执行控制活动的非正式方式带来的。再次，从中小型企业内高层管理者的大量直接参与控制活动中，也可以找到答案。发现重大错误的合理保证常来自管理层对系统所产出信息的持续运用，并将他们对控制活动直接掌握的信息与其他人实施的关键措施的相联系。

评估

必须按照管理层针对企业每项重要业务的既定目标而做出的风险管理的指示，对控制活动进行评估。因此，评估者将考虑控制活动是否与风险评估过程相关，以及它们是否恰当地保证了管理层的指示得以实施。这种评估将针对每项重大的业务活动，包括对计算机信息系统的一般性控制。（这些将是在评价风险评估中确认的每项活动——见第三章）评估者将不仅考虑确定的控制活动是否与风险评估过程相关，而且还考虑它们的应用是否正确。

第五章 信息和沟通

本章概要：相关的信息必须以一种能使人们行使各自职能的形式和在一定的时限内被识别、掌握和沟通。信息系统产生的报告，包括使企业的运营和控制成为可能的经营性的、财务的以及与合规性相关的信息。信息系统不仅处理内部生成的资料，而且还处理形成企业决策和外部报告所必须的、关于外部事件、行为和条件的信息。有效的沟通还必须广泛的进行，要遍及组织的各个方面。所有人员都要从高级管理层获得清楚的信息：控制职能必须被认真对待。他们必须明白各自在内部控制制度中的角色，明白个人的行为如何与他人的工作相联系。他们必须有自下而上传递重要信息的方法。在与象顾客、供应商、监管者和股东这样的外界之间，也必须有有效的沟通。

每个企业都必须获取相关的信息——财务及非财务的，与外部及内部事件和行为相关的信息。信息必须经过管理层确认与企业的经营相关。这些信息也必须以一种能使人们行使各自的控制和其它职能的形式和在一定的时限内传递给需要的人。

信息

为了业务经营和达成企业所有类别的目标——经营的、财务的和合规性的目标，组织的各个层次都需要信息。信息被多元应用。比如，财务信息不仅被运用于编制公开的财务报表，它也被用来制定决策，监控业绩和资源分配。以货币或其它度量为单位的管理层报告使得对品牌的盈利能力、按顾客类型划分的应收帐款、市场份额、顾客投诉倾向和统计意外事故之类的监控成为可能。可靠的内部财务指标对于计划、预算、定价、评估供应商的业绩、评价合资企业和其它联合体也很关键。

同样，经营信息对编制财务报表很关键。这包括常规的（采购、销售以及其它的交易）以及有关竞争对手的产品发布和经济环境的信息——这些信息会影响存货和应收帐款估价。要想实现合规性的和财务报告方面的目标，需要诸如在空气中的颗粒排放情况或人事的信息。因此，由内部或外部的来源产生的信息，无论是财务的还是非财务的，都与所有目标相关。

信息由信息系统来识别、掌握、加工和报告。“信息系统”这个词经常用于

处理与交易相关的内部生成的资料——例如采购、销售以及象生产过程之类的内部经营行为。信息系统——可能是电子化的，手工的，或二者结合的——当然涉及上述事物。但用在这儿的却是一个更广义的概念。信息系统也处理关于外部事件、行为和条件的信息。这些信息包括：表明企业生产或服务需求变化的市场或行业的专门经济资料；有关企业生产过程所需要的货物和服务的资料；对于包括顾客的偏好或要求的市场调查；有关竞争对手的产品发展行为以及新设的法律和法规的信息。

信息系统有时以监管的方式运行，以例行地获取特定的数据。在另外一些情况下，需要采取特殊的行为来获得信息。设想一下诸如获取有关顾客对企业产品满意度的信息系统。信息系统可能会例行的按产品和地区报告销售情况，顾客的损益、退货和折扣的要求，产品保修条款的兑现，以及投诉或其它评价形式的直接反馈。另一方面，有时可能会作出一些特殊的努力来获得关于技术产品规格或顾客对于送货或服务要求的信息。这类信息可以通过问卷、采访、广泛的市场需求的调研或针对特定群体的调查获得。

信息系统可以是正式的或非正式的。与顾客、供应商、监管者以及员工的谈话经常会提供识别风险和机遇所必需的重要的信息。同样，参加专业或行业的研讨会或贸易团体以及其它的组织也可以提供有价值的信息。

当企业面临基本的行业变化，面临有高度创新能力反应迅捷的竞争对手或面对重大的顾客需求变化时，保持信息与需求间的一致性就变得至关重要。信息系统必须变化，以支持产生新的企业目标比如，与缩短产品投放市场周期、外包特定的职能，以及生产人员的变化有关的目标。在这样的情况下，特别需要把早期的预警指标同严谨的历史会计数据分开。这两者都很重要，而后者当被有效运用时也能提供告警信号。但为了做到有效，信息系统不仅必须识别和掌握所需要的财务和非财务的信息，还必须在一定时限内并依照有利于控制企业行为的方式来加工和报告这些信息。

策略性的和整合性的信息系统

信息系统通常是经营行为的一个组成部分。如上所述，它们不仅获取决策所需要的信息来影响控制，而且还更多地被设计来执行战略意图。一项最发布

的研究表明，90年代对于管理层最重要的挑战是将信息系统的规划、设计和应用同组织的整体战略整合在一起。

信息系统支持战略创新。对于很多机构来说，战略性地运用信息系统就意味着成功。这样运用的早期的例子象一家航班订座系统，能使旅客便捷地获得航班信息并定票。另一个经常被引用的例子是医院服务提供商，能使其系统与医院在线直接联系，这样便产生了通过终端即时订购的巨大竞争优势。这些以及其它的例子表明，系统确实在获得竞争优势上有重要的作用。

当商界知道怎样运用新的系统来获取更好的信息时，更多的企业跟踪其产品在其目标区域内的销售情况，发现是否某个渠道比另外的渠道更好。当系统被运用于支持事前而不是事后反应的商业战略时，运用技术来帮助对了解得更好的市场作出反应，已经成为逐渐增长的趋势。

信息系统和经营的整合。信息系统的战略性运用表现了这样一种变化：从纯粹的财务系统变为整合进企业经营中的系统。这些系统帮助控制商业流程，跟踪和记录实时基础上的交易，通常还包括在整合性的、复杂的系统环境中许多经营行为。

在生产过程中，信息系统支持生产的各个阶段。收据、原料接受检测、要素的选择与结合，产成品的质量控制、存货更新、顾客记录、以及产成品的分配都可以运用这些系统。在多数情况下，这些步骤与过程控制系统和机械化操作的联系达到了这样一种程度，使得只要很少的人手就能完成产品订单。

正如在适时存货制度（JIT）中体现出来的那样，一个整合的经营系统的效果是非常突出的。公司运用 JIT 保证最少的存货，显著的削减了支出。通过频繁地使用电子数据交换，信息系统自身下命令并制定计划，使得原料自动到货。采用 JIT 的企业依赖它们的信息系统来实现生产目标，因为没有信息系统，这样密切的监控是不可能实现的。

多数新的生产系统与企业其它的系统，可能还包括企业的财务系统，高度地整合为一体。当系统执行其它的运用时，财务数据和会计记录会自动更新。

下面的例子可以表明有这样的系统如何能够起作用。在今天的保险公司里，索赔权可以在线提出。调解员就某种索赔类型的限制向系统提出询问，查明素

赔者是否被保险，并为索赔开出支票。同时，保险单据、保险统计数据以及其它的相关文件都被更新。把这同非整合型的系统对比，后者在每一个应用程序或子系统中分别处理单个的索赔。整合性的系统帮助控制经营，因为在线解决比起过去的纸张解决的方法更迅速、效率更高、也更有效果。它产生财务信息，并能回答这样的问题：这段时间支付了多少索赔？付了多少钱？它还能通过下述这类问题促进符合监管的要求：索赔及时地支付了吗？损失准备是否充分？

共存技术。如不考虑要跟进信息系统技术革命的挑战，仅仅因为这些系统是新的就认为新的系统能提供更好的控制，这种认识是错误的。实际上，反过来才可能是对的。旧系统通过使用可能已得到测试和检验，并且已经提供了所需要的东西。通常是这样的，一个企业的系统通常要不断发展以适应一些需求，因此就变成了多种技术的混合物。

技术的采购是公司战略的一个重要方面，而技术的选择对于实现增长的目标则是关键。技术的选择和运用依赖于许多因素。其中包括企业的目标，市场需求，竞争的要求，更重要的是，为了促进企业目标的实现，新系统如何帮助影响控制，反过来又遵从必要的控制。

信息质量

系统产生信息的质量影响管理层在管理和控制企业行为时作出适当决策的能力。现代的系统通常会提供在线问讯的能力，以便得到最新的信息。

报告要包含足够的恰当数据来保证有效的控制，这一点很重要。信息的质量包括确认：

- 内容是否适当——它是所需要的信息吗？
- 信息是否适时——需要时，就有吗？
- 信息是当前的吗？——最近的信息有吗？
- 信息是否准确——数据正确吗？
- 信息是否畅通——相应的部门能容易地获得信息吗？

所有这些问题在设计系统时必须提到。如果没有提到，有可能系统就会不能提供管理层和其它人员需要的信息。

因为适时适地地获得正确的信息是影响控制和信息系统的关键，因此信息系统自身也是内部控制的组成要素，并且也要被控制。正如第四章讨论过的，信息的质量依赖于控制活动的职能实施。

沟通

沟通是信息系统固有的。正如上面讨论过的，信息系统必须把信息提供给相应的人员，使他们能够履行经营性的、财务报告以及合规性方面的职责。但是沟通必须是更广意义上的，能够处理预期、个体和群体的职责以及其它重要事情。

内部沟通

所有的人员，特别是那些有着重要的经营和财务管理职责的人员，除了接受相关的信息来管理他们的活动外，还需要从高层管理那里层清楚地知道一条信息，那就是必须严肃地履行内部控制的责任。这条信息的清晰程度和这条信息传递的有效性，都是很重要的。

另外，特定的职责必须明确。每个人需要理解内控系统的相关方面，它们如何运行及个人在系统中的职责。不理解这个，就很容易产生问题。比如，在一个公司中，要求部门领导签署一份月度报告，证明规定的核对已经完成了。每一个月，这样的报告都要尽职尽责地签署并提交。但后来，严重的问题被揭发出来，至少有两位部门领导不知道他们真正要做什么。一位认为，只要了解了两个数据之间的差异量，核对就完成了。另一位也只是把这种核对的过程往前推进了一步，认为只要每个核对项目确认了，核对就完成了。实际上，只有当差别的原因被确认，并且作了适当的修正后，所要进行的核对程序才算完成。

在执行自己的职责时，每个人都应该知道，当意外发生时，不仅要注意事件本身，还要注意事件的原因。这样，就可以了解到系统潜在的缺陷，并采取预防的措施。比如，发现滞销的存货不仅要在财务报告上留下准确的记录，更重要的是对存货滞销的原因作出判断。

人们还要知道自己的行为怎样与他人的工作相联系。这样的知识对于认识到问题或对问题的原因作出判断和修正是必要的。人们需要知道什么样的行为是被期望的，什么是可以接受的，什么是不可接受的。曾经有过欺诈性财务报告的案例，该管理者屈于完成预算的压力，错误的报告了经营成果。在许多类似的

例子中，没有人告诉这些人这种错误报告可能是不合法的，甚至没人告诉他们这是不恰当的。这就表明了信息在企业内部怎样交流的关键属性。如果一位经理这样指导下属：“实现预算——我不管你怎么做，只要实现”，那么他就是在无意地传递错误的信息。

员工也需要有在企业中自上而下传递重要信息的方法。每天处理重要经营事项的一线员工最容易认识到刚产生的问题，销售代表或会计主管可能了解重要的消费产品设计需求。生产人员能意识到代价巨大的程序的缺陷。采购员会遇到来自供应商的不适当的诱惑。会计部门的人员可以了解到财务报表中对于销售和存货的夸大，或者了解到中饱私囊的现象。

为了使这些信息可以自下而上报告，必须既有开放的沟通渠道又有清楚的倾听意愿。员工必须相信他们的上级确实想了解问题并愿意有效地解决问题。从理性上讲，许多经理明白要避免“打击告发者”。但是当面临每天的压力时，他们可能会不能接受人们向自己报告一些正当的问题。员工们会迅速地根据上级没有时间或兴趣处理他们发现的问题的信号作出说还是不说的反应。这些问题交织在一起，不愿接受麻烦的信息的经理通常会是最最后一个知道沟通的渠道已被严重堵塞的人。

在多数情况下，正常的报告渠道就是适当的沟通渠道。然而，在特定条件下，需要独立的沟通途径作为一个预防失败的机制，在正常渠道不起作用时加以运用。一些公司为员工直接接触象首席内部审计师或企业法律顾问这样的高层领导提供了渠道。某一公司的总裁每周有一个晚上是开放的，并且让人知道员工为着任何事情的来访都是受欢迎的。另有一位总裁会定期去车间拜访他的员工——形成一种人们能够交流难题和关心的问题的氛围。既无开放的沟通渠道又无倾听的愿望，企业中自上而下的信息的传达就被堵塞了。

