王仰富 刘继承 编著

清华大学出版社

中国企业的IT治理之道

如何优化IT资源配置，保证IT与业务目标一致？

IT决策的依据是什么？

保障IT投资效益最大化的有效手段有哪些？

国际视野 融合 中国智慧 指导信息化实践

中国企业的IT治理之道

王仰富　刘继承　编著

清华大学出版社

北　京

图书在版编目(CIP)数据

中国企业的IT治理之道/王仰富，刘继承　编著. —北京：清华大学出版社，2010.3

ISBN 978-7-302-22008-4

I. 中…　II. ①王…　②刘…　III. 企业管理—信息管理系统—中国　IV. F279.243-39

中国版本图书馆CIP数据核字(2010)第015356号

责任编辑：崔　伟

封面设计：王晓阳

版式设计：孔祥丰

责任校对：胡雁翎

责任印制：杨　艳

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座

http://www.tup.com.cn　　**邮　　编**：100084

社　总　机：010-62770175　　**邮　购**：010-62786544

投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn

质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn

印 刷 者：清华大学印刷厂

装 订 者：三河市新茂装订有限公司

经　　销：全国新华书店

开　　本：170×240　**印　张**：21.5　**字　数**：497千字

版　　次：2010年3月第1版　　**印　　次**：2010年3月第1次印刷

印　　数：1～4000

定　　价：39.00元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177转3103　　产品编号：035407-01

前　言

世间的问题，极复杂的事情都可以用极简单的事例来说明。哲学家罗尔斯的“分粥理论”就是这样一个简单而寓意深刻的故事。

有7个人组成的小团体，其中每个人都是平凡而且平等的。他们没有凶险祸害之心，但不免自私自利。他们想用非暴力的方式，通过制定制度来解决每天的吃饭问题——要分食一锅粥，但并没有称量用具或有刻度的容器。

大家试验了不同的方法，发挥了聪明才智，多次博弈形成了日益完善的制度。大体说来主要有以下几种。

制度一：指定一个人负责分粥事宜。很快大家发现，这个人为自己分的粥最多。于是又换了一个人，结果总是主持分粥的人碗里的粥最多、最好。这说明权力会导致腐败，绝对权力会导致绝对腐败。

制度二：大家轮流主持分粥，每人一天。这样等于承认了个人为自己分粥的权利，同时给予了每个人为自己多分粥的机会。虽然看起来平等了，但是每个人在一周中只有一天吃得饱而且有剩余，其余六天都挨饿，大家认为这种办法造成了资源浪费。

制度三：大家选举一个信得过的人主持分粥。开始这位品德尚属上乘的人还能公平分粥，但不久他开始为自己和溜须拍马的人多分，直接导致他自己的堕落和风气败坏。

制度四：选举一个分粥委员会和一个监督委员会形成监督和制约。公平基本做到了，可是由于监督委员会常提出各种议案，分粥委员会又据理力争，等分粥完毕时，粥早就凉了。

制度五：每个人轮流值日分粥，但是分粥的那个人要最后一个领粥。令人惊奇的是，在这个制度下，7个碗里的粥每次都是一样多，就像用科学仪器量过一样。每个主持分粥的人都认识到，如果7个碗里的粥不相同，他确定无疑将享用那份最少的。

分粥理论告诉我们：制度至关重要，制度是人选择的，是交易的结果。制度不同，结果大相径庭。

制度是什么？经济学家诺斯认为，制度是一个社会的游戏规则。或者更规范地说，制度是构建人类相互行为的人为设定的约束。大到整个社会，小到一个企业之中，人们

追求自身利益的行为常常是相互牵制乃至相互冲突的。如果只有行为主体的功利性计算，就会出现好事没人做，坏事人人争先的结局。为了协调人们之间的利益冲突，维持集体的生存和社会的秩序，人们无时不需要用制度去规范个体的行为。

那么，究竟什么样的制度才是好制度？好制度的标准又是什么？从上面的分粥过程来看，第五种分粥制度是好制度，其原因是它与前四个制度相比，显得既公平又有效。而前四个制度，要么是如第一和第三个制度，有效率而无公平；要么是如第四个制度，有公平而无效率；要么是如第二个制度，既无公平又无效率。由此可知，有效、公平就是好制度应具备的两个基本特征。

