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

商业银行信息系统研发风险管控

蔡钊 张方 陈典友 等编著

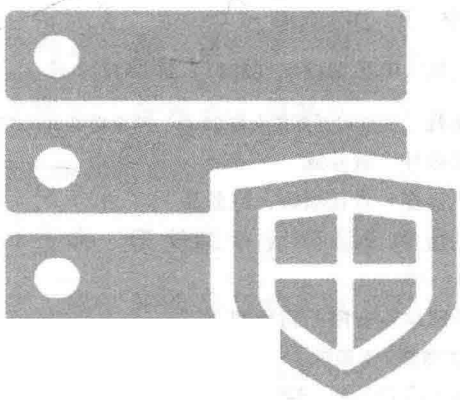
Information System Development Risk Management of Commercial Banks

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

商业银行信息系统研发风险管控

蔡钊 张方 陈典友 等编著



Information System Development Risk Management of Commercial Banks

机械工业出版社
CHINA MACHINE PRESS

本书通过对商业银行信息系统研发风险的定义、成因、分类和问题的分析研究，提出了商业银行开展信息系统研发风险管控的理论依据、实践方法和实践过程。全书分为基础篇、管理篇和技术篇。基础篇主要介绍了商业银行信息系统研发风险的概念、法规、政策与相关标准；管理篇主要介绍了商业银行信息系统研发风险管控模型、管控体系、管控方法、实践案例等内容；技术篇主要介绍了信息系统安全开发的策略、方法和相关技术。

本书可用于指导商业银行开展信息系统研发风险管控工作，可供商业银行信息科技部门的信息系统研发风险管控人员使用，也可供商业银行及其他相关机构信息科技风险管理人员、信息安全管理人员、信息系统安全设计和开发人员参考。

图书在版编目（CIP）数据

商业银行信息系统研发风险管控/蔡钊等编著. —北京：机械工业出版社，2015.10

（银行业信息化丛书）

ISBN 978-7-111-51949-2

Ⅰ.①商… Ⅱ.①蔡… Ⅲ.①商业银行－管理信息系统－系统开发－风险管理－研究 Ⅳ.①F830.49

中国版本图书馆 CIP 数据核字（2015）第 255223 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：赵磊磊 责任编辑：赵磊磊

责任校对：刘怡丹 封面设计：徐 超

责任印制：李 洋

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 · 17.25 印张 · 424 千字

0 001—5 500 册

标准书号：ISBN 978-7-111-51949-2

定价：69.80 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，我们也应该清醒的认识到，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

信息技术的发展浪潮势不可挡。以信息技术为代表的第三次科技革命，极大地推动了人类社会经济、政治、文化领域的变革，也影响了人类的生活方式和思维方式。信息技术在给人类的生产、生活带来巨大便利的同时，也带来了日趋严峻的信息安全问题。中国共产党的十八届三中全会以来，中央相继成立了国家安全委员会、网络安全和信息化领导小组，将信息安全提升至国家战略高度，并提出了保障网络安全、维护国家利益、推动信息化发展、建设网络强国的奋斗目标。习近平主席在中央网络安全和信息化领导小组第一次会议上指出“没有网络安全就没有国家安全，没有信息化就没有现代化”。商业银行信息安全事关金融稳定和国家经济安全，是国家整体信息安全战略的重要一环，确保商业银行的信息安全对于维护整个国家安全具有重要意义。

在商业银行全面风险管理体系中，信息科技风险管控领域的重要任务之一就是贯彻执行国家信息安全战略，提高信息系统的安全性，进而保障商业银行业务的连续性。从成本和效益的比较来看，信息系统研发阶段无疑是加强安全投入、修复安全问题的最佳阶段。因此，做好信息系统研发风险管控工作，从信息系统生命周期的源头预防和遏制信息安全问题，是商业银行落实国家信息安全战略、提高信息系统安全水平、提高自身风险防控能力的一种有效手段。

中国农业银行高度重视研发风险管控工作，早在2007年就作为全国首家实施信息系统安全等级保护的银行，通过贯彻落实等级保护标准，开始了对研发风险管控的研究和试点工作。2014年，中国农业银行完成了总行科技部门信息科技风险管理体系的建设工作，对多年的研发风险管控理论和实践经验进行了一次全面总结和推广。尽管研发风险广泛存在于商业银行信息系统的研发过程中，但目前该领域的研究专著较少，此次借银行业信息科技高层指导委员会组织编写“银行业信息化丛书”的契机，中国农业银行总结前期管理经验，编著本书，与各商业银行就如何进行研发风险管控进行探索、讨论、分享。同时，也希望本书有助于拓展商业

银行同业的管理思路，使大家重视研发风险，防控研发风险，共同打造一个安全、高效的金融科技环境，维护国家金融安全，促进我国商业银行业务的健康快速发展。

中国农业银行股份有限公司

前　言

随着信息科技与商业银行业务的深度融合，商业银行业务对信息系统的依赖性日益增强，银行信息化的快速发展，对信息科技风险管理提出了更高的要求。如何防范信息科技风险，已成为商业银行必须认真面对的一个重要课题。其中研发风险管理是信息科技风险管理的一个重要领域。

