

基于信息科技风险视角的商业银行监管研究综述

汪轶

(西南财经大学中国金融研究中心, 成都, 610074)

摘要: 伴随着银行信息化程度的不断提高, 伴随信息科技与银行业务融合度越来越高, 信息科技风险事件频繁发生。因此, 目前商业银行信息科技风险已经成为全世界各国金融监管部门关注的焦点, 就有必要从信息科技风险的视角对商业银行的监管进行文献综述, 以期提升当前我国商业银行对信息科技风险的理论认识, 同时推动我国商业银行监管机构的监管实践更加科学高效。

关键词: 信息科技风险; 商业银行; 金融监管; 系统性风险

引言

信息科技对商业银行的作用和影响是深刻的和全方位的。从信息科技创新的发端起, 商业银行就开始接受并逐步大量使用该领域几乎最前沿的技术成果。从最初的单纯的信息传递, 到后来对手工劳动的简单替代, 直到现在信息科技改变了银行的经营模式、组织结构、决策过程等几乎所有方面。今天的银行, 几乎所有的产品、流程、业务活动、风险管理和决策都需要信息科技的支撑, 信息科技已经成为现代商业银行正常经营运转的基础设施, 其对于商业银行的作用几乎类似于法律对于人类社会的作用。因此信息科技的安全、可靠、有效对整个银行业提高运营效率、加强风险管理具有极其重要意义。但是伴随信息科技在商业银行领域的不断运用, 各类风险事件和重大信息科技事故频繁发生, 导致商业银行正常经营管理受到重大影响, 出现重大损失, 甚至引发金融系统性风险。尤其伴随着电子化经营, 存款人的财富已经完全电子化, 一旦出现系统崩溃, 数据无法恢复等重大信息科技风险时, 存款人的利益完全得不到保证, 整个经济金融系统难以正常运转, 甚至整个社会、经济都将出现严重紊乱。

近年来, 国外商业银行信息科技风险事件带来惨重损失的教训比比皆是。2008年初, 法国兴业银行由于资金交易系统应用控制存在严重缺陷, 导致发生欺诈交易, 造成巨额损失等等。多数欧美大银行风险主管甚至认为信息科技风险加剧了2008年全球金融危机的突发, 认为银行既利用IT又受制于IT。金融监管是特殊形态的金融服务, 对金融市场发展和一国经济增长有着重要的影响。因此, 金融监管作为金融行业的重要组成部分, 必须不断的调整适应金融业出现的新变化。这要求金融监管在理论、制度、观念、方法和手段上不断调整和改进, 以增强金融监管的针对性和有效性。随着信息科技在商业银行的广泛运用和迅猛发展, 信息科技风险问题日益凸显, 与传统的商业银行风险监管相比, 信息科技风险监管还是一个新课题。对信息科技风险监管这一问题进行研究在理论和实践上均具有重要意义。

一、信息科技风险的内涵与边界

经济学意义上, 风险通常具有两种解释。一种观点认为风险即损失的不确定性。如果把风险视为损失的不确定性, 那么风险通常只能表现出损失, 无法从风险中获利, 这属于狭义风险; 另一种观点认为风险表现为不确定性。这表明风险产生的结果可能带来损失、获利或是无损失也无获利, 因而属于广义风险。金融学理论中通常接受狭义风险的概念, 认为金融风险是指金融机构经营中可能遭受损失的可能性。一般意义上认为, 风险和收益成正比。

传统上, 商业银行风险管理理论指出, 商业银行风险是指商业银行经营管理过程中, 由于事前无法预料的不确定因素的影响, 使商业银行的实际收益与预期收益产生背离, 从而导致银行蒙受额外损失的可能性。商业银行主要面临的风险有: 市场风险(如利率、汇率风险等)、信用风险、流动性风险、法律风险、会计风险、资讯风险、策略风险等。巴塞尔委员会将银行面临的风险分为信用风险、市场风险、操作风险、流动性风险、国家风险、信誉风