那么好的制度由何而来？

故事中，7 个人组成的小团体，在尝试了制度一、制度二、制度三、制度四之后，终于找到了一种好的制度五。一个重要前提，在于这是一个民主团体，他们对分粥中的不公平能够议论、表达不满，且对于如何改进能够发表意见、民主协商。试设想在一个权力集中的组织中，一个专权跋扈的领导者把握了绝对的权力，分粥者由他指定，不管粥分得多么不公平（当然决不会亏待有权者）也不准提意见，谁胆敢提意见就会遭到打击报复。这样，富有激励作用且公平高效的机制就永远不会产生，组织也可能长期锁定在一种无效率的状态中，忍受低效率和停滞。

更根本、更基础的制约因素是体制。好的体制是好的机制产生的前提。实际上，在有缺陷的体制下，即使仿效先进体制建立好的机制，也往往不能得到有效遵循而在执行中走样。在企业中，这种体制主要表现为公司治理结构。

公司治理是指有关公司控制权或剩余索取权分配的一整套法律、文化和制度性安排，这些安排决定公司的目标，谁拥有公司，如何控制公司，风险和收益如何在公司的一系列组成人员，包括股东、债权人、职工、用户、供应商以及公司所有的部门之间分配等一系列问题。这些安排决定了公司的目标、行为，决定了在公司利益相关者中在什么状态下由谁来实施控制，如何控制，风险和收益如何分配等有关公司生存和发展的一系列重大问题。它是公司具体管理、分配机制形成的背景平台。

具体到信息化建设来说，制度也是决定成败的重要因素。目前，不少单位拥有与其国际竞争对手一样的系统、软件，甚至技术和设备强于对方，所以单从技术的成熟性和先进性而言，整体应用水平不低，但是为什么就没有对方做得好呢?其实原因很简单，IT仅仅是个工具，并且这个工具并不是改善管理、业务流程、商业实践的万能工具，和其他工具一样，必须通过有效的应用才能体现价值。而要想让 IT 得到有效应用，并让 IT 系统绩效最优，最根本的不取决于信息技术和设备的先进与否，而是由制度安排的优劣、

治理水平的高低决定的。这就引出一个IT治理的话题。

对国内的企业来说，“IT治理”并不是一个陌生的词汇。对于什么是IT治理，什么样的治理才是最优的，如何构建最适合企业的IT治理机构，企业界已经开始进行有益的探索，并产生了一系列的优秀成果。我国的IT治理与IT管控，也越来越受到包括政府部门、监管部门、学术界以及行业用户在内的各界的重视。但我们尴尬地发现，IT治理相关的理论总结却严重滞后，我们遍寻国内的理论研究成果也没有发现一套完整、可行的IT治理理论体系，大家甚至对IT治理概念的理解也都迥然不同，急需要一本书总结、整理一套完整的IT治理体系，以指导实践，本书就是在这样的背景下产生的。

本书构建了一套以企业架构为核心的IT治理体系，认为IT治理有十大基本流程体系，这十大流程体系可以归纳为三大类：决策、激励、控制，这是IT治理的三大支柱。本书就围绕这三大支柱展开。本书共分为四篇13章。第一篇构建IT治理的基本框架，包括3章：其中第1章介绍IT治理的基本概念，为全书奠定一个理论基础；第2章介绍目前国际上主流的IT治理标准和最佳实践；第3章是本书的总括，整理了IT治理的整体框架。第二篇是决策，包括第4、5两章：第4章介绍了基于企业架构的IT决策体系；第5章介绍了IT投资决策的基本流程与制度。第三篇是激励，包括第6、7两章：第6章论述了IT部门的模式；第7章是IT绩效评估与IT人员的激励。第四篇是控制，包括8~13共6章，依次介绍IT内部控制、IT项目治理、IT运维治理、信息安全治理、IT供应商治理、信息系统审计等内容。这些内容共同构建了一个符合中国企业实际需求的IT治理框架和内容体系。

本书在写作过程中参考和引用了大量业界的研究成果，虽然书后已经列出很多，但仍难免遗漏，在此，我们对这些作者一并表示感谢。

最后要说的是，由于IT治理在国内还属于一个新生事物，再加上我们的能力和时间所限，呈现在大家面前的这本书肯定会存在这样那样的问题，但我们希望这块“石”能引出您的“玉”。我们的电子邮箱是：itgov2009@163.com，期待您的来信。

编　著　者

2010年1月

目　录

第一篇　IT 治理体系的构建

第二篇　决策——IT 治理的第一大支柱

第三篇 激励——IT 治理的第二大支柱

第四篇 控制——IT 治理的第三大支柱

第一篇

IT治理体系的构建

对很多人来说，IT 治理是一个既熟悉又陌生的概念。说它熟悉是因为近年来 IT 治理频频见诸报端，也是各种论坛活动的热门话题之一，已经被人们所熟知；说它陌生是因为到目前为止，IT 治理还没有一个得到广泛认可的概念，大家虽然都在谈同一个词汇，但经常感觉是“鸡同鸭讲”，缺少共识。

