中国金融四十人论坛书系
CHINA FINANCE 40 FORUM BOOKS

银行业金融机构信息科技风险监管研究

RESEARCH ON INFORMATION TECHNOLOGY RISK SUPERVISION OF BANKING INSTITUTIONS

阎庆民 谢翀达 骆絮飞◎著

中国金融出版社

中国金融四十人论坛书系
CHINA FINANCE 40 FORUM BOOKS

银行业金融机构信息科技风险监管研究

RESEARCH ON INFORMATION TECHNOLOGY RISK SUPERVISION OF BANKING INSTITUTIONS

阎庆民 谢翀达 骆絮飞◎著

中国金融出版社

责任编辑：张　铁
责任校对：张志文
责任印制：陈晓川

图书在版编目（CIP）数据

银行业金融机构信息科技风险监管研究（Yinhangye Jinrong Jigou Xinxi Keji Fengxian Jianguan Yanjiu）/阎庆民，谢翀达，骆絮飞著．—北京：中国金融出版社，2013.4
（中国金融四十人论坛书系）
ISBN 978-7-5049-6832-6

Ⅰ.①银… Ⅱ.①阎… ②谢… ③骆… Ⅲ.①信息技术—应用—金融机构—金融风险防范—研究—中国 Ⅳ.①F832.1-39

中国版本图书馆 CIP 数据核字（2013）第 050174 号

出版发行　中国金融出版社
社址　北京市丰台区益泽路 2 号
市场开发部　（010）63266347，63805472，63439533（传真）
网上书店　http://www.chinafph.com
　　（010）63286832，63365686（传真）
读者服务部　（010）66070833，62568380
邮编　100071
经销　新华书店
印刷　北京松源印刷有限公司
尺寸　180 毫米×250 毫米
印张　20.25
字数　309 千
版次　2013 年 4 月第 1 版
印次　2013 年 4 月第 1 次印刷
定价　50.00 元
ISBN 978-7-5049-6832-6/F.6392

CHINA FINANCE 40 FORUM

中国金融四十人论坛

致力于夯实中国金融学术基础，探究金融界前沿课题，引领金融理念突破与创新，推动中国金融改革与实践。

中国金融四十人论坛书系编委会

序

信息科技革命浪潮势不可挡。如果说农业革命将人类从游牧部落变成城市居民，工业革命带来现代机械化经济，那么信息科技革命将彻底改变世界，改变商业、社会和经济。信息科技的重要性已被提升到国家战略高度。党的十八大报告提出，坚持走中国特色信息化道路，建设下一代信息基础设施，发展现代信息技术产业体系，健全信息安全保障体系，推进信息网络技术广泛运用，推动信息化和工业化深度融合。

银行业作为资金和技术密集型行业，高度依赖信息科技。信息科技对金融基础设施、金融安全网建设发挥着重要的支撑作用，正在急剧改变银行经营模式和服务手段，不断拓展银行服务的空间。当前，信息科技在银行中的作用集中体现在四个方面：一是拓展服务渠道。网上银行、手机银行、自助银行的发展，突破银行经营的地域和时间限制，实现随时随地服务。二是实现业务处理电子化。现在银行业务都要通过信息技术平台实现，其中约有2/3的交易通过电子交易实现，电子交易提升银行服务效率，降低服务成本。三是提升管理能力。银行通过建立客户关系管理、数据分析、风险管理等信息管理系统，提升管理效能和风险控制能力。四是保障信息安全。通过建立灾备系统、集中监控、数据安全等信息安全系统，维护银行信息安全。

但是，随着互联网、移动网络、云计算、智能终端等技术的快速发展，信息科技在带来银行服务便利化的同时，引发的风险也日益凸显。当前，我国银行业信息科技风险管理面临诸多挑战：一是核心技术受制于人。国内银行使用的关键硬件和基础软件都是进口的，制造商处于绝对垄断地位，与硬件设备相关的技术服务也集中在少数供应商手中。二是网络安全形势严峻。银行服务体系对网银等电子渠道的依赖程度加深，网络攻击呈组织化规模化利益化态势，任何流程缺陷或者安全漏洞都有可能导致客户信息泄露或不当

利用，产生严重后果。三是信息科技外包依赖度和集中度较高。特别是许多中小银行信息科技大量依赖外包，而对外包机构的管理控制不到位，存在风险隐患。四是银行业务快速扩张，新系统上线快，安全管控经验不足，信息科技人才缺乏，管理和维护跟不上，加之信息技术受众面广，一旦业务系统和网络出现故障，很可能导致系统性风险和灾难性后果。