险、法律风险以及战略风险八大类。

近年来,伴随商业银行信息科技应用的不断推进,现代的信息技术成果为银行创造出新的效率空间及利润增长。但是,信息技术并不必然带来银行收益的增加。在信息技术条件下,商业银行将银行业务和信息技术紧密结合在一起,整合资源形成合力,获取竞争优势,商业银行在获取经营收益的持续增加的同时,所面临的信息技术相关的风险也在不断加大。商业银行随着信息科技的快速发展,信息科技风险加剧并不断显现。

2004年6月,作为国际银行业行业规则的制定者,巴塞尔银行监管委员会公布了新巴塞尔资本协议。新协议中首次将操作风险引入了对于银行资本要求的框架。新巴塞尔资本协议明确指出,商业银行信息科技风险主要表现为操作风险,但也会连带导致商业银行法律、信誉风险和战略风险。在新巴塞尔协议中,操作风险是由不完善的内部流程、人员、系统或外部事件而导致损失的风险。信息科技风险指的是任何由于使用计算机硬件、软件、网络等系统所引发的不利情况。总的来看,信息科技风险包括了程序错误、系统宕机、软件缺陷、操作失误、硬件故障、容量不足、网络漏洞及故障后恢复能力等诸多方面。

商业银行信息科技风险(Bank Technical Risk)通常是指由于商业银行在使用与计算机、网络等IT技术相关的产品、服务、传递渠道等时,所产生或引发的银行经营的不确定性或对银行经营管理造成的不利因素¹。在我国,2009年银监会出台的《商业银行信息科技风险管理指引》中明确给出了信息科技风险的定义:信息科技风险是指信息科技在商业银行运用过程中,由于自然因素、人为因素、技术漏洞和管理缺陷产生的操作、法律和声誉等风险²。由此可见,作为操作风险的一类,信息科技风险的管理不仅要涉及到银行内部的程序和流程,同时也涉及到银行的组织结构、政策以及操作风险的管理流程。

一般来说,商业银行信息科技风险按照不同的分类标准具体可以划分为不同种类。按照信息科技在商业银行的运用大致可分为三种类型,即IT环境风险(如合规性风险、物理风险、外包风险等)、IT运行风险(如误操作风险、网络欺诈风险、系统中断风险等)和基于IT的金融产品或服务风险。

二、商业银行信息科技风险形成机理

商业银行信息科技风险的形成机理,既要考虑银行的金融特性,也要考虑到信息科技本身的特点。银行作为金融机构,其信息科技应用程度将直接或间接地影响资金融通活动,本身也存在决策问题,可能因为信息科技某些因素的变化导致银行资金、财产、信誉遭受损失。银行信息科技风险一般归类到操作风险中,其诱因主要有以下几种:

(一) 制度风险

主要表现在当出现新的信息技术运用过程中,配套的法律和制度不能及时跟进,给一些不法分子可乘之机,从而给银行和银行客户造成损失;或是由于信息技术本身的特点,特别是网络银行、电子银行和虚拟银行的出现,即使有法律也存在执行的障碍。

(二) 技术风险

体现在技术方面的风险是多方面的,包括网络的健壮性、设备的可靠性、安全措施的科学性以及系统的稳定性等等。具体包括:

1. 外部技术支持风险

出于降低成本等考虑,银行往往依靠外包服务商的服务支持来解决系统建设和管理等问题。这将产生银行无法掌握核心技术,受制于人的风险,甚至可能导致外包服务商泄露信息安全或是侵犯银行系统而造成极大的安全隐患,另一方面是外部技术支持者无法完全理解银行的业务需求而无法提供高质量的系统及服务。

¹ 陈朝晖.商业银行信息科技风险及防控策略研究[D].北京交通大学硕士学位论文,2009

² 银监会《商业银行信息科技风险管理指引》。

2. 网络技术风险

随着信息科技在银行的运用，网络已成为确保银行正常经营的关键，无论是具体业务经办、还是管理决策都离不开网络的支持，因此网络一旦出现问题，后果不堪设想。网络风险一般体现在网络故障、网络设备故障、网络配置被非法更改导致网络中断或网络效率降低、网络安全出现问题等。