本书旨在指导商业银行开展信息系统研发风险管控工作，防范信息系统研发过程中的安全需求风险、安全设计风险、系统安全漏洞、合规风险、外包风险等各类研发风险，提高商业银行信息系统的安全可靠性，以增强银行的核心竞争力和可持续发展能力。本书采取理论模型指导实践的思路，从组织、制度、标准、技术等方面入手，提出了开展研发风险管控的管理依据、理论模型、管理策略、管理方法、技术手段和实践案例。为了提高本书的专业性和指导性，提高内容深度和质量，本书在全面讲解商业银行信息系统研发风险管控体系的基础上，积极跟踪行业发展趋势，扩展了研发风险管控体系理论解读、商业银行研发风险管控理论、研发风险管理实践指导、研发风险管控案例、研发风险管理技术研究、管理探索、新技术探索等相关内容，为读者提供了更广泛的借鉴。

本书注重理论与实践相结合，具有较强的现实意义，为商业银行深入开展研发风险管理提供全新的视角，适合我国商业银行软件风险管理团队、研发管理团队使用。本书分为基础篇、管理篇和技术篇，共计十章。基础篇介绍了商业银行研发风险的概念、法规、政策与相关标准；管理篇介绍了商业银行信息系统研发风险管控模型、研发风险管控体系、研发风险管控工作方法、研发外包风险管控等内容；技术篇介绍了信息系统安全开发策略方法和安全开发的相关技术。为了使读者能够更深入地理解研发风险管控体系，书中还收集了部分商业银行研发风险管控实际案例，以有效提供参考，使理论与实践能够有机结合。

本书由中国农业银行研发风险管控课题组共同编著。编著团队的主要成员有蔡钊、张方、陈典友、李阳、姜帆、王琰、曹玉磊、孙玮、薛建伟、姚元庆和毛南。范瑾辉、高松、李涵阳、王喜辉、罗志云、关磊和王衍锋等同志也参与了本书部分内容的编写。

在本书编著过程中，得到了中国农业银行信息化建设技术专家委员会的大力支持与帮助。同时，衷心感谢中国农业银行王俊、张红喜、赵晓东、张冰等各相关领域技术专家对本书初稿的审阅和建议，衷心感谢中信银行申贵平、工商银行杨雷、华夏银行张志田三位银行业信息科技发展与风险管理专家对本书提出的评审意见；衷心感谢中国银监会银行业信息科技监管部的谢翀达主任、梁峰处长对本书的高度重视和深切关怀。此外，还要衷心感谢机械工业出版社的大力支持与帮助。

在编著过程中，编著团队查阅和参考了大量文献资料，限于篇幅，未能在书后的参考文献中全部列出，在此一并致谢。由于编著团队水平有限，书中难免存在谬误和不足之处，希望各位读者批评指正。

编著者

目　录

管理篇

技术篇

基础篇

第 1 章　商业银行信息系统研发风险管控基础知识

第 2 章　商业银行研发风险管控相关法规、政策与标准

第 1 章
商业银行信息系统研发风险管控基础知识

1.1 信息系统研发风险管控概述

1.1.1 信息系统和信息系统研发

1. 信息系统的概念

21 世纪是信息科学技术飞速发展的时代，在全球经济一体化趋势下，信息技术也呈现全球化趋势，对人类社会的发展和人们的生活方式产生了巨大影响。在经济领域，信息技术的广泛应用使得网络经济和电子商务逐渐普及，成为助推企业发展、区域经济增长乃至国家经济发展的重要动力，也大大改变了传统经济发展模式和企业管理模式。为了应对机遇和挑战，现代企业日益依赖信息系统进行经营管理。信息系统也逐渐成为影响企业生存和发展的关键因素。

从广义上讲，信息系统是指进行信息处理的系统，它是一系列相互关联的可以采集、操作、存储、传播数据和信息，并提供反馈以实现其目的的元素或组成部分的集合。狭义的信息系统专指计算机信息系统。根据 GB 17859—1999 的定义，计算机信息系统是由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行加工、存储、传输、检索等处理的人机系统。

作为广义的信息系统，在任何时代、任何社会环境下都存在，只是到了现代，信息系统的概念才被提炼出来。这是因为在现代社会，信息系统总是与计算机技术和因特网的应用联系在一起。因此，现代的信息系统总是指以计算机为信息处理工具，以网络为信息传输手段的信息系统。也正因此，现在只要说到信息系统，一般指的就是计算机信息系统[1]。

（1）信息系统的结构 信息系统一般由计算机硬件、操作系统、网络和通信设备、数据库、程序语言、应用软件、信息资源、用户、组织机构、规章制度构成，如图 1-1 所示。