HZ BOOKS
华章经管

信息系统与财务管理系列丛书

企业内部控制

王立彦　张继东　编著

- 展现企业内部控制发展历程的精彩画卷
- 介绍当前国际成熟的内部控制制度和方法
- 提供当今信息环境下内部控制的实用架构和技术

机械工业出版社
China Machine Press

信息系统与财务管理系列丛书

企业内部控制

王立彦 张继东 编著

机械工业出版社
China Machine Press

本书不是会计信息系统与控制信息系统的简单相加，其内容设计和体系的基本思路主要把握两点：一是信息技术大环境下的内部控制；二是内部控制如何在信息化环境中运作与发挥作用。内部控制是指以保护资产安全、防范舞弊行为、保障财务报告真实完整、提高经营活动的投入产出效率，并由此提高企业价值为目的的控制体系。本书可作为企业经理、财务管理人员及相关人员的工作参考书。

图书在版编目（CIP）数据

企业内部控制/王立彦，张继东编著．－北京：机械工业出版社，2007.8
（信息系统与财务管理系列丛书）
ISBN 978-7-111-21779-4

Ⅰ.企…　Ⅱ.①王…　②张…　Ⅲ.企业管理：财务管理　Ⅳ.F275

中国版本图书馆 CIP 数据核字（2007）第 095394 号

机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码　100037）
责任编辑：吴亚军　　版式设计：刘永青
北京京北制版厂印刷 · 新华书店北京发行所发行
2007 年 8 月第 1 版第 1 次印刷
170mm × 242mm · 10.5 印张
定价：28.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线：（010）68326294
投稿热线：（010）88379007

信息系统与财务管理系列丛书

编委会

PREFACE 前言

以我个人的观察，要让任何组织（企业、政府及非营利机构）的管理者重视内部控制，首先需要有两个前提：第一，管理者有内在动力，这有赖于激活利益动机的所有制变革，或推动激励机制的管理制度变革；第二，管理者将注意力由寻求“走捷径”转向重视“练内功”，这有赖于组织所处的法规、市场、税制等外部环境趋于规范，减少甚至消除各种“歪门邪道”。

上述两个前提在中国的经济领域中正在逐渐显现出来。所以，内部控制最近几年开始得到了实务界、理论界以及政府机构的重视。

在本前言中，我觉得有必要借此强调一些书中很少涉及而又有关的背景，以及作者对内部控制机制及实施的基本认识。

1. 内部控制架构

谈及内部控制，就不能不提美国的 COSO 报告（The Committee of Sponsoring Organizations' Reports）。1992 年，COSO 报告作为针对企业内部控制的规范文件，在实务界、理论界具有相当广泛的影响力。世界各国许多企业或非企业组织在设计内部控制系统时，普遍借鉴和采用 COSO 报告的基本内容，如对内部控制的定义、内部控制管理目标和报告目标的阐释以及内部控制系统核心要素的划分。

2001 年，美国安然公司、世通公司及之后的一系列公司财务舞弊案件引致了 2002 年《萨班斯－奥克斯利法案》（SOA）的诞生、颁布和实施。根据 SOA 第 404 条款的要求，在美国证券交易委员会（SEC）备案的上市公司必须提交年度内部控制报告。为此，所有公司必须建立基于 COSO 框架的内部控制系统，

并聘请上市公司会计监督委员会（PCAOB，依据SOA而成立，对SEC负责）认可的机构，对公司内部控制系统进行审核并出具评价报告。显然，SOA更加强化了COSO报告的影响力。

考虑中国企业内部控制的演进历史和特殊的社会经济背景以及企业内部控制实务，我曾经提出在设计组织的内部控制系统框架时的“三层次模式”，以考虑企业治理机制、管理控制设计以及运营控制实施和优化，并对三者之间的逻辑联系给以充分的重视（见图0-1）。