在任何情况下，员工知道不会因报告相关信息而受到报复都是至关重要的。如在第二章提到的，现有的机制要传达明确的信息，鼓励员工报告被怀疑是违反企业行为准则的行为，以及传达报告者会受到的待遇。保护“打小报告者”的企望已经有许多描述，大多数是在政府雇员的背景下。但因为注意到一些公司疲于处理不满雇员的无根据的言论，部分评论者对此提出反对。

当然，应该取得某种平衡。管理层向下传达正确的信息以及为合法的自下而上报告提供合理机制，两者都很重要。

管理层与董事会及其委员之间的沟通至关重要。管理层必须使董事会了解最新的业绩、发展、风险、主要的革新以及其它任何相关的事件或事故。与董事会的沟通越好，董事会越能有效地行使监督职能，并能够对于关键的事务作出合理的行为，提供建议和忠告。同样，董事会也应该向管理层传达所需要的信息，并提供指导和反馈。

外部沟通

企业不仅在内部需要有适当的沟通，而且在外部也是。通过开放的沟通渠道，顾客、供应商对于产品或服务的设计或质量可以提供非常重要的信息，使公司注意顾客的需求和偏好。而且，任何管理企业的人都要认识到不适当的行为，比如回扣以及其它不适当的收入，都是不能容忍的。公司可以同供应商直接沟通，比如，解释公司期望供应商雇员在与其打交道时应怎么做等等。

与外界沟通通常会为内部控制机构提供重要的信息。外部审计师对于企业经营和相关交易事项的理解可以为管理层和董事会提供重要的控制信息。

诸如州银行或保险公司之类的监管者关于合规性检查结果的权威报告能够使控制的缺陷更加明显地表现出来。对于运输、收据、帐单以及其它行为的抱怨和要求通常会表明经营中存在的问题。这些问题应该由非交易人员来检查。检查人员应该认识到这类情况的含义，对其进行调查并作出必要的修正。

与股东、监管者、财务分析师以及其它外界的交流可以提供与那些外界相关的信息，这样他们就能很容易明白企业所面临的情况和风险。这些交流应该是有意义的，能够提供恰当的、及时的信息，当然，也应按照法律和规则的要求。

管理层同外界（无论是公开的、即将进行的、严格跟踪的还是其它的）的交流也可以向整个公司内部传递信息。

沟通的方式

沟通可以采用诸如政策手册，备忘录，布告通知，录像录音带的形式。口头传递消息时（在许多人中间，在小的会议上，或者在两个人会面时），语调和身体

语言可以用来强调所说的内容。

另一种有影响力的沟通手段是管理层对下属采取的行为。经理应该提醒自己“做比说更有效”。他们的行为反过来又受到公司的历史和文化的影 响，特别是受他们对于他们的上级过去怎样处理同样的事情的观察的影响。

具有悠久而丰富整合性经营的历史，并且文化为所有员工充分了解企业，在信息沟通上不会遇到很大的困难。而没有这样传统的企业就需要付出更多的努力寻找信息沟通的方法。

对中小型企业的应用

小企业的信息系统可能没有大企业的正式，但信息系统的作用同样重要。在大多数企业中，无论企业是大还是小，内部产生的数据都可以运用今天的电脑和信息技术迅速有效地处理。小型企业的信息系统也能识别和报告相关的外部事件、行为和条件，但其有效性通常会特别受到高级管理人员对外部事件的监控能力的影响，并且也依赖于后者。比如说，所有者兼经理以及其它管理人员同重要顾客和供应商的交流，是获取顾客偏好或供货源信息的关键来源，这些信息对于监控变化的环境及其相关风险来说是必须的。

在中小型企业中，高级管理人员与雇员之间有效的内部沟通会比大企业中更容易实现，因为中小型企业规模小，层次少，总裁更容易接触到。实际上，内部沟通通过总裁和主要经理所参加的日常会议就可以实现。许多小企业发现，他们虽然没有大企业那种正式的沟通渠道，但更频繁的日常联系以及对高级管理人员的门户开放政策也可以提供有效的沟通。“做比说更有效政策”在小企业中可能是更重要的（内部和外部的）沟通手段，因为高级管理人员直接同企业的大部分雇员、顾客以及供应商相互影响。

评估

评估者会考虑信息和沟通系统对企业需要的恰当性。下面所列出的事项是人们会考虑到的。但列出的并不是全部，也不是对每个企业都适用，然而，这些可以作为一个起点。

信息

- 获取外部与内部的信息，向管理层提供与确定目标相关的、关于企业业绩的必要报告。
- 及时向相应的人提供详细的信息，使他们能有效地行使自己的职责。
- (与企业的整体战略联系在一起) 根据信息系统的战略性计划来发展或修改信息系统，并对企业层面和行为层面的目标作出反应。
- 管理层对于必要的信息系统的支持要由相应资源——人力和财务——的运用来证明。

沟通

- 在沟通员工职责与控制责任时的有效性。
- 为人们报告可疑的不正当行为建立沟通的渠道。
- 管理层对员工所建议的提高产量、质量以及类似改进的方法的接受性。
- 贯穿整个企业的充分沟通（比如在采购与生产行为之间），信息的完整性、及时性及信息的充分性足以使人们有效履行其职责。
- 渠道的开放性与有效性，这些渠道是为了与顾客、供应商以及其它外界来沟通不断变化的顾客需求信息。
- 外界能够了解企业道德标准的程度。
- 管理层根据与顾客、供应商、监管者及其它外界的交流而采取的适时恰当的相应措施。

第六章 监 控

本章概要：内控系统需要被监控——这是一个评估系统在一定时期内运行质量的过程。这一过程通过持续性的监控行为、独立的评估或两者的结合来实现。持续性的监控行为发生在经营的过程中。它包括日常管理和监管行为，以及其他人在履行职责时发生的行为。独立评估的范围和频率主要依赖于风险评估和持续性监控程序的有效性。内部控制的缺陷应自下而上进行报告，重要事项应报知高层管理人员和董事会。

内部控制随着时间而变化。实施控制的方式可能不断发展。曾经有效的程序可能会变得不太有效，或将不再实施。这些可能源自新员工的到来、培训和监控效果的变化，时间和资源的限制，或额外的压力。另外，最初制定内控系统的环境也可能改变，使其警示新环境带来风险的能力下降。相应地，管理层需要判定内控系统是否继续有效并能应对新风险。

监控保证了内部控制持续有效。这一过程涉及由适当的人员及时评估控制的设计和执行，并采取必要措施。它应用于企业的所有行为，有时还适用于外部订约人。例如，将健康险处理过程外包给第三方管理人，这一过程直接影响福利的成本，企业将希望监控该管理人的活动和控制的执行情况。

监控可通过两种方式进行：通过持续性的活动或独立的评估。在某种程度上，内控系统通常在一种持续性的基础上进行组织，以实行监控。持续监控的程度和有效性越强，独立评估的需求就越少。为了使管理层对内控系统的有效性获得合理保证，所需要的的独立评估的频率有赖于管理层的判断。要做出这样的判断必须考虑以下问题：变化发生的性质和程度及其相关风险，执行控制的人的能力和經驗，以及持续性监控的效果。一般地，持续性监控和独立评估的结合有利于保证内控系统在一定时期保持有效性。

必须意识到，持续性的监控活动是植根于企业日常、重复发生的活动中的。与独立评估相应的程序相比，由于监控性程序在实时基础上实施、动态地应对环境的变化，并在企业中根深蒂固而显得更加有效。

由于独立评估发生在事实之后，比起持续性监控程序，可更快地发现问题。

一些具有完善的持续性监控行为的企业也同样会每隔几年对其内控系统或某些部分进行独立评估。一个感到有必要进行经常性的独立评估的企业，应重点关注改进持续性监控的途径，并强调“嵌入”而非“外加”的控制。

持续性监控行为

在日常经营中用于监控内部控制有效性的行为是多样化的。他们包括日常的管理和监督行为、比较、协调和其他例常活动。

持续性监控行为有下面一些例子：

- 在执行常规管理行为时，经营经理取得内部控制持续运转的证据。当经营报告与财务报告系统结合在一起，或与之核对，并用于持续地管理经营，很快就能发现重大错误或与预期结果的偏离。例如，在部门、子公司和公司层次的销售经理、采购经理和制造经理可以接触到与他自己对经营的了解大不相同的经营报告和问题报告。内控系统的有效性通过及时和完整地报告和解决例外问题而得以增强。
- 来自外界的交流确认了内部产生的信息或明显的问题。顾客通过支付发票暗示其确认了帐单数据。相反地，顾客对帐单的诉讼则表明销售交易过程存在系统缺陷。类似地，投资经理关于证券损益的报告也能指出企业（或经理）会计记录中的问题。保险公司对保险政策和措施的复核提供了关于控制（这些控制从经营安全性到合法性）运行功能的信息，因此可作为一种控制技巧。监管者也可能就合法性或其他反映内控系统运行的事件与企业进行交流。
- 适当的组织结构和监管行为提供了对控制行为的复核和对缺陷的确认。例如，员工对交易正确性和完整性的控制活动在日常经营中得到监管。另外，对员工职责进行合理分工以便相互制衡，有利于防止员工舞弊，因为这样限制了个人掩盖其可疑行为的能力。

将信息系统所记录的数据与实物资产核对。例如，产成品存货应定期进行盘点，将盘点的数据与相应的会计数据核对并记录存在的差异。

- 内部及外部审计师定期为进一步加强内部控制提供建议。在许多企业中，审

计师十分重视评价内控的设计并测试其有效性。因此，他们常常能够发现一些潜在的问题并向管理层提供解决问题的建议，这些信息将有助于管理层作出符合成本效益原则的决策。内部审计师及执行类似评价职能的企业人员在监督企业活动方面尤为有效。

- 培训研讨会、计划会议及其他会议能向管理层提供有关控制是否有效的重要反馈。这种方式不但能指出控制中存在的个别问题，还能增强参与者的控制意识。

- 定期询问职员理解及执行企业相关规定的情况。也可向经营及财务人员询问相关的控制程序，如调整特定数据的程序是否正常运行。所有这些信息都将最终经过管理层或内部审计人员的确认。

由此可见，这些持续性监控活动关注每个内部控制要素的重要方面。

独立评估

尽管持续性监控程序可以提供关于其他控制要素有效性的重要反馈信息，但经常地对系统的有效性直接进行评估也是十分必要的。这样同时也提供了一个机会来评价持续性监控程序是否有效。

范围和频率

由于所控制风险的大小及内部控制在减小风险中的重要性不同，对于内部控制进行评价的范围和频率也不一样。例如，那些致力于重大风险或对减小风险具有重要作用的控制就应经常地进行评价。对整个内部控制系统进行评价并不象对个别控制进行评价那样频繁，它主要取决于以下几个因素：主要战略及管理层的变更，重大并购或处置，经营活动或财务处理方法的重大变更。当作出决策对企业的内部控制系统进行评价时，应当特别注意每个内部控制要素及其所有的关键活动。此外，控制对于三类目标——经营、财务报告及合规性的侧重点不同，评价范围也将随之不同。

评价主体

评价通常以自我评价的方式进行，即负责某一单位或职责的人员对其控制自身活动的有效性进行评价。例如，一位部门主管应指导本部门内部控制的评价活

动。他或她可能亲自评价控制环境因素，然后请部门内负责各种经营活动的人员评价其他要素的有效性。生产经理可能主要关注经营和符合性目标，而部门会计主管可能更重视财务报告目标。然后，所有结果都将由主要执行人审阅。最后，部门的自我评价将与其他部门对其的内控评价一起交由公司的管理层审阅。

评价内部控制是内部审计人员的职责之一，有时，在董事会、高级管理层、子公司及部门主管的特殊要求下，内审人员也会对内控进行评价。同样，在评价内控时，管理层也可利用外部审计人员的工作。在管理层认为必要的时候，也可结合以上两种方式来执行特定的评价程序。

评价程序

对内部控制系统进行评价本身也是一种程序。当方法或技术改变时，这种评价程序也应有一定之规并有一定的内在基础。

评价者须理解企业每项活动及内控系统的每项要素。因此，首先关注系统的运行过程或内控系统的设计是十分有用的。这其中包括同企业职员进行探讨并审阅已有的文件。

评价者需要确定系统实际是如何工作的。已经设计好的特定的操作程序可能因时间的推移而有所变动，抑或不再实施。有时确立了新控制，但描述系统的人却不知道或未将之归入文件。为确定系统实际是如何工作的，可以通过与实施控制或受控制影响的人进行讨论，或通过检查控制执行记录或其他程序的组合来进行。

评价者必须分析内部控制的设计和测试结果。分析必须在已确定的准则的背景下，并结合内控系统是否对既定目标提供了合理保证这一最终目标进行。

方法体系

有许多的评估方法可供选择，包括检查清单、调查问卷和流程图等方法。量化方法在商业和学术文件中有阐述。另外，还列示了控制目标，确定了内部控制的一般性目标。

作为其评估方法体系中的一部分，一些公司将其内控系统与其他企业——通常

是可作为比较基准的企业相比。比如，一公司可能将其内控系统与那些被认为在内控系统方面具有良好声誉的公司相比。对比可能直接与另一公司进行，或在行业协会的赞助下进行。管理顾问也能提供可比信息，在一些行业中进行的企业间横向比较，也有利于企业将其内控系统与同行进行对比评价。需要提醒一下，在比较内控系统时，必须考虑目标、事实和环境的差异。另外，必须考虑内部控制的五项要素及内部控制的局限性。