3. 设备、系统安全风险

银行大量使用终端设备，如交换机、路由器、防火墙和各类操作系统。设备及系统自身的安全性对银行的正常运转至关重要，而任何设备和系统都可能存在漏洞，至今尚无绝对安全的防火墙可以保证不受外界侵袭。因此任何操作故障、系统漏洞等都可能造成信息外泄或是被攻击。

（三）道德风险

一方面是银行内部员工疏忽或是利用职务之便欺诈篡改账户数据、盗取客户信息、截留账户资金等，导致银行损失及声誉风险；另一方面是外界不法分子利用网络、技术、系统本身的缺陷，非法入侵，给银行造成损失。

（四）自然风险

信息科技设备、网络通讯线路难免受到停电、火灾、雷电、地震等自然灾害的影响。如果在供电、灭火和防雷等方面不采取相应措施，就会在发生自然风险时，造成运行中断、数据丢失和设备损坏的可能。

三、相关文献综述

在与商业银行信息化相关的经济学文献中，在信息化与商业银行效率增进方面累积较多文献，但对信息科技风险却鲜有深度研究，原因或在于商业银行信息科技风险度量困难且相关数据涉及银行机密难以获得，从而导致许多经济学的方法和工具在这一领域难以直接运用。与信息科技风险监管直接相关的学术文献更为缺乏，发达国家的监管文件、指引和国际组织的相关文件成为这一领域最前沿和直接的文献。在此背景下，本文的文献综述实际包括两方面的内容，一是监管机构的监管文件、指引和国际组织的相关文件，二是相关度较高的学术文献，在叙述上则按照国外文献和国内文献分别展开。

（一）国外相关文献

1. 国外信息科技风险监管文件、指引

美国是信息科技风险监管较为成熟的国家，联邦存款保险公司、货币监理署和联邦金融检查委员会均发布了一系列与信息科技风险相关的指引、手册或检查程序；新加坡金管局发布了外包和电子银行风险管理方面的指引；香港金管局发布了业务连续性和电子银行方面的两个监管文件；英国金融服务局发布了业务连续性规划指引；澳大利亚审慎监管局发布了外包审慎监管标准。

表1 国外信息科技风险监管文件、指引

美国	<ul style="list-style-type: none">● FDIC, 2002, Information Technology Examination Procedures● FDIC, 2006, Guidance for Financial Institutions on the Use of Foreign-Based Third-Party Service Providers● FDIC, 2001, Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information● OCC, 1999, OCC Examination Handbook on Internet Banking● OCC, 2001, Uniform Rating System for Information Technology● FFIEC, 2003, Business Continuity Planning● FFIEC, 2005, Authentication in an Internet Banking Environment
----	--

	<ul style="list-style-type: none"> ● FFIEC, 2001, Supervision of Technology Service Providers
新加坡	<ul style="list-style-type: none"> ● MAS, 2005, Guidelines on Outsourcing ● MAS, 2008, Internet Banking and Technology Risk Management Guidelines
香港	<ul style="list-style-type: none"> ● HKMA, 2002, 持续业务运作规划 ● HKMA, 2004, 电子银行的监管
英国	<ul style="list-style-type: none"> ● FSB, 2006, Business Continuity Planning Guide
澳大利亚	<ul style="list-style-type: none"> ● APRA, 2006, Prudential Standard APS 231 outsourcing

2. 与信息科技风险监管相关的国际标准

(1) COSO 风险管理框架

COSO 是行业监管者及企业管理者最常使用的风险管理框架。2004 年, 美国 COSO (Committee of Sponsoring Organization) 委员会颁布了《全面风险管理框架》(The Enterprise Risk Management—Integrated Framework)。COSO 委员会认为企业风险管理是一个由企业的董事会、管理层和其他员工共同参与的, 应用于企业战略制定和企业内部各个层次和部门的, 用于识别可能对企业造成潜在影响的事项, 并在其风险容纳量范围内管理风险, 为企业目标的实现提供合理保证的过程。此框架要求企业管理者以风险组合的观点看待风险, 对包括 IT 风险在内的所有风险进行识别并采取措施使企业所承担的风险在风险容纳量的范围内。