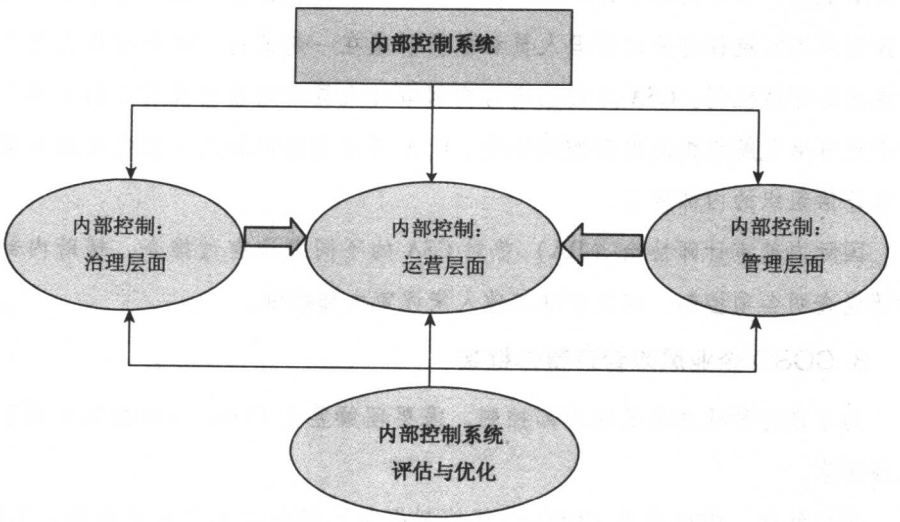

图0-1　内部控制系统框架

由图0-1可以看出，就控制重心和控制实施主体而言，内部控制系统由三个子系统组成：治理层面的内部控制子系统、运营层面的内部控制子系统、管理层面的内部控制子系统。从动态角度来看，在内部控制系统实施中，每个内部控制子系统与总系统都需要持续地加以测试、改进和优化。

2. 控制自我评估

对内部控制系统的解析、评价、优化和改进，谁是评价主体？

我认为，可以分为内部评价主体和外部评价主体两大类。内部评价主体包括组织内部上级单位对下级单位的评价和内部职能机构对组织整体的评价。外部评价主体包括注册会计师执行定期财务报告审计职能时的例行评估和注册会

计师或专业咨询机构对组织进行的专项评估。

内部评价主体和外部评价主体对公司内部控制系统进行评价的立场、角度及目的会有所不同，不过，就评价内容和方法而言是相似的。

内部评价也可以说是控制自我评价（Control Self Assessment，CSA）。CSA源于20世纪80年代后期，加拿大海湾能源公司将CSA作为评估内部控制效果及商业流程、检验传统的内部审计工具能力的手段。当时该公司面临内部控制的两难境地，公司内部审计群体就发起了协调性自我评估方法，将与专门的内部控制问题或流程有关的管理人员和职员召集在一起商讨。这个过程成为了一个成功的评估机制。CSA方法已成为内部审计人员的新型的强有力的工具，有助于更好地了解组织的内部控制环境。CSA要求内部审计人员正式组成专家小组来评估组织的内部控制。

国际内部审计师协会（IIA）曾对CSA的不同方法有过推介，辅助内部审计职能查明各项控制，或是帮助其他人来评审内部控制。

3. COSO企业风险管理整体框架

为了设计和建立有效的内部控制，需要理解整个COSO内部控制环境下的风险要素。

我们知道，1992年的COSO内部控制框架已经包含风险评估要素。不过，虽然COSO倾向于注重某个过程中的风险，2004年COSO新公布的“企业风险管理”（ERM）框架提供了用于评估贯穿整个组织或企业的风险的工具。ERM框架初稿最初公布于2003年7月，并在2004年9月发布终稿。ERM框架提供了用于理解和评价企业层面所有机构风险的一致性综合框架或方法。

ERM框架将企业风险管理定义为：企业风险管理是一个受机构的董事会、管理层以及其他人员影响的过程，它可以运用在战略制定上并贯穿于企业过程之中，设计企业风险管理旨在确认影响机构的潜在事件，并在风险偏好内管理风险，为机构目标的实现提供合理的保证。

