“十一五”国家重点图书出版规划项目

公司治理·内部控制前沿译丛

（荷）杰普·布勒姆　梅农·范多恩　皮亚士·米托尔　著

程治刚　张翎　张劲　译著

SOX环境下的IT治理

Making IT Governance Work in a Sarbanes-Oxley World

Jaap Bloem
Menno van Doorn
Piyush Mittal

东北财经大学出版社
Dongbei University of Finance & Economics Press

WILEY

“十一五”国家重点图书出版规划项目

公司治理·内部控制前沿译丛

(荷) 杰普·布勒姆　梅农·范多恩　皮亚士·米托尔　著

程治刚　张翎　张劲　译著

SOX环境下的IT治理

Making IT Governance Work in a Sarbanes-Oxley World

Jaap Bloem
Menno van Doorn
Piyush Mittal

东北财经大学出版社
Dongbei University of Finance & Economics Press
大连

WILEY

图书在版编目（CIP）数据

SOX 环境下的 IT 治理 /（荷）布勒姆（Bloem, J.），（荷）范多恩（Doorn, M.），（荷）米托尔（Mittal, P.）著；程治刚，张翎，张劲译. —大连：东北财经大学出版社，2008.1
（公司治理·内部控制前沿译丛）
书名原文：Making IT Governance Work in a Sarbanes – Oxley World
ISBN 978 – 7 – 81122 – 225 – 8

Ⅰ. S… Ⅱ. ①布… ②范… ③米… ④程… ⑤张… Ⅲ. 信息工业 – 工业企业管理 Ⅳ. F49

中国版本图书馆 CIP 数据核字（2007）第 202080 号

辽宁省版权局著作权合同登记号：图字 06 – 2007 – 130 号

东北财经大学出版社出版
（大连市黑石礁尖山街 217 号 邮政编码 116025）
总 编 室：（0411）84710523
营 销 部：（0411）84710711
网 址：http: //www. dufep. cn
读者信箱：dufep @ dufe. edu. cn
大连金华光彩色印刷有限公司印刷 东北财经大学出版社发行

幅面尺寸：170mm × 240mm 字数：300 千字 印张：16 3/4 插页：1
2008 年 1 月第 1 版 2008 年 1 月第 1 次印刷

责任编辑：孙冰洁 责任校对：毛 杰
封面设计：冀贵收 版式设计：钟福建

ISBN 978 – 7 – 81122 – 225 – 8

定价：40.00 元

译者简介

程治刚，惠普 IT 管理学院资深顾问。武汉大学工学硕士，获得 ITIL 认证、PMP 认证、ISACA COBIT 认证。2001 年加入惠普公司，参与多项 IT 服务管理方面的咨询项目，并负责惠普 ITSM、IT 治理等课程开发，将 ITSM 经典方法论与惠普的 IT 管理经验有机结合。曾担任 ITSMF 官方出版图书《IT 服务管理基础篇》、《IT 服务管理指标》、《服务协议管理导论》中文版编审。

张翎，中国网通（集团）有限公司北京市分公司副总工程师，常年从事电信网络规划设计、企业信息化战略管理与控制、电信运营 IT 系统的设计实施等工作。主持制订完整的符合企业内部控制（SOX 符合性）要求的电信运营商信息化管控政策、管理规则和实施操作层面的细则。这些政策与规则在企业实践应用中得到执行，并顺利通过国际会计师审计机构的 IT 内部控制 SOX 符合性测试。

张劲，惠普 IT 管理学院副院长，在 IT 管理领域具有深厚的理论功底和培训经验，长期从事 IT 服务管理、业务分析与规划、项目管理、应用管理等培训与咨询工作，为电信、金融、电力等行业的多家企业以及政府提供过培训与咨询服务。他通过了 ITIL 服务管理认证、COBIT 认证等多项专业认证。合著有《惠普之道——IT 服务管理》一书并发表过多篇专业文章。

