

文化·组织·IT治理智库—IT治理丛书

ISO Certification and Practice 20000

侯维栋 主编 | 麻德琼 高军 副主编 | 虞衍 周彦调 执行主编

认证与实践

- ◆ 看国际“最佳实践”如何在中国落地开花
- ◆ 银行业首家通过ISO 20000认证企业的实践精华



清华大学出版社

文化·组织·IT 治理智库—IT 治理丛书

ISO 20000 认证与实践

侯维栋		主 编
麻德琼	高 军	副 主 编
虞 街	周彦侗	执行主编

清华大学出版社

北 京

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

ISO 20000 认证与实践/侯维栋 主编. —北京:清华大学出版社,2010.1

(文化·组织·IT 治理智库—IT 治理丛书)

ISBN 978-7-302-21634-6

I. ①I… II. ①侯… III. ①信息工业—国际标准, ISO/IEC 20000: 2005 IV. ①F49-65

中国版本图书馆 CIP 数据核字(2009)第 232248 号

责任编辑:张立红 张 颖

封面设计:唐 宇

版式设计:孔祥丰

责任校对:成凤进

责任印制:孟凡玉

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:北京市世界知识印刷厂

装 订 者:北京市密云县京文制本装订厂

经 销:全国新华书店

开 本:180×250 印 张:21 字 数:351 千字

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

印 数:1~6000

定 价:48.00 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:032593-01

本书编委会

主 编：侯维栋

副 主 编：麻德琼 高 军

执行主编：虞 街 周彦侗

编 委：孙 莉 金 琪 王 洁 王 磊

樊 嵩 郑 君 张淑芹 颜 艳

张 群 金 辉 殷 祺 金恩华

袁 荣 郭 罡 汪 瑾 俞 颖

吴天磊

客观总结信息化实践，深入探索 信息化理论(代序)

信息技术及其应用的飞速发展已将技术革命演变为产业革命和社会革命，由此带来的变革以及由这种变革造成的影响，已经超过以蒸汽机、电气化为代表的工业革命。信息产业已经成为规模最大、渗透性最强的支柱产业和战略产业。从冲绳宪章到罗马宣言，走向信息社会成为世界各国的共识。信息网络正成为最重要的基础设施，与信息技术、信息资源相结合，构成了最活跃的生产力。以信息技术创新能力、信息技术应用和信息资源开发利用广度和深度为标志的信息化能力，成为国家竞争力的主要标志。电子政务、电子商务、电子社区、远程教育和医疗已广泛实践。许多国家制定了应对这一历史变革的国家战略。

党中央、国务院对信息化发展做出了一系列重大战略决策和部署。《中共中央关于制定国民经济和社会发展第十个五年计划的建议》中指出：信息化是当今世界经济和社会发展的的大趋势，也是我国产业优化升级和实现工业化、现代化的关键环节，明确要求在“十五”计划中把推进国民经济和社会信息化放在优先位置，并于2001年成立了由国务院总理任组长，中央、国务院和军队主要领导任副组长的国家信息化领导小组，同时成立了国务院信息化工作办公室作为其办事机构，以加强对推进信息化的领导和协调。随即，党的十六大报告提出，要以信息化带动工业化，以工业化促进信息化，走新型工业化道路。国家信息化领导小组随即对一系列信息化发展的重大任务做出了决策和部署，于2005年11月审议通过了《2006—2020年国家信息化发展战略》。党的十七大报告更进一步提出要全面认识工业化、信息化、城镇化、市场化、国际化深入发展的新形势和新任务，要大力促进工业化和信息化

融合。2007 年全国人大审议通过《政府机构改革方案》，决定组建工业和信息化部，主要职责包括指导推进信息化建设、协调维护国家信息安全等。

我国在数十年信息化发展中，各方面都取得了十分显著的成绩，但也存在不容忽视的困难、矛盾和问题。实践促进理论研究、理论促进实践的成熟。面对信息技术进展快、信息资源增长快、信息产业发展快、信息网络扩散快、信息技术应用渗透快、信息化环境变化快的形势，迫切需要客观总结实践经验、深入探索具有中国特色的发展规律，引导信息化走上科学、健康的轨道。

信息技术在经济和社会领域的应用过程中逐渐改变着组织结构、管理制度和业务流程，并为制度创新和管理创新提供新的工具和平台，从而对建立现代企业制度、完善公司法人治理结构产生不可忽视的重要作用。