4. 超越COSO：内部控制的其他框架

由于2002年美国《萨班斯－奥克斯利法案》对COSO内部控制框架的肯

定，COSO 框架正在成为定义、理解和评价内部控制系统的全球性框架基础。

然而，COSO 框架并不是唯一的内部控制框架。其他可供选择的内部控制框架有：①CobiT 框架。CobiT 为理解和记录 SOA 第 404 条款要求下的具有高度自动化系统的组织的内部控制提供了有用的工具。②Turnbull 框架。它适用于英国以及多数欧盟组织。③CoCo 框架。它由加拿大特许会计师协会（CICA）制定。

上述内部控制框架同样具有国际性，与 COSO 一样是恰当而有力的。以 CobiT 框架为例，它非常有特点。

5. 内部控制与信息技术

如何将内部控制与信息技术两者结合起来呢？

信息技术的飞速发展使会计领域中计算机的应用越来越广泛，从计算机账务和编表处理，延伸拓展到会计核算、财务管理和管理实践的各个领域。随着信息技术在管理领域的广泛应用，原有的内部控制越来越不适应企业的业务发展和管理的提升，信息技术的应用必将对内部控制的方方面面产生深远的影响。信息技术的发展为管理工作的重心从经营成果的反映向经营过程的控制转移创造了技术条件。为了保证企业经营方针和系统最优化目标的实现，需要采用计划、预算、内部控制、分析、稽核、报告等会计方法和手段，利用财务信息对企业生产经营过程进行控制，控制的内容包括效益控制、资产控制和风险控制等。

综上所述，强化内部控制已经成了一个世界性的管理理论和管理实践的主题。研究的空间还很大，尤其在我国，还只是刚刚开始。

王立彦

2007 年 6 月于北京大学

CONTENTS 目 录

第1章

导　论

1.1　信息技术对内部控制的影响

信息技术给企业的内部带来了新的变革、新的组合、新的变化，也伴随着新的风险。随着经济全球化及市场竞争力度的加剧，许多企业加快了信息化的步伐，以提升企业竞争力。信息技术在企业的广泛应用，不仅改变了传统的手工数据处理的方式，而且触发了企业管理模式、生产方式、交易方式、作业流程的变革，人们的行为模式也随着企业业务流程化、组织扁平化、作业信息化而发生变化。虽然信息技术没有改变企业内部控制目标，但企业内部所发生的变革对传统的内部控制观点和控制方法产生很大的冲击。因此，如何构建基于信息技术环境下的企业内部控制系统已成为目前亟待解决的问题。

1.2　信息技术对内部控制内容的影响

1.2.1　内部控制环境的改变

控制环境构成一个单位的控制氛围，是所有控制方式和方法赖以存在的运

行环境。它包括员工的诚实度和胜任能力、董事会或审计委员会、管理理念和经营方式、组织结构、授予权利和责任的方式、人力资源政策和实施。信息技术使企业内部控制环境发生以下变化。

企业组织结构趋于扁平化。由于计算机信息处理技术替代大量业务层和中间层的人工数据处理工作，数据以磁介质的方式存储在数据库中，并能通过网络迅速传输到企业的各个角落。信息技术能减少信息在传统组织的信道传输中发生延迟、失真以及噪音干扰等的几率，降低信息获取成本，扩大信息发布范围，增进组织各层次人员的信息传递与交流。原先多人分工协作的工作被信息技术重组后只需一个人就可以完成，大量的人工控制被信息系统的自动控制所取代。这种变化导致企业组织结构趋于扁平化：内部控制层次明显减少、岗位更加精简、责任更加明确、效率更加提高。

提高员工地位和素质要求。随着组织扁平化和业务流程化与信息化的发展，企业决策层次向下移动，基层员工获得更多的决策机会，同时对员工素质也提出了更高的要求。在新的信息技术平台下，员工需要熟悉计算机信息系统，持有实时、积极的控制观点，认识业务发生时信息技术所能提供预防、检查及纠正错误和识别舞弊的机会，充分应用信息技术与自己的专业知识控制企业的经营活动。企业人力资源管理将结合信息技术特点制定员工雇用、培训、提升和奖励政策。内部控制设计更强调以人为本、人－机结合的原则，通过增强员工识别风险的能力、发现问题与解决问题的能力、与其他业务人员协同配合的能力，从而利用信息技术的控制能力来提高企业内部控制的质量。