鉴于信息科技风险具有复杂性、突发性、破坏性等特征，加强银行信息科技风险监管变得十分重要和紧迫。研究银行业信息科技风险监管的理论、工具和方法，加强信息科技风险的预警、识别、评估和度量，也因此成为加强系统性风险防范、提高监管有效性的重要内容。

阎庆民同志主持的银行业金融机构信息科技风险监管研究，是中国金融四十人论坛重大研究课题。课题组历时一年，对信息科技风险监管问题进行深入研究，形成高质量的报告。报告并不长，但视野宽广，在银行业信息科技风险监管方面作了有益探索，提出许多新理念、新思想、新措施，有不少突破和创新。一是将信息科技风险从操作风险中分离出来进行独立管理和计量。课题全面论证了信息科技风险的特征、与操作风险的区别，认为现有操作风险管理体系没有全面覆盖信息科技风险，提出将信息科技风险从操作风险中拆分并进行独立管理。二是初步构建了信息科技风险监管框架。研究报告结合银行业信息科技风险特点，将信息科技风险领域划分为若干领域，包括信息科技治理、风险管理、业务连续性、信息科技运行、信息系统研发测试维护、信息安全等。初步建立了涵盖非现场监管、现场检查、风险评估与监管评级等在内的持续监管框架。三是设计信息科技风险核心监管指标，提出了两类信息科技风险监管核心指标。一类是基于结果的核心监管指标，包括信息系统可用率、重大生产事件数、系统交易成功率、信息系统中断导致的资金损失占比、重大信息安全事件数、客户投诉率等；一类是基于过程的核心监管指标，包括信息科技治理、信息科技风险管理、信息系统运行、信息安全、信息系统开发测试维护、业务连续性管理等。四是根据信息科技损失特点设计资本计量方法。研究报告从金额和时间两个维度定义信息科技风险损失，参照操作风险标准法计量的思路，提出用时间加金额的方式量化计算科技风险损失，提出科技风险的计量框架、模型和方法。

总体而言，我认为这是一项具有开创意义的研究，必将推动银行业信息科技风险管理和监管工作。当然，信息科技风险监管是个新问题，非常复杂。

目前，国际上尚未形成成熟的信息科技风险监管框架。从实践看，各国信息科技风险监管各有侧重，但共同关注的领域包括数据安全、业务持续运营、电子银行安全、跨境风险等。要从根本上提升中国银行业信息科技服务能力和风险管控能力，必须立足国情，实施信息科技自主可控战略、持续发展战略、流程服务创新战略，建立有效的银行信息科技监管框架，坚持过程控制与目标控制相结合，探索有效的信息科技风险监管方法和手段，提升科技支撑作用，维护金融安全。

尚福林

2013 年 3 月

前　言

信息科技是银行业务运营的基础平台，也是现代银行必不可少的重要基础设施。当前，信息科技比以往任何时候都更快地改变着银行业的格局，信息技术成倍缩短产品创新速度，优化银行内部专业分工，快速提高管理能力，显著提升客户体验，信息科技已与业务高度融合，成为我国银行业打造核心竞争力、持续发展的关键环节。信息科技创造价值的同时，也衍生风险。随着信息科技在银行业的广泛应用，银行几乎所有的业务运营和管理活动都高度依赖于信息系统，随之而来的信息科技风险对银行业稳健发展带来巨大挑战，资金安全、信息安全、业务中断等风险事件对银行产生全面影响，科技风险甚至成为唯一可能使银行业务在瞬间全部瘫痪的重要风险。随着互联网、移动网络、云计算等技术的快速发展，信息科技还将对金融模式、服务格局、金融市场发展产生深远的影响，并对现有的风险管理与监管理论、模式带来新的挑战。因此，加强银行业信息科技风险的研究，深入思考、探索信息科技风险管理和监管的理论、工具和方法，探讨解决当前银行业信息科技风险管理面临的突出问题，推动银行业将信息科技风险纳入全面的风险管理体系，在当前具有非常重要的现实意义和前瞻价值。

虽然信息科技的发展历史悠久，但信息科技风险仍是一个全新的概念，有关信息安全管理理论研究虽已有三十多年的历史，但信息科技风险管理和监管的理论仍处于起步和探索阶段。本书通过对中国银行业信息科技风险监管面临的突出问题、信息科技风险的定义、分类和成因等的深入分析，研究探讨了信息科技风险与操作风险、全面风险管理间的关系，明确了信息科技风险的定位，构建了信息科技风险监管框架，并对信息科技风险核心监管指标和信息科技风险资本计量方法进行了思考和设计。本书的研究，为监管部门不断完善银行业信息科技风险监管理论方法，进一步提高监管有效性，提供参考意见和思路。