(2) COBIT 信息科技管理标准

2006 年, ISACA (信息系统审计和控制联合会) 制订了《信息及相关技术的控制目标》(Controlled Objectives for Information and Related Technology), 它是面向过程的信息系统审计和评价的标准。对信息化建设成果的评价, 按照系统属性可以划分为若干方面, 如: 对最终成果评价、对建设过程评价、对系统架构评价等。COBIT 是一个基于 IT 治理概念的、面向 IT 建设过程的 IT 治理实现指南和审计标准。

(3) 巴塞尔操作风险管理指导原则

2003 年, 巴塞尔委员会发布了《操作风险管理和监管的良好操作》(Sound Practices for the Management and Supervision of Operational Risk), 提出了 10 项操作风险管理指导原则, 这些原则也适用于信息科技风险监管。

3. 国外学术文献

国外以信息科技风险监管为研究对象的学术文献相对较少, 以下综述的是一些与信息科技风险监管重点领域 (如信息安全、业务连续性、外包等) 相关的文献。

在风险认识和技术标准运用方面, Robert A. Rosen, Esq (2004) 认为信息科技有效降低了商业银行传统业务的风险, 但是信息科技工作本身又给商业银行带来了新的风险, 有效防范商业银行信息科技风险的措施包括建立有效的风险管理程序、制定业务连续性计划、审慎选择信息科技服务提供商等。Fredric William Swierczek, Pritam K. Shrestha (2003) 认为计算机软硬件不兼容、信息系统负载过多等因素容易产生信息科技风险。Ahmad Abu-Musa (2009) 通过调查发现银行、金融机构的用户比其他行业用户更好地执行了 COBIT 技术标准。

在外包方面, Clark, Zmud, McCray (1995) 对外包风险进行了总结, 他们认为在外包中, 公司依赖于外包商, 但却无法像控制公司自己职员的行为那样对外包商进行控制。Earl (1996) 经过对许多公司 IT 外包实践的研究总结出 IT 外包中的 11 种风险。Sineenad Paisittanand a, David L. Olson (2006) 利用仿真模型研究了商业银行信用卡业务信息科技工作外包, 提出针对外包风险要加强对外包服务商的选择、核心业务要自身掌握、避免对外包服务商的过度依赖。

在信息安全方面, Steve Cocheo (2007) 调查发现资产规模大的商业银行在客户敏感数

据保护工作上做的比资产规模小的商业银行好。Brian Cleary (2008) 认为未经许可和不恰当访问信息系统产生了诸多风险。防范此类风险需要加强监控、管理, 并使用适当的科技工具。在业务连续性方面, Karen Kahler Holliday (2006) 认为信息科技应急预案应在商业银行的公司治理层面加强。应制定与员工岗位职责匹配的应急预案, 使每个员工知悉出现应急处理流程。

(二) 国内相关文献

目前, 我国对银行信息技术风险监管的研究才刚刚开始, 缺乏对银行信息技术风险及其监管研究的系统性和全面性。相关的研究主要集中在以下几个方面:

1. 网络银行业务风险监管研究

20 世纪末以来, 国内一些大型银行及部分股份制银行先后开办了网上银行业务, 网络银行得以迅速发展, 并对既有银行制度与法律法规形成了巨大冲击。针对这种情况, 银行监管当局根据网络银行的业务特点, 开始从事网络银行监管研究。

2001 年, 人民银行科技司组织有关信息系统的专家和银行科技工作者, 研究国外银行信息技术风险监管的有关情况, 尤其是对网络银行技术风险监管进行重点研究, 并出版了《网络银行-技术风险及其监管》。同年 7 月, 中国人民银行颁布实施《网上银行业务管理暂行办法》, 对商业银行开办网络银行实施市场准入与退出监管, 并明确规定了网络银行的风险管理责任和法律责任承担要求。2002 年 4 月, 人民银行“网上银行发展与监管工作组”成立, 该工作组致力于学习和研究其他国家先进的网络银行发展及监管经验, 用来指导我国商业银行网络银行业务稳健发展, 提升商业银行自身对网络银行业务的风险管理水平。