面对这种状况，我们在全书的最开始部分试图总结目前对 IT 治理的理解、认识、最佳实践和国际标准，概括出了 IT 治理的基本概念、总体框架和模型，并将这一模型归纳为三大部分，命名为“IT 治理的三大支柱”，既为读者理解 IT 治理提供了理论基础，又为全书内容的组织提供了思路。

本篇共包括 3 章，其中：

- 第 1 章在概述了信息化乱象之后，引出了 IT 治理的概念。在总结国内外 IT 治理概念、内涵的前提下，提出了我们对 IT 治理内涵和本质的基本认识，并提出了 IT 治理三大支柱的初步思路。
- 第 2 章总结了目前国际上主流的治理领域的国际标准和最佳实践，包括 ITIL、COBIT、CMMI、ISO 27000 等，并对比了各标准之间的异同，为构建中国企业 IT 治理模型奠定了基础。
- 第 3 章承接前两章的内容，构建了中国企业 IT 治理的框架和模型，并把这一模型归纳为 IT 治理的三大支柱。第 3 章是全书的纲，较全面地阐述了我们对 IT 治理体系的认识和理解。

拨开IT治理概念的迷雾 1

我们面对的重大问题无法在我们制造出这些问题的思考层面上得到解决。

——爱因斯坦

横看成岭侧成峰，远近高低各不同。不同的人对同一个事物会有迥然各异的看法，对IT部门的评价就是这样。

企业领导的疑问：IT部门不断伸手要钱，IT投资不断增加，难道IT投资真是个“无底洞”？怎么样才能让我看到IT投资的实效？花巨资“养”这个部门是否值得？

业务部门的责难：信息系统总是出现问题，信息部门的人都是干什么吃的？公司为信息部门投入了那么多，怎么一点改善都没有？我们怎么没有感觉到IT带来的收益？

IT部门的委屈：一天到晚忙忙碌碌，通宵达旦加班，工作得不到认可，郁闷！IT初期需要高投入，回报却是长期的，怎么才能算清楚？信息中心难道永远是“有苦劳没功劳”，总是受气的“童养媳”？

要解决这些信息化的乱象，传统的IT管理已无力面对这些挑战，需要引入公司治理的思想，从战略层面加强IT 决策、实施、评价等方面的控制与管理，确保IT价值的实现。IT治理就是在这样的背景下提出来的。

IT治理几年前就已进入中国，近年来已成为一个热门词汇，但时至今日，连最基本的概念都还没有统一。每个新来者都在其中播下一粒种子，形成了一个繁复的“概念丛林”，这说明IT治理的理论研究和实践还都属于初级阶段，因此有必要在全书的第1章明晰IT治理的内涵与外延，为全书做一个铺垫。

1.1 信息化的乱象催生IT治理

切入正题之前，先来分享一个小故事：

一个和尚挑水吃，两个和尚抬水吃，三个和尚没水吃。总寺的方丈大人得知情况后，就派来了一名主持，负责解决这一问题。主持上任后，发现问题的关键是管理不到位，

于是就招聘一些和尚成立了寺庙管理部来制定分工流程。为了更好地借鉴国外的先进经验，寺庙选派唐僧等领导干部出国学习取经；此外，他们还专门花钱请了国际知名的咨询公司做咨询。顾问待了不久，留下两个“屁”就屁颠屁颠地走了：一个“屁”叫BPR，一个“屁”叫ERP。

在咨询公司的灌输下，主持认为“人才是寺庙的最大财富”，于是就成立了人力资源部和寺庙工会，面向全国广招人才，并认认真真地走起了竞聘上岗和定岗定编的过场。

一段时间后成效出来了，三个和尚开始拼命地挑水了，可问题是怎么挑也不够喝。不仅如此，小和尚都忙着挑水，寺庙里没人念经了。日子一长，来烧香的客人越来越少，香火钱也变得拮据起来。为了解决收入问题，寺庙管理部、人力资源部等连续召开了几天的会，最后决定，成立专门的挑水部负责后勤和专门的烧香部负责市场前台。同时，为了更好地开展工作，寺庙提拔了十几名和尚分别担任副主持、主持助理，并在每个部门任命了部门小主持、副小主持、小主持助理。

老问题终于得到缓解了，可新的问题跟着又来了。前台负责念经的和尚总抱怨口渴水不够喝，后台挑水的和尚也抱怨人手不足、水的需求量太大而且没个准儿，不好伺候。为了更好地解决这一矛盾，经开会研究决定，成立一个新的部门——喝水响应部(洋名叫on call)，专门负责协调前后台矛盾。

