银行业信息科技风险管理高层指导委员会
银行业信息化丛书

银行信息安全技术与管理体系

洪崎　林云山　牛新庄　等编著

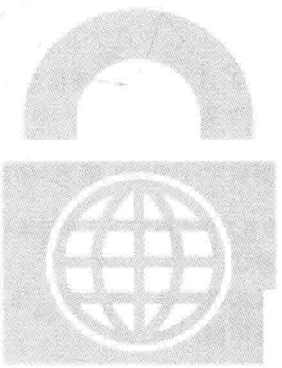
Information Security Technology and Management System in Banking

机械工业出版社
CHINA MACHINE PRESS

银行业信息科技风险管理高层指导委员会
银行业信息化丛书

银行信息安全技术与管理体系

洪崎　林云山　牛新庄　等编著



Information Security Technology and Management System in Banking

机械工业出版社
CHINA MACHINE PRESS

本书力图通过对我国银行业信息安全最新实践的介绍，让读者对我国银行业在信息安全的管理思路、管理方法、管理内容及使用技术等方面有一个清晰和全面的认识。全书分为四篇，分别介绍了我国银行业信息安全的发展现状，分析了银行业面临的威胁，总结了我国银行业在信息安全建设上取得的巨大成就。从信息安全管理角度出发，将银行信息安全管理体系作为一个整体，系统地分析它所包含的相关内容，并给出了银行业信息安全管理体系参考的框架结构；从技术的角度出发，从作用方式和作用层次两个维度对我国银行业采用的各种信息安全技术进行了梳理和总结。通过具体的案例，使读者更加深刻地理解银行业信息安全技术与管理体系，对我国银行业信息安全实践有一个直观的认识。

本书主要供银行信息科技人员阅读，也可供从事信息安全的工作人员和研究人员参考，还可作为信息安全与金融类专业的教学参考书。

图书在版编目（CIP）数据

银行信息安全技术与管理体系/洪崎等编著. —北京：机械工业出版社，2015.12

（银行业信息化丛书）

ISBN 978-7-111-52252-2

Ⅰ.①银… Ⅱ.①洪… Ⅲ.①银行—管理信息系统—研究

Ⅳ.①F830.49

中国版本图书馆 CIP 数据核字（2015）第 289607 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

总 策 划：张敬柱 黄养成

策划编辑：马 晋 责任编辑：马 晋 高 伟 责任校对：黄兴伟

封面设计：徐 超 责任印制：乔 宇

保定市中画美凯印刷有限公司印刷

2016 年 1 月第 1 版第 1 次印刷

184mm × 260mm · 20 印张 · 491 千字

0001— 5500 册

标准书号：ISBN 978-7-111-52252-2

定价：79.80 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务

服务咨询热线：010-88361066

读者购书热线：010-68326294

010-88379203

网络服务

机 工 官 网：www.cmpbook.com

机 工 官 博：weibo.com/cmp1952

金 书 网：www.golden-book.com

教育服务网：www.cmpedu.com

“银行业信息化丛书”编委会

总　序

信息化是推动经济社会变革的重要力量。坚持走中国特色的新型工业化、信息化、城镇化、农业现代化道路，是党中央立足全局、放眼未来、与时俱进的战略决策。2014年2月27日，中央网络安全和信息化领导小组的成立，更加体现了中央保障网络安全、推动信息化发展、维护国家利益的决心。银行业作为国家经济体系的重要行业之一，是信息化的重要推动主体、参与主体和受益主体。银行业持之以恒地贯彻落实国家信息化战略，不仅是推动加快我国信息化进程的必然要求，也是银行业改革发展、转型升级和更好服务实体经济的内在需求。

近年来，我国银行业审时度势、积极作为，坚持基础建设与科技创新并重、提升服务与保障安全并举的科学发展导向，以推进信息化为契机，调整经营理念、优化经营机制、完善服务模式，在服务手段信息化、管理模式信息化、信息安全保障等方面取得积极进展，推动了银行业的核心竞争力、市场适应力和贴身服务能力的进一步提升。一是服务手段信息化发展迅速。电子银行、自助银行、智能支付终端等信息化服务渠道日渐普及，使得金融服务覆盖面更加广泛、服务方式更加便捷、服务产品更加丰富。二是管理模式信息化迈出实质性步伐。注重依托核心数据库、运用先进数据挖掘分析工具，推进银行经营决策逐步智能化，风险管理日趋精细化，产品创新逐渐体现个性化，银行业经营管理信息化水平不断提升。三是信息安全保障取得积极进展。银行业信息安全越来越受重视，相关科技基础设施建设步伐加快，多层次、立体化、全方位的信息安全保障体系正在逐步形成。