改善信息不对称状况，提高对“内部人”的监控水平。现代企业由于所有权与经营权分离，因此真实的会计信息披露对公司治理起着重要的作用。信息技术集成了业务信息处理流程与会计信息处理过程，由于数据同源并在计算机内部连续处理，有效地提高了会计信息的实时性和准确性。而投资者经过合适权限的授权，通过计算机网络就能随时访问企业数据库的相关数据，在一定程度上改善了信息不对称的状况，增强信息的透明度以及对企业经营者的监控能力，促使企业内部人员提高诚信度与道德观，规范企业经营行为。

1.2.2 风险的鉴别

信息技术应用在改变企业传统营运模式同时也带来业务流程和信息系统的新风险。例如企业在信息技术平台上运行 ERP 系统、电子商务系统、供应链管理系统、客户关系管理系统等，通过企业之间、企业内部的信息传递实现协同合作、优化资源配置。企业物流和资金流的流量、流速均由计算机精密排程，与联盟企业、市场情况环环相扣，以求用最低的成本、最快的速度、最好的质量来组织企业经营活动。因此，供应链的任何环节出现突发事件都会波及企业的正常运行，给企业带来损失。此外，由于企业所有数据存放在数据库服务器内，网络开放性、数据共享性必将增加信息系统的风险，如数据可能被非授权人员拷贝、删除、修改或破坏；计算机病毒感染、黑客入侵、使用人员违规操作也会造成计算机系统故障或信息系统崩溃。企业风险识别、评估与防范，不仅要考虑内外部环境，而且要考虑业务流程与信息流程的耦合度、协作企业的关联度、信息系统的依赖度等因素，从而规避业务流程和信息系统的新风险给企业带来的危害。

1.2.3 信息与交流方式的改变

信息与沟通是指企业在其经营过程中识别企业内、外部信息，并在组织内沟通，以便员工了解、执行其职责。

信息技术应用改变企业信息孤岛的状况，大量的企业环境信息、政策信息、经营信息、财务会计信息、作业信息集中存储在企业数据库系统内，并不断被实时更新。基于互联网、企业网、数据库技术的客户/服务器（C/S）和浏览器/服务器（B/S）混合结构的网络平台为企业成员提供了很好的沟通条件。在这个平台上，员工可以十分便捷地从计算机数据库中查阅有关的政策和法规，获取与其职责相关的控制信息，明确各自的权利与责任，了解自己的活动如何与他人的工作相关以及例外情况如何报告或处理的途径。另外，企业在网络平台上构建与利益相关者联系的机制，使组织的相关成员可以实时获取经营信息

与财务会计信息，及时进行沟通，达到最佳协同合作和利益共享。

1.2.4 监控方式和重点的改变

监控是评价一段时间的内部控制质量过程，包括及时评估控制制度的设计和运行，以及在必要的时候采取的行动。在信息技术环境下，内部控制是基于一种人－机结合的控制模式，许多控制程序、控制指标、控制方法被设置在计算机信息系统内部。因此监控的一项重要内容就是要及时了解原来设置在信息系统内的控制程序、控制参数是否过时，并针对企业经营环境变化情况，及时评估业务流程控制点的运行状态，重新调整或更改设置在信息系统的控制参数或程序。

1.3 信息技术对内部控制技术的影响

1.3.1 内部控制框架中体现“软控制”