为了便于沟通、协调，每个部门都设立了对口的联系和尚。协调虽然有了，但效果却不理想，仔细一研究，原来是由于水的需求量不准、水井数量不足等原因造成的。于是各部门又召开了几次会，决定加强前台念经和尚对饮用水的预测和念经和尚对挑水和尚的满意度测评等，让前后台签署协议、相互打分，健全考核机制。为了便于打分考核，寺院特意购买了几个计算机系统，包括挑水统计系统、烧香统计系统、普通香客捐款分析系统、大香客捐款分析系统、挨上必死系统(简称IBS系统)、马上就死系统(简称MIS系统)等，同时成立香火钱管理部、香火钱出账部、打井策略研究部、打井建设部、打井维护部等等。由于各个系统出来的数总不准确、都不一致，于是又成立了信息管理部，负责各个系统的维护、二次开发。由于部门太多、办公场地不足，寺院专门成立了综合部来解决这一问题，最后决定把寺院整个变成办公区，香客烧香只许在山门外烧。

一切似乎都合情合理，但香火钱和喝水的问题还是迟迟不能解决。问题在哪呢？有的和尚提出来每月应该开一次分析会，于是经营分析部就应运而生了。分析需要很多数据和报表，可系统总是做不到，于是每个部门都指派了一些和尚手工统计、填写报表，给这些挨上就死的信息系统打工。

寺院空前地热闹起来，有的和尚在拼命挑水，有的和尚在拼命念经，有的和尚在拼命协调，有的和尚在拼命分析……忙来忙去，水还是不够喝，香火钱还是不够用。什么原因呢？这个和尚说流程不顺，那个和尚说任务分解不合理；这个和尚说部门界面不清，那个和尚说考核力度不够。只有三个人最清楚问题之关键所在，那三个人就是最早的那三个和尚。说来说去，就是闲人太多了！他们说：“整天瞎折腾个屁！什么流程问题、职责问题、界面问题、考核问题，明明就是机构臃肿问题！早知今日，还不如当初咱们仨自觉自律一点算了！如今倒好，招来了这么一大帮人，一个个不干正经事还人五人六的，甩都甩不掉！”

又过了一年，寺院黄了，和尚们也都死了。人们在水井边发现了几具尸体，是累死的；在寺院里发现了几千具尸体，是渴死的。

无疑，这个故事是荒诞不经的，笑过之后我们又觉得似曾相识，这里面的场景或多或少在我们的企业里一遍一遍地上演着，其中关于信息化的论述更是让我们感同身受。

中国企业信息化建设已有近三十年，其中成绩是显著的，问题也是不容回避的，很多企业的信息化之路和这个寺庙搞得如出一辙，可以说是乱象丛生。

1、信息化建设领导者错位

中国的信息化建设仍然属于“人治”时代，信息化的随意性较大，企业还没有就信息化形成相关的制度，缺少对信息化进行整体规划、实施与控制的决策机制和责任担当框架。信息化成功与否往往在很大程度上取决于最高管理层对信息化的理解和个人领导力的大小，这种不确定性增加了组织的信息化风险。

2、本位主义严重

在很多企业中，由于业务流程不畅、业务部门条块分割、多头管理和本位主义，使得各部门在使用信息系统时仅从本部门的角度来考虑流程设置和管理标准，忽略企业整体流程的顺畅和优化需要，严重影响了信息系统的使用效果，影响了企业整体的管理能力和工作效率。

3、决策的技术经济论证不足

信息化建设项目具有投资大、风险大的特点。事实证明，系统规模越大、与管理联系越密切、集成度越高的系统，风险也越大，失败概率越高，其中最明显的例子就是ERP。信息化建设项目的高风险和高失败率就要求企业在信息化建设决策之前，要进行充分的技术经济论证，综合论证项目技术上的先进性和可行性，财务上的实施可能性，经济上的合理性和有效性。

4、风险管理缺位

目前，大多数组织的最高管理层都已树立不同程度的安全和风险意识，但对信息资产所面临的严重性认识不足，仅局限于IT方面的安全，突出表现为重视安全技术，轻视安全管理，没有形成合理的信息安全方针来指导组织的信息安全管理工作，在安全规划、风险管理、应急计划、安全教育培训、安全系统的评估等多方面，总是出现了问题才去想补救的办法，是一种就事论事、静态的管理，不是建立在安全治理基础上的动态的全局管理方法。国内的信息化就应用系统而言，几乎所有企业的信息系统都存在隐患。