张冬梅，惠普 IT 管理学院资深顾问。长期从事 IT 服务管理（ITSM）及项目管理（PM）相关课程的研发及培训工作，是国内较早通过英国 ISEB/EXIN 的 ITIL 经理认证的咨询顾问之一，并获得了 PMP 认证、COBIT 认证。先后为电信、金融等行业客户及政府提供了多方面的顾问与培训服务，得到客户的高度评价。

刘屹，惠普 IT 管理学院资深顾问，工学硕士，获得 ITIL 服务管理经理级别认证、COBIT 认证，是 ISEB/EXIN/APMG 授权 ITIL 培训讲师。曾领导并参与多项 IT 服务管理方面的咨询项目，合著有《惠普之道——IT 服务管理》。

译者序

随着诸如《萨班斯—奥克斯利法案》、Basel II 和 HIPAA 等各种国际管理控制法规的生效，IT 治理以及法规遵循的要求正在快速成为企业需要解决的一个关键问题。此类法规所覆盖的范围和牵涉的领域要求企业重新思考其开展业务的方式。如果我们不能做出根本性的调整和变化，以符合法规遵循和 IT 治理的要求，就将耗费大量资源，并存在诸多的风险，同时还会带来大量的成本支出。

这些法规旨在通过强调内部控制认证、确保信息保密性和建立可靠的记录保留政策，强制企业改进业务透明度，以保持或重新赢得市场、客户、投资者和员工的信心。不遵守这些法规将会导致非常严重的后果，包括遭受到巨额的罚金、丧失市场信心、损害品牌资产以及丢失发展机会。

法规遵循并不会成为企业的一项沉重负担，相反，企业将有机会将法规遵循的要求转变成一项重要的竞争优势。IT 治理的一个关键性问题是，公司的 IT 投资是否与战略目标相一致以构筑必要的核心竞争力。对 IT 治理而言，要能体现未来信息技术与未来企业组织的战略集成，还要尽可能地保持开放性和长远性，以确保系统的稳定性和延续性。IT 治理有助于建立一个灵活的、具有适应性的企业。

惠普公司构建法规遵循和 IT 治理的 IT 环境基础是，以控制和自动化为特征，能够促进实现可持续的一致性，同时能够持续满足各种治理法规的复杂需求。要应对挑战，企业必须将过去的“一次性”想法，转变为“可持续的一致性”。通过整合人员、流程和技术，企业将可以经济高效地满足这些法规规定的标准，同时还可以降低运营风险。

惠普公司提供了广泛的服务来帮助公司持续遵守行业法规的要求，改善 IT 治理的架构。这些解决方案和服务可以支持企业找到受限于法规要求的业务流程、应用与基础架构；找出并实施正确的内部控制流程，以及实现自动化，以确保流程得到遵守；快速、轻松且准确地评估风险，并采取措施减轻这些风险。

本书由中国惠普有限公司惠普 IT 管理学院的程治刚（负责统稿并翻译第

一部分、撰写第四部分的第 10 章）、张劲（负责翻译第二部分）、张冬梅（翻译第三部分）、刘屹（翻译第三部分）共同译著。通信行业 IT 治理专家张翎先生结合实践，撰写了关于中国电信行业 IT 治理实践应用的一章（第四部分的第 11 章），使本书更加贴近实际。

感谢中国惠普培训部岳灏、孙涛在整个翻译审校工作中的大力支持与指导。在此谨致谢忱！

由于时间紧迫和译者水平有限，错误和疏漏在所难免，恳请斧正（电子邮箱：zhi - gang. cheng@ hp. com）。

译者

2007 年 12 月

序

在快速出现的新型商业模式、客户的力量、全球业务和网络时代全新技术的推动下，IT 业正在悄悄地进行着一场变革，这一变革可能是 IT 业最重大的变革，它将对技术管理方式产生深远的影响，就像技术对数据中心的影响一样。