2. 银行计算机安全管理研究

21 世纪伊始, 中国人民银行就颁布了《关于加强银行计算机安全、防范金融计算机犯罪若干问题的决定》, 并第一次召开全国范围内会议讨论银行计算机安全问题。此后, 各家银行成立专门机构负责计算机安全管理, 标志着银行信息技术风险这一问题正式开始进入商业银行风险管理的视线。

2003 年银监会成立后, 银行业信息科技风险监管的职能由人民银行和银监会共同承担。2006 年, 人民银行又下发了《关于进一步加强银行业金融机构信息安全保障工作的指导意见》, 明确了我国银行业金融机构“十一五期间”信息安全保障工作的目标和主要任务, 同时详细调查金融机构重要信息系统及运行中心(如数据中心、备份中心)的基本情况, 在全面调查的基础上, 建立了跨部门应急协调机制, 用来协调处理银行重要信息系统的突发事件。银监会于 2006 年底发布了《银行业金融机构信息系统风险管理指引》, 该指引成为银行业金融机构信息科技风险管理的重要指南, 对运用信息系统开展业务处理、产品开发、经营管理或者内部控制过程中产生的风险及其防范都进行了有关规定。

3. 国内主要学者关于信息技术风险及其管理的研究

贺建华(2001)指出, 对于网上银行的安全防范措施, 可以用“防、堵、滤、检、惩”五个字来概括。其中, “防”就是要打好安全基石, 从源头上防范风险; “堵”就是要完善网上银行系统, 构建有效的防火墙拒绝黑客、病毒等进入; “滤”就是通过设置必要的验证码或对合法客户进行授权等方式, 使其起到过滤的作用, 阻止非法用户或者病毒入侵; “检”就是开发专家系统, 对出现的网络攻击进行分析研究, 进而快速检测出是否存在非法入侵者行为; “惩”是指运用法律手段, 对于发现的网上银行犯罪分子严惩不贷。

姜灵敏(2004)认为, 主要应该从两方面来加强银行计算机信息系统安全建设, 一是从制度上保证计算机安全管理工作开展, 加强组织领导, 建立健全完善的计算机安全管理制度和工作体系, 二是从技术上保证计算机系统安全运行, 不断研发新技术, 加强基础设施建设, 构建有效的技术防护体系。

张成虎(2005)认为电子银行除了面对传统银行所面对的全部风险外, 还面对其他三大类

风险：第一类电子银行业务风险，第二类由基础环境带来的风险，第三类由开发和运行方式带来的风险。并在此基础上，深入研究了银行信息技术风险的形成机理和主要诱发因素，提出了相应的风险防范和管理措施；李果仁(2005)对网络银行风险种类进行了研究，认为网络银行风险与传统银行业务风险一致，并将风险类型划分为九大类风险。

高彩霞(2006)，对产生银行业信息技术风险的原因进行了研究，认为管理层决策失误、科技歧视、既有技术缺陷、违规进行操作、缺乏有效的监管是信息技术风险的根源。聂丽文(2007)认为，银行信息技术风险是由客观因素、主观因素(缺乏足够的防范意识和防范能力)、制度不健全和管理手段落后等原因造成的。

龙江涛等(2008)指出，网络技术的迅速发展，催生网络银行的产生。网络银行突破了时空的限制，为银行客户提供了低成本、个性化、全方位的服务，网络银行将是银行经营发展的方向。但信息技术在改变传统银行经营方式的同时，也不可避免地给银行带来了各种新形式的风险，对此，他对网络银行的各种风险进行分析并提出相应的对策建议。

李翔(2006)提出信息科技已经从商业银行发展的辅助性技术工具转变为商业银行的操作、制度平台以至是商业银行的战略环境，信息科技在对商业银行业务发展提供支持的同时，带来了新的风险，需要加强对信息科技的审计工作，将信息科技审计作为一种有效手段，促进商业银行对信息科技风险进行识别、计量和管理。张摘月、王峰(2004)指出银行业监管应包括信息科技风险监管，必须设立有效的监管制度，对商业银行信息科技风险进行评估、检查和检测。

