IT RISK MANAGEMENT

FOR COMMERCIAL BANKS: THEORIES AND PRACTICES

IT風雲 險中求勝

——商业银行信息科技风险管理理论与实践

杨兵兵◎主编

中国金融出版社

IT 风云，险中求胜

——商业银行信息科技风险管理理论与实践

IT Risk Management for Commercial Banks: Theories and Practices

杨兵兵　主编

中国金融出版社

责任编辑：吕　楠
责任校对：刘　明
责任印制：丁淮宾

图书在版编目（CIP）数据

IT 风云，险中求胜：商业银行信息科技风险管理理论与实践（IT Fengyun，Xianzhong Qiusheng：Shangye Yinhang Xinxi Keji Fengxian Guanli Lilun yu Shijian）/杨兵兵主编．—北京：中国金融出版社，2014.3
ISBN 978-7-5049-7150-0

Ⅰ.①I…　Ⅱ.①杨…　Ⅲ.①商业银行—信息管理—风险管理—研究—中国　Ⅳ.①F832.33

中国版本图书馆 CIP 数据核字（2013）第 239991 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　利兴印刷有限公司
尺寸　169 毫米×239 毫米
印张　12.25
字数　198 千
版次　2014 年 3 月第 1 版
印次　2014 年 3 月第 1 次印刷
定价　48.00 元
ISBN 978-7-5049-7150-0/F.6710

主　编：杨兵兵

编　委：黄登玺　赵锁柱　张橙艳
　　龙　潇　郑慧莹

前　言

银行业在社会的经济活动中扮演着举足轻重的角色，商业银行作为知识密集型产业，在业务流程、客户服务、日常经营等方面呈现出高度信息化、数据化的特征。信息科技帮助银行业实现了从传统手工流程向电子化的转变，同时，其服务范围也从内部用户扩大到外部客户，直接关系到银行客户的服务体验。尤其是近年来，移动信息技术的快速发展打破了地域、时间等限制，在为客户带来便捷金融服务的同时，也为银行提供了拓展业务的全新舞台，无疑将成为未来银行业竞争的焦点。而挑战永远是与机遇并存的。如今，社交媒体的普及使得所有消费者都能够针对所接受的服务发表自己的看法，舆论得以更快速、更广泛的传播。而信息科技风险能够直接带来声誉风险，后者在自媒体时代所产生的社会影响是巨大的，因此信息科技风险的重要性也日益凸显。

在我国，银行业信息科技的发展也经历了全面联网、数据大集中、以客户为中心的核心业务系统建设等阶段，大集中模式虽然带来了管理上的便利，但也造成了各种风险隐患集中的客观现状。同时，信息系统与业务流程的结合程度日益密切，其中牵涉到的包括软件、硬件、基础设施、服务、数据标准等各方面因素之间的关系也变得更加复杂。此外，信息系统作为银行各种数据、信息的基本载体，其安全性也引起了监管机构、同业机构、投资者等社会各界的广泛关注。以上情况客观上导致我国银行业面临系统集中度、业务复杂性、信息安全等突出的信息科技风险，因此，实现全面有效的银行业信息科技风险管理刻不容缓。

在现有的巴塞尔资本协议框架下，操作风险被视为单独的风险进行计量，信息科技导致的风险主要体现为操作风险类型项下的子类或子领域，作为操作风险的组成部分之一，与人员、流程、外部事件导致的操作风险并列出现，并不直接参与到风险资本的计量过程中。而通过对信息科技风险管理的重要性和特殊性的分析，将银行业信息科技风险区别于操作风险中的其他风险而

进行独立管理，对于银行自身的稳定经营和风险控制具有现实意义。作为全面风险管理中三大风险之一，针对操作风险管理的理论框架已较为成熟和完善，但有关信息科技风险管理的理论研究和实践还处于探索过程中，这也是本书研究的初衷。