文件化

企业内部控制文件化的程度根据各企业的规模、复杂性和类似因素的不同而存在差异。大一些的组织通常有书面的政策手册、正式的组织图、书面的工作描述、经营指导、信息系统流程等。小一些的公司内部控制文件化的程度一般低得多。

许多控制是非正式和非书面的，但却经常运用并高度有效。测试这些控制的方法与文件化的控制是一致的。控制没有文件化并不意味着内控系统是无效的或无法评估。适当程度的文件化常常有利于使评估更有效。它在其他方面也是有益的：有利于增进员工对内控系统如何运行及各自职责的理解，更易于必要时对其修改。

评估者可能决定将评估过程本身文件化。他会常常参照企业内控系统的现有文件。这一般作为附加的制度文件，加在对评估过程中进行测试和分析的描述之后。

当需要向更多人提供有关内部控制的阐述或评估时，内部控制文件化的性质和程度将会提高。当管理层希望向外界提供关于内控系统效果的申明时，他们应会考虑形成文件来支持该申明。如果该声明今后被质询，这些文件将很有用。

行动计划

第一次指导评估内控系统的管理人员可以考虑下列建议，决定对何处着手和如何去做：

- 决定评估的范围，包括目标的分类、内部控制要素和需采取的行动。
- 确定对内部控制的有效性提供常规保证的持续的监控行为，。

- 分析内部审计的控制评估工作，考虑外部审计师与控制相关的发现。
- 按照单位、要素或高风险区域划分重要性程度和先后次序，保证及时的关注
- 在以上基础上，开发含有近期和远期内容的评估程序。
- 汇集所有进行评估的各方，共同考虑下列问题：不仅要考虑评估范围和
时间表，而且要考虑所使用的方法体系，应用的工具，来自内外部审计师和
监管者的建议，报告所发现问题的方式以及设定最终的文件化程度。
- 监控进展和复核发现。
- 保证采取必要的追踪措施，必要时修改后续的评估部分。

许多工作要进行分工。但是，负责评估的人要对直至完成的全过程进行管理，这一点非常重要。

报告缺陷

企业内控系统的缺陷源自很多方面，包括企业的持续性监控行为，内控系统的独立评估，以及外部因素。

这里的“缺陷”被广泛定义为内控系统中值得注意的问题。因此，缺陷可能代表一个假想的，潜在的或实际的缺点，或一个强化内控系统的机会，以提供更大的可能性来实现企业目标。

信息来源

内部控制缺陷信息的一个最佳来源是内控系统本身。企业的持续监控行为，包括管理行为和对雇员的日常监管，从直接涉及企业活动的人那里获得深入的了解。这些洞察是实时获得的，能迅速地识别内部控制缺陷。其他了解控制缺陷的来源是对内控系统的独立评估。由管理层、内部审计师或其他人进行的评估，内部审计师或其他人能够提醒需要改进的地方。

很多外部因素经常提供有关企业内控系统运行的重要信息。这些外部因素包括顾客、供货商和其他与企业交易的人员、独立注册会计师和监管当局。必须仔细考虑外界报告中涉及内部控制方面的内容，并采取适当的纠正措施。

应该报告什么

应该报告什么？不可能有一个普遍适用的答案，因为这是高度主观的。但可以有一些参考。

当然，若发现内部控制缺陷可能影响企业实现既定目标，应向能采取必要行为的人士报告，这一点将在下一节讨论。所报告情况的性质取决于听取汇报人员处理问题的职责。

在考虑何种情况需要汇报时，有必要弄清所发现情况的本质。例如，销售人员认为自己所获佣金算错了。工资部门人员经过调查，发现某个产品仍用的是过去的旧价格，所以少算了该销售人员的佣金，也少收了顾客的货款。针对这种情况，应采取的措施可能包括重新计算所有销售人员的佣金和所有顾客的账单。但是，这些措施也许仍不能解决一系列相关问题，为什么没有在第一时间采用新价格，存在什么控制来确保价格上调能及时准确进入信息系统，计算销售佣金和顾客账单的计算机程序是否存在问题，如果存在的话，是否需要注意软件开发或更换软件，如果该销售人员没有提出质疑，有没有其他内部控制程序能及时发现问题。

因此，对于一个看似简单的问题，提出一个显而易见的解决方案，可能还有更深远的内部控制方面的意义。这就强调了向上级报告错误或其他问题的必要性。最根本的是，不仅应汇报特别交易或事件，而且潜在的人员控制也应重新评价。

可能有人认为，没有什么问题是如此无关紧要以至于对其内部控制进行调查会是小题大作。例如，雇员因个人需要从备用金中拿走几美元，与特别事件相比并不重要，或与备用金的全部金额相比可能也不重要，因此，进行追查似乎并不值得。但是，原谅该雇员私用备用金这一事件，也许会向雇员们全体员工传递一个非期望的信息。

向谁汇报

雇员在日常经营活动中获得的信息通常通过正常渠道传递给他们的直接上司，上司再向上或横向传递这些信息，使得信息能到达最终负责人。正如第五章讨论的那样，应有可供汇报非法或不当行为的多条渠道。

发现内部控制的缺陷,通常不仅应向负责的个人汇报,由他采取正确的措施,还至少应向该责任人的上一级汇报。这一过程使得责任人能提供所需的支持或进行监督以保证采取正确的措施,并与企业中受影响的他人进行沟通。缺陷的发现,突破了企业各部门的界限,不仅横向传递,而且向上级汇报以确保正确措施的实行。

报告指引

向恰当的当事人提供有关内部控制缺陷的必要信息,对内部控制制度的持续有效运行很关键。可以确立报告指引来指明在决策的各个层级需要什么样的信息。

这样的指引应该基于一条通用的原则,那就是一个经理应收到必要的内控信息来影响其职属下的人员的行为,或者来达成活动的目标。而确立的这些指引就是以这一点为基础的。例如,总裁通常希望被告知关于各种政策或程序的严重违规行为,想要得到对一些有可能产生重大财务后果和战略影响,或影响企业的声誉的事件的支持信息。高级经理应被告知影响各业务单位的控制缺陷。这样的例子有,哪里特定价值的资产存在风险,哪里人员能力存在欠缺,或哪里重要的财务稽核未恰当实施。越在基层,经理知道其业务单位中存在的业务缺陷的情况应越详细。

指引应由监管者制定,向下属定义应该汇报的内容。详细程度应有不同,在企业越低层次,所需的信息越详细。如果报告指引的定义过于狭窄,会妨碍报告的有效性,而如果具有充分的弹性,则对报告过程会起促进作用。

有时听取关于缺陷报告的人 would 提供特别的指示来要求报告何种信息。例如,董事会或审计委员会可能要求管理层或内外部审计师仅仅报告那些符合一定严重性标准和重要性标准的缺陷。关于这种标准,注册会计师运用的术语是“需报告的情形”。他们的定义如下:

内部控制系统设计或运行的重要缺陷,其可能对企业记录、处理、汇总和报告与管理层财务报表申明一致的财务数据产生不利影响。

这一定义与财务报告目标有关,但也可以进行修订来满足经营性和合规性目标的要求。

中小企业的运用

中小企业的持续性监控行为可能更为不正式，并涉及总裁和其他关键的管理人员。他们对控制的监控行为通常是管理业务的副产品，通过其对经营中绝大多数方面（如果不是所有方面的话）的直接参与而实现。他们对经营的密切参与常常能发现与预期显著的偏离以及经营或财务数据的错误。

一个小企业的所有者兼经理可能经常视察车间、生产线或仓库，将实际库存与数据处理系统报告的数据相比较。顾客和供货商的重大诉讼，以及与外界监管者的联系，都能提醒小企业的管理层注意那些表明内控失效的经营性或合法性问题。

中小型企业不太可能对其内控制度进行独立评估，对独立评估的需要被高度有效的持续性监控所替代。中型公司可能有一位进行独立评估的内部审计师。甚至小企业也可能分配给会计人员评估控制的工作职能。一些企业要求其外部审计师对内控制度的某些方面进行评估，在循环的基础上，向总裁提供有关控制系统有效性的信息。

限于更有限的组织结构，监控程序的缺陷能够很容易地向合适的人传达。小企业的员工通常对需要自下而上传递何种信息有清楚的了解。而由谁负责判定问题的原因并采取纠正措施可能不总是那么明确。这一点无论对中小企业还是大企业都很重要。

评估

在考虑内部控制的持续有效性应监控到何种程度时，必须考虑持续性监控和对内控制度的独立评估活动，或其中一部分。下列是一些可能考虑的问题。该列示并非全面的也不是每一条都适用每个企业；但它可以作为起点。

持续性监控行为

- 从事日常活动的人员在多大程度上能获取内控制度是否持续起作用的证据。
- 来自外界的信息在多大程度上印证了内部产生的信息，或者指出了问题。
- 定期进行帐实核对
- 对内外部审计师关于加强内部控制的建议的回应

- 培训研讨会、规划及其他会议在多大程度上向管理层提供有关内部控制是否有效的反馈
- 是否要求员工定期声明其是否理解和遵行了企业行为准则，并经常实施重要的控制活动。
- 内部审计的有效性

独立评估

- 对内控制度进行独立评估的范围和频率
- 评估过程的适当性
- 评估方法是否合乎逻辑和适当
- 合适的内部控制文件化程度

缺陷报告

- 存在发现、报告内部控制缺陷的机制
- 报告指引的适当性
- 后续措施的适当性

第七章 内部控制的局限

本章概要：无论内部控制设计和执行得多好，它也只能对于管理层和董事会就企业目标的实现提供合理的保证。实现的可能性受所有内部控制系统固有的局限的影响，这包括以下的事实：决策人判断上的失误；由于简单差错或错误导致的失败。而且控制还会由于两个或更多的人联合欺诈以及管理层越过内部控制而失效。还有一种限制是要考虑与控制相关的成本和收益。

一些研究者认为，内部控制可以确保企业不会失败——就是说，企业总会实现它的经营、财务报告以及遵循性的目标。这样看来，内部控制有时就会被期望可以消除所有现存以及潜在的企业缺陷。这种观点是种误导。内部控制并不是万灵药。

在考察内部控制的局限时，有两个不同的概念一定要被认识到：

- 第一，内部控制——即便是有效的内部控制——根据不同的目标，在不同的层面运行。因为目标同企业经营的效益和效率相关——企业基本任务，盈利及相关目标的实现——内部控制可以帮助确保管理层意识到企业有无进步，但它甚至不能为企业目标的实现提供合理的保证。
- 第二，就上述三类目标而言，内部控制不能为其中的任何一个提供绝对的保证。

第一类限制表明有些事件和条件在管理层控制之外。这已经在第三章“目标的实现”中讨论过了。第二类限制同这个事实相关：没有哪个内部控制系统会一直做它打算要做的。内部控制所能做的最好的就是达到合理的保证，这就是本章所要讨论的内容。

合理的保证当然并不意味内部控制系统会经常失效。许多个别的以及共同的因素都用于为合理的保证这个概念提供支持。内部控制满足多重目标的累积作用以及控制的多重目的性减少了企业无法实现自身目标的危险。而且，日常的经营行为和不同层次人员的职责分工都有助于实现企业的目标。的确，在一个控制良好的企业的不同部门中，大多数部门很可能经常被告知朝向其经营目标运行，通常会实现遵循性目标，并且一贯地编制每期及每年度的可靠财务报表。然而，由于上述的固有局限，并不能保证诸如不可控制的事件、错误或不当报

告的事件绝不会发生。换句话说，即便有效的内部控制系统也会出现失败。合理的保证并非绝对的保证。

判断

在企业决策中，控制的有效性会受到人的局限的限制。决策是由人在合适的时间，依据现有的信息，在企业经营的压力下作出的。一些依据人的判断作出的决策，经由事后的观察发现很难产生预想的结果，因此就需要改变。

必须依据人的判断而作出的与内控相关决策的特性在下面讨论失效、管理层的越权以及成本收益原则时会进一步言及。

失效

即便设计得很好的内部控制也会失效。职员会对指导误解，会作出错误判断，甚至会由于粗心、注意力分散或疲倦而出差错。负责调查例外因素的会计部门主管可能忘记或者对于调查做得不够好，就不能作出适当的修正。代替缺席或生病雇员的临时职员可能不能正确地执行控制的职责。在职员还没有接受培训，能够对错误运行的迹象作出适当的反映之前，内部控制系统的变化可能已经发生了。

管理层的越权

内控系统的效果取决于负责其运行的人员。即便在有效控制的企业——那些具有高度的整体性和控制意识的企业——中，经理也可能越过内部控制。

“管理层的越权”这个概念在此指为了不合法的目的而不遵守既定的规定和程序以获取私人的获益，或夸大企业的财务状况或合法地位。单位或部门的经理，或者高级管理层成员会出于各种目的而越过控制制度：增加报告中的收入来掩盖市场份额始料不及的下跌，增加报告中的赢利以符合不现实的预算，在公开发售或销售之前就吹嘘企业的市场价格，为了满足销售或赢利计划支持与业绩相联系的分红，想要掩盖对债务合同的违反，或者遮盖对法规的违反。越权行为包括对银行家、律师、会计或销货商有意作出的不正确的表达，有意地提供错误的文件，如：订货单和销售发票。