当然，我们也应该清醒地认识到，银行业信息化面临着复杂的内外部环境，核心技术受限、网络安全威胁、隐私保护和信息保密等挑战将长期存在，银行业自身认识不尽到位、技术储备不够充分、资源投入相对不足、过度依赖外包等问题仍较为突出，针对银行业特殊需求的信息化产品、工具和方法还比较单一，缺乏应对复杂需求的灵活创新能力。总的看来，银行业信息化还有很长的路要走，信息科技风险将成为当前和未来较长时期银行业的重要风险领域之一。

银行业信息化既不能因为成绩而骄傲自满，也不可因为差距而妄自菲薄，更不可因

为困难而畏首畏尾。各银行业金融机构要勇于直面困难、主动迎接挑战，坚决按照国家信息化总体战略部署，切实坚持“自主可控、持续发展、科技创新”的基本方向，紧紧抓住信息化发展机遇，推动信息服务和信息安全再上新台阶。一是借助信息化推动银行业金融机构治理能力现代化。积极引入先进的信息科技治理和管理理念，运用现代信息技术缓解治理中的信息不对称问题，推动流程银行建设，提高治理有效性。同时，理顺信息化建设的体制机制，加快信息化建设进程，为银行业转型发展提供有力保障。二是依托信息化推动金融服务智慧化。要充分利用互联网、移动计算蓬勃发展的大环境，积极应用大数据等新兴技术，创新思维模式，充分发挥金融数据和信息的价值，研发智能化、个性化、便捷化的产品和服务，灵活响应客户诉求，努力改善客户体验，尽力发掘潜在客户需求，增加产品和服务的吸引力，培育更为坚实的客户基础，形成新的业务和利润增长点。三是以自主创新增进安全可控能力。要坚持市场起决定作用的基本方针，探索形成以研发创新支持应用推广、以市场应用激发创新动力的良性正反馈机制。推动应用自主创新信息技术，建立自主创新信息技术落地银行业的配套机制，力争金融领域关键信息技术自主创新占比逐步提高，不断提升信息系统的开放性、灵活性和整体集约化水平。四是利用信息技术强化行业协作。要加强银行业信息化建设的统筹规划，促进信息化资源的集约共享，提升数据（灾备）中心布局的合理性，增强同业协同协作，共同应对外包集中度等风险。

为更好地推进落实银行业信息化战略，由银行业信息科技风险管理高层指导委员会指导推动，编著了“银行业信息化丛书”（简称“丛书”）。这套“丛书”致力于挖掘、研究、总结、提炼和传播国内外信息化最佳实践、宝贵经验和最新成果，内容涵盖银行业信息科技治理与管理、信息系统开发与应用创新、信息安全、基础设施与运行维护、信息科技监管等主要领域，可为银行业信息科技人才培养提供一些基础性、前瞻性、实用性的知识和信息。

展望未来，银行业信息化任务艰巨、时间紧迫。希望银行业在有关各方支持下，推动信息化工作更加积极主动、规范有效、科学前瞻，为我国银行业持续健康发展、提升服务水平提供坚实的支撑，为增强国家网络安全保障能力、提升信息化建设水平提供有力支持，为贯彻落实创新驱动发展战略、实现中华民族伟大复兴的中国梦做出积极贡献。

尚福林

序

自改革开放以来，我国银行业飞速发展，取得了丰硕的成果。随着信息技术的迅猛发展，银行业对信息系统的依赖也日益加重，银行信息化将成为我国银行参与国际竞争的重要手段。目前，全国性股份制商业银行基本完成了数据大集中工程，建设完成了新一代综合业务处理系统。随着银行业改革与创新步伐的持续加快，金融服务水平和服务能力将进一步提高，银行的业务发展将会越来越依赖信息系统。因此，信息系统的安全稳定运行已经成为银行业务发展的必要保障。

银行业作为我国信息化前沿的关键核心行业，其信息安全形势和自主可控体系一直是行业建设的重点，而银行业的信息安全也日益受到社会的关注。我国银行业的信息化建设虽然成绩斐然，信息安全水平也在不断提高，但也必须清醒地看到，当前针对银行业的网络攻击行为还在不断增加，信息技术固有的安全隐患也越发突显出来，如自然灾害、病毒攻击、人员操作失误等。特别是目前银行业在向互联网和移动互联网方向快速转型，网络安全形势非常严峻，针对银行业的网络攻击事件频发，近几年银行业的网络犯罪数量急剧攀升，银行业已经成为主要的攻击目标。为了保证银行业务的正常运营，建立一个完整的、稳定的信息安全防护机制，已逐渐成为银行业信息技术发展的一个重要课题。

当前，云计算时代的金融信息安全的形态正发生着变化，信息安全问题时刻威胁着国家安全，银行业作为国家重要信息系统的一部分，其信息安全已上升到国家战略高度。国务院、公安部、人民银行、银监会等政府部门通力合作，已经逐渐形成完整的信息安全规范及管理体系，建立和完善了与银行业信息化发展相适应的信息安全保障体系，满足银行业业务发展的安全性要求，保证信息系统和相关基础设施功能的正常发挥，有效防范、控制和化解信息技术风险，增强信息系统安全预警、应急处置和灾难恢复能力，保障数据安全，显著提高了银行业业务持续运行保障水平。

