商业银行IT治理结构建设实践研究

孙建光，陈 燕
（大连海事大学，辽宁 大连 116026）

摘 要:提出一种通过IT战略制定、CISR模型、COBIT实施、IT项目管理流程、CMM、ITIL和ISO27001等国际标准的融合运用来指导商业银行IT治理实施的新模式,该模式解决了中国商业银行现阶段关于IT治理实施研究所面临的模式混乱和范围不清等问题。

关键词:公司治理；IT治理；治理模型；信息技术发展战略； IT标准

中图分类号:TP399 **文献标识码**： B

IT governance implementation research in commercial bank industry

SUN Jian Guang, CHEN Yan
(Dalian Maritime University; Dalian 116026,China)

Abstract: A new model of implementing the IT governance with integrated utilization of industry standards like IT strategy,CISR model,COBIT, IT project management, CMM, ITIL and ISO27001 has been proposed .With this new model we aim to solve the chaos of model and scope for commercial banks in China in current stage.

Key words: corporate governance; IT governance; governance model; IT strategy; IT standard

构建社会主义和谐社会，是目前从全面建设小康社会、开创中国特色社会主义事业新局面的全局出发，提出的一项重大任务，而银行业更因其特殊功能而成为构建和谐社会的关键角色，负有历史使命。为了在现有国际金融危机下更好地发展中国银行业，中国银监会提出“以存款为基础，以风险管理立行，以金融服务兴行”的理念，公司治理在国际金融危机这个大环境下再次被提出并需给予足够重视。IT治理是公司治理的重要组成部分，良好的IT治理能提高公司治理的水平，商业银行IT治理在协助商业银行企业朝良性的整体运营发展方面发挥着重要作用，同时也帮助提高银行的信息管理水平、加强公司治理环节的信息披露和内部控制，为股东和客户提供更多信息等方面来提高公司整体治理水平。

1 IT治理的国内、国际研究与发展情况

国际信息系统审计与控制协会(ISACA)认为，IT治理是一个内涵丰富的术语,包括信息系统、技术及连通性、商业活动、法律相关事宜以及所有利益相关者－公司董事、高级管理人员、业务流程的执行者、IT供应商、IT的使用者以及审计人员等。为推动IT治理的理论与实践,ISACA于1998年成立了IT治理协会(ITGI),强调IT治理是董事会和高级管理层的责任,是企业治理的一部分。

Patel认为应该将产品和服务质量包含进来，IT治理能提高组织的IT投资回报，像COBIT和ITIL这些IT治理框架在国际范围内被广泛接受并可帮助实现这些利益。WESSELS E和VAN L J提出公司董事会成员、高级管理人员和IT管理人员希望通过采用IT治理来保证企业的效率、降低成本并提高对IT环境的控制[1]。

几年前IT治理的概念被引入到国内，在媒体、IT业及金融等IT应用水平较高的行业一度炒得很热，专家学者也在不断呼吁IT治理的重要性，但真正将IT治理实践到公司运营层面的案例在国内还不是很多，目前我国的IT治理仍处于起步阶段。

根据IT治理协会（ITGI）2006年发布的《2006年全球IT治理调查报告》，通信和金融服务行业明显比零售和制造业等行业要好，COBIT的认知度在逐渐增加。据中国IT治理论坛的数据表明国内企业IT治理的有效性

能达到60%的企业比例仍然很低，约为15%左右，目前绝大多数企业的IT治理的有效性在30%～60%。

2 我国商业银行IT治理现状

目前，我国的商业银行可简单分为3大类，分别为国有大型商业银行、中资背景中小商业银行和外商独资商业银行。

根据调查,目前外资商业银行在IT治理方面一般是参照其母行的公司治理及IT治理模式并结合自身情况进行定制和调优[2]，一般情况下是符合国际通用的IT治理模式，与其公司治理一起构成一个相对完善和协调的整体，利用其在公司治理和IT治理方面的理念和实践经验并结合公司自身的发展和认知摸索出一条相对可行的IT治理实施方案。简单归结为如下的IT治理路线图：

（1）识别企业业务模式 ；

（2）分析现有IT治理状况；

（3）制定IT治理规划及实施计划 ；

（4）实施改善计划；

（5）定期回顾并改善。

部分企业在实践中参考上述策略完成公司IT治理规划与实施模型、确定IT治理的决策范围和实施优先级，而具体的日常工作内容则通过CISR模型、COBIT、Prince2、CMM、ITIL和ISO27001等行业标准的融合运用来实施。