《文化·组织·IT 治理智库》，将引进经典专著和邀请专家学者编著相结合，从总结信息化经验、指导信息化实践，以及通过信息技术应用完善公司治理结构两个方面，繁荣着我国信息化学术园地，将对我国信息化发展起到积极的引导作用。希望有更多的专家学者投身信息化理论研究和实践总结，为我国信息化发展奠定坚实的理论基础。

是以为序。

工业和信息化部副部长 杨学山

2008 年 6 月 12 日

文化·组织·IT治理智库—IT治理 丛书序言

21 世纪以来，IT 技术的迅猛发展，已经重构人类社会的图景，有效的 IT 治理是竞争优势的源泉，是管理创新和构建组织核心竞争力的决定因素之一，也是保证组织创新发展和基业长青的关键所在。IT 治理正在成为各国政府、行业组织、学术界和产业界等共同关注、研究的一个全球性课题。

一、IT治理的背景

IT 治理的提出，一方面是因为信息已经成为我们最宝贵的资产之一，IT 在组织中已经扮演一个影响到上层建筑、组织全局、治理层面的角色，信息技术不仅仅是生产力，也在生产关系中发挥重要作用。另一方面，IT 治理与全球瞩目的焦点难题——政府治理，亦有着深刻的渊源。

政府治理在我国目前主要表现为行政管理体制改革，电子政务在推进行政体制改革中发挥着至关重要的作用。建设“电子政府”也已经成为世界新一轮政府治理创新和衡量国家及城市竞争力水平的标志之一。

那么，什么是 IT 治理呢？为什么说它与政府治理密切相关呢？

ITGov 中国 IT 治理研究中心认为：IT 治理是指设计并实施信息化过程中各方利益最大化的制度安排，其内容包括业务与信息化战略融合的机制、权责对等的责任、担当框架和问责机制、资源配置的决策机制、组织保障体系、绩效评估体系以及覆盖信息化全生命周期的风险管控体系。该制度安排的目的是实现组织的业务战略、

促进管理创新、合理管控信息化过程的风险、建立信息化可持续发展的长效机制。目前,许多国家已经开始研究 IT 治理理论,并开发了 IT 治理的实践模型,在政府和企事业等单位得到良好的应用。

2001 年 1 月,英国 BIS 发布了关于“重要支付系统核心准则(CPSS43)”的报告,指出系统治理对于增强对市场和管理者的信心尤为重要。美国信息系统审计与控制协会于 1999 年成立了 IT 治理研究所,专门研究 IT 治理,并提供了信息及其相关技术的管理体系模型和最佳实务,帮助组织领导层认识有效实施 IT 治理的必要性与益处,从而保证组织的可持续发展,并且增强利益相关者的价值。

2006 年 6 月,国务院国有资产监督管理委员会出台《中央企业全面风险管理指引》;2006 年 11 月,中国银行业监督管理委员会发布《银行业金融机构信息系统风险管理指引》;2008 年 9 月,中国证券业协会和中国期货业协会共同发布《证券期货经营机构信息技术治理工作指引(试行)》。

可见,IT 治理已成为国内外政府治理关注的新领域。

二、中国 IT 治理的发展历程

ITGov 中国 IT 治理研究中心从 IT 治理和组织治理出发,结合中国源远流长的文化思想,创造性地提出信息社会统筹治理新范式,即 G3 框架。G3 框架以文化治理为核心,研究信息社会文化治理、组织治理和 IT 治理综合治理的新范式理论(理论范式和方法论范式),贯彻东方文化的整体性思维、关系性思维、复杂性思维、系统性思维和非线性思维的思想,把关于对象系统发生、发展的各个要素,直接因素和间接因素,要素之间的直接联系和间接联系分析清楚。在这个基础上为管理学家及实际管理工作提供价值观念、思维方式、评价标准、方法论和具体方法。

G3 框架的提出,起源于我们对 IT 治理的研究,IT 治理的研究起因于我们长期在思考信息化建设中深层次体制与机制问题。在互联网泡沫破灭之后,我们开始认识到:推动信息化可持续发展同样是“制度创新重于一切”,例如,建造一个信息系统是容易的,让这个系统有效地运转起来则是现实的难题。反过来,我们也非常清楚地看到在公司治理、政府治理过程中 IT 治理的重要作用。推进可持续发展的中国信息化建设,需要“解决信息化建设中深层次的体制与机制问题,建立一整套明