管理层的越权不能与管理层的干预相混淆，后者指的是管理层为了合法的目的而偏离制定的规章和程序的行为。管理层的干预对于特殊的和非标准的交易和事件是必须的，因为控制机构有可能对这些会作出不当的处理。为管理层的干预作出预备在所有的内部控制制度中都是必须的，因为没有哪一个控制机构能够被设计成可以预料到所有的情况。管理层干预的行为一般是公开的并且通常是记录在案的，否则就要让相关的职员了解，而越权的行为由于是有意要掩盖，一般不会被记录在案或为人所了解。

合伙同谋

两人或更多人的合伙同谋行为会导致控制的失效，一些合伙违法并隐藏事实不让被察觉的人会以控制机构不能识别的方式更改财务信息或其它的管理层的信息。比如，可能在一名行使重要控制职能的雇员同一位顾客，供应商或另一名雇员之间存在着同谋。在不同的部门，不同的销售人员或部门经理可能会同谋使控制失效以使报告的结果满足预算或满足激励的目标。

成本收益原则

资源总是有限的，因此企业必须考虑与建立控制相关的开支和收益。

在决定是否应该建立一个控制时，控制失败的风险及其对于企业潜在的影响应该和与建立一个新的控制相关的支出放在一起考虑。比如，如果一个公司在生产过程中消耗的原料成本低，原料不易变质，有现成的供应资源和贮存空间，这个公司就不会花钱建立复杂的存货控制来监控各种原料。

对于建立控制所需的成本与收益的计算具有不同程度的精确性。一般来说，成本更容易计算，因为成本在许多情况中可以一种十分精确的方式来量化。所有与建立控制相关的直接支出与实际上可计算的间接支出通常都是可以考虑到。一些公司也把与资源利用相关的偶然的支出包括在其中。

然而在另外一些情况下，支出很难被量化。因为很难将相关的事件和努力加以量化，比如，某些控制环境的因素，诸如管理层道德价值方面的约束或职员的能力；对于风险的估计；对于顾客偏好的市场调查等类似的外部信息的掌握。收益方面要求一种更为主观的估算。比如，有效培训的收益通常是显而易见的，却很难量化。当然，下列一些因素在对潜在的收益进行估算时可以考虑进去：意外情况发生的可能性，行为的性质，以及事件对于企业可能造成的潜

在财务或经营影响。

成本-收益原则的复杂性因控制与企业经营的内在联系而加剧。当控制同管理层和企业的经营联系在一起，或“嵌入”这二者的过程中时，很难将成本或收益独立出来考虑。

同样，许多控制经常会分别的或一起用于消除某一种风险。看看退货这种情况。当退货被记录下来时，是否将现有存货和应收账款的总帐记录与所有退货进行核对就足够了？是否需要单个顾客的帐户代码进行核对，并到何种程度呢？每月将总帐与明细帐进行核对是否足够？或者，是否需要更深入的程序来保证明细帐已对退货及时记录？有何机制来关注退货是哪个环节系统问题的症状，是产品设计，制造，运输，定价，还是客户服务？问题的答案取决于在特定环境中涉及的风险以及确定每种控制程序相关的成本和收益。

成本-收益的定律也随着企业性质的不同而变化。比如，计算机系统提供关于顾客订货频率、订货价值、每次订货数量的信息，对一个邮寄供货的公司就非常重要。而对一个帆船制造商，如此详细的信息对其就没有那么重要了。对其而言，这样的信息系统很可能被认为不符合成本-收益原则。由于某一行为或相关风险相对不重要，可能甚至都不必进行成本-收益分析。进行这样的分析是不合理的。

关键是要找到合适的平衡。过分的控制是浪费和低效的。进行电话订购的顾客不能容忍那些麻烦、费时的接受订单程序。那些使有信誉的潜在借款人渡过难关的银行将不会簿记很多新贷款。另一方面，控制不足也带来坏账风险。在激烈竞争的环境中，需要一个合适的平衡。尽管有困难，还是需要考虑成本-收益原则。

第八章 作用与职责

本章概要：在一个机构中每个人对于内部控制都承担某种职责。而管理层则对企业的内部控制系统负责。总裁负最终责任，因此被认为对内控系统具有“所有权”。尽管所有管理人员都具有重要的作用，并且对其部门行为的控制负责，但财务和会计主管对于管理层行使控制的方式起着主要作用。同样，内部审计有利于促进内部控制系统的持续有效，但对于系统的建立和保持却并不具有主要的职责。董事会及审计委员会对内部控制制度提供重要的监管。一些外部成员，比如外部审计通常服务于企业目标的实现，并提供有用的信息影响内部控制。但他们并不对企业的内部控制制度的效果负责，也不是其中的一部分。

内部控制受到各方影响，每方的职责都很重要。董事会（直接的或通过其成员），管理层，内部审计和其它职员对于一个有效的内部控制制度都具有重要的作用。其它的成员，比如外部审计和常规人员经常同内部控制联系在一起。企业内部控制制度的构成成员和非构成成员——但其行为可以影响内部控制制度或者帮助实现企业的目标——之间存在着区别。

一个机构内部的成员是内部控制系统的一部分。他（她）们各以自己的方式去影响内部控制——就是为实现特定的企业目标提供合理的保证。企业的外部成员也会通过各种行为帮助企业实现目标：向企业提供有用的信息影响控制，或通过一些的独立行为而有益于企业目标。但是，他们并不能仅仅因为直接或间接地促进企业目标的实现就算作企业内控系统中的一部分。

负责的成员

企业中每个人对内部控制的影响都有某种作用。作用随着各自的职责和参与程度而变化。下面讨论管理层、董事会、内部审计和其它人员的职责。

管理层

管理层直接为包括内部控制制度在内的企业的全部行为负责。当然，企业中不同的管理层具有不同的内部控制的职责。他们的职责根据企业的性质而常常大不相同。

在任何机构中，总裁都是最终负责人。他或她对于内部控制制度负有最终所有

权责任。行使这项职责的最重要的一个方面就是确保存在积极的控制环境。除了总裁，没有任何个人或部门能够“定调”来影响控制的环境因素以及内部控制的其它要素。在整个机构中，总裁的影响也不能夸大。总裁对于董事会选举的影响并不是很清楚。一位具有很高道德标准的总裁有利于保证董事会对他的价值观念有所回应。而一位不诚实的总裁就不能或不想获得那些诚实的董事会成员的赞成。一位曾经服务于董事会及其审计委员会的人士直截了当地说，如果他对于总裁的诚实有看法的话，他会很坦率地拒绝出任的邀请。有效的董事会及其审计委员会也会认真考察总裁的诚实和道德价值观念，来判断内部控制制度是否有必须的关键性支持。

总裁的职责包括监管内部控制的所有要素是否到位。总裁一般通过下述方法来实现这种职责：

- 向高级经理提供领导与指导。并与这些高级经理一起制定构成企业内部控制制度基础的价值观念、原则以及重要的经营策略。比如，总裁要和主要的高级经理制定企业层面的目标以及总体策略。对企业的组织机构，重要策略的制定和交流以及企业要使用的预算类型和报告制度采取行动。
- 定期召开那些负责主要部门（销售、市场、生产、采购、财务、人力资源等等）的高级经理会，检查他们包括对企业的控制在内的职责。总裁可以了解经营本身所需要的控制、以及正在进行的努力。要完成这项职责，总裁明确规定自己所需要的信息是很重要的。

部门的高级经理对于与其部门目标相关的内部控制负责。他们指导与其部门目标相关的内部控制策略和程序，并确保与企业整体目标的一致。比如，他们为单位的组织机构、人员的聘用和培训、预算以及促进对单位行为控制的其它信息系统提供指导。从这个意义上说，每位部门的经理实际上就是各自部门的总裁。

高级经理一般将特定的内部控制程序分配到各部门或单位负责人。因此，这些低层经理一般在设计和执行内部控制程序时发挥着更切实的作用。这些经理经常直接负责规定与单位目标相关的控制，比如制定购买原料的授权程序，接受新的顾客，检查生产报告以监管生产。他们也会对控制提出建议，监控其应用，

并与高级管理人员会晤，向其报告控制执行的情况。

通过企业中这一层的管理人员，即下属的经理以及更底层的经理或监察人员可以直接深入地参与到控制政策和程序的实施中。他们有责任对于产生的问题和意外采取行动。这包括调查数据登录错误以及意外报告中记录的交易，调查部门费用预算变化的原因，或者跟踪顾客的销售退回或生产存货情况。重大问题，无论属于某一特定交易还是大问题的迹象都要向机构上层反映。

与经理各自的职责相伴随的不仅是必要权力，而且还有责任。每位经理都要为其在内部控制系统中发挥的作用向自己的上级负责，而总裁最终向董事会负责。

虽然不同管理层有不同的内部控制职责和作用，其行为应包括在内控系统中。

财务人员。

财务和控制部门的作用就是监管，其行为贯穿整个企业各个部门的运行中。这些财务人员通常参与整个企业的预算和计划的制定。他们通常根据经营性的、遵循性的、以及财务的观点跟踪分析企业的业绩。这些行为一般是企业中央的或集团组织的一部分，但它们通常也具有监管各职能部门、分公司以及事业部行为的“虚线”职能。因此，一个企业中财务总监、首席会计师、主控长和其他财务人员对于管理层行使控制的方式起着决定作用。

首席会计师在防止和监察欺骗性的财务报告中所起作用的重要性在 Treadway 委员会的报告中得到强调：“作为高级管理层的一员，首席会计师协助企业为道德行为准则定下了基调；他负责财务报表；对公司财务报告体系的设计、贯彻和监管负主要的责任；而且，在对欺骗性财务报告导致的非常情况进行调查时，首席会计师的地位是独一无二的”。这个报告提到财务总监或主控长可以发挥首席会计师的作用。

从内部控制的构成要素可以清楚地看到，财务总监（首席会计师）及其职员起重要的作用。如果企业的目标已经建立，策略已经确定，风险已被分析，怎样处理影响企业的变化的决定也已作出，那么，财务总监（首席会计师）就应该成为主角。

因此，财务总监（首席会计师）应该与其它部门的领导具有同样的地位，管理

层对其关注范围限制的任何企图——比如，仅限于财务报告和资金管理领域——都会严重限制企业成功的可能性。

董事会

管理层要向董事会或监事会负责，而后者提供监管、指引和督导。通过选举管理层，董事会对于它所期望的诚信和道德价值的确定发挥重要作用，并且能够借助督导行为来确证它的期望。同样，借助在某些重要决定上保留的权力，董事会能够对于高层次目标以及策略的制定发挥影响，并且以其提供的督导来深入地参与到内部控制中。

有影响力的董事会成员应是客观、有能力、积极热心的。他们对于企业的行为和环境具有实用的知识，并且会为董事会职责的充分实施付出必要的时间。他们会利用资源调查他们认为重要的任何事情，并同企业所有员工有一种开放的不受限制的交流渠道，其中包括内部审计，外部审计和法律顾问。

许多董事会很大程度上通过委员会来行使自己的职责。委员会的作用及关注随企业的不同而有差异，但通常都会包括审计、补偿、财务、任命以及员工的福利。不同的委员会对于内部控制的不同部分进行强调。比如，审计委员会对财务报告有直接的作用，人事委员会通过对于潜在的董事会成员资格的考察在内部控制中发挥重要的作用。实际上，所有的董事委员会通过他们督察的作用，就成为内部控制制度的一个重要组成部分。如果有某个委员会没有建立，相应的职能只有由董事会自己来行使。

审计委员会。

多年以来，监管和专业机构的注意力都集中于建立审计委员会。尽管这些年来审计委员会已经受到越来越多的重视，它们并非是普遍需要的，其特定的职能和行为也没有规定。不同企业的审计委员会具有不同的职责，其参与的层次也不一样。

尽管职责和义务上的差异是必要的，也是适当的，但有效的审计委员会一般仍具有共同的性质和功能。管理层对财务报表的可靠性负责，但有效的审计委员会对其也具有重要的作用。审计委员会（如果没有审计委员会，就是董事会自己）具有独特的地位：它有权向高级管理层询问财务报告职能行使的情况，它还有权保证这种行为正确。当管理层越过内部控制或企图错误报告财务结果

时，与强大的内部审计功能相联系或促进了内部审计功能的审计委员会，对于这类事件的调查和反应在企业中处于最佳地位。因此，上述这些就是例子说明：审计委员会或董事会必须行使其督导的职责达到直接关注重大的事件或情况。

Treadway 委员会为此提供了“一般的指导”，包括：委员会的规模，任期，会议日程和参与者，董事会的全面报告，成员对于公司运营的知识，内部、外部审计计划的检查，对于新的会计原则的采用，重要的估计，留存收益，或有损失及年度间的变化。

Treadway 委员会强调审计委员会的价值，并认为所有的上市公司都要建立由独立董事组成的审计委员会。纽约证券交易所要求建立这样的审计委员会，全美证券商联合会要求那些在纳斯达克上市公司的审计委员会要有多数的独立董事。Treadway 委员会认识到，特别是对于小的新上市的公司，要招募到足够的有资格的独立董事存在着实际上的困难。它也认识到，也可能存在着与审计委员会具有同等功能的程序和控制。尽管没有对于审计委员会的普遍要求，但很清楚，内部控制会因审计委员会的存在而加强。甚至对于小的公司从实际的角度来看，具有由独立董事组成的审计委员会也至关重要。