张同建(2008)运用 URSIT 框架为研究基础，结合我国商业银行信息系统业务与技术流程的实地调查结果，通过因子分析方法得出：我国银行技术风险控制测评体系可以加强我国银行业信息化建设，降低技术风险的危害程度，为大幅度提高银行经营效益提供了系统性的指导措施。我国银行业技术风险管理过程中对内部审计、外部审计、安全策略没有高度重视，软件分发效率较低，客户服务能力不足。我国银行业的技术风险控制距理想状态尚有较大差距，特别是管理层，不要为单项措施(如数据库建设、高级人才引进)的表面成熟与成功所迷惑，要深入分析每一项风险控制措施的功能性效应和关联性效应，最大限度地发挥投入资本的价值创造功能。

张东向(2008)从商业银行风险管理的角度出发，分析国内外商业银行风险管理的发展历程及存在的差距，围绕如何提高国内商业银行风险管理水平，重点论述了信息技术在实现商业银行风险管理过程中的重要意义，对如何运用信息技术实现银行授信业务风险管理进行了探讨；王淳(2008)认为，当前商业银行的信用风险管理处在向模型化转型的关键时期，信息技术体系也正处于重构的重要阶段，在同步升级信用风险管理与重新构建信息技术体系的过程中，信用风险管理技术的应用范围要从传统产品扩充到衍生产品、形成具有可操作性的资产组合风险管理功能、实现信用风险管理在资本层面应用，最终完成新型管理技术的内化。邵勉也(2009)指出，我国银行信息化的发展战略，需要适应经济和金融全球化的发展，应选择安全稳定可靠、可持续发展的道路，制定完善的银行信息化风险防范的法律法规制度。为应对银行系统信息化面临的风险，提出了完善我国银行信息化危机风险防范体系的构想。

四、结论

从国内学者的研究结论中可以看出，我国银行业信息化起步较晚，信息科技风险管理滞后于银行业信息技术发展，对信息技术风险缺乏较为系统的监管政策、监管体系和评价指标体系，大多停留在单项信息技术服务的监管上和单项信息技术服务指标的控制上。由于相关信息技术人才的缺乏和信息的管理制度、审查监督等政策的滞后，使得我国银行业信息技术风险监管存在一定的空白。

随着信息技术的不断升级、银行业务的发展，信息科技风险形式的不断变化，我国银

行业信息技术风险的监管面临着巨大的挑战,不但要对传统信息科技风险进行监管,还要加强对新暴露的信息技术风险的监管,要重构并升级银行业信息技术风险的服务和监管体系,以适应金融、经济、社会的发展。监管机构可以充分借鉴国外银行业信息科技风险监管的先进理念,结合我国国情进一步完善银行业信息科技风险监管的法规制度体系。信息科技风险评估体系构建、现场检查制度框架的设立、非现场监测预警系统的研发、单项风险的重点监管等将成为银行业信息技术风险监管的发展方向。