确决策权归属和责任承担的制度安排”，并且鉴于中国和西方完全不同的世界观、文化及治理思想，中国需要走有中国特色的 IT 治理之路。在此基础上，ITGov 中国 IT 治理研究中心成立。

2002 年，ITGov 中国 IT 治理研究中心开启走有中国特色 IT 治理之路的伟大征程。同年 3 月我们起草了《关于建立我国信息系统审计制度的建议》，并向时任国务院信息化工作办公室领导做了汇报。同时，我们发起成立了中国信息系统审计与控制专业委员会筹备组，并积极倡导在我国信息化建设中引入信息系统审计，开启了我国 IT 治理和信息系统审计研究的先河。同年 7 月，我们发表《信息系统监理与信息系统审计：中国的实践与美国的经验》，首开我国信息系统监理与信息系统审计比较研究的方向。2002 年 10 月，ITGov 专家团队(孙强、郝晓玲、孟秀转)联合发表《IT 治理：中国信息化的必由之路》，首次在中国提出并倡导“IT 治理”的理念。该份宣言式的文件在互联网上引发极大反响，被广泛地转载和讨论，这是中国 IT 治理发展史上的第一个里程碑。同年，ITGov 专家团队(孙强等)又发表了《信息安全治理：创造新的战略竞争机遇》，首次在中国提出“信息安全治理”理念并倡导治理层面(高管层和董事会)必须履行对信息安全管理职责。

2003 年 2 月，围绕着 IT 治理这一核心理念，我们首开信息系统审计与监理、信息安全管理、IT 项目管理、IT 服务管理、信息化战略规划、管理信息化六大领域培训与推广工作，首次在国内从制度、战略、标准和体系的高度，大规模成系列地开展信息化管理研究、培训、会议等工作，在政府、行业用户、媒体及专家学者的共同推动下，IT 治理、信息化管理、绩效评估、信息系统工程监理、IT 服务管理、信息化战略规划、IT 风险管理等成为 2003 年的热门关键词。此后，ITGov 在探索中前行，创下了许多中国第一，如：中国第一套 IT 治理丛书，中国第一个 IT 治理咨询项目，中国第一个电子政务绩效评估项目，中国第一个“三位一体(战略实施、项目管理、风险管控)”的企业信息化绩效评价模型，中国第一个企业信息化管理控制体系咨询项目(荣获 2005 年度国家级管理创新奖)，中国第一个 IT 治理暨全面风险管理人才培养计划，中国第一家开展 COBIT、ISO 17799、ITIL、COSO、SOX、ISO 20000、PRINCE2、ITPMBOK、信息化工程监理标准等多个国内外标准体系之间的整合研究工作。同时还参与制定国务院国有资产监督管理委员会出台的《中央企业全面风险管理指引》，承担财政部“金财工程 IT 服务管理体系研究”、“电子

政务运维费预算标准及外包管理规范研究”、“北京市 IT 外包服务业调研”、“北京市电子政务项目(甲方)运维管理知识体系和管理规范研究”、“中国光大银行信息系统审计体系研究”、“中国人民银行 IT 治理与信息系统审计标准研究”(2004 年央行重点研究课题)、国务院国有资产监督管理委员会“电信运营信息化与管理创新调研”、国际 IT 治理学会“IT 控制框架标准”，并推动研究制定我国的信息系统审计、IT 服务管理行业标准。

2005 年末，正值中国在美上市企业距离 SOX 法案合规的最后期限临近的关键时刻，由 ITGov 主办的中国公司治理暨 IT 治理年会(简称 G2 峰会)在北京开幕，为中国企业寻找全球风险时代的“航海图”，并同期成立了 G2 俱乐部，旨在建立推动公司治理和 IT 治理的长效机制。

目前，ITGov 致力于成为非营利性质的世界级的 IT 治理研究机构，以“参与国际信息化治理与管理标准制定，推动信息化建设的高效可持续发展为己任”为共同使命，正在成为凝聚海内外优秀专家的资源平台。

正是在各方的努力倡导和积极推动下，短短数年，我们迎来了探索和实践适合中国政府和企业的 IT 治理机制的新时代。

三、IT治理的研究与实践

近年来，在 IT 治理研究与推广方面，我们以信息时代的文化治理、组织治理和 IT 治理为研究方向，依托 ITGov 中国 IT 治理研究中心的资源平台优势，开展了基础性、应用性的重大理论和现实问题研究，形成了与国内外紧密合作的网络优势，承担了国家自然科学基金、中国人民银行等部委的重点研究课题，已经初步建成了我国第一个开放式的 IT 治理科学研究平台。