补偿委员会

这样一个委员会可以使补偿的安排得到强调，这种补偿有助于企业实现目标，避免不恰当地以长期业绩为代价来强调短期结果。

财务委员会

这个委员会用于控制资金的主要运用和确保资本支出的预算同经营计划的一致。

任命委员会

这个委员会提供对董事或许还有高级经理候选人选举的控制。

职工福利委员会

这个委员会督导职工福利计划，并使其同企业的目标一致，使信托职责得到恰当分散。

其它委员会

还可能有督导特殊领域的董事会的其它委员会，比如道德委员会，公开政策委员会或技术委员会。一般说来，这些委员会只是建立在大的机构中，或者有时建立在处于特殊情况中的企业。

内部审计师

内部审计师直接检查内部控制并提出改进意见。根据国际内部审计师协会制定的标准规定，内部审计的范围应该包括检查和评估企业内部控制制度的充分性和有效性，以及履行所承担职责达到的工作质量。这个标准规定，内部审计应该：

- “检查财务和经营信息的可靠性和完整性，以及用于确认、衡量、归类和报告这类信息的方法。
- “检查那些用于确保政策、计划、程序、法律以及规章（这些对经营和财务报告有很大的影响，并且决定企业是否合法）等制度得以遵循的控制系统。
- “检查保护资产的手段方法，而且，如果合适，证实这些资产的存在。
- “评估资源利用的经济性和效率性
- “检查确定日常运营或项目的工作结果是否同既定的目标一致，是否按照计划进行”。

企业中所有的行为都包含在内部审计的职责范围内。在一些企业中，内部审计的职能主要是对于经营的控制。比如，内部审计师可能会定期检查生产质量，检查给顾客送货的及时性，或者评估车间安排的效果。在另一些企业中，内部审计的职能可能主要集中于遵循性或与财务报告相关的行为。

内部审计师协会标准也规定了内部审计师履行其职责的职业特点。这些标准规定了内部审计师必须独立于其审计的活动。他们通过在企业中的地位 and 权力以及对审计目标的认识，具有或应具有这样的独立性。

审计机构的地位和权力包括向组织中有足够的权力个人（他能确保适当的审计范围、审计考虑的因素和反应）的报告路线；在董事会或审计委员会同意的情况下选举和罢免内部审计的负责人；内部审计师进入董事会或审计委员会的途径；作为内部审计师跟踪所发现的问题并提出改进意见的权力。

内部审计师只有在其对于审计事务的判断不受他人辖制时才是客观的。这种对

客观性最主要的保障就是内部审计人员的适当分工。这些分工应该避免潜在或实际的利益冲突和偏见。人员的分工应该定期轮换，并且内部审计师不应承担经营的职责。同样，他们也不应负责审计其最近涉及的与以前运营分工有联系的行为。

应该认识到，内部审计的功能并不象一些人认为的那样，对建立或维持内部控制制度有主要的职责。正如前所述，那是总裁和一些被规定了职责的主要经理的职责（其中可能包括首席审计师）。内部审计师在评估内部控制制度的效果上发挥着重要作用，因此有益于持续的效果改善。由于在一个企业中所具有的地位和权力，行使职能时具有的客观性，内部审计部门在影响内部控制中发挥着非常重要的作用。

其它部门人员

 内部控制在某种意义上是企业中每个人的职责，因此应该成为每个人工作中明示的或暗含的一部分。这可以从两个方面来说。

- 首先，所有的员工实际上都会对控制有所影响。他们会产生内部控制制度所需的信息——比如，存货记录，生产周期资料，销售或支出报告——或者作出其它影响控制的行为。这些行为可能包括进行协调、跟踪例外报告、进行实物盘点或调查成本变化或其它行为的表现。对这些行为的关注直接影响内部控制制度的效果。

- 其次，所有人员都有责任向高层机构报告经营中存在的问题，对行为守则的违反，或其它对于政策的违反或不合法行为。内部控制依赖检查和制衡，包括职责的分离和员工的不违规（“looking the other way”）。所有人员应该明白抵制上司要求参与不适当行为的压力的必要性，而且在正常的报告途径之外应该还有允许报告此类事情的渠道。

内部控制是所有人的事，而所有人员的作用和职责都应该规定清楚并能有效地交流。

外界机构

许多外界机构也能促成企业目标的实现——有时与企业内部控制活动相平行进行。在其它情况下，外界会为企业的内部控制活动提供有用的信息。

外部审计

大概没有哪个外界机构在促成企业的财务报告目标实现上发挥的作用会象独立注册会计师那样重要。他们为管理层和董事会提供唯一独立和客观的意见，并且促成企业财务报告目标及其它目标的实现。

在审查财务报表时，审计按照公认会计原则对报表的公允性提出意见，借此促进企业财务报告目标。虽然企业的内部控制制度可以为财务报表的公允性提供一定程度的保证，审计却可以使这种保证达到更高层次。而且，审计经常为管理层实行自己的控制职能提供有用的信息。

关于财务报表的审计对企业的内部控制制度的关注，人们有不同的看法，有人认为，对企业的财务报告表达了一种标准的，无保留的，“清楚的”意见的审计师就是认为这个企业的内部控制是有效的。其它人认为，至少，审计师为了要查知企业所有的或大部分的缺陷，必须对内部控制制度进行充分全面的检查。这两种观点都不准确。

对财务报告审计深入地考察，首先可以帮助认识到企业可能有一个效率低的内部控制制度，但审计师仍然可以提出这样的意见，说财务报表“表达得公允”。这是因为审计师的注意力集中于财务报表上。如果需要对财务报表进行修正，他们就对其进行修正，在这种情况下，也能形成“清楚的”意见。审计师是对财务报表，而不是对内部控制制度提出意见。不充分的控制会影响审计，并使其成本更高，因为审计师在形成意见之前需要对财务报告的账面余额进行更深入的检查。为了制定审计计划，审计师必须对内部控制制度获得足够的认识。对于内部控制注意的程度随不同的审计而变化。在一些情况下，会给予相当多的注意，而在另外一些情况下，会给予相对少的注意。但即便在前一种情况下，审计师通常也不会去调查所有可能存在的内部控制缺陷。

在多数情况下，审计师进行财务报告审计确实为管理层实行与内部控制相关的职责提供有用的信息：

- 通过交流审计发现，分析性信息以及提出应采取必要措施以实现既定目标的建议
- 通过交流发现的有关内部控制缺陷并提出改进的建议。

这些信息经常不仅与财务报告相关，也与经营以及遵循性的行为相关，而且会对促进企业在各个领域的目标实现。这些信息报告给管理层，并且视其重要性的程

度，向董事会或审计委员会报告。

立法者与监管者

立法者与监管者通过建立内部控制的要求或对特殊部门的检查来影响许多企业的内部控制制度。许多相关的法律和规则仅仅针对财务报告的内部控制，当然也有一些——特别是运用于政府机构的那些——针对经营与遵循性目标。

1977 年的国外腐败实务法 (The Foreign Corrupt Practice Act) 要求上市公司建立和维持满足特定目标的内部会计控制制度。其它联邦法律和规则应用于联邦财务资助计划，这项计划提到了从公民权利到现金管理等许多事项，并详细规定了内部控制的程序或施行。1984 年的独立审计法 (The Single Audit Act) 要求独立审计师报告企业对那些要求的遵守——就如象金融服务之类的行业中一些规则所要求的那样。1991 年的联邦储备保险公司改进法 (The Federal Deposit Insurance Corporation Improvement Act) 要求一些银行报告他们对于财务报告的内部控制的效果，并要求有独立的审计师的鉴证报告。

一些监管机构对他们有督导职责的企业进行直接的检查。比如，联邦和州银行的检查者指导对银行的检查，并且经常集中于银行内部控制制度的一些方面。这些监管机构提出建议，并且经常被赋予强制执行的权力。

因此，立法和监管机构从两个方面影响企业的内部控制制度。他们建立规则，为管理层确保内部控制制度满足法律和监管的最低要求提供动力。而且，依照对于某个企业的检查，他们向企业的内部控制制度提供有用的信息，提供建议，甚至有时也就内部控制制度所需要的改进向管理层提供指导。

与企业相互作用的外界

顾客、供应商以及其它与企业交易者都是提供有关控制有益信息的重要来源。

- 比如，顾客会向公司报告运输延误、产品质量差或者在生产或服务上不能满足其需要。甚至，会有顾客很积极地反应，并同企业一起努力推动必要的产品改进。
- 供应商会提供有关已经完成或正在进行的装运及帐单的报告和信息，这可以用于调查、改正单据与货物不符、核对余额。
- 潜在的供应商会将员工索取回扣告知高级管理层。

这些外界提供的信息，在某些情况下对于企业实现经营、财务报告以及遵循性目标可能特别重要。企业必须有一个接受这些信息并采取适当反应的机制。适当的

反应不仅包括处理报告反映的特殊情况,而且还包括调查问题内在的原因并对其进行修正。

除了顾客和供应商,其它人员,比如债权人,也能对企业目标的实现提供督导。比如,银行会要求提供企业履行债务条款的报告,并且推荐业绩指标或其它所需的目标或控制。

金融分析家, 债券评级机构和新闻媒体

金融分析家和债券评级机构可考虑到与企业投资价值相关的许多因素。他们分析管理层的目标和策略、以前的财务报表和潜在的财务信息、根据经济与市场条件作出反应的能力、短期和长期成功的潜能、行业业绩以及与同行业的对比等。媒体,特别是金融记者有时也会进行类似的分析。

这些部门的研究和监督行为可以为管理层在外界如何看待企业的业绩、企业所面临的行业和经济风险,可能提高业绩的创新经营和融资策略、行业未来等方面提供视角。这些信息有时会在这些部门同管理层的会面时直接提供,或者在对投资者、潜在的投资者以及公众的分析中间接地提供。无论哪一种情形,管理层都应考虑金融分析家、债券评级机构以及新闻媒体所提出的有益于内部控制的观察和意见。

附注 A 学习本文的相关事项及背景知识

早期的政府、宗教及商业机构的领导人已意识到需要在机构内部实施控制。建立了用于引导和监督各项活动的内部控制，以确保目标的实现。

随着时间的推移，不仅机构内的领导，许多其他有关方面的人也都意识到内部控制的重要性。一些人甚至指望内部控制解决一些商业领导们最初需求以外的问题。

近年来，许多公共、私有部门以及专业团体对内部控制投入了相当的关注，并对此提出了相应的建议和要求。这种活动引发了大量思考和探索，并由此产生了内控的目的、本质及有效方法等问题的不同看法。为了更好的了解这方面的知识，这里简要的回顾一下内控理论的重大发展。

对内部控制认识的重大转变源于控制的效果要保证可靠的信息。管理成长型企业越来越重视使用财务及非财务信息控制企业的活动。并为提高信息的有用性和可靠性而制定相关的制度。管理层还发现，面对机构的愈发庞大和雇员的增多，引导并限制雇员的谨慎变得至关重要了。有效的管理实践的变革为雇员及其行为的更广泛控制提供了指导。

从审计的角度看，对一家具备有效的内部控制系统的企业进行财务状况审计，把注意力集中到内控制度上，审计效率会更高。从 20 世纪 40 年代起，公共的会计和内审专业团体发表了一系列报告、指南和标准，用以说明内控制度在审计中的作用。这些出版物还指出了内控的定义及内容，其不断完善的方法以及不同部门对内控的责任。

水门事件

直到 70 年代中期，有关内控理论的发展还主要集中在制度的设计，完善内控制度的方法以及如何在审计中最好对它加以利用。1973—1976 年水门事件调查后，法律及管理部门才开始给予内部控制相当的重视。水门专项检察官办公室和证监会的单独调查揭示美国许多大公司一直对外国政府官员进行非法的或可疑的政治捐助包括行贿。为回应这些调查，国会委员会就美国公司对外国政府官员不正当的支付举行了听证，由此引出一项法案并最终通过《1977 国外腐败实务法》

(FCPA)。

《1977 国外腐败实务法》(FCPA)

除了反行贿条款，FCPA 还包括有关会计及内控的条款。这些条款要求公司的管理部门保留账簿、记录和资料以准确和公允地反映公司的交易和资产的分布，制定并修改内部会计控制制度使其足以完成一定的目标。这样，该法案的主题意思是完善的内控制度应有效地遏制不合法的支付。

紧随 FCPA 法案的实施又发生了大量与内部控制有关的事情。许多大公司扩大了内部审计的范围和职能，并且更加关注内控制度。此外，许多机构，无论是专业机构还是管理机构，都仔细研究了内部控制的各个层面并提出许多建议和指导。

Cohen 委员会

审计师职责委员会，即人们熟知的 Cohen 委员会，是美国注册会计师协会 1974 年成立的，目的是研究审计师的职责。该委员会的建议中的一项是公司的管理层应提供一份报告和披露公司内控制度状况的财务报表。还有一项建议是审计师应就管理层的报告出具审计报告。继 1978 年 Cohen 委员会发布报告后，财务主管协会 (FEI) 向其会员发出一封信，附有 Cohen 委员会的报告建议，这封信要求会员协助执行 Cohen 委员会的建议。这种管理报告越来越频繁的出现在公司提交给股东的年报中。

证券交易管理委员会 (SEC)