实施过程中发现，按照此种路线图来实施IT治理可以按部就班，结合公司发展状况，清楚地确定IT治理的实施范围，并且实施也会符合公司的业务、IT发展需求和整个行业的发展要求。

对于国有大型商业银行，以工商银行、中国银行等为代表的居于领导地位的银行经过股份制改造或境内外上市建立起了较好的IT治理结构。

但对于年轻的中资背景中小商业银行来说大多数IT治理仍处于起步阶段。由于行业的趋同性和国际化程度的提高，绝大多数的新兴中资银行开始采用ITIL和COBIT作为实施策略，但目前只是简单的导入，而非真正建立IT治理架构，同时对于除ITIL和COBIT之外的其他标准的导入还很少。本文将探讨借鉴国外和国内外资银行的先进经验进行我国商业银行的IT治理规划与实施模型，以提出一种适用于我国商业银行建立IT治理实施模式并清楚定义IT治理范围的新模式。

3 商业银行IT治理实施模型与最佳实践

在此，以某中型商业银行为例分析我国商业银行进行公司IT治理规划与其实施模型的建立方法，根据分析该行处于一个变化不快并以产品服务的差异化为竞争基础的商业环境，这就决定了消费者的需求、竞争格局、政府监管、技术及供应商等方面的变化都不是快速的，另一方面因为对产品服务差异化的要求又力求先于竞争对手提供新的业务和服务能力以此获得竞争优势[3]。期望利用信息技术来提高运营水平和决策能力，并开发新的产品和服务，以高投资回报率来抵消不断增长的IT支出[4]。

在此基础上该银行对公司IT治理做出了一个比较清晰的定位：IT治理作为公司治理的一部分，需要充分保证IT战略与公司战略的匹配及其执行，体现现有及未来信息技术与企业组织的战略集成；指导公司通过对业界标准和股东方最佳实践的实施合理配置并有效利用IT资源、加强信息风险控制和满足公司内控需求。

根据上述分析和定位并结合IT治理最佳实践，笔者提出适合我国商业银行的IT治理规划与实施模型如图1所示，通过IT战略制定、CISR模型、COBIT、IT项目管理流程、CMM、ITIL和ISO27000等标准的融合运用来指导公司IT治理和IT管理的工作。

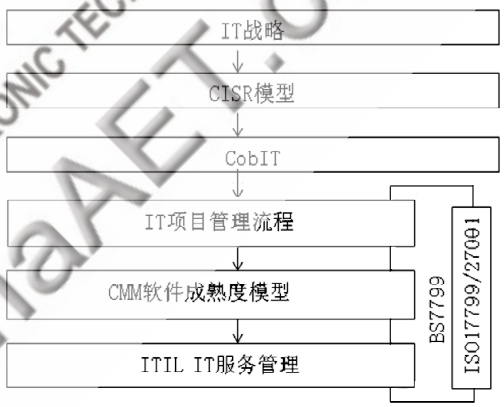

图1 IT治理规划与实施模型

目前，业界通常认为CISR模型和COBIT为2大主要的IT治理模型，笔者研究认为这2种模型均不能涵盖决策权和合规遵从两大问题，CISR模型更多的是侧重决策权及决策制定过程，COBIT则停留在IT管理的一些具体过程，根据经验和研究，建议将IT战略制定、CISR模型、COBIT、IT项目管理流程、CMM、ITIL和BS7799等标准的融合运用，力图通过标准化的方法论和实践将商业银行的IT治理和管理水平提升到一个新的高度。IT治理框架可能在各银行各不相同，但是他们基本的目标是一致的，即提高银行IT的效能，寻求IT资源的最大化。下面从实践的角度对上述模型进行阐述。

3.1 商业银行CISR模型及IT治理的决策范围

参照业界实践，银行IT治理的决策范围可由以下5个方面组成，分别为组织模式、投资、架构、标准、资源。

（1）组织模式

根据对公司业务模式的分析，IT治理的组织模式通常可采取集权模式、分权模式或集权与分权混合的模式，不同模式下IT对于预算和IT决策负有相应的责任，对于采用分权模式或混合模式的公司通常设有一个虚拟的集权部门IT指导委员会来对公司IT行为进行重要决策。