在 IT 治理理论体系建设上，探索内涵以信息时代的文化治理、组织治理和 IT 治理为核心范畴，外延涵盖 IT 服务管理、IT 管控体系、信息系统审计、信息安全管理体系、业务持续管理体系、信息化绩效评估、IT 风险管理、IT 领导力等理论体系。在国内较早地针对 CIO 的制度框架、管理框架和能力框架这三大框架，进行开创性研究，为我国引入 CIO 制度、发挥信息技术优势、推动管理创新提供了一些理论支持。

在 IT 治理实践与应用研究方面，我们坚持为政府决策和企业实践服务，重视将理论研究付诸实际应用，在 IT 治理原则、政府部门与集团企业 IT 治理和 IT 治理评价体系方面，针对重大现实问题展开研究，先后进行了近百家公司的实证调查，承担多项与大型企业合作的横向课题，取得的系列成果为政府或监管部门制定政策、监管制度，以及企业的 IT 治理决策提供了咨询支持。已经完成或正在进行的研究如下：

- 第一，中国 IT 治理应用研究；
- 第二，文化治理、公司治理、IT 治理和中国企业国际竞争力研究；
- 第三，中国信息化管理控制体系研究；
- 第四，中国企业 IT 治理评价体系研究；
- 第五，中国信息系统审计研究；
- 第六，中国信息安全管理研究；
- 第七，中国 IT 服务管理体系构建研究；
- 第八，IT 领导力研究；
- 第九，合规时代的信息安全治理研究；
- 第十，电子政务绩效评估体系研究。

ITGov 中国 IT 治理研究中心

孙强

2009 年 7 月 21 日

前 言

随着信息化的不断发展和渗透，人类生活受信息化的影响无论是在深度或是广度上都达到了前所未有的程度，对信息化的依赖也日益提高。在一些信息化发展较快的行业里，如何深化信息化的应用和加强信息化的运维管理备受管理者关注，很多组织都在思考如何从“以产品为中心”向“以客户和服务为中心”转变，从关注“技术创新”向关注“服务创新、管理创新”转变，这种转变的需求催生了 IT 服务管理的国际标准——ISO/IEC 20000:2005(以下简称 ISO 20000)。

ISO 20000 是在 ITIL 基础上发展完善形成的国际标准，它为 IT 管理者提供一套可以持续优化 IT 服务的流程化管理体系。随着 ITIL 的方兴未艾，ISO 20000 也得到越来越多的关注和重视，它不仅为组织提供管理依据和帮助，也为组织提供一个验证和证明自身服务管理能力的方法。由于国内引入 ITIL 的时间不长，很多组织的 IT 服务管理基础相对薄弱，因此国内通过 ISO 20000 认证的组织目前并不多。此外，无论是 ITIL 还是 ISO 20000 都是“舶来品”，如何与国情和组织实际情况相结合，使其真正落地，不至于沦为通过认证的“表面工夫”，也是众多希望借助 ISO 20000 改变 IT 服务管理水平的管理者所担心的问题。

与众多介绍 ITIL 体系的书不同，本书旨在从 ISO 20000 认证和实践的视角，与读者分享 ISO 20000 实施的经验和体会。因此，本书对 ISO 20000 体系和 IT 服务管理理论基础的介绍点到为止，更多着笔于 ISO 20000 的认证方法和如何实践 ISO 20000 的管理体系和管理流程，也为读者提供一些有借鉴意义的工具范例。本书中的工具、范例和方法论并非完全由编者原创，而是编者在实践过程中综合利用并检验有效的。本书可以作为组织信息化建设过程中，建立 IT 管理控制体系的实践指南，也可以作为组织通过 ISO 20000 认证前的参考书。

全书 14 章共分为三个部分。其中第一部分为 ISO 20000 介绍，涉及的主题包括 ISO 20000 背景、ISO 20000 体系、与其他管理体系和管理工具的比较。通过这一部分读者可以了解 ISO 20000 是如何从 ITIL 演变而来，组织为什么要实施 ISO 20000，