如果将 IT 想象为一座主体藏于水面之下的冰山的话，水面以下的部分就代表最基本的技术，例如布在墙壁内的线路、网络协议、服务器和存储器，以及财务、工资和人事等的应用。水面之上的 IT 部分代表那些能够带来竞争优势的技术。当它们达到某种平衡时，IT 部门就可以重点关注那些能够推动竞争优势的方面，例如跨渠道的集成和优化或者是以需求推动的供应链业务。

《萨班斯—奥克斯利法案》与这种稳定性有什么关系呢？人们对 IT 的关注从传统的法规范畴和技术管理的稳定性，开始转向快速应变和 IT 服务本身的价值。

现在我们的那些 IT 人员让事情顺应社会的趋势而发展。我们曾把自己当作一个神奇世界的统治者，并且取得了圆桌骑士英雄般的成就。我们做的工作充满了创造力。当然，我们的工作需要投资，但我们觉得我们不需要对结果负责。现在所有这一切都已改变。

现在“让 IT 治理在《萨班斯—奥克斯利法案》环境中发挥效用”要求实现一致性、可预测性和可审计性，将越来越多的技术置于“IT 水面”之下，使其成为一种常用的必备技术，这样我们就可以将精力更多地投入到需要关注的业务方面。

从 Forrester 的 CIO 集团调查结果中学到的最佳实践在下列方面支持了这个观点：

■ 取得成功的 CIO 们如何来优化 IT 对业务的影响？高效运作 IT 部门的 CIO（即那些能够把 IT 运营成功地融入到公司业务的 CIO）报告说：他们的成功源于关注业务流程，而不是功能，他们利用 IT 活动和资源的透明度，推动成功的实现。

■《萨班斯—奥克斯利法案》与高绩效 IT 的流程关注度和透明度有什么

联系？IT 部门通过在稳定性，而不仅是在特定投资方面的努力，将显著增强遵循《萨班斯—奥克斯利法案》的程度。通过标准化、共享服务和外包服务，关注于创建一致的、可预测的和可审计的 IT 运营环境，整个工作都会生成相应记录，以确保其遵循《萨班斯—奥克斯利法案》。

■ 要产生所要求的 IT 透明度需要什么？这是关于资产组合管理（用一个单独的企业级的工具创建所有基于 IT 活动的有关信息）的，通过通用的 IT 领导的流程，例如确定优先级、IT 治理和价值实现管理来维护。这是必要但不充分条件，高绩效 IT 部门具有某种形式的资产组合管理，但只有资产组合管理的流程并不能保证获得高绩效。

Bobby Cameron

Forrester 调研公司 CIO 集团副总裁兼负责人

“人是一种过高估计自己的动物。”

——伦敦政治经济学院

政府管理系欧洲思想教授 John Gray

前言

本前言概括说明和介绍了本书探讨的主题，信息和 IT 的管理，我们称之为“IT 治理”。虽然这个词在 IT 界日益频繁地出现，但在 IT 界内并非人人都很清楚它的具体含义。参与 IT 治理的每个人的目标都是一致的，即应对从 IT 投资中发现获得更多业务价值的新方法这一挑战，因而需要对“IT 治理”的意义达成共识。

让 IT 治理在《萨班斯—奥克斯利法案》环境中发挥效用

在很多人看来，“萨班斯—奥克斯利（Sarbanes - Oxley）”也仅仅代表着参议员 Paul Sarbanes 和众议院议员 Michael Oxley 的姓氏。2002 年 7 月 25 日，美国国会通过了《萨班斯—奥克斯利法案》（简称 SOX 或 Sarbox）。2002 年 7 月 30 日，该法案经美国总统布什签署后，正式成为法律并生效。这项法案对上市公司的治理、内部控制和公司报告提出了更严格的要求和限制，并对经理和董事在经济方面的过度行为做出了反应。仅世通公司的倒闭就意味着惊人的 1 800 亿美元的市值顷刻间化为乌有。投资银行和会计师合谋虚报市值，反映虚假情况。因此，2000 年 3 月美国股市开始下跌，并最终导致新经济公司的倒闭。安然、世通公司、安达信会计师事务所和其他公司已不复存在。