1979 年，美国证券交易管理委员会将 Cohen 和 FEI 的行动更向前推进一步，提议要求委托管理人应出具企业内部会计控制的报告，该规定还要求独立审计师同时出具审计报告。

SEC 的提议从很多方面看来有主要意义。它指出制定内控制度是管理层的一项主要责任。同时，它还指出有效的内控制度使投资者更好地评价经营者的业绩和他的代理责任，也便于评价中期财务报告和其他未经审计的财务信息。尽管这项提议由于其庞大的费用最终被撤销，企业披露信息的不真实以及与 FCPA 的密切相关意味着执行这项提议（经营者有义务制定有效的内控制度确保中期财务报告和其他未经审计的财务信息的真实性）的重要性。在撤销该提议时，SEC 说以后将继续探讨公开报告（信息披露）问题。

Minahan 委员会

为了在一定程度上响应 FCPA 立法和报告内控制度的提议，美国注册会计师协会 1979 年创建了内控专门顾问委员会，以帮助指导制定和评价内控制度。该委员会恰恰成立于 FCPA 实施前，目的是为了有助于查找弥补内控的漏洞。现存的内控指南主要包括审计的内容，是主要为审计师们设计的。人们认为有必要添加内容帮助管理层完成他们内控的责任。尽管该委员会不是专门为此目的成立的，但它承认报告中的指南应有助于管理层及董事会成员分析他们的公司是否遵循了 FCPA 有关内控的条款。

财务主管研究基金会

为响应 FCPA 的要求，财务主管研究基金会成立一个研究小组专门研究美国公司内控的状况。这项研究的一个主要贡献是 1980 年发表的报告，报告列举了内控的特点、条件、实践、程序和对内控定义、本质和目的的许多不同观点，以及如何有效的实施内控制度。

另一项财务主管研究基金会的研究报告发表于 1981 年，该报告指出了评价内控广义上及概念上的标准。

审计宣言

从 1980—1985 年这个期间，关于内控的审计准则得到了修改和完善。

1980 年，美国注册会计师协会发布准则要求独立审计师评价并报告被审计单位的内控情况。

1982 年，美国注册会计师协会发布公告修订了独立审计师在财务报表审计中研究和评价被审计单位的内控制度的指南。

1983 年，内部审计师协会发布一项准则，建立并修改了内审师进行内控的作用，以及他们在建立、维护和评价内控制度发挥的作用。

1984 年，美国注册会计师协会就实行计算机操作对内控的影响发布了补充指南。

法律创制权

直到 1985 年，人们对内控的关注越来越强。在受到一系列商业失败和审计失败的冲击后，一个国会的小组委员会开始就许多公共公司的规章制定者的行为，财务报告的合理性以及独立审计的有效性等问题举行听政。

为制止听政中出现的财务报告问题，立法部门被要求增加新的法律条款，包括要

求公共公司的经营者评价并报告其公司内控的有效性。此外还要求审计师就企业规章制定者的报告发表审计意见。

尽管这项新的立法并没有实施，小组委员会扩大了财务报告问题的听政，并将内部控制作为关注的焦点。

Treadway 委员会

1985 年美国注册会计师协会、会计协会、财务主管协会、内部审计师协会、管理会计师协会联合创建了财务报告欺诈全国委员会，即 Treadway 委员会。该委员会的主要目的是找出财务报告欺诈的起因，并采取措施以减少它的发生。该委员会 1987 年度的报告为公共公司的经营者、董事会成员、注册会计师业、证券交易管理委员会及其他法规制定部门、管理部门以及学术团体提出了补救措施。委员会提出了一系列指导内控的补救措施。它强调控制环境，行为标准，审计的能力以及一个活跃的、有目的的内控机能。同时再次强调经营者需报告其企业内控制度的有效性。此外，委员会呼吁赞助机构共同努力统一内部控制的概念和定义，达成共识。这些指南旨在帮助公共公司改善内控制度，提高判断其有效性的能力。

基于委员会提出的建议，在一些机构的赞助下，一个工作小组对内控理论的发展进行了全面审查，并发表了审查报告。报告建议赞助机构为建立内控制度，评价其有效性提供广泛接受的、有操作性的标准。该工作组认为这些标准应首先考虑经营者的需求，因为经营者负有建立、监督、评价和报告内控制度的首要责任。但同时，他们还建议这些标准应满足其他利益相关者的需求，被他们接受。这些人包括内部和外部审计师，教育者和管理部门。

近期的发展

此外还有一些关于内控的其他举措。美国注册会计师协会 1988 年修改了内控的审计准则。这个准则更加明确地界定了企业内控制度的结构，提高了独立审计师审查的责任，并对财务报告审计中如何评价控制风险提供指导。

此外为响应 Treadway 委员会的建议，1988 年证券交易管理委员会提出一项规定要求经营者就其内控责任和评价内控制度有效性提交报告。同时，该规定还限制独立审计师参与这个报告的提交。

此后的几年，法规的制定者就内部控制问题还采取了其他一些举措。有些针对特

殊行业如银行，借贷机构和防御设备承包商。其它的一些举措则影响所有在证券交易管理委员会注册的机构。这些立法提案包括要求经营者评价和报告内控的有效性，同时独立审计师要证实经营者的报告。一项与银行业有关的提案已经通过成为《联邦储备保险公司 1991 年增补法》。很多观察家期待更多的立法出现。

1991 年有两项内控的举措。第一，内部审计师研究基金会发布一项报告对控制和信息系统的审计提出指导。此后在这一年，美国刑罚委员会为刑事公正系统对白领犯罪量刑发布指南。这些指南大大降低了对拥有有效手段防止违法行为产生的企业的惩罚。指南主要涉及内部控制制度的遵循。

研究

多年来，内控的一些概念和观点在不断地发展，这些发展反映在法律、法规、专业准则和指南、公开的及不公开的报告和还有大量的学术刊物上。

这些出版物的范围象内控制度所能达到的作用一样广泛。包括内控的不同定义，内控作用的不同观点，如何建立内控制度，以及内控制度有效性的不同观点。

公共和私有部门对内控的日益关注使得公司的管理层，内部审计师，独立审计师，立法机构，管理部门，学术团体以及公众更加意识到有效的内控制度对管理和控制企业活动的作用。这项研究使全社会各界对内控的重要性达成共识，并帮助经营者对企业实施更好的控制。

附注 B

方法体系

本次研究使用的方法旨在使报告达到下列目标：帮助管理层改善其内部控制系统；使利益相关各方对内控制度有一个大体的了解。其发展的方向是使报告做到既与理论相符，又能满足企业管理当局实际应用的需要。

由于不同的需要，此次研究项目计划寻求利益各方的协调，包括公司管理层，立法机构，管理部门，学术界以及审计师。参与者来自不同规模的公司管理层，公有及私有部门，以及不同行业，包括总裁、财务总监、主计长及内部审计师。

该项目共分 7 个阶段：

1. 理论探讨——明确当今关于内部控制的不同概念、观点及视角。
2. 一对一访问——从专家那里获得有关概念以及公司管理层如何控制经济活动。
3. 调查表——项目小组归集前阶段获取信息，区分需要澄清信息或另外的观点，以进一步收集资料。
4. 研讨会——对初步草拟的理论框架征求意见和建议。
5. 公开披露——证实该框架是否合理，符合逻辑，是否对管理层和有关各方适用。
6. 实地测试——获得该框架中评价标准、方法和工具等方面的反馈信息。
7. 再次披露，开会讨论——以确定对前阶段暴露出的问题所作的修正是否合理。

该项目计划设计为一个渐进的过程。不是在某个阶段提出全部问题。相反，一个阶段的研究结果将作为设计下一阶段的初始投入。相应地，报告中的概念、内容及标准将随着项目的进行而不断改进，最终结论是项目各阶段收集信息的综合结果。

正如人们预料到的，一个阶段或不同阶段的许多问题存在着不同甚至相互矛盾的观点。该项目小组支持不同观点的存在，无论是单独的问题还是与其它相关的问题。同时小组重视那种相关的、符合逻辑的、和内部一致的框架。在整个项目的进行中，小组接受赞助机构顾问团的建议和咨询。该顾问团由高级财务管理、

内部外部审计师、学者定期组成，与项目小组会面审查项目计划的进行，研究草拟的框架和其它相关事宜。顾问团的意见充分的反映在报告中。

各阶段简述如下：

理论探讨

这个阶段工作主要是从现存的公开发表刊物上寻找关于内部控制的各种概念、观点和视角等相关的信息。集中在两个数据库。

会计指标数据库用于与内部控制项目直接相关的资料处理，商业信息摘要（信息库）获取的数据与财务报告的内部控制项目不直接相关，而更注重会计和审计以外的其它方面。例如：理论确定一项研究的有效性和发展与标准相关，而学术机构则关心熟练程度。

项目小组阅读大约 1700 篇被认为包含有用信息的信息、书籍及其它出版物的摘要，只要这些出版物被认为有能含有有用的信息。从这些摘要中，选出大约 700 个有用的信息来源。这些来源会被引起小组的重视的其它资料补充。

一对一的访问

访问的对象主要是公司总裁，财务总监，立法者，规章制定者，注册会计师，管理咨询人员及学者。

根据公司的规模、地理位置、所处行业和业主特点等组成的 FINEX 数据库，由决策研究公司（DRC）从该数据库中随机选出受访的公司管理人员。此外还需要补充由财务主管研究基金会、项目组和顾问团选出的其它个人代表。

访问由下列人员组成：

总裁	7
财务总监	14
主计长	2
内部审计师	1
立法者和规章制定者	8
大、中、小型会计和咨询公司的高级主管	8
学者	5
合计	45

许多受访者由其同僚陪同。访问通常由项目小组的两位成员按照项目小组在决策研究公司协助下制定的访问指南进行，访问结果按照标准的格式归纳收集。

调查表

调查表是为了在前一阶段获取信息所反映出问题的基础上，以利于项目小组获得更多的信息来源。

调查表寄给公司主管（包括总裁，财务总监，主计长，内审师），董事会成员，立法者和规章制定者，外部审计师和学者。

被选中的公司主管由 DRC 按 FINEX 数据库随机选取，董事由项目小组根据前一年发表的代理协议选出。立法者和规章制定者由项目小组根据访问的结果选出，且有特定的职能划分如银行业和保险业。外部审计师在美注协提供的名单上选出，此外还包括遍布在全国范围内不同规模的会计和咨询公司的合伙人。学者，包括会计、金融和管理领域的学者，是由项目小组根据 1989 年出版的《会计及从业人员目录》或由各商学院的院长推荐而来。

下面的表格归纳了这些人员的构成：

总裁	34
财务总监	108
主计长	78
内部审计师	86
董事会成员（包括审计委员会主席和成员）	26
立法者和规章制定者	60
外部审计师	49
学者	81
合计	522

研讨小组

为了收集人们对前一阶段形成的草拟报告的意见和建议建立了 8 个研讨小组。为 5 家赞助机构分别设置研讨小组，还要为联邦立法者和规章制定者，金融服务行业的主管，以及美国律师协会的商业会计和法律委员会代表分别设置研讨小组。每家赞助机构选派代表出席研讨小组，项目小组派代表出席由立法和管理机构组

成的研讨小组，FERF 派代表出席金融服务业的研讨小组，美国律师协会（ABA）主席派代表参加律师协会的研讨小组。

每个研讨小组在两名项目小组成员的主持下进行。研讨前，与会者每人收到一份需要讨论的草拟报告，小组讨论包括对项目及草拟报告的简要陈述，对由项目小组及与会人员选中议题的讨论。

公开披露

公布报告的草案以收集公众的意见。大约有 40000 份报告会被分发到 5 家赞助机构的成员、各公司总裁及立法者和规章制定者手中。

从下表显示的人员中共收到 211 份反馈意见：

总裁	13
财务总监及主计长	107
内部审计师	37
立法者和规章制定者	12
外部审计师	23
学者	14
其他	5
合计	211

实地测试

为了获得更多的反馈，由 5 家公司对框架中的评价标准、方法和工具进行实地测试。这些公司来自不同的行业，规模从年销售收入 1000 万美元以下到数十亿美元不等。每个测试单位在关注测试各部分的同时，至少要对一个具体项目进行测试，有些单位测试财务报告的控制评价，还有的单位将控制的执行及操作情况也包括在测试范围内。

再次披露，开会讨论

修改后的报告分发给前一次披露中有回反馈意见的人们，赞助机构指定的团体和其他索取报告的人手中。这次披露大约发出去 3000 份报告，共收到 45 封反馈信。同时，与以前的研讨会规模相似，共举行了 12 次会议以收集对就修改后草案的意见和建议。四家赞助机构共举行了 5 次会议，联邦银行的代表，证券交易管理

委员会和通用会计办公室，美国律师协会的商务会计和法律委员会，美国银行协会，董事会成员，审计委员会成员，美国注册会计师协会的监管委员会也分别举行了会议。此外还为没有出席上述会议的其他人举行了一次公开会议。