ISO 20000 标准中的基本要求,从而对体系有一个初步的认识。第二部分为 ISO 20000 认证,涉及的主题包括认证准备、差距分析、流程实施与改进、认证审核。通过这一部分读者可以了解认证过程中需要完成的工作内容,并学习到一些实用的工具范例。第三部分为 ISO 20000 实践,涉及的主题包括 IT 服务体系管理、规划和实施服务管理、规划和实施新/变更服务管理、服务交付过程、解决过程、关系过程、控制与发布过程。通过这一部分读者可以全面了解 ISO 20000 各流程的实践要点,以及如何建立维护服务管理体系,保持流程的持续改进。

在本书的编写过程中,编委会的各位成员付出了辛苦的劳动,向他们表示感谢。另外还有大量的“无名英雄”,虽然没有参与本书的编写工作,但在 ISO 20000 的实践过程中做出了最大的努力,本书描述的内容也凝聚着他们的智慧结晶,特别提出感谢的有杨蔚蔚、修永春、郑仕辉、张剑、王海东、周珠玲、夏卫民、孙磊、邹嘉麟、胡丹、艾敏、潘浩、赵莉、茹惠蕊、潘艳、张岚(排名不分先后)。感谢史文博协助修改全书的图片和表格。

本书出版过程中,清华大学出版社的编辑给予了大力支持和帮助,在此表示衷心感谢!

由于本书的编写过程较为仓促,编者的水平也有限,存在错漏在所难免,请广大读者谅解并批评指正。

侯维栋

目 录

第一部分 ISO 20000 介绍

第 1 章	ISO 20000 背景	2
1.1	ISO 20000 起源	2
1.2	ISO 20000 的意义	6
第 2 章	ISO 20000 体系	8
2.1	ISO 20000 基本框架	8
2.2	ISO 20000 的流程概述	10
2.3	ISO 20000 流程的相互关系	22
2.4	PDCA 方法论	25
2.5	指标体系	31
第 3 章	其他管理体系和管理工具	37
3.1	ISO 20000 与其他 IT 管理体系	37
3.2	ISO 20000 与其他管理体系	41

第二部分 ISO 20000 认证

第 4 章	认证准备	46
4.1	前期准备	46
4.2	认证启动	54
第 5 章	差距分析	58
5.1	差距分析概述	58
5.2	差距分析过程	63
5.3	差距分析结果	65

第 6 章 流程实施与改进	71
6.1 流程实施和改进总体过程	71
6.2 流程体系实施	74
6.3 文档体系建制	81
第 7 章 认证审核	90
7.1 审核基本概念	90
7.2 内部审核	91
7.3 外部审核	96
7.4 审核后的工作	103

第三部分 ISO 20000 实践

第 8 章 IT 服务体系管理	110
8.1 管理职责	110
8.2 能力、意识和培训	110
8.3 文档管理	114
第 9 章 规划和实施服务管理	122
9.1 服务管理规划	122
9.2 服务管理监控和回顾	123
9.3 服务管理中的 PDCA 实施指导	127
第 10 章 规划和实施新/变更服务	130
10.1 流程概述	130
10.2 流程目标	130
10.3 与其他流程的关系	131
10.4 活动和过程	132
10.5 流程控制	133
10.6 流程 KPI	134
10.7 改进方向	134
10.8 实施难点和解决办法	135

第 11 章 服务交付过程	136
11.1 服务级别管理	136
11.2 可用性管理	150
11.3 可持续性管理	161
11.4 容量管理	174
11.5 信息安全管理	188
11.6 IT 服务的预算与核算	206
11.7 服务报告流程	214
第 12 章 解决过程	224
12.1 事件管理	224
12.2 问题管理	241
第 13 章 关系过程	257
13.1 业务关系管理	257
13.2 供应商管理	265
第 14 章 控制与发布过程	271
14.1 配置管理	271
14.2 变更管理	286
14.3 发布管理	302

第一部分 ISO 20000介绍

在介绍 ISO 20000 的认证和实践之前，本书将首先从 ISO 20000 背景开始对 ISO20000 这个 IT 服务管理领域的国际标准进行详细介绍。从 ITIL 诞生到 ISO 20000 成为国际标准，历经了近 20 年的时间，IT 服务管理从最佳实践中产生，又指导实践的开展，这正是它具备强大生命力的最大原因。

此外，ISO 20000 作为管理体系的新军，需要管理者与其他的一些管理体系或方法论进行比较、取舍或融合，使之发挥更大的效用。