《萨班斯—奥克斯利法案》要求公司将内部控制作为最优先考虑的事情，这需要借助于广泛而全面的控制框架，例如（美国）Treadway 委员会的发起组织委员会（以下简称 COSO）制定的控制框架或者加拿大注册会计师学会发布的《评估控制指南》（Guidance on Assessing Control），或者英格兰和威尔士特许会计师协会公布的《特恩布尔报告》（The Turnbull Report）。

IT 治理协会（The IT Governance Institute，ITGI）由信息系统审计与控制协会（Information Systems Audit and Control Association，ISACA）于 1998 年成立，是使用“IT 治理”术语的首家机构，因而赋予了这个词语某种声望。该协会还通过引入基于 COSO 的框架，信息及相关技术控制目标（COBIT），为良好的 IT 治理铺平了道路。COBIT 现在作为一个重要的工具来使用，以遵循

目前更严格的公司报告规则。使用此类控制框架的需要有时会导致奇怪的情况出现。某些知名的企业在经过充分考虑后，拒绝将 COBIT 作为控制框架，因为它太不实用，难以实施。一段时间后，审计机构不得不宣布将强制使用 COBIT。

本书讨论了自上而下的治理指令与自下而上的正常运行要求之间的紧张关系。IT 治理要想发挥作用不仅仅是简单地意味着要遵守 ABC，即（A）制定更多规则，（B）实施控制框架和（C）记录良好的结果。本书不仅仅是简单的控制框架和法规遵循的指南，我们的目标是描述资源的整个指令系统，从而有助于更好地进行 IT 治理。COBIT 只是这些资源中的一个。自下而上的治理原则（例如分布式领导）构成了另外一个资源。第三个资源就是资产组合管理。

自上而下的控制获得了强大的法律援助，而同时企业又要尽一切努力教人们自下而上地思考，这本身就是一个矛盾。公司治理的现代思想家们，例如 Shoshana Zuboff 和 Claudio Ciborra，对过度控制将导致的危险提出了警告，并指出如果我们不允许人们实际做他们能够决定的工作，我们就可能“从控制者转为旁观者”。

在本书中，我们试图适当分析现实所碰到的管理难题。我们所说的“《萨班斯—奥克斯利法案》环境”不是通过内部控制就能自动达到更好治理的世界，它首先要我们必须找出新的和更好的治理形式，以使立法者、股东和员工都能满意。在“让 IT 治理发挥效用”这几个词中，重点在最后一个——发挥效用。虽然我们需要分析实际情况，寻求建议并引入控制框架，但最终良好的 IT 治理，必须对所期望的组织内人员的行为施加某种影响，以发挥出 IT 治理的作用。

严厉的惩治措施

《萨班斯—奥克斯利法案》的正式名称是美国《公众公司会计改革和投资者保护法案》。投资者需要得到保护，因此必须对现行的会计制度进行改革。由于美国采用了终身监禁这种更严厉的态度，董事们有了真正的恐惧感。

《萨班斯—奥克斯利法案》使高层管理人员必须对他们公司的财务报告负责。违反这些规定可能导致入狱，就像在 Jamie Olis 的案例中描述的那样。Olis 的婚姻幸福美满，有个 6 个月大的女儿，他为一家名为 Dynegy 的美国能源供应商工作。Dynegy 陷入了财务困境，分析师发现运营现金流的账目中存在某些错误。Olis 负责阿尔法项目，Dynegy 称这是一个长期的供气项目。按照

证券交易委员会（SEC）的判断，阿尔法项目只不过是个幌子。Olis 相信自己的行为光明正大，并不服法庭判决。他声称自己从未有过欺诈行为，并且相信公司的顾问们也很清白。但证据表明：证券交易委员会的判断是正确的，Jamie Olis 因此被判处 24 年的有期徒刑。他信任自己的顾问，但分析师们并不相信那些数字。