内部控制由人来进行并受人的因素影响，保证组织内所有成员具有一定水准的诚信、道德观和能力的人力资源方针与实践是内部控制有效的关键因素之一。实践表明，基于环境现状构建内部控制机制是一种被动性的做法，故此，我们应越来越重视将道德规范、行为准则、能力素质的建设直接纳入内部控制结构的内容中来，更加强调“软控制”的作用。在信息技术环境下，企业尤其应该注重培养组织中人员的信息观念，理解企业信息化建设和管理改革、内部控制创新之间的关系，并重视和实现这个改革。信息时代同样是知识经济的时代，企业发展将主要依靠科技、知识与人才。“人本主义”作为构建内部控制机制的信条已经越来越多地被企业接受，企业管理者应当重视对人员的选择、使用和培养，这不再单纯只是内部控制的环境因素，它也日益成为内部控制结构的有机组成部分。

1.3.2 现代信息技术设计特定的控制程序

对于内部控制的研究不可能脱离其赖以存在的环境及企业内外部的各种风险因素，因此，必须从环境及其风险的分析入手。在内部控制制度下，先识别内部控制的目标，然后提出一系列与之相适应的控制政策和程序，再通过这些特定的控制程序来控制风险。在IT高速发展的今天，信息的传播、处理和反馈的速度都大大加快了，由此导致企业会经常同时改变业务和信息过程，在这个改变过程中，不能再盲目地采用传统的控制政策和程序，而必须重新评价它，以适应新业务发展的需要。我们应把注意力集中在评估特定业务环境下的风险，而不是拘泥于特定的控制程序。职责分离是内部控制的一个重要组成部分。传统上，控制程序将不同的责任分派给不同的人员以期达到互相制约的作用。但随着IT的发展，许多传统上由人来做的工作可以由计算机来代替，自动控制处理代替了分离的人的角色，从而消除了一个人执行两项不相容的工作的风险。当然，计算机环境下也要有职责分离，例如，一旦某种软件被安装并用于执行某项功能以后，它的编码、运行和维护职责就必须相分离。职责分离仍然是形成内部控制的重要程序，但在IT背景下，这个程序的适用方式发生了变化。

信息技术环境下的企业需要分离新的职责，取消旧的职责，以反映用来设计和运行系统的手段的更新。为了不断改善内部控制，使其保持高标准，应识别与更高过程相关的风险，并制定相应的控制程序以有效地降低风险。而不能让特定的控制程序限制了对技术的使用，使用技术将会使业务运行的效率和准确率更高。

1.3.3 信息技术提供了许多新的控制方法和手段

银行的资金清算系统就是明显的例证，在传统环境下，在途清算资金往往是舞弊者的通道，信息技术使实时清算成为可能，舞弊者的通道消失了，发生风险的可能性大大降低。可以说，新技术将造就新型的有效的内部控制机制。传统环境下，内部控制只能更多偏重于在检查性职能和纠正性职能上发挥作用，而信息技术将提供突破这一局限的机会。可以说，信息技术将使内部控制的“预防性职能”充分发挥，预防性职能的发挥是增加企业价值的最佳方式。

第2章

内部控制信息技术的控制架构

2.1 当今信息技术实现内部控制的特点

信息系统的实施是对企业管理的根本变革，信息系统实施的重点是观念的转变以及企业流程的重组和优化，IT 人员只是对系统的技术支持；管理人员（尤其是最高决策者）是实施工作的领导与主要参与者；企业最高决策层对信息系统要有深入的了解，对本企业存在的问题要有客观的认识，对新的系统的期望要有清晰的描述，对管理的转变要有合理的预期。

2.1.1 当今信息技术条件下内部控制的功能

信息系统下内部控制的功能主要体现在创造价值和业务集成。首先，在“价值面”上，必须对信息系统实施的内部控制能够给企业带来什么样的价值以及企业所需的投入进行分析、研究和比较，从而做出相应的“业务案例”和“价值估算”。如果没有这些，整个信息系统的实施就是纯粹的“撞大运”。其中，信息系统实施的“价值估算”是由每个业务价值链的每个环节发展而来的（见图 2-1）。