为了进一步贯彻合规、安全的管理运营理念，满足国家部委、主管部门和监管机构的要求，提升信息科技风险管理和防控能力，银行业应基于现有的信息安全管理水平，积极开展信息安全技术及管理体系的落地建设工作，优化升级整体信息安全管理和技术

体系架构，完善信息科技风险管理体系和业务连续性管理体系，全面提升信息安全管理水平，这必将有效推动银行业信息化建设工作，为银行业业务战略转型提供坚实的技术基础和安全保障，维护国家金融安全。

中国民生银行董事长　洪崎

前　言

本书作为“银行业信息化丛书”中的一本，对我国银行业信息安全技术与管理体系进行了分析和探讨，力图通过对我国银行业信息安全最新实践的介绍，让读者对我国银行业在信息安全的管理思路、管理方法、管理内容及使用的信息安全技术等方面有一个清晰和全面的认识。

为了与我国银行业当前的实际情况紧密结合，本书在编写过程中，分别调研了大型股份制银行、城市商业银行及农村商业银行等几种不同类型的典型银行。本书编写组从2014年11月开始，经过准备、调研、编写、完善、评审、修订等阶段，历经7个月的时间，最终于2015年5月完成了本书。全书共分为四篇：

第一篇为现状篇，主要介绍了我国银行业信息安全的发展现状，分析了银行业面临的威胁，总结了我国银行业在信息安全建设上取得的巨大成就。

第二篇为管理篇，从信息安全管理角度出发，将银行业信息安全管理体系作为一个整体，系统地分析了银行信息安全管理体系所包含的相关内容，并给出了银行业信息安全管理体系参考的框架结构。在此基础上，对信息安全管理的各个组成模块进行了详细介绍，具体包括信息安全方针、信息安全组织、信息安全制度、信息安全运作、信息安全技术。其中信息安全运作又包括信息安全风险管理、信息安全检查、信息安全监控、信息安全事件管理、业务连续性与灾难恢复管理、信息安全审计等内容。

第三篇为技术篇，从作用方式和作用层次两个维度对我国银行业采用的各种信息安全技术进行了梳理和总结。从作用方式上根据WPDRRC模型可将信息安全技术划分为预警、保护、检测、响应、恢复和反击六类；而从作用层次上，可将信息安全技术分为面向物理安全、网络安全、主机安全、应用安全和数据安全共五个层面，由此提出了基于WPDRRC的层次技术模型，并以此为基础对信息安全技术展开了论述。

第四篇为实践篇，通过具体的案例，对我国银行业信息安全管理实践进行了详细的介绍，帮助读者对我国银行业信息安全实践有一个直观的认识。具体内容包括某股份制商业银行安保平台建设实例、基于大数据的网络安全态势实践和同城双中心灾备建设实例。

本书力求在下述几个方面取得一定的突破：

1）通用性：在编写本书的过程中，我们广泛参考了国际国内相关标准、法规、指南，与主流的标准规范保持了一致，具有很好的通用性。

2）结构化：无论是信息安全技术，还是信息安全管理，其主要内容均以结构化的方式呈现，并由此提出了信息安全管理的参考框架和信息安全技术模型，使读者能够从整体上对银行业信息安全工作进行把握。

3）全面性：本书力求涵盖银行业信息安全管理与技术的方方面面。

4）实践性：本书以银行业实际为基础，通过逻辑梳理，又反过来指导实践。为了更有效地反映银行当前信息安全实践，本书专门添加了实践篇，对银行业信息安全进行了更为深入的介绍。

本书的具体编写工作由中国民生银行承担，由洪崎、林云山、牛新庄、穆新宇、吕晓强、宋涛、李吉慧、张维华、袁丽欧、钱伟明编著。在编写过程中，得到了中国民生银行各级领导的高度重视和大力支持，提出了大量实质性修改意见，在此对他们的辛勤付出表示感谢！同时，感谢毕马威公司的蒋辉柏、崔巍、肖腾飞，北京国舜公司的姜强、汤志刚、董芸逢等同志对本书的结构和内容方面提供的大量帮助！感谢中国建设银行、中国邮政储蓄银行、上海浦东发展银行、中信银行和江南农村商业银行提供的大量资料！感谢中国工商银行、中国农业银行、中国银行、中国建设银行、华夏银行在本丛书评审中提出的宝贵建议！在本书的编写过程中，还参阅了大量文献资料，在此向这些文献资料的原作者表示衷心感谢！

由于银行业信息安全工作本身的复杂性和编者水平所限，书中难免存在疏漏、不足甚至错误，恳请读者不吝赐教。

本书编写组

目　录

第二篇 管 理 篇

第三篇 技 术 篇