负有责任的高层管理人员也被有关当局追究责任。安然公司的 CEO 和创始人 Kenneth Lay 声称，他不懂会计学，因此在安然事件中按理不应受到谴责。他也不服判决。对他的判决已在 2006 年 1 月开始执行。安然公司的前首席财务官 Andrew Fastow 承认伪造了安然的账目。他同意以 10 年的刑罚作为交换条件，在审讯中合作，指证 Kenneth Lay 和安然的其他高管。世通公司的前首席财务官 Scott Sullivan 在一桩涉及 110 亿美元的会计丑闻中，被确认有罪，并进入了有罪辩护的阶段。他证明世通公司的首席执行官 Bernie Ebbers 也有违法行为。Sullivan 说：Ebbers 要求他隐瞒成本，夸大收入。与 Jamie Olis 一样，Bernie Ebbers 也宣称自己是无辜的，但纽约法院最后认定 Ebbers 有罪。他的律师立即宣布将要上诉。在 4 个月后，Ebbers 被判入狱 25 年。

在这些法庭诉讼充斥媒体时，公司在忙于引入额外的措施以确保他们遵守《萨班斯—奥克斯利法案》。有时，为了满足法案的要求，大家处心积虑，甚至创造了像“如何使老板免于锒铛入狱”这样露骨的项目名称。

Jamie Olis、Bernie Ebbers、Kenneth Lay、Scott Sullivan 和许多其他人一样，在他们的合作系统中，可能是“受骗者”（参与这个系统的其他机构和个人，例如银行和会计师，我们将在第 2 章进行更深入的说明）。他们相信他人的建议，而他人在商业交易中又相信他们。这种盲目信任再也不可能发生了。

被欺骗的股东感到非常愤怒，情况很严重，必须立即采取应对措施。布什总统在企业责任的讲话中指出：“我们不允许我们的经济因恐怖袭击而受到破坏，更不允许它被欺诈行为所破坏”。反恐战争开始于世贸双子塔的遭袭，反欺诈的战争开始于股市上金额难以想象的资金被蒸发之后。这里的对手不是恐怖分子，而是那些操纵数据改善自己公司的财务状况，通过夸大市值“设法”使股东满意的董事和经理。

生活在《萨班斯—奥克斯利法案》环境中

我们都生活在《萨班斯—奥克斯利法案》的环境中：美洲、欧洲、亚洲，大家都一样。虽然涉及的是美国法律，但来自其他国家的董事也有进入美国监狱的风险。凭借 8.4 亿美元的预算，证券交易委员会能够轻松地访问位于欧洲

的某跨国公司总部。受到该法案直接管辖的公司是那些在美国证券交易所上市和在美国拥有巨大资本利益的公司。这些公司还必须要求他们的供应商在开展业务时要遵照《萨班斯—奥克斯利法案》。因此，这项法案具有直接而广泛的影响，并且不以每个人的意志为转移。ABN-AMRO 银行——一家起源于欧洲的银行——的首席执行官 Rijkman Groenink 看到了一种可能的情形：以美国利益为中心的倾销，将会超越这项美国法律的界限。英国和法国的公司甚至威胁道：如果不推迟《萨班斯—奥克斯利法案》的实施，他们就要退出美国股市。因此，对于所有外国公司以及资产少于 7 500 万美元的美国公司，该法案推迟到了 2006 年才开始实施。

信息治理

对付数据操纵最有力的武器就是透明度和责任明确到人。具有准确数据和董事签名的业务决策将会恢复公众对公司的信心。

我们将《萨班斯—奥克斯利法案》视为公司治理的转折点，尤其是那些直接参与信息技术的管理和使用的公司。对透明度的相应要求随着社会的发展而不断提高，“9·11”事件在其中无疑发挥了重要的作用。恐惧占据了统治地位，而这种恐惧只能通过信息来缓解。立法者和股东要求深入了解事件的经过，还要保证他们所接收的信息是准确的。总之，我们希望自己所处的《萨班斯—奥克斯利法案》环境是个透明的世界。