致谢

此项目顾问团和 Coopers & Lybrand 真诚感谢为此次研究做出贡献的人们。

下面的人在小组讨论中提出过意见和建议，他们是：Lewis E. Burnham, Phillips 石油公司总审计师；John H. Dykes, Engraph 有限公司副总裁兼财务总监；Williard E. Hick, Mass. 互助生命保险公司第二副总裁；James K. Loebbecke, Utah 大学商学院会计系；James L. Moody Jr., Hannaford Bros 公司主席兼总裁；Donald S. Perkins, Jewel 公司前任董事会主席；Ewen Robbins, Eeradyne 公司副财务总监；Robbert J. Sack, Virginia 大学 Darden 研究生院讲师；Edward J. Sot, Merck & Co. 主计长；John B. Sullivan, 德勤会计师事务所合伙人；Wanda A. Wallace 博士, William and Mary 大学商学院。

下面的人在此次研究中作为 Coopers & Lybrand 公司的顾问，他们是：Henry R. Jaenicke, Drexel 大学会计教授；Alan J. Winters, 南卡罗里那大学会计教授；Maureen Berman, 决策研究公司。

财务主管研究基金会的 Roland L. Laing 参与了该项目初期的研究工作。

许多其他人，包括公司管理人员，立法者，审计师和学者也将他们宝贵的时间和精力投入到的此项研究的不同方面。在此一并致谢。

很多团体都使用“内部控制”这个词，但对他们来说，这个词表示的含义却不尽相同。在实务和理论中，不同的团体选择不同的术语和涵义以满足其内部控制的需要。

尽管对内部控制的不同看法是有必要的，但这种不同也阻碍人们对内部控制达成共识。企业经营者，财务主管，董事，独立审计师，内部审计师，立法者及规章制定者，投资人及债权人等对内部控制均有不同的理解。

在尝试给内部控制下定义前，我们有必要重温一下“控制”及“内部”这两个词的含义，然后再对看一下各个组织的不同看法。

“控制”一词现有的定义包括：执行、限制或引导影响；指导和管理的能力和权威；引导、规范和协调商务活动；以及用来规范并指导操作系统的一种机制。这些定义的共同点是他们都有规范并引导商业活动的含义，但对于他们期望的结果却有不同的看法。这种不同引出了下面的定义：

“对既定的目标进行有目的的影响”。

这个定义包含两个含义：

为了影响控制，必须有既定的目标，没有目标，控制则毫无意义。

这种控制包括影响某些人或某些事——如某一经济实体的人，某一部门，或者整个企业——以最终朝着既定的目标前进。

建立目标并采取行动实现目标对控制的概念至关重要。这些行动可能包括引导、规范、限制和管理。控制的结果是，他们必须努力实现既定的目标。

字典里对控制的定义是：“在某物/事的范围和限制内存在或调整。”这个某物/事是指一个企业或一个实体。即焦点要集中在某一企业内部，或某一实体内部如大学、政府机构、慈善机构或雇员福利计划。这样，内部控制则包括如某一实体的董事、管理层或其他人包括内审师的活动，但不包括规章制定者及外部审计师的活动。

不同的观点

对内部控制的不同观点并不是不能接受的。内部控制与实体的目标紧密相关，而

不同的群体出于不同的原因有着不同的目标。

管理层

管理层对内部控制的想法是从整个机构的全局出发。它的责任是发展该实体的目标和战略，引导其人力和物力资源实现目标。

对管理层来说，内部控制有广泛的含义，包括为确保实体完成目标所定的政策、程序、和采取的行动。具体指所有采取的活动，以确保管理层能够引导和监督各项操作，对内部和外部发生的相关事宜有所察觉，辨别并处理风险。

内部控制使管理层根据变化的情况及时采取行动。如生产、销售、存货水平及其他方面的信息影响决策的有效制定。其它相关的外部事物如生产工艺的变化，行业革新，竞争者、消费者、供销商采取的行动，法律的新动态等也同样影响决策的制定。这就要求管理层尽量减少负面影响的冲击，利用出现的机会。内部控制有助于管理层完成其环境、社会及法律方面的责任。包括员工福利计划，工人安全条例以及正确排放废弃物的规定。遵纪守法可保护企业的声誉。

内部审计师

内部审计师协会将内部控制定义为“管理层为确保其完成既定目标所采取的一些行动。”明确指出这些活动的本质：控制是管理层合理计划、组织和引导的结果。对内部控制的这种观点与内审协会对内审作用的认识是一致的。“内部审计检查、评价计划、组织和引导过程，以确定其是否能合理的保障目标的实现。”一个实体内所有的系统、过程、机制和活动都包括在内部控制的范围内。实务中，内审机构的活动范围根据该实体的特点而变化。

独立审计师

由于注册会计师作为财务报表的审计者，他们对内控的关注主要集中在支持或影响该实体外部财务报告的那些方面。

美国注册会计师协会最初将内部控制定义为“为合理确保特定实体目标的实现而制定的政策和程序。”这个定义与前面提到的管理层和内审师们所作的定义是一致的。

但这个广义的定义通常被缩小到与注册会计师的责任相关的内部控制的范围。当某一实体记录、加工、综合并且报告财务数据的能力与财务报告中体现的声明一致时，内部控制的范围就被缩减为与财务报表审计相关的政策和程序了。

尽管通过审计计划的执行，注册会计师能够了解一个实体的目标、战略和其竞争地位。他们在审计财务报表时无需了解企业内部控制的各个方面。这种关注范围的缩小在其它团体那也是类似的。

其它外部各方

立法者、规章制定者、投资者、债权人对内部控制有各自不同的观点。

立法者和规章制定者已形成了许多符合他们职责的内部控制的定义。这些定义通常与其监管的活动类型相关，有可能超出企业的目标：资源的使用需符合法律和规章制度，减少资源的浪费、损失和滥用。在特定的时候，如 1977 年的 FAPC 法案，政府主要关注某个特定领域。FCPA 将内部控制定义为下列事情提供保障：完成既定的目标；根据管理层的授权处理经济活动；按照公共会计准则记录交易事项；接近企业的资产必须有管理层的授权，比较实物资产和账目价值。

投资者和债权人需要的主要是财务方面的信息，这些信息需经过注册会计师的确认。其它外部各方需要不同的信息。但是，他们却很少有要求特定的实体提供他们所需的信息。所以，他们通常不对内部控制下定义。

定义

存在对内部控制的不同认识的同时，还存在共同点。内部控制通常被认为整个机构内部的一系列活动。此外，内部控制还被普遍认为是有助于实现机构的目标，同时还是实现目标的一种手段。一个实体的内部控制包括为培养其员工有恰当行为而采取的积极措施。这些共识与前面提到的内部控制是“朝着既定的目标作有目的的影响”的观点是一致的。这里内部控制的定义包含两个重要内容：

一个实体必须有要实现的目标。

为实现这个目标，必须采取一定的行动。

尽管不同团体可能使用不同的定义，某些特定的定义必须足够明确，以免引起误解。因为实现目标是建立内控制度的目的，所以，内部控制的基本定义应该是非常全面的，全面到足以概括所有实体的大部分目标。内部控制和目标之间的这种联系给内部控制下定义提供了基本要求。

核心定义

这次研究中所使用的核心定义满足了这些要求。

内部控制是一个过程，它受一个实体董事、管理层和其它人员的影响，它的制定

应满足下面目标的实现：

经营的效果和效率

财务报告的可靠性

遵守法律和法规的规定

上述三个目标既是独立的，又是相互重叠的，它们满足的是不同的需要。单独强调任何一个目标通常都能很好地评价控制的有效性。

上述内部控制的三个或其中之一个方面是有效或无效的。如果一个实体的董事能够为下列事项提供保障，则可以独立的判断内控的任一方面的有效性。

这些董事了解该实体目标实现的程度。

公布的财务报告是可靠的。

遵守法律和法规的规定。

特殊目的的定义

尽管一个实体或许会考虑到内部控制的三个目标，它往往更关注某个目标，甚至是某个目标中的特定活动。这种对特定方面的关注导致对某些活动或目标下特殊的定义。当明确了特定的目的后，特殊目的的定义通常由核心定义衍生而来。

一个为保障销售活动的效果和效率这一特殊目的而下的定义，从内部控制的核心定义中衍生出来可能是这样的：

对销售活动的内部控制是一个过程，它受到该经济实体销售副总裁和其它人的影响，它的设计是为了保障该实体 19xx 年销售预算目标的实现。

如果某一实体的销售副总裁能够保证他或者她了解该实体 19xx 年销售预算执行的程度，那么这个实体关于销售活动的内部控制制度可以说是有效的。

对于财务报告的可靠性这个特殊目的来说，内部控制的定义可能是：

编制会计报表的内部控制是一个过程，它受到董事会、公司管理层和其他人员的影响，它的设计是为了保障该实体能够编制出可靠的财务报告。

如果某一实体的董事会或管理层能够保证该实体的财务报告是可靠的，那么这个实体关于编制会计报表的内部控制制度可以说是有效的。

同样的，以遵守政府制定的法规法纪为特殊目的的定义可能是：

遵守政府制定的法规法纪的内部控制是一个过程，它受到董事会、公司管理层和其他人员的影响，它的设计是为了保障政府制定的法规法纪能够得到遵守。

如果某一实体的董事会或管理层能够保证政府制定的法规法纪得到遵守的话，那么这个实体关于遵守政府制定的法规法纪的内部控制制度可以说是有效的。

附注 D

反馈意见

如附注 B 中提到的，这份报告的草案发出去征求意见和建议，共收到 211 封回信。这些信包括了几千个人就所讨论问题的意见。另外，报告的修改稿又发给第一次回信的那些人手中，还举行了多次讨论会议，这次收到了 45 封回信和许多口头意见。在修改报告时所有这些回馈意见都经过仔细的考虑。

本附注总结了一些回馈意见和报告的最后修订结果，还说明了为什么有些意见被采纳了而有些意见却没被采纳。

定义

定义的广度 披露的草案对内部控制下的定义是广义的，它包括一个实体要达到的三个目标——经营的效果和效率，财务报告的可靠性，法律和法规的遵循性。有些人认为内部控制的定义应当是广义的，其他人则认为这个定义范围太广了，应当只包括财务报告的可靠这个目标。后来收到的反馈意见指出范围太广的定义可能会使一个实体在实现这些目标时产生误解或不适当的期望，并且这样的定义与框架中提交外部报告的指导思想不一致，框架里只提到了财务报告的可靠性这个目标。

下面总结一下广义的内部控制定义三个理由：

概念的基本要求应是全面的。因此内部控制的定义应当包括它要达到的所有目标，其中包括具体目标。广义的定义有助于沟通，减少误解，减少“期望落差”（对内部控制期望达到的目标和实际能够达到的目标之间的差异）。

广义的定义容纳了狭义的内部控制定义，它允许着重注意内部控制的某一具体方面。

内部控制的三个目标——经营、财务报告和法律法规遵循之间是相互关联的。同时，内部控制本身是管理和经营的组成部分。因此，如果仅给内部控制下一个狭义的定义，它们之间的大部分联系将会中断。如，仅限于财务报告。

内部控制目标的分类 披露的草案指出了内部控制的三个目标，但没有明确给出内部控制的定义。有些人建议应当将这些目标包括在定义中。

将这三个目标明确的包括在定义中是出于两个方面的考虑：一是因为它们对内部

控制的非常重要，二是将它们包括在定义中有助于明确的关注其中任一方面。

过程 披露的草案将内部控制定义为一个过程。有些人同意这种观念，其他人则认为内部控制是一种状态或条件。

最终的结论是内部控制实际上是一个过程，为了更好的将它与管理过程联系起来，同时突出它的动态特性，内部控制应继续定义为一个过程。当然，一个过程在特定的时点上可以是一种状态，因此最终决定将内部控制定义为一种状态的定义也应写出来。于是，最终的报告给内部控制下了两个定义：一个是内部控制是一个过程，另一个说动态内部控制是一种条件或状态。

特定目标 披露的草案提到了实现内部控制的“特殊目标”。有人建议正确的术语应是“某一实体的特殊目标”，因为没有任一目标是适用于所有实体的。修改后的报告反映了这一点。有效的内部控制的定义反映出，“经营目标是特别针对某一实体”这种观念。但这个定义同时指出财务报告的可靠性以及合法合规是适用所有实体的。

合理的保证 报告草案的定义中提到了“合理的保证”这一术语。有些人认为尽管内部控制不能提供绝对的保障，“合理”这一词也不应出现在“合理的保证”这一术语中，因为管理层将使用它来规避责任。还有些人认为“保证”这词用词不当，因为“保证”意味着保证目标的实现。因此“合理的”这一词是另一种选择。

“合理的保证”这一词最终保留在定义中，因为它被认为最恰当地描述了内部控制的局限性。许多这方面的文章都使用这一术语，并且在经济领域它能够得到正确的使用和理解。为了更好地阐述“合理的保证”的含义，最终的报告在内部控制的局限这章中将这一术语与其它问题联系起来。这种联系是为了全面地描述“合理的保证”一词，同时也反映了一些人的考虑。

就“合理的保证”一词的另一个争论是对谁提供保证。报告的终稿阐明内部控制是一个管理工具，是管理当局和董事会使用的工具。

定义中内部控制的具体内容 披露草案的定义包括了内控的 9 项内容。有些人建议将这 9 项内容排除在定义外，因为它使定义变得冗长且很难理解。其他人则认为定义中应保留这九项内容，因为它们是内控的核心内容，应作为定义的一部分，此外，将它们保留在定义中有助于理解所有的内容都适用于内控