（2）投资

针对IT战略和使命，IT投资应主要集中在支持现有业务运行、优先发展新业务以及进行IT安全和风险管控活动；按照公司要求和业界最佳实践，整体IT运营费用占公司全部运行费用的比例一般会设定一个经验值，以衡量公司IT投资是否在一个正常状态。

（3）架构

根据商业银行现实情况及其行业特点，一般认为稳定性与灵活性都很重要。结合各公司情况实践，建议选择一种可适应的IT架构作为公司的参考架构模型，根据此模型及其规则，制定出商业银行相应的解决方案架构、业务架构、系统架构和技术架构，通过这些架构指导银行的IT行为。

（4）标准

商业银行希望在整体上加强其IT架构，遵从行业技术和运营的标准化，但是在有正常的业务需求下可以有所背离。目前商业银行一般开始实施的标准包括ITIL、COBIT、ISO27000、Prince2/PMP、CMM、银行业务模型等。

（5）资源

在资源方面，商业银行可综合利用银行内外部资源的组合，结合相应的专业外部顾问服务，同时公司需要注重IT治理方面人力资源的培养。

3.2 商业银行COBIT实践

我国商业银行COBIT的实施相对较晚，现阶段商业银行主要集中在COBIT上层中对IT运行内部控制和内、外部审计，确保IT资源管理的安全性、可靠性和有效性，以期实现对IT持续不断的应用和改进[5]。

商业银行大多在实际工作中利用COBIT的一些常用工具如平衡记分卡等来帮助提高管理的水平。

部分外资银行开始结合COBIT模型制定多道风险如图2所示防线的治理模型[6]，综合利用一线用户/经理人员、信息风险管理/危机管理、内部审计和外部审计来对公司IT风险进行管理和防范。三道防线模型如图2所示。

COBIT通常能成为商业银行业企业战略目标和信息技术战略目标的桥梁，使得信息技术目标和企业战略目标之间实现互动，之后通过采用COBIT成熟度模型，

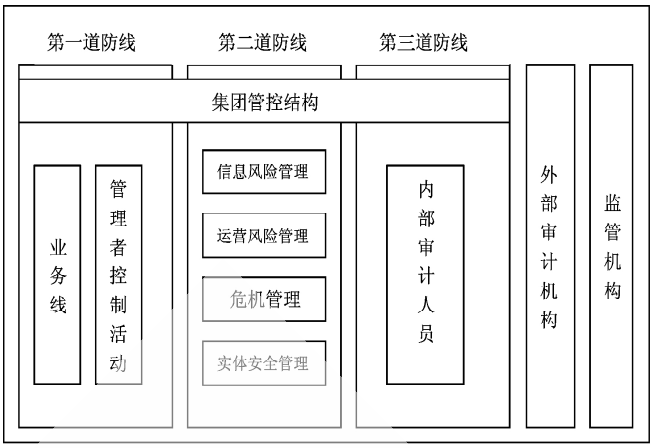

图2 三道防线模型

可以定位自己企业的IT管理目前在业界所处的位置，以及未来努力的方向[7]。

3.3 商业银行项目管理实践

商业银行可根据公司实际情况及项目管理经验推出自己公司的基于Prince2的精简版本作为项目管理的方法论来标准化公司的项目管理工作，将Prince2中的项目周期具体化，并结合不同阶段提供相应的标准的交付物。通过实践可以证明Prince2在界定琐碎的业务需求及选择最适合最节约成本的解决方案方面具有有效的方法。

Prince2和PMP是当今最流行的2种项目管理方法论，推荐Prince2而不是PMP，主要是因为Prince2更加关注提高组织的项目管理能力，而PMP则更侧重于提高个人的项目管理能力。

3.4 商业银行IT服务管理实践

不同规模的外资银行可以根据公司规模进行不同的ITIL流程实施。现在大多数实施是参照ITIL v2的，ITIL v2包括服务支持和服务提供2个方面，ITIL v3是由英国商务部于2007年5月份出版发布，其中规定了管理IT组织以及整合IT和业务的方法论。ITIL v3官方评论家KENT指出“ITIL v3以v2为基础，旨在推动IT专业人员实现IT和业务的整合，而不仅是关注于IT与业务的一致性。ITIL v3与以往单一从技术角度或企业经营角度出发的思考模式不同，它不仅帮助企业建立业务服务管理的合理目标，还帮助企业由关注IT基础架构转变为关注IT资产和服务的关系，最终将IT基础架构的事件和业务成果联系起来。IT管理人员需要完成从一种静态、垂直的思维模式，转换成一种生命周期的模式”。