然而，大量的商业信息离透明还相去甚远。在这个现代化的世界里，员工个人电脑里的自己的电子数据表格在工作中仍然发挥了关键的作用。使用这些数据表格将会带来风险。数据可以被故意操纵，并且可能由于误操作而导致错误。

在这个领域，可能的突破口就寄希望于使用“可扩展商业报告语言(XBRL)”。虽然这项技术尚未启用，但其应用也已指日可待。证券交易委员会的前主席 William Donaldson 最近宣布在财务报告中可以接受 XBRL。在为某些技术确定商业标准方面，最近取得了很大的进展。这些标准对 XBRL 的成功至关重要。接受 XBRL 对于长期忽视此技术的许多公司来说，可以视为唤醒其的信号。(您可以通过主题报告“聚焦标记资料和 XBRL”(网址：*www. sec. gov/spotlight/xbrl. htm*)，了解证券交易委员会的意见)。

使 IT 投资获得回报

公司董事们正日益关注 IT 投资所产生的回报。目前，全部资金总额的 50% 都投入到 IT。IDC 公布的统计数字显示：2005 年，全球在 IT 方面的总投资额超过了 1 万亿美元。所有这些投资肯定会产生某些回报的想法也是非常合理的。

如何使 IT 治理发挥作用对管理者和董事们来说都是一项挑战。现在和未来的 IT 管理与十年前的 IT 管理大不相同。产生这种变化最重要的原因就是 IT 的支出增加、IT 的重要性（仍然）不断提高，还有 IT 与业务的中间界线越来越模糊。方便起见，我们来谈谈 IT 治理。在我们与 IT 和业务领导人进行的多次讨论中，我们确信，实际上我们要处理的是业务治理的问题。因为 IT 无处不在并且将涉及每个人，所以业务和 IT 行为将越来越难以区分。

IT 治理发挥作用就意味着：首先这些行动必须能取得成功，技术方面的投资回报率才能更高。正确的决策结构，更加明确的项目优先次序，以及成功所需的工作空间的承诺都至关重要。

为在《萨班斯—奥克斯利法案》环境下的 IT 治理生存而战

由于三个主要的原因，在今后的几年中，“让 IT 治理在《萨班斯—奥克斯利法案》环境中发挥效用”可能是最重要的一个业务问题。首先也是最重要的，业务与 IT 的界线已经变得非常模糊。其次，许多公司仍然缺乏良好的 IT 治理实践。最后也是相当重要的，就是目前仍然无法明晰我们所处的这个《萨班斯—奥克斯利法案》（以下简称 SOX）环境究竟是什么样的。

在 SOX 实施的第一年，内部和外部审计师设法自己解决这个问题，这给公司的管理者带来了沉重的负担。“审计员每工作 1 小时，管理者就要工作 10 小时。”北卡罗来纳州州立大学的会计学教授 Mark Beasley 说（*soxmonitoring. blogspot. com/2005_01_23_soxmonitoring_archive. html*）。

对于高管人员，内部和外部审计员之间对审计准则的讨论得出了令人吃惊的结论：有关 SOX 的问题仍然很需要被挑选出来。2005 年 7 月 1 日的《CIO》杂志，引用了 Arch Chemicals 公司 IT 副总裁的一段话：“审计员不断提出问题。这非常耗时间，大大超过了我所经历的所有事情。”该杂志警告说：具有讽刺意味的是，第二次 SOX 审计可能“需要更多的时间，花费更多的金钱，引起更多的痛苦”，其原因就是缺少必要的自动化工具的帮助（*www. cio. com/*

archive/070105/sox. html)。

IT 治理将会被置于怎样的位置？在互联网和 IT 泡沫破裂后，可能的情况是遵守 SOX 的压力会妨碍 IT 治理工作的进一步地尽快展开。CIO 们需要在自己的公司里采取相应的措施阻止这种情况发生。对于许多高管人员，“让 IT 治理在《萨班斯—奥克斯利法案》环境中发挥效用”的挑战在于他们很可能会开始背水一战，为在这个《萨班斯—奥克斯利法案》环境中的 IT 治理生存而战。本书将帮助他们进行这个重要的战斗。