目录

第一章

银行业信息科技风险管理概述

计算机的出现对人类社会的发展和生活方式产生了巨大影响，尤其是20世纪末国际互联网的普及和应用，使获取、转换、传递信息的成本急剧下降，改变了各行各业的经营方式，并最终带来社会经济发展方式的巨大改变。进入信息化时代，各行各业的经营方式都不断适应着信息科技的发展，银行业也不例外。回顾我国银行业改革发展历程，信息化建设从起步到发展、从引进学习到自主创新，信息科技深刻改变了银行业传统的经营模式和服务手段，显著提升了银行客户体验，从根本上改变了银行自身的经营管理模式，快速推动了银行的改革与业务创新，促进了银行风险管理水平的全面提升，引领了业态变革，推动了银行商业模式转型，成为核心竞争力之一。

近年来，在我国银行业向集约化、自动化、流程化、智能化发展过程中，各银行对信息科技的认识逐步加深，投入不断加大。截至2011年末，银监会信息科技监管重点监测的254家银行业金融机构共建立各类数据中心296个，工、农、中、建等国内大中型商业银行信息科技网络遍布国内城乡及世界发达国家（地区），核心信息系统业务交易笔数屡创新高，其中，工商银行日交易峰值超过2亿笔，建设银行日交易峰值已达1.9亿笔。信息科技已经成为银行业务日常运营的操作平台、业务创新的基础工具和管理决策的重要手段。银行信息科技发展水平及其与银行业务的融合程度，已经成为影响现代银行业务客户服务以及衡量经营管理水平高低的重要因素，成为全球各大银行打造核心竞争力的关键领域。总体而言，我国银行业充分把握了信息化发展机遇，在信息科技有力支撑下，业务规模不断扩大，经营管理水平逐步提高，整体实力显著增强。

信息技术的广泛应用提高了交易效率、办公效率，也增强了银行业对信息科技的依赖性。信息科技创造价值，同时衍生风险，随着业务快速发展和数据高度集中，银行业金融机构信息系统运行环境越来越庞大、复杂，银行业信息科技风险日益集中、不断增大。近年来大型国际机构发生的典型信息科技风险事件如表1－1所示。

表1－1　　大型国际机构典型信息科技风险事件表

时间	机构	事件
2003	美国银行	2003年1月，美国银行（Bank of America）13000台ATM机因病毒瞬间宕机，该行客户无法通过ATM完成存取款交易。

续表

时间	机构	事件
2005	日本瑞穗证券公司（Mizuho Securities）	2005 年 12 月，日本瑞穗证券公司（Mizuho Securities）误将客户的“以 61 万日元卖出 1 股 J - COM 公司股票”指令输入为“以每股 1 日元卖出 61 万股”，东京股票交易所（Tokyo Stock Exchange）电脑系统对该公司取消下单的指令不能给予回应，随后瑞穗的错单全部成交，引发了投资者抛售股票，使日经指数重挫超过 300 点，瑞穗证券损失超过 400 亿日元。
2006	花旗银行	2006 年日本最大的美资银行花旗银行（Citibank Japan）出现交易系统故障，5 天内约 27.5 万笔公用事业缴费遭重复扣划，或交易后未作月结记录，造成该行在日本的重大声誉损失。
2010	埃森哲	2010 年 5 月 6 日的“闪电暴跌”（Flash Crash）中，世界最大管理咨询公司埃森哲（Accenture）的股价在惊心动魄的 20 分钟内跌至每股 1 美分。事件的发生，并非因为单个机构的不力，真正的罪魁是系统中各个部分的活动，它们看似没有关联、毫不起眼，但一旦同时发生，便能掀起一场金融“完美风暴”。
2011	澳大利亚国民银行	2011 年 11 月 24 日，澳大利亚国民银行电脑系统的一个文件出现故障，随即整个支付系统被堵塞。在随后的两天中，不仅国民银行电脑系统的故障没有能及时修复，而且影响进一步扩大。包括联邦银行、澳盛银行、西太银行、汇丰银行和花旗银行等在内的澳大利亚主要银行都证实，它们的一些客户的转账也受到国民银行技术故障的影响而无法进行。
2012	骑士资本集团	2012 年美国规模最大、技术最先进的经纪自营商——骑士资本集团，因为新安装的软件出现一个小小的故障，结果导致大量交易数据错误，造成 4.4 亿美元的损失，损失额度超过其 3.65 亿美元的现金资产头寸。事情发生后，公司第一天股价跌了 32%，第二天跌了 53%。
2012	BATS Global Markets	美国第三大证券交易所 BATS Global Markets 的母公司首次公开发行（IPO）时，开盘价是 15.36 元，技术问题使得 1 秒半的时间，股价跌到了 0.001 美元，一分不值，只得停止交易，IPO 失败。