参考文献

- [1] Brian Cleary, How Safty is Your Data?[J] STRATEGIC FINANCE, October2008 P33-37
- [2] Basel Committee on Banking Supervision.Working Paper on the Regulatory Treatment of Operarional Risk[Z].Jan 2001.
- [3] Basel Committee on Banking Supervision. Electronic Banking Risk Management Issues for Bank Supervisors, Electronic Banking Group Initiatives and White Papers, Oct 2000
- [4] FDIC, 2002, Information Technology Examination Procedures
- [5] FDIC, 2006, Guidance for Financial Institutions on the Use of Foreign-Based Third-Party Service Providers
- [6] FDIC, 2001, Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information
- [7] Jurison, J. The role of risk and return in information technology outsourcing decisions[J]. Journal of Information Technology, 1995, 10: 239-247
- [8] MAS, 2008, Internet Banking and Technology Risk Management Guidelines
- [9] OCC , 1999, OCC Examination Handbook on Internet Banking
- [10] OCC , 2001, Uniform Rating System for Information Technology
- [11] Pinnington, A., Woolcock, P. How far is IS/IT outsourcing enabling new organizational structure and competences?[J]. International Journal of Information Management, 1995, 15(5): 353-365.
- [12] 谢平,尹龙.对我国网络银行及其监管问题的研究[J].金融研究.2001(1)
- [13] 谢平,尹龙.网络经济中的金融理论与金融治理[J].经济研究.2001(4): 24-31
- [14] 尹龙.网络银行与电子货币——网络金融理论初探[D].西南财经大学博士学位论文,2002
- [15] 谢平,尹龙.网络银行-21世纪金融领域的一场革命[J].财经科学.2000(4):1-5
- [16] 姜灵敏.我国银行计算机系统安全管理现状分析与对策研究[J].华南金融电脑.2004(9):31-34.
- [17] 张成虎,孙景,李叔彪.银行技术风险监管[J].北京:经济管理出版社,2005.
- [18] 李果仁.我国网络银行风险及防范对策[J].华南金融电脑,2005(3):9-12.
- [19] 高彩霞.防范银行业信息化风险的建议[J].时代金融.2006(4):48-51.
- [20] 聂丽文.浅议银行计算机风险的防范[J].科技情报开发与经济.2006(5):21-23.
- [21] 张同健.国有商业银行信息技术风险控制绩效测评模型研究[J].武汉科技大学学报(社会科学版),2008(2):39-44.
- [22] 张东向.试论信息技术在商业银行授信风险管理中的应用[J].金融理论与实践.2008(5):30-33.
- [23] 王淳,史旭.信息技术在商业银行信用风险管理中的应用[J].金融论坛,2008(8):38-42.
- [24] 邵勉也.完善我国银行信息化风险防范体系的构想[J].上海金融,2009(10):90-93.
- [25] 何茂春.商业银行信息科技风险的量化计量研究[J].金融论坛,2009(2):42-48
- [26] 郭利根.在银行业信息科技风险奥运专项自查工作部署会上的讲话,2008.
<http://www.cbrc.gov.cn/chinese/home/jsp/docView.jsp?docID=20080219F8F638EFC971B033FF528179F5C8A300>.
- [27] 银监会.《银行业金融机构信息系统风险管理指引》
<http://www.cbrc.gov.cn/chinese/home/jsp/docView.jsp?docID=2840>.

- [28] 任莉.商业银行电子化风险及监管研究[D].浙江大学学位论文, 2009
- [29] 陈朝晖.商业银行信息科技风险及防控策略研究[D].北京交通大学硕士学位论文, 2009
- [30] 吕春鹏.商业银行信息技术操作风险分析[D].西南财经大学硕士学位论文, 2008
- [31] 邓宾劲.网络金融风险及其监管探析[D].电子科技大学硕士学位论文, 2005
- [32] 何禹.新形势下银行业信息科技风险监管[J].中国金融电脑, 2010 (8): 41-42
- [33] 李德胜.我国商业银行信息科技风险评级体系重构研究[D].山东大学硕士学位论文, 2009
- [34] 胡海华,崔维琪.银行业信息技术风险的监管[J].银行家, 2008 (4): 120-121
- [35] 叶贵添.商业银行信息科技风险分析及管理策略[J].硅谷, 2010 (8): 185-185
- [36] 李东卫.对商业银行信息科技风险的几点思考[J].金卡工程 (经济与法) 2008 (9): 101-102

A Literature Review about Commercial Bank Regulation in view of Information Technology Risk

Wang Yi

(Chinese Financial Research Centre of Southwestern University of Finance and Economics, Chengdu, 610074)

Abstract: With the increasing application of IT system, and along with the coherence between information technology and bank business which is getting higher and higher, IT risk events happen frequently. For now, IT risk has been the supervisory focus for supervisors worldwide. It's necessary to conduct the literature review about commercial bank regulation from the perspective of IT risk, so as to enhance the theoretical research and the supervision of IT risks.

Keywords: information technology risk; commercial bank; financial regulation; systematic risk

收稿日期: 2011-10-19

作者简介: 汪轶, 西南财经大学中国金融研究中心金融学博士, 研究方向: 金融理论与实践