的三个目标。

最后，定义中没有包括内控的九项内容，这样的定义更简洁也没有因此减少强调与此有关的概念。并且，为了更好地阐述内控的目标和内容之间的关系，又增加了一个图表来说明它们之间的关系。

实现经营目标 有人说披露的草案中的定义带有“一个实体有效的内控必须实现它的所有目标”这样的含义。他们普遍同意内控制度能够为经营目标的实现提供信息，他们建议定义中应反映这点。

报告终稿的定义增加了这点。报告明确指出有效的内控应使经营者和董事会能够了解企业经营目标实现的程度。

财务报告的可靠性 披露的草案中对财务报告使用了“可靠性”这一词。有人指出使用这个词带有不可靠的含义，所以应该替换。同样，“重大方面正确”也应避免。

最终的报告保留了“可靠”一词，由于它通常的用法，现在用于公允地编制财务报表。“重大方面正确”一词被删除了。

资产保全 有些人，尤其是那些主张内控仅限于保证财务报告目标的狭义定义的人，建议将资产的安全、完整包括在定义中。

最终的报告维持了草案中对保护资产的概念，指出保护资产属于经营目标的内容，它的某些方面属于内控三个目标的具体内容——经营、财务报告、遵循性。报告继续讨论了保护资产内部控制的环境。

内容

内容的分类 有人同意前面提到的内控九项内容，然而，也有人则认为九项内容太多了，而且这此内容中存在重叠和冗余。对于如何重新分类有很多建议。

最终决定内控内容的分类应是有效率的，在不遗漏主旨的情况下避免不必要的重复，下面是这些内容的重新分类：

—

草案	终稿
公正，道德和有效内控环境	内控环境
目标	—

评估风险、变化管理	评估风险
控制程序	控制活动
信息系统沟通	信息和沟通
监控	监控

草案中的“目标”已被删除并作为一项单独的内容。有人认为建立目标是管理的一部分而不是内控的一部分，这种观点被采纳了。终稿体现了这个认识，将制定目标作为内部控制的前提。

术语的使用有两种变化，“控制程序”变为“控制活动”，这样反映出无论是政策还是执行的程序都包括在内。“系统”一词不再和信息连起来使用，以避免受数据处理系统意思的限制。信息和沟通是一个更广的概念。

确定效果 披露的草案中要求提到内部控制的全部九项内容以说明内控的有效性，有人对此提出质疑。他们认为这些内容应综合考虑，其中一项内容的不足或漏洞可以通过其它内容弥补。

终稿中保留了草案的这项规定。但也同意这九项内容可以互换，其中一项不足可以通过其它各项弥补。。。。。

内部控制和管理过程

管理活动 有人认为内控是管理活动的一部分，是管理过程中的一个重要部分。但草案中没有指出内部控制包括整个管理过程。他们说这就意味着内部控制可以保障该实体目标的实现，这必然继续并加大了现存的期望落差。

考虑到这项建议，终稿中明确区分了内部控制和管理过程其它方面的不同。它明确制定目标、做出决策、执行交易和计划等管理责任属于管理活动，它们和内部控制组成一个整体，而不是内部控制系统的一部分。

避免经营失败 除了上面提到的各项外，有人指出草案有“有效的内部控制制定能够避免经营失败和其它问题”这样的含义。这同样会扩大期望落差。他们建议强化内部控制的局限性。

报告的终稿中特别强调了内部控制的局限性，指出内控不能保证目标的实现。内部控制不是一剂万灵药。有效内控定义的增加部分和内部控制与管理过程的区别中也谈到了这点。

作用和责任

经营者的责任 有人建议报告应更明确指出经营者对董事会负有经营管理责任。

报告经过修改后指出经营者有义务建立内控制度，向董事会表明这些内控制度能够为实现该实体的目标提供合理保障。反过来，董事会进行管理、指导和监督。

董事会和审计委员会 有人建议报告应建议审计委员会由外部董事组成，因为独立能够加强委员会工作的效力。有人说正如有效的内部控制要求的，董事会应有大部分外部董事。必要的时候，这对经营者是个挑战，他们能够对经营者的道德和公正有个客观的看法。

人们同意独立的审计委员会带来的好处是很值得的。正因如此，报告的终稿建议并要求有一个独立的审计委员会。报告还指出独立审计委员会的优点和期望，也意识到有些公司实际的局限性。最终报告明确了一个活跃的董事会对有效的内部控制是必要的（这里也有例外，象小公司它们通常没有外部资金来源）。尽管审计委员会中可能没有必要大部分是独立董事，但有相当一部分是独立董事却是必要的。

大公司与小公司

有人说草案主要适用于大公司，对中小公司不太适用。

讨论结果表明尽管报告的草案本意是要适用于所有公司，尤其是那些需要引导、评价和提高内部控制制度的小公司，但这一要求在草案中体现的不明显。为此，就内部控制如何适用于中小企业这个问题增加了讨论，报告的终稿将这些讨论加进每一相应的章节。

对企业外部各方的报告

草案中有一章讨论了经营者向企业外部各方报告其内部控制制度。人们对此反应不一，还提出了许多建议。

反对者认为向企业外部报告内控制度超出了研究范围。此次研究是应 Treadway 委员会的要求进行的。目的是为了给内部控制下一个通用的定义，指导和判断内控制度的效果，改善内控制度。如草案中提到的，经营者的报告不是内部控制的一部分，所以一个实体无需因为它有个有效的制度而对外报告。这些人认为经营着对外报告是一个重要的公共政策问题，应寻求适当的法律法规论坛解决。

赞同者认为管理报告是经营管理的一个重要问题，并且与建立内控框架的报告相

关。他们指出许多大公司都要提交给股东年度管理报告，对此给予指导是很有用的。

有人建议将管理报告作为附注或形成单独的文件。他们说尽管这个讨论不是内部控制的一部分，但应该给对此感兴趣的人提供指导。

讨论结果将管理报告从主报告中单独分离出来。管理报告与内控的定义无关，也不能决定内控的效果。但是由于许多公司需要或者准备出具内部控制的报告，因此决定就此问题进行讨论，以期对读者提供指导，讨论的结果将单独成册。

其它

谨慎人概念 在谈到内部控制的局限性时，草案提出谨慎人这个概念。有人说谨慎人一词来自民事侵权法，与法律的可靠性相关，放在这里不合适。后来这个讨论换成了另外一个讨论：做与内部控制相关的决策时需要的判断。

表达形式 草案的长度、格式、形式和语气都经过了讨论，就报告的表达形式提出了许多建议。

讨论结果是报告将根据这些建议重新排版。草案中的管理层总结被更简单的概述替换，并单独发表。草案中对外的管理报告和评价工具，由于它们不属于这个框架的组成部分而单独成册。此外，重复的词语被删掉了，报告显得更简洁有效。

目录 有人建议应提供参考文献的目录，这些文献是指该项目研究阶段参考的文章和出版物。最终决定文献研究中使用的参考文献不编制目录。因为文献研究仅仅是形成这个框架的众多信息来源之一，并且一个阶段的研究成果是作为设计下一阶段的投入，文献与最终的报告之间没有直接联系。因此得出结论没有必要编制参考文献目录，它甚至会引起误解。

术语汇编 有人建议加上本次研究中使用的术语汇编会有一定帮助。大家一致同意术语汇编有助于理解关键词汇，促进沟通，因此，报告的终稿加上一节术语汇编。

评价工具 有人反映评价工具可能会被理解成评价内部控制有效性的标准。如果要求出具管理报告，规章制定者有可能用这些评价工具替代他们目前使用的评价工具，对于这一点，代表们表示了关注。还有人认为评价工具代表着重要的指导思想。

报告草案中提到的工具旨在表明一种技术，这种技术有可能在评价内部控制时全

部或部分地使用。报告的终稿更加突出了这个意图，并强调这些工具作为一种指导去示范如何进行评价。为了说明评价工具不属于本次主要框架的一部分，它们单独成册。同时还指出那些使用这些评价工具的公司，应做必要的调整以适应其各自的需要。

不受保证的规则 这个框架可能导致不受保证的规则，较高的执行成本和增强的可信度。这与内部控制定义的广度和管理报告相关联。对此，代表们表示了关注。

正如前面提到的，最终的报告指出了内部控制的三个种类的不同，并讨论了它们之间的区别。此外，对企业外部各方的报告进一步探讨了这种区别并且对第二类即财务报告的控制提供明确的指导。

附注 E

术语汇编

应用程序控制——应用软件中设计的程序和 Related 的人工操作程序，旨在确保完成准确的信息处理。如：电算化的支票，连号支票和操作程序。

种类——内部控制、控制活动或控制的三个目标之一。这些种类是经营的效率和效果，财务报告的可靠性及法律法规遵循性。它们之间有重叠，以致某一特定的目标可能属于不同种类。

遵循性——指对适应于一个实体的法律和法规的遵循性。

要素——内部控制的五个要素，即控制环境，风险评价，控制活动，信息和沟通，以及监管。

计算机控制——（1）由计算机执行的控制，如已设计好的软件控制程序（与人工控制相对应）。（2）对计算机信息处理的控制，包括总控制和应用控制。

控制——（1）名词，用于主语，如某一控制的存在—属于内部控制的某一政策或程序。一个控制可以存在于任意五个内容中。（2）名词，用于宾语，如影响控制—政策和程序执行的结果，这个结果可能是或不是有效的内部控制。（3）动词，如控制—管理、建立或执行某一政策以影响控制。

准则——一套评价内部控制是否有效的标准。内控的五个要素，由于内部控制固有的局限性，表明内控是否有效。对某一类，如财务报告的可靠性，有更具体的标准。

缺陷——某一正在酝酿中的、潜在的或真实的内部控制的不足之处，或者是需要改进的地方，这种改进能够提供某一实体实现其目标的可能性。

设计——（1）目的：正如内部控制定义中使用的，内部控制的设计是为实现经营目标提供合理保障，如果这个目的达到了，则认为内控系统是有效的。

（2）计划：一个系统设定的工作方式，与实际工作方式对应。

侦查控制——一种旨在发现意想不到的事情或结果的控制。（与预防控制对应）

受影响的——在内部控制系统中使用：修改后的和保持的。

有效的内部控制——如果董事会和管理层能够合理保障下列事项，则内部

控制的三个目标可认为是有效的：
他们能够知道经营目标实现的程度。
对外公布的财务报告是可靠的。
遵循适用的法律法规。
这是内部控制的一种状态或条件

有效的内部控制系统——有效的内部控制的同义词。

实体——为某一特定目的而建立的任何规模的组织。一个实体可能是个商业企业，非盈利组织，政府机构或学术组织。其同义词包括组织和企业。

道德价值——使决策者做出适当行为的道德标准。这些价值超越了“合法”的标准而建立于“正确”的基础上。

财务报告——与“目标”和“控制”一起使用：财务报告的编制必须真实可靠。

一般性控制——确保计算机信息系统持续、正确运作而采取的政策和程序。包括数据中心操作的控制，系统软件的使用、维护、安全进入和应用系统的发展。全面控制支持应用控制的运作。其它同义词有全面计算机控制和信息技术控制。

固有的局限性——内部控制系统的全部局限性。这些局限与以下各方面有关：人们的判断水平，资源的限制，成本和收益的配比，会产生漏洞的事实，管理忽略和腐败。

诚信——指道德标准健全的一种质量或状态，正直，诚实和真诚，有做正确事情的愿望，按一定的价值和期望生活。

内部控制——是一个过程，它受董事会、经营者和其他人的影响，旨在为实现下列目标提供合理保障：

经营的效率和效果

财务报告的可靠

法律法规遵守性

当内部控制满足上述标准时，它被认为是有效的。

内部控制系统——内部控制的同义词

管理控制——由一个组织内任意级别的经理执行的控制。

管理层干预——经营者为了合法目的对既定的政策和程序进行的干预。这

种干涉在处理意外或不标准的事务时是必要的，否则如按既定程序进行则可能处理不当。（这个词与管理忽略相对应）

管理层越权——为了某种个人原因或出于提高企业的财务形象等违法目的，经营者对既定的程序和政策进行的干预。

管理过程——管理层经营一个实体进行的一系列活动。内部控制系统是管理过程的一部分。

人工控制——由人工而非计算机操作的控制。（与计算机控制对应）

经营——与“目标”和“控制”同时使用，并同一个实体经营的效率和效果相关，包括执行、盈利性目标和保护资源的安全。

政策——管理层用于影响控制的命令，是执行程序的基础。

防止性控制——为避免意料之外的情况发生而制定的控制。（与侦查控制对应）

程序——执行政策的行为。

公开财务报表——公开发布的财务报表，包括中期财务报表，简要的财务报表，以及从这些报表中摘出的数据，如盈余。

合理保证——这个概念表明内部控制，无论它设计或执行的多么完好，都不可能保证一个实体的目标的必然实现。这是因为内部控制的固有的局限性。

财务报告的可靠性——可靠指财务报告是遵循公共会计准则和其它法规编制的。公允的反映企业的财务状况包括五个基本声明：存在和发生，完整性，权利和义务，估价或分摊，表达与披露。当出具中期财务报告、简要的财务报告或者从报告中摘取数据时，公允的反映只适用与它相关的表达。

应报告的事项——内部控制中与财务报告相关的不足之处。它是内部控制设计或操作的重大缺陷，这种缺陷对该实体按照它在财务报告中声明中记录、整理、总结和报告数据的能力有负面影响。