SOX 背后的根本原因当然在于“在这样一个时代，所有文档中 93% 以上都以电子方式生成，而且这些文档中的 75% 从来没有进行过打印，所以用于诉讼或法规遵循目标的‘确凿证据’很可能存在电脑中，而不是藏在档案柜里”（*www. legaltechnology. com/digital/pdf/2004/1ti163. pdf*）。但是只要适当关注你的工作方式，包括财务、决策、机制、人员管理、内容管理和体系架构，遵守 SOX 就会成为你努力的副产品。克服法律一致性的压力，达到绩效要求是最终的治理目标之一，SOX 只是一种手段而已。

从法规遵循的压力到绩效乐趣

让 IT 治理在《萨班斯—奥克斯利法案》环境中发挥效用使我们面临着一个非常困难的选择：我们怎样确保为遵守新法规而投入的金钱能够做好公司治理，特别是 IT 治理？根据 AMR Research 公司的估计：2005 年，在遵循 SOX 上的花费达到 61 亿美元。2003 年 8 月 14 日出版的证券交易委员会的《最终规则》提到：为了遵守 SOX 昂贵的第 404 条款，总共需要 12. 4 亿美元。显然，这些估价必须在经验的基础上进行相应调整。

法规遵循压力是巨大的。面临的挑战是把这种法规遵循的压力转化为良好的绩效。有许多人建议将 SOX 分解为容易管理的部分，因为许多机构希望将法规遵循压力变为业绩乐趣。企业不再需要为了遵守 SOX 而片面地追求 COBIT 的所有审计目标。

在公司内部，忙于满足 SOX 的人员在许多情况下，与忙于改善 IT 绩效的人员不同。法规遵循与绩效的结合是一种完美的状态，我们只能够在小范围内实现。如果法规遵循本身成为目标，那么我们的工作就只能是应付差事了。在理论上，万事看起来都很美好，但制定的程序被制定规则的经理们精明地破坏了，以适应他们自己。当然，应付差事只是一种毫无意义的方式，它浪费了彼此的时间。规则必须得到很好的遵守，这样它们才能成为公司 DNA 结构的一部分。证券交易委员会的前主席 William Donaldson 这样解释它：

> ……仅仅遵守规则是不够的。就像我以前说过的，他们应该使这种方法成为公司 DNA 的一部分。对于采用这种方法的公司，关于法规遵循的主要担心就消失了。此外，如果公司将新法规看成机会（改进内部控制、机构绩效及其公开报告的机会），他们将最终更好地运营，更加透明，所以更吸引投资者。*

理想的情况下，法规遵循带来更好的运营和更透明的机构，从而使股东满意。按照 Donaldson 的说法，当法规遵循成为机构 DNA 的一个组成部分时，就会产生这种效果；否则什么也不会改变。

没有控制框架、程序和方法就改进绩效在任何大公司都是不可能的。IT 治理有点像耐久性测试，需要重复和透明的决策过程。控制框架在这样艰巨的任务中是一种辅助工具。那些真正相信 SOX 并且按照 COBIT 的要求实施控制框架的公司，它们无疑真正是有这样的需要。法规将形成更好的 IT 治理。实用主义者会说：我们必须充分利用它，抓住治理现在拥有的能量和动力，利用它实现 IT 治理的最佳和透明形式。怀疑主义者会继续将 SOX 看作麻烦的事情，只会付出尽可能最小的努力在形式上遵守规则。