由于信息科技风险管理领域的相关研究较少，研究成果多为独立文章，鲜有系统性书籍。在研究素材匮乏的情况下，本书通过将实践经验抽象化，开创性地总结出了一套行之有效的信息科技风险管理体系，为我国银行业提升信息科技风险管理水平提供了有价值的参考指南。本书立足于国内外银行业科技风险管理的现状，通过梳理和比较国际先进的信息科技风险管理理论和方法，并结合我国银行业信息科技应用和管理的特点，探索动态的、可实践的信息科技风险管理框架。依托于该框架，本书从多个角度、全方位地阐述针对信息科技风险的治理结构、管理策略、管理文化、管理流程、管理工具和方法等基本的风险管理构成要素，综合运用风险控制评估、事件分析和关键指标等方法建立科技风险识别与评估、应对与控制、评价与计量、监控与报告等风险管理基本流程，提出了切实可行的、适合我国银行业的信息科技风险管理体系。

信息科技风险作为一种特殊的风险类型，已经引起了全球范围内的广泛关注。各国监管机构充分重视，并且为之设计了专门的监管指引、标准以及监管模式，各金融机构也不断在信息科技管理和风险管理方面探索着适合于自身特征的信息科技风险管理实践。本书也是在此背景下，为有效推进银行业信息科技风险管理，对信息科技风险进行的一些前瞻性研究和系统性总结。

目　录

图目录

表目录

1 银行信息科技风险管理面临的挑战

1.1 银行信息科技风险管理面临挑战

作为信息科技引入最早、应用最广的行业之一，我国银行业在业务处理、客户服务、产品创新、管理决策等领域对信息科技的依赖呈现越来越深入的特点。尤其是近年来，随着信息科技与银行业务日益融合，信息科技已经成为银行实现战略目标和日常业务运营最重要的基础，同时也发展成为客户服务、业务管理方面的一项核心竞争力。但任何事物都有两面性，信息科技在银行业的“双刃剑”效应也非常明显，它在给银行带来各种竞争优势和效益的同时，也给银行业带来了各种与信息科技应用相关的风险——信息科技风险。

为了应对日益突出的信息科技风险，越来越多的银行开始重视信息科技风险的管理，而且行业内领先的银行也已经开始在信息科技治理、企业风险管理、项目实施、内部控制和内部审计等领域开始对信息科技风险管理进行探索。当前我国多数银行已经将信息科技风险管理作为高级管理层的一项重要工作，建立了覆盖全面信息科技风险领域的管理框架，组建了独立的管理部门和相关机制，有些银行已经设立了首席信息官制度。但是，我们必须意识到这些探索无论从深度还是广度上都存在局限性，距离有效的风险管理要求尚存在明显的差距。尤其以下几方面内容值得特别关注：

第一，银行缺少信息科技风险管理框架。信息科技风险防范重要性日益凸显，我国部分银行已在内部初步建立了信息科技开发和运维体系，且陆续完成 ITIL、CMMI 等国际认证。但是很少有银行能够基于以风险管理改善业务绩效的信念进行主动的信息科技风险管理工作，风险偏好与风险容忍度的设定、风险识别、评估、监测、计量等环节的控制在执行过程中也不能充分融合。

造成上述现状的原因是多方面的，但无疑缺乏能够与银行业特点密切结合的风险管理理论和框架是主要原因。国际上虽然有众多关于信息科技风险管理和操作风险管理的理论，但没有哪一种理论能够直接被中国银行业用来构建信息科技风险管理体系。

第二，信息科技风险管理手段欠缺。我国银行业在应对伴随业务增长而快速发展的信息科技风险过程中，缺乏对于先进管理工具和手段的了解和应用，例如关键风险指标、风险控制自评估、风险清单、事件收集和分析工具、信息科技风险诊断工具等。

第三，信息科技风险管理制度、流程不足。我国银行业风险管理流程和制度有较多尚待完善之处，不少银行尚未建立起与较为完善的信息科技管理制度对应的科技风险管理制度和流程，部分已经制定的信息科技风险管理制度和流程的完整性也存在不足。