建议对于各个正在进行ITIL v2实施的商业银行集中精力继续进行未尽流程的实施，对于已经完成实施并熟练掌握此工具和方法论的商业银行可以逐步考虑参照ITIL v3进行优化和持续改进管理。

3.5 商业银行信息安全管理

ISO27000即国际信息安全管理标准体系的实施在我国商业银行相对来说是比较早的，商业银行大多在实际工作中利用ISO27000的一些常用工具等来帮助提高信息风险管理的水平。

建议商业银行对ISO27000的实施从ISO27002的实施和内部认证开始，期望通过这一标准的引入建立一个完整的信息安全管理体系，对信息安全进行动态的、以分析机构及企业面临的安全风险为起点，对企业的信息安全风险进行动态的、全面的、有效的、不断改进的管理，并强调信息安全管理的目的是保持机构及企业业务的连续性不受信息安全事件的破坏，要从机构或企业现有的资源和管理基础为出发点，建立信息安全管理体系，不断改进信息安全管理的水平，使机构或企业的信息安全以最小代价达到需要的水准。根据公司的发展情况判断是否进行外部的认证。

对于ISO27001，建议结合PDCA循环模式=“计划（Plan）、实施（Do）、检查（Check）、行动（Action）”模式进一步规范公司IT管理，以达到“持续改进”的目的。虽然实施ISO27000体系并不能使商业银行彻底远离信息安全破坏，但实施该标准可以降低信息安全被破坏的可能性，因此降低IT投资损失和信息安全事件的影响程度。

4 发展方向及进一步研究

在确定上述IT治理规划及实施模型后，将模型中涉及的相应子模型和标准融合运用进行对商业银行的IT治理建设，它可以帮助银行更好达成IT治理目标。这些标准需要逐步地贯彻到工作实际中，这主要是通过有选择性地阶段性实施来进行，实践表明，针对这些活动的实施可以很好地帮助达成分阶段IT治理的目标。未来对IT治理的实施可以利用IT治理成熟度模型来进行评估。

关于此模式仍需进一步研究，重点应该放在如下几点：

（1）对于模型中涉及的几个复杂标准如何能有效地融合运用；

（2）考虑开发通过此模型进行IT治理实施的标准化工具；

（3）模型实施步骤如何，如何结合公司实际进行相应的选择；

（4）IT治理实施的效果及其成熟度评估；

（5）如何在实施过程中平衡并最大化利用现有IT资源，保证最大的投资回报。

本文通过国内商业银行IT治理存在的问题和最佳实践进行分析，提出通过融合运行IT战略、CISR模型、COBIT实施、Prince2、CMM、ITIL和ISO20000等国际标准建立IT规划与实施模型的创新模式，在协助商业银行企业改善运营提高公司甚至整个行业的竞争力方面发挥重要作用，通过加强和完善商业银行IT治理可以提高银行业的信息管理水平，提高信息披露和内部控制质量，为中国银行业顺利渡过金融危机并全面建设有中国特色的银行业保障体系和现代银行业监管体系服务。

参考文献

[1] WESSELS E, VAN L J. IT governance: theory and practice[C]. Pretoria, South Africa: 2006.

[2] Marianne B, PETER W, Gartner EXP premier report,Effective IT Governance. January 2003.

[3] PETERSON R. Crafting information technology governance [J].Information Systems Management. 2004, 21(4): 7- 22.

[4] 李维安,曹廷求. 保险治理:理论模式与我国的改革[J]. 保险研究, 2005(4):4-8.

[5] 相关商业银行网站:http://www.icbc.com.cn 中国工商银行http://www.boc.cn 中国银行http://www.cmbchina.com 招商银行http://www.socgen.com.cn 法国兴业银行(中国)有限公司http://www.citibank.com.cn 花旗银行(中国)有限公司http://www.hsbc.com.cn 汇丰银行(中国)有限公司.

[6] 孙晓琳,王刊良. IT治理相关工具的对比分析[J]. 情报科学, 2008,26(9):1402-1407.

[7] 中国人民银行武夷山支行课题组. 我国央行IT审计和IT治理的现状与思考[J]. 上海金融, 2007(12): 88-89.

(收稿日期 2009-05-14)