我们相信：只有公司内部人员的行为符合 IT 为之奋斗的目标，让 IT 治理在《萨班斯—奥克斯利法案》环境中发挥效用才会有效。从理想的意义上说，法规遵循和绩效代表着相同的事情：就是为股东创造价值。

股东有权获得准确的信息和良好的 IT 治理，这正好就是 IT 的业务治理。所以本书的三个部分叫做“管理、问责制和监督”不是没有理由的。它们都包含“完成事情”所需的内容。使 IT 治理起作用取决于良好的管理，修改规范使它们可以被说明和测量，而监督适当地进行自下而上的控制。

强调业务绩效

正确的 IT 治理以及信息和 IT 的良好管理只有一个衡量标准：就是企业在市场的成功。所以关键是我们努力实现 IT 治理以绩效为导向的形式。IT 部门过去遇到的困难导致了这个必然的结论。管理、问责制和监督的适当结合一定会确保信息和 IT 将在实际上改善业务绩效。

---

* W. H. Donaldson, “Speech by SEC Chairman: Remarks on the National Press Club,” U. S. Securities and Exchange Commission, Washington, D. C., July 30, 2003. *www. sec. gov/news/speech/spch073003whd. htm.*

在我们对那些 IT 负责人（资产组合经理、公司总监、业务需求分析员和架构师）进行的大量采访中，一个问题被反复提到。IT 治理涉及每个人，它发生在人类中间，围绕着整个公司。人人都与 IT 有关，并且必须尽自己的一份力量确保 IT 成功地融入公司的业务流程，并成为公司内每个人的日常行为。

在许多采访中还讨论了时代的精神。目前我们的互动方式与 15 年前的不同，并且很可能会与 15 年后的也不同。在这个意义上相当重要的一点是：IT 治理从未“结束”。当然，虽然这涉及公司内的 IT 角色转换，但我们不要忽视社会的变化，以及这种社会变化与商业文化间的相互作用。

IT 治理的发展

关于有效的 IT 的管理已经说得太多并写得太多了，第 3 章涉及这个领域的发展思想。长期以来，我们认为 IT 治理或多或少会自发产生需求。只要我们关注业务与 IT 的结合，让业务自己决定和 IT 之间需要发生点什么，万事就会顺理成章。然而，作为这种自发努力结合的结果，IT 实现的实际业务利益仍然远低于预期。遗憾的是，发生在现实生活中的危机事件促使了业务与 IT 部门间要以有意义的方式进行对话。

目前，IT 完全融入到业务的流程中，一年到头，大量的金钱被投入到对 IT 的需要。因此，IT 必须确实对企业的市场竞争和财务业绩有所贡献。IT 始终应该具有这样的影响。然而长期以来，我们一直满足于仅仅承诺技术会对业务的成功做出重要的贡献。此外，由于外界对 IT 效果的误解，我们都时常面对因此而引起的失望和达不到预期的指责。

处理这种情况需要的“只是”以下的方法：确保我们的流程、我们的 IT、我们的机构和所有其他的环境因素（共同完成公司的工作）的结构正确，并且能够很好地整合在一起。为了达到这个目标，我们必须持续地把握企业的脉搏和财务问题，还有涉及雇员行为的所有事情。只有这样我们才能够避开困难。

公司的员工必须能够做到积极地影响企业按计划执行的能力。只要可能，这最好成为习惯。最后，人员的组织要成为一个有机的系统，一台润滑良好的机器，具有尽可能最小的摩擦力。这样的运营投入最少，产出最多。当我们谈论让 IT 治理发挥效用时，我们说的是自己怎样认识这个因素，还有我们现在怎样开始按它行动。本质上，这是我们已经知道的事情，包括做“生意”所固有的选择和行动。这些行动包括制定目标、估算费用和好处、评估风险、保护利益和鼓励适当的行为。这些活动及其含意全方位地关系到整个公司的