第四，科技风险管理机制尚待完善。我国银行业在信息科技风险方面缺乏有效的管理机制。例如缺少专职负责信息科技风险管理的人员，科技风险汇报路线和决策机制不明确等。少数银行即使已经建立针对信息科技风险管理的专门组织机构，也由于职能、人员、资源投入及管理意识等方面的限制，缺乏清晰的岗位设置，有效的汇报和沟通机制等，使得信息科技风险管理形同虚设，其参与银行战略决策制定的程度明显不足。

上述信息科技风险管理的不足和挑战也使得国内许多商业银行有进一步强化银行科技风险管理的强烈愿望，包括加大对科技风险管理建设的投入，加强银行科技风险管理与战略规划的结合，同时完善科技风险的治理、监测与报告机制。

1.2 银行信息科技风险管理体系初探

无论是信息科技风险自身的情况还是信息科技风险管理的现状，都凸显了一个事实：我国银行业需要加快在信息科技风险管理方面的努力和探索，通过对先进技术手段、最佳实践的多方尝试，结合前沿管理工具的运用，寻求一套适合银行的有效信息科技风险管理体系。在探索有效信息科技风险管理体系的过程中，我们可以从以下方面寻找研究的突破点：

第一，参考当前风险管理理论。风险管理的理念在银行业具有悠久的发

展历史，而信息安全、信息科技风险管理的相关理论和方法也可以追溯到信息科技实现业务应用的早期。时至今日，这些理论和方法在各自的领域内被不断地运用和优化。这些已有方法为国内银行业探索信息科技风险管理框架提供了一条有效的捷径，也是构建信息科技风险管理体系并进行相关实践的重要参照标准和依据。

第二，参考国内外银行业信息科技监管要求。国内外信息科技监管方面发展迅速，也提出了很多理论、方法和工具，这些内容是构建银行科技风险管理体系的重要参考因素。

第三，关注信息科技风险的特点。探索信息科技风险管理体系，离不开对信息科技特点的分析和解读。只有深入了解信息科技本身的复杂性、技术性和不易管理等特点，并对科技风险的成因、结果、传导方式等方面有了客观的判断，才能探索出契合信息科技风险特点的管理体系。

第四，结合我国银行业实际情况。我国银行业有数据大集中、银行业务创新快、交易数据量大等特点，因此，构建的信息科技风险管理体系要能适应我国银行业实际情况。

第五，构建风险管理策略、流程、保障机制等多维度体系。信息科技风险管理体系的构建与信息化建设一样，是一个系统性课题，而非孤立的几个事件。因此应该从信息科技治理、绩效评价、管理制度与规范、风险文化、人员培训、资源投入等多方面进行完善和丰富。

2 银行业信息科技风险管理在全面风险管理中的定位

在日常的信息科技风险管理中，银行普遍面临信息科技风险与操作风险及全面风险管理间界定不清的问题，厘清各相关方面的关系对更合理、有效地开展信息科技风险管理工作至关重要。为此，本书将对银行业信息科技风险管理在全面风险管理之中的定位进行全面分析和阐述。

2.1 信息科技风险管理理论

2.1.1 信息科技风险管理理论发展历程

信息科技风险相比其他风险，尤其是操作风险中与信息科技无关的其他风险，具有更加清晰的管理方法和实践参考。作为信息科技应用“排头兵”的银行业，将信息科技风险作为一个专门的风险管理对象进行管理几乎不存在任何的理论障碍和实践困难。信息科技风险管理经历了由狭义定义到广义定义的发展历程，从最早的信息安全风险，到后来的信息系统风险，再到自成体系的信息科技风险，人们对信息科技风险的认识越来越深入和全面。

一、信息安全风险

信息科技风险历史悠久，其概念的出现最早可以追溯到20世纪60年代。银行业对信息科技风险的认识是从信息安全相关风险开始的，随着信息科技的快速发展和广泛应用，由此引发的信息安全问题很早就引起了各国银行监管部门、理论界和银行的重视，一直以来，信息安全风险也往往作为信息科技风险的代名词在不同场合使用。

二、信息系统风险

在2002年7月，美国技术标准局（NIST）在其文献SP800－30中首次提