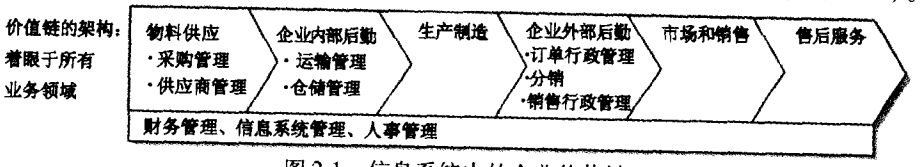

图 2-1 信息系统中的企业价值链

公司价值链的创造内容是广泛的，具体如图 2-2 所示。

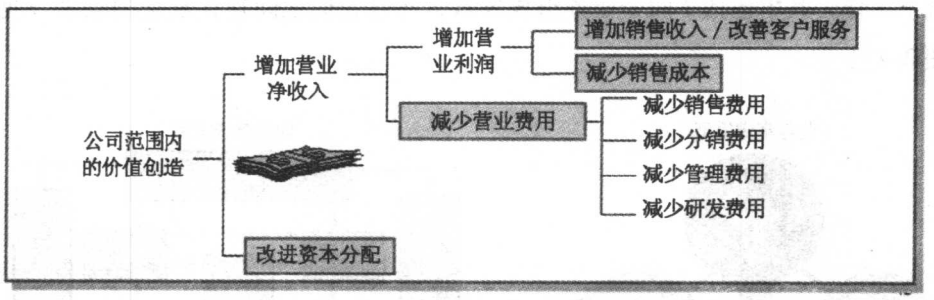

图 2-2 企业价值链的内容

由于信息系统的实施是一个企业的变革过程，因此，在信息系统的价值创造上，着眼于“企业变革”和“单纯的手工自动化”所能够带给企业的价值也是不同的（见图 2-3）。

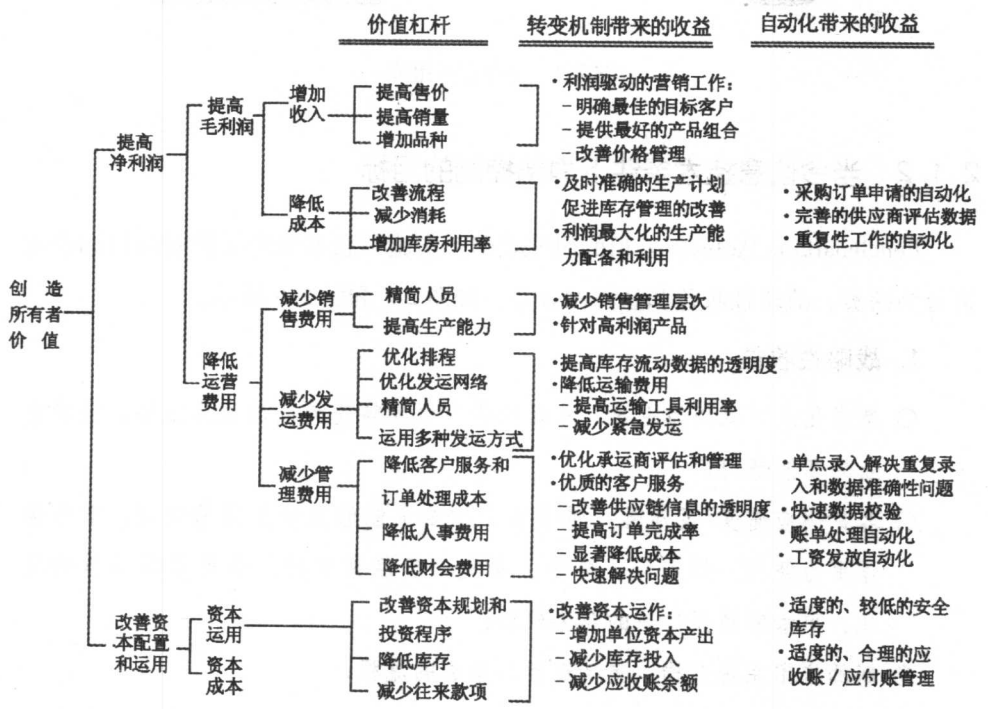

图 2-3 企业价值创造