实践说明，信息科技的安全运行和健康发展，直接影响到银行稳健经营，关乎银行声誉、金融安全和社会稳定。信息科技风险可能导致银行全部业务瞬间瘫痪，已经成为银行业金融机构的主要风险之一，是银行风险管理的重要对象。相对于信息科技建设的飞速发展，我国银行业科技信息管理方面还比较薄弱，重建设、轻管理，重眼前、轻长远的现象还普遍存在，尚缺乏对信息科技风险的全面认知和信息科技风险管理的统筹考虑。

第一节　信息科技风险定义、分类及特点

一、信息科技风险的定义

风险是一个古老的词汇，信息科技风险却是随着信息技术广泛应用而新生的词汇，最早出现在20世纪90年代。目前业界对于信息科技风险尚缺乏统一的认识，国际上存在三种主流的定义。

一是从逻辑角度给出抽象的定义。如国际标准组织（ISO）指出，信息科技风险是一个给定的威胁（Threat）对一项或者一组信息科技资产的脆弱点进行攻击，并对整个组织造成伤害的一种潜在的可能性，信息科技风险就是该威胁发生的可能性与其造成损失的乘积。

二是从技术角度给出偏技术化的定义。如美国国家标准技术机构（National Institute of Standards and Technology，NIST）指出，信息科技风险是指对信息系统脆弱部位的有意或者无意的攻击，及其对组织可能造成的损失。与信息科技相关的风险主要是由于非授权的信息披露、验证和信息损坏，无意或者故意泄露信息，以及其他人为的或者自然的因素等原因引起。

三是从应用角度给出偏重于管理的定义。如国际信息系统审计协会（ISACA）对信息科技风险的定义：信息科技风险即组织内使用、获取、操作、参与、应用信息科技所造成的业务风险。

中国银行业监督管理委员会指出，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。

从国内银行业信息科技风险管理实践来看，中国银行业监督管理委员会关于信息科技风险的表述更具体，更贴近中国银行业信息科技风险管理的实际情况。

二、信息科技风险分类

业界从多种角度对信息科技风险进行了分类，包括日常管理领域、风险

来源、风险影响的对象和风险对组织的影响等。

按信息科技日常管理领域分，可划为：开发风险，即信息系统在采购、开发、测试、上线的管理过程中存在的风险；运维风险，即信息系统在日常运行和维护管理的过程中存在的风险；信息安全风险，即信息系统数据在使用、维护和管理过程中存在的风险；以及外包风险、业务持续性风险等。

按信息科技风险来源分，可划为四类：一是自然原因导致的风险，包括地震、台风等自然灾害造成的风险；二是系统风险，由信息系统相关软硬件缺陷引起，包括基础设施和硬件设备老化、应用和系统软件质量缺陷等；三是管理缺陷导致的风险，主要体现在由管理制度的缺失或组织架构的制衡机制不完善，管理流程不足；四是由人员违规操作引起的操作风险。

按信息科技风险影响的对象分，可划为三类：一是数据风险，银行提供的金融服务反映在信息科技领域就是数据处理，一旦管理不善将出现客户信息泄密、资金差错等数据风险；二是运行平台风险，金融服务涉及的数据处理都需要稳健的运行平台，硬件设备、网络、操作系统、数据库、中间件以及应用系统内在缺陷或管理差错，将影响信息系统运行平台的质量，出现运行平台风险；三是物理环境风险，信息系统的安全运行有赖于适宜的物理环境，地震、雷雨、群体事件以及机房设备故障将影响机房供电、温度、湿度等，形成物理环境风险。

按信息科技风险对组织的影响分，可划为四类：一是安全风险，即信息被篡改、盗用或被非授权组织使用的风险；二是可用性风险，即由于系统的失败、自然灾害等导致信息或应用程序不可用的风险；三是绩效风险，指由于系统、应用程序或人员的表现不佳，从而导致公司交易和运营效率降低和公司价值下降的风险；四是合规风险，指对信息的处理加工不能满足法律、监管要求或 IT 和公司政策需求而导致公司声誉受损的风险。

三、银行业信息科技风险特点

当前银行业信息科技风险特点主要表现在以下几方面：

信息科技风险专业性强、复杂程度高，新技术运用产生了新的风险。作为金融业务与信息技术结合的产物，银行业信息科技风险不但兼具两者的专业性特点，由于技术的交叉，又衍生出了新的特性。特别是近年来，互联网、云计算、移动通讯、智能终端、社交网络等新兴技术的